Oracle Autonomous Health Framework User's Guide

F19065-64
April 2024

Oracle Autonomous Health Framework User's Guide ,

F19065-64

Primary Author: Nirmal Kumar

Contributing Authors: Aparna Kamath, Mark Bauer, Richard Strohm

Contributors: Alex Wu, Amar Gorla, Anand Pandey, Arjun Upadhyay, Ashwinee Khaladkar, Barry Gleeson, Bill Burton, Bob Caldwell, Bryan Vongray, Carol Colrain, Chandrabhushan Nagur, Christian Diaz, Damian Garcia, Daniel Semler, Daniel Torres, Deepak Tayade, Erick Mendoza , Gareth Chapman, Girdhari Ghantiyala, Guldeep Sahu, Hairong Qin, Harish Rajora, Itzel Velazquez, Jose Tovany, Juan Carlos Perez Castellanos, Juan Manuel Sanchez, Juigil Kishore, Kamakshi Sethi, Kavitha Dhanasekar, Leela Kumaraswamy Lakkana, Luis Rocholl, Luis Trujillo, Macharapu Prasanth , Manuel Antonio Garcia Chang, Maximiliano Catalan, Nikhil Nischal, Nishith Khandelwal, Pallavi Kamath, Pedro Cornejo, Pradeep Ganesh Bhandarkar, Praveen Kumar, Rajeev Chaurasia, Ravi Ranjan, Raziel Zavaleta , Refugio Cornejo, Rishabh Vishwakarma , Rohit Juyal, Sarahi Partida, Shirdivas Dharmabhotla, Srishti Bhatia , Thomas Herter, Troy Anthony, Vaishakha R, Vern Wagman, Wataru Miyoshi

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

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

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

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Contents

Preface

Changes in this Release

Changes in Previous Releases

1 Overview

2 Get Started

3 Run Compliance Checks

4 Collect Diagnostic Data

5 Explore Diagnostic Insights

6 Analyze Issue Root Cause

7 Resolve Database Issues

8 Troubleshoot

9 Command Line Reference

Preface

This guide explains how to use the diagnostic tools, Oracle Orachk, Oracle Exachk, and Oracle Trace File Analyzer.

It also explains the prerequisites to install and configure the diagnostic tools.

Audience

Oracle® Autonomous Health Framework Checks and Diagnostics User's Guide provides conceptual and usage information about the diagnostic tools for the database administrators.

This guide assumes that you are familiar with Oracle Database concepts.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documentation

For more information, see the following Oracle resources:

Related Topics

- *Oracle Database Concepts*
- *Oracle Database Upgrade Guide*
- *Oracle Grid Infrastructure Installation and Upgrade Guide*
- *Oracle Real Application Clusters Installation Guide for Linux and UNIX*
- *Oracle Real Application Clusters Installation Guide for Microsoft Windows*

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Third-Party License Information

Oracle Autonomous Health Framework consumes third-party code. Oracle is required to provide the following notices. Note, however, that the Oracle program license that accompanied this product determines your right to use the Oracle program, including the third-party software, and the terms contained in the following notices do not change those rights.

pexpect 4.9.0

pexpect version 4.9.0 license, http://pexpect.readthedocs.io/en/latest/api/pexpect.html?highlight=license

Lucene 8.11.2

Lucene version 8.11.2 license, https://lucene.apache.org/core/downloads.html

requests 2.31.0

requests version 2.31.0 license, https://libraries.io/pypi/requests/2.31.0

beautifulsoup4 4.11.1

beautifulsoup4 4.11.1 license, https://libraries.io/pypi/beautifulsoup4/4.11.1

Jackson Core 2.16.1

jackson-core version 2.16.1 license, https://mvnrepository.com/artifact/com.fasterxml.jackson.core/jackson-core/2.16.1

Paramiko 3.4.0

Paramiko 3.4.0 license, https://pypi.org/project/paramiko/3.4.0/

Python 3.11.5

Python 3.11.5 license, https://docs.python.org/3.11/license.html#history-and-license

ipykernel 6.25.2

ipykernel 6.25.2 license, https://pypi.org/project/ipykernel/

traitlets 5.9.0

traitlets 5.9.0 license, https://pypi.org/project/traitlets/5.9.0/

ptyprocess 0.7.0

ptyprocess version 0.7.0 license, https://github.com/pexpect/ptyprocess/blob/master/LICENSE

ipython 8.10.0

ipython 8.10.0 license, https://ipython.readthedocs.io/en/stable/about/license_and_copyright.html

pywin32 306

pywin32 306 license, https://pypi.org/project/pywin32/

Papermill 2.3.4

Papermill 2.3.4 license, https://pypi.org/project/papermill/2.3.4/

Apache Commons IO 2.13.0

Apache Commons IO 2.13.0 license, https://mvnrepository.com/artifact/commons-io/commons-io/2.13.0

pyarrow 14.0.1

pyarrow 14.0.1 license, https://pypi.org/project/pyarrow/14.0.1/

picocli 4.7.5

picocli 4.7.5 license, https://mvnrepository.com/artifact/info.picocli/picocli/4.7.5

nbconvert 7.2.3

nbconvert 7.2.3 license, https://pypi.org/project/nbconvert/6.5.0/

Apache Log4j Core 2.22.0

Apache Log4j Core version 2.22.0 license, https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core/2.22.0

Apache Log4j API 2.22.0

Apache Log4j API version 2.22.0 license, https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-api/2.22.0

Jakarta Mail 2.1.2

Jakarta Mail 2.1.2, license https://mvnrepository.com/artifact/jakarta.mail/jakarta.mail-api/2.1.2

Jakarta Json Processing API (JSON-P) 2.1.2

Jakarta Json Processing API (JSON-P) 2.1.2, license https://mvnrepository.com/artifact/jakarta.json/jakarta.json-api/2.1.2

OCI SDK for Python 2.115.1

OCI SDK for Python version 2.115.1 license, https://pypi.org/project/oci/2.115.1/

Jackson Databind 2.16.1

jackson-databind version 2.16.1 license, https://mvnrepository.com/artifact/com.fasterxml.jackson.core/jackson-databind/2.16.1

Commons CSV 1.10.0

Commons CSV 1.10.0 license, https://mvnrepository.com/artifact/org.apache.commons/commons-csv/1.10.0

Jakarta Activation API (JAF) 2.1.2

Jakarta Activation API (JAF) 2.1.2, license https://mvnrepository.com/artifact/jakarta.activation/jakarta.activation-api/2.1.2

Plotly 5.18.0

Plotly 5.8.0 license, https://pypi.org/project/plotly/5.18.0/

NumPy 1.22.4

NumPy 1.22.4 license, https://numpy.org/doc/stable/release/1.22.4-notes.html

NumPy 1.26.0

NumPy 1.26.0 license, https://numpy.org/doc/stable/release/1.26.0-notes.html

Jackson Annotations 2.16.1

jackson-annotations version 2.16.1 license, https://mvnrepository.com/artifact/com.fasterxml.jackson.core/jackson-annotations/2.16.1

xarray 2022.3.0

xarray 2022.3.0 license, https://pypi.org/project/xarray/2022.3.0/

Eclipse Parsson 1.1.5

Eclipse Parsson 1.1.5, license https://mvnrepository.com/artifact/org.eclipse.parsson/parsson/1.1.5

Angus-activation 2.0.1

Angus-activation 2.0.1 license, https://mvnrepository.com/artifact/org.eclipse.angus/angus-activation/2.0.1

python-oracledb 1.4.0

python-oracledb 1.4.0 license, https://pypi.org/project/oracledb/1.4.0/

Pandas 1.4.2

Pandas 1.4.2 license, https://pypi.org/project/pandas/1.4.2/

Angus Mail 2.0.2

Angus Mail 2.0.2, license https://mvnrepository.com/artifact/org.eclipse.angus/angus-mail/2.0.2

Fourth-Party Dependencies

Fourth Party Dependency: numpy

Python Package : numpy
Version >= 1.14.3
Maintainer/Licensor: NumPy Developers
License: BSD License
Page : https://pypi.org/project/numpy/

Fourth Party Dependency: python-dateutil

Python Package : python-dateutil
Version >= 2.5.0
Author: Gustavo Niemeyer
Maintainer: Paul Ganssle
License: Apache Software License, BSD License (Dual License)
Page : https://pypi.org/project/python-dateutil/

Fourth Party Dependency: pytz

Author: Stuart Bishop <stuart@stuartbishop.net>
License: MIT license.
This code is also available as part of Zope 3 under the Zope Public License, Version 2.1 (ZPL).
Page: http://pytz.sourceforge.net/#license

Fourth Party Dependency: six

Python Package : six
Version > =1.5
Author: Benjamin Peterson
License: MIT License (MIT)
Page : https://pypi.org/project/six/

Changes in this Release

This preface lists changes in the Oracle Autonomous Health Framework Checks and Diagnostics User's Guide 24.3.

- Diagnose and Resolve ORA-04031 and ORA-07445 Using AHF
  Oracle Database has published two AHF Fix Flow articles and a video, showing how to use AHF to diagnose and resolve ORA-04031 and ORA-07445 errors.
- Compliance Checks for GoldenGate Microservices Architecture
  AHF now support compliance checks for GoldenGate Microservices Architecture.
- Insights Accessibility Improvements
  As part of the efforts to provide the most accessible experience to our users, AHF 24.3 introduces the next accessibility features.
- Enhancements to Unified AHF CLI
  The AHF release 24.3 adds new command options to `ahf analysis create`, `ahf configuration set`, `ahf configuration get`, `ahf configuration unset`, and `ahf configuration check`.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 24.3 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Diagnose and Resolve ORA-04031 and ORA-07445 Using AHF

Oracle Database has published two AHF Fix Flow articles and a video, showing how to use AHF to diagnose and resolve ORA-04031 and ORA-07445 errors.

ORA-04031: unable to allocate bytes of shared memory, occurs because more shared memory was needed than was available.

ORA-07445 exception encountered: core dump, can happen anywhere within Oracle code. It’s caused by an operating system exception occurring which should result in the creation of a core file.

Both of these error are frequently seen by Database customers.

The AHF team have created two new Fix Flow articles showing how to use AHF to collect diagnostic collections for either error. Each article explains why the error occurs and gives step-by-step guidance to use AHF to capture a diagnostic collection, then how to use it to either find a resolution or get more help from Oracle Support.

For more information, see *Resolve Database Issues*.

Related Topics

- ORA-04031 Fix Flow

- ORA-07445 Fix Flow
- Resolve Database Issues

Compliance Checks for GoldenGate Microservices Architecture

AHF now support compliance checks for GoldenGate Microservices Architecture.

AHF has supported compliance checks against GoldenGate classic for several years. This release now expands that support to include *GoldenGate Microservices Architecture*.

To run the new GoldenGate compliance checks configure the REST connection details by running:

```
ahf configuration set --type goldengate --all
```

Then run either Orachk and Exachk with the `goldengate` profile:

```
orachk -profile goldengate
```

```
exachk -profile goldengate
```

Related Topics

- Oracle GoldenGate Microservices Architecture

Insights Accessibility Improvements

As part of the efforts to provide the most accessible experience to our users, AHF 24.3 introduces the next accessibility features.

Accessibility refers to the design and implementation of digital products and environments that are usable by all people, regardless of their abilities or disabilities. This includes ensuring that people with disabilities can perceive, understand, navigate, and interact with digital content and interfaces effectively.

Accessible Home Button

Revamped **Home** tab to make it more user-friendly, especially for those using screen readers. Now, it behaves exactly like a tab should, eliminating any confusion caused by its previous behavior as a button.

Enhanced Accessibility within Home Page Regions

Support for screen readers to all items within the **Topology** and **Insights** sections in **Home** page. This means that users relying on screen readers can now easily identify and understand each item they’re focusing on along with the valuable information it provides.

Accessible Navigation in Timeline

Replaced the old pagination component in Timeline it with a sleek new scroll bar, making it easier for you to navigate through content without losing focus. The new scroll bar ensures a seamless browsing experience, specially for the users using screen readers.

Introducing Accordions

Now, within the **Best Practice Issues** section, you'll find accordions that act as top-level details for each check. When expanded, these accordions reveal check-related data points, providing you with a clear and organized view of the information you need. This not only preserves the functionality of the previous layout but also eliminates the nested tables pattern, ensuring better accessibility support for all users, including those relying on screen readers. With this update, accessing and understanding your reports has never been easier!

For more information, see *Explore Diagnostic Insights*.

Related Topics

- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Enhancements to Unified AHF CLI

The AHF release 24.3 adds new command options to `ahf analysis create`, `ahf configuration set`, `ahf configuration get`, `ahf configuration unset`, and `ahf configuration check`.

- `ahf analysis create --type insights --tag <tag>`
- `ahf configuration set --type upload <options>`
- `ahf configuration get --property reposizeMB`
- `ahf configuration get --property repositorydir`
- `ahf configuration get --type upload <options>`
- `ahf configuration unset --type upload <options>`
- `ahf configuration check --type upload --name <upload_config>`
- `ahf configuration check --type fleet-insights`

Additionally, AHF 24.3 adds a command option `--to-json` for rendering the output in JSON format. Except for `ahf software get-mrp-level --oracle-home <oracle-home>`, use `--to-json` when you run any `ahf` command.

```
ahf software get-version --component ahf --to-json
{
  "api_invocation": {
    "api": "categories.software.version",
    "args": [],
    "kwargs": {}
  },
  "version": "24.3.0",
  "ahf_version": "24.3.0",
  "tfa_version": "",
  "compliance_version": "",
  "compliance_metadata_version": "",
  "build_timestamp": "20240305221412"
}
```

Related Topics

- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.
- ahf configuration
  Use the `ahf configuration` command to change AHF configuration.
- ahf observer
  Use the `ahf observer` command to retrieve status of AHF components.
- ahf software
  Use the `ahf software` command to retrieve the details of AHF software and Monthly Recommended Patches (MRP).
- ahf data
  Use the `ahf data` command to retrieve information about AHF repositories.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 24.3 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Best Practice Checks Common to Both Oracle Orachk and Oracle Exachk

- Verify no orphaned files exist in ASM

Oracle Orachk Specific Best Practice Checks

- Verify grid inventory node list

Oracle Exachk Specific Best Practice Checks

- Exadata Critical Issue EX85

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

Changes in Previous Releases

AHF Release 24.2

- Enhancement to tfactl purge Command
  The AHF release 24.2 adds new `tfactl purge` options for deleting collections and log files from AHF components.
- Combine Diagnostics From All Machines in a Single Zip File
  The AHF release 24.2 adds a new `tfactl diagcollect` option `-singlearchive` for merging remote zip files into a single zip file on the initiating node.
- Enhancements to Unified AHF CLI
  The AHF release 24.2 adds new actions and options to `ahf`, `ahf configuration`, and `ahf software`, and a new command `ahf data`.
- Enhancement to tfactl diagcollect to Collect Exadata Netdiag Output Files
  AHF can now collect Netdiag output files on Exadata systems as part of `-os` component diagnostic collection.
- Enhancement to SRDCs to Collect Audit Vault Server Logs
  The AHF release 24.2 adds a new SRDC `avs` to collect Audit Vault Server logs.
- Insights in Diagnostic Collections
  AHF diagnostic collection zips now include a sub-zip named `<machine>_insights_<time>.zip` containing the Insights report. This makes it quicker and easier to understand and resolve problems.

- Insights for Single Instance Systems
  With AHF 24.2 Insights now adds support for single instance Linux systems.
- Diagnose and Resolve ORA-00600 Using AHF
  ORA-00600 is a generic internal error. It indicates the relevant process has encountered a low-level unexpected condition – which typically means a bug. The impact can vary from just being an annoyance that shows up in logs occasionally, to something major that brings the database down.
- Troubleshooting Option to fix Oracle Trace File Analyzer Fails to Collect Diagnostic Traces Issue
  The AHF release 24.2 includes a troubleshooting option to fix Oracle Trace File Analyzer failing to collect diagnostic traces of components such as CRS, DB, ASM, and so on issue.
- Latest Python and Java Third-Parties
  AHF has upgraded the versions of Python and Java third-party software to fix Common Vulnerabilities and Exposures (CVEs).

Enhancement to tfactl purge Command

The AHF release 24.2 adds new `tfactl purge` options for deleting collections and log files from AHF components.

Related Topics

- tfactl purge
  Use the `tfactl purge` command to delete collections and log files from AHF components from the local node.

Combine Diagnostics From All Machines in a Single Zip File

The AHF release 24.2 adds a new `tfactl diagcollect` option `-singlearchive` for merging remote zip files into a single zip file on the initiating node.

For example:

```
tfactl diagcollect -last 1d -os -singlearchive
```

```
tfactl diagcollect -last 1h -singlearchive -par <par_url>
```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

Enhancements to Unified AHF CLI

The AHF release 24.2 adds new actions and options to `ahf`, `ahf configuration`, and `ahf software`, and a new command `ahf data`.

Related Topics

- ahf
  Use the `ahf` command to generate diagnostic analysis report, generate AHF Balance reports, and query the version of AHF running on the local node.

- ahf configuration
  Use the `ahf configuration` command to change AHF configuration.
- ahf software
  Use the `ahf software` command to retrieve the details of AHF software and Monthly Recommended Patches (MRP).
- ahf data
  Use the `ahf data` command to retrieve information about AHF repositories.

Enhancement to tfactl diagcollect to Collect Exadata Netdiag Output Files

AHF can now collect Netdiag output files on Exadata systems as part of `-os` component diagnostic collection.

To ensure netdiag files are included within a collection use the command:

```
tfactl diagcollect -os -last 1h
```

Related Topics

- Collecting from Specific Components

Enhancement to SRDCs to Collect Audit Vault Server Logs

The AHF release 24.2 adds a new SRDC `avs` to collect Audit Vault Server logs.

Related Topics

- Oracle Trace File Analyzer Service Request Data Collections (SRDCs)
  Oracle Trace File Analyzer Service Request Data Collections (SRDCs) enable you to quickly collect the right diagnostic data.
- Collecting from Specific Components

Insights in Diagnostic Collections

AHF diagnostic collection zips now include a sub-zip named `<*machine*>_insights_<*time*>.zip` containing the Insights report. This makes it quicker and easier to understand and resolve problems.

Related Topics

- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Insights for Single Instance Systems

With AHF 24.2 Insights now adds support for single instance Linux systems.

To generate an Insights report, run:

```
ahf analysis create --type insights
```

Transfer the resulting zip to a system with browser support, extract it, and open `index.html`.

Related Topics

- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Diagnose and Resolve ORA-00600 Using AHF

ORA-00600 is a generic internal error. It indicates the relevant process has encountered a low-level unexpected condition – which typically means a bug. The impact can vary from just being an annoyance that shows up in logs occasionally, to something major that brings the database down.

For more information, see *Resolving ORA-00600 Internal Error Codes*.

Related Topics

- Resolving ORA-00600 Internal Error Codes

Troubleshooting Option to fix Oracle Trace File Analyzer Fails to Collect Diagnostic Traces Issue

The AHF release 24.2 includes a troubleshooting option to fix Oracle Trace File Analyzer failing to collect diagnostic traces of components such as CRS, DB, ASM, and so on issue.

Related Topics

- Oracle Trace File Analyzer Is Not Collecting Diagnostic Traces of Components Such As CRS, DB, ASM, and So On

Latest Python and Java Third-Parties

AHF has upgraded the versions of Python and Java third-party software to fix Common Vulnerabilities and Exposures (CVEs).

AHF 24.2 has upgraded the versions of many third party libraries in both Python and Java. The following CVEs are all fixed:

- Pip upgraded to 23.3.2 to resolve:
  - https://nvd.nist.gov/vuln/detail/CVE-2023-5752
- Urllib3 upgraded to 2.2.0 to resolve:
  - https://nvd.nist.gov/vuln/detail/CVE-2023-45803
  - https://nvd.nist.gov/vuln/detail/CVE-2023-43804
- Jackson-databind upgraded to 2.16.1 to resolve:
  - https://nvd.nist.gov/vuln/detail/CVE-2023-35116

- jinja2 upgraded to 3.1.3 to resolve:
  - https://nvd.nist.gov/vuln/detail/CVE-2024-22195
- openssl upgraded to 3.0.13 to resolve:
  - https://nvd.nist.gov/vuln/detail/CVE-2023-5678

For more information, see .*Third-Party License Information*

Related Topics

- Third-Party License Information

AHF Release 24.1

- Option to Collect Oracle Auto Service Request (ASR) Client Logs
  Starting with AHF 24.1, Oracle Trace File Analyzer collects Oracle Auto Service Request (ASR) client's logs present under `/var/opt/asrmanager/log/`. Collecting these logs enables to you triage ASR related failures in Oracle Database Appliance (ODA).
- AHF Print Collections Improvements
  A new option `-id` has been added to the `tfactl print collections -json` command to display collection details for a specific collection ID.
- Oracle Orachk/Oracle Exachk Diff Report Enhancements
  In the **Configurations Comparison** section, certain parameters that are expected to have different values are now reported under the **Common Configs** table.
- Terminal Release for AIX and Solaris Platforms
  Several old operating systems are approaching their end of life, as a result AHF is announcing terminal releases.
- Compliance Checks for Oracle RAC Extended Clusters
  AHF adds support for running compliance checks against Oracle RAC Extended Clusters.
- Insights Helps Explain Why Events Occurred
  AHF Insights now provides the ability to drill into **Major Events**, showing the CPU and I/O stats, providing context for why the event occurred.
- Insights Timeline Makes Problem Analysis and Resolution Easier
  AHF Insights timeline chart and table now dynamically adjust time ranges and allow to copy results as plain text.
- Insights into Disk Space Problems
  AHF Insights shows the number of disk space problems detected and color-codes disks based on their usage.
- Latest Python and Java Third-Parties
  AHF has upgraded the versions of Python and Java third-party software to fix Common Vulnerabilities and Exposures (CVEs).
- Deprecated Oracle Trace File Analyzer Masking Feature
  Deprecated `tfactl set redact=mask|sanitize` in release 24.1
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 24.1 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Option to Collect Oracle Auto Service Request (ASR) Client Logs

Starting with AHF 24.1, Oracle Trace File Analyzer collects Oracle Auto Service Request (ASR) client's logs present under `/var/opt/asrmanager/log/`. Collecting these logs enables to you triage ASR related failures in Oracle Database Appliance (ODA).

Collect ASR log files using the new `-asr` or the existing `-oda` component, for example:

```
tfactl diagcollect -asr
```

or

```
tfactl diagcollect -oda
```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

AHF Print Collections Improvements

A new option `-id` has been added to the `tfactl print collections -json` command to display collection details for a specific collection ID.

```
tfactl print collections -id <collection ID> -json
```

```
tfactl print collections -id 20240104010433stbm000004-vm18 -json
[
    {
        “CollectionId”: “20240104010433stbm000004-vm18",
        “InitiatedNode”: “stbm000004-vm18",
        “CollectionType”: “Manual Collection”,
        “RequestUser”: “root”,
        “NodeList”: “[stbm000004-vm17, stbm000004-vm18]“,
        “StartTime”: “2024-01-04T00:04:30.000-0600",
        “EndTime”: “2024-01-04T01:04:30.000-0600",
        “ComponentList”: “[omsi, emagent, acfs, asmproxy, sosreport,
crsclient,
emagenti, oms, qos, dbwlm, ocm, cha, cfgtools, afd, avs, dbclient, rdbms,
cvu,
os, crs, syslens, hami, em, chmos, goldengate, asmio, dataguard, install,
compliance, tns, asm, rhp, emplugins, wls]“,
        “UploadStatus”: “FAILED”,
        “CollectionStatus”: “COMPLETED”,
        “NodeCollection”: [
            {
                “Host”: “stbm000004-vm18”,
                “Tag”:
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/“,
                “ZipFileName”:
```

```
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/stbm000004-
vm18.tfa_Thu_Jan_04_01_04_36_CST_2024.zip”,
                “ZipFileSize”: “38896",
                “CollectionTime”: “183",
                “CheckSum”:
“d882835fe5bcee4b8d5381b59572f2b75dc7499ddf3adf5771e3ea75fa39e975",
                “checksum_algo”: “sha256"
            },
            {
                “Host”: “stbm000004-vm17",
                “Tag”:
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/“,
                “ZipFileName”:
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/stbm000004-
vm17.tfa_Thu_Jan_04_01_04_36_CST_2024.zip”,
                “ZipFileSize”: “42759",
                “CollectionTime”: “186",
                “CheckSum”:
“b090611f11e94814782b12f798e60ef0e054fbad47e94d950a3a24c698a79986",
                “checksum_algo”: “sha256"
            }
        ]
    }
]
```

Related Topics

- tfactl print
  Use the `tfactl print` command to print information from the Berkeley DB (BDB).

Oracle Orachk/Oracle Exachk Diff Report Enhancements

In the **Configurations Comparison** section, certain parameters that are expected to have different values are now reported under the **Common Configs** table.

Related Topics

- Comparing Two Reports
  Oracle Autonomous Health Framework automatically compare the two most recent HTML reports and generate a third diff report, when run in automated daemon mode.

Terminal Release for AIX and Solaris Platforms

Several old operating systems are approaching their end of life, as a result AHF is announcing terminal releases.

AHF 23.8.1 will be the terminal release for:

- AIX 7.1
- Solaris 11.3

This terminal release will continue to be supported on these platforms, but future AHF releases will not support these operating system versions.

For more information, see *Unsupported platforms*.

Related Topics

- Supported Platforms
  You can use Oracle Autonomous Health Framework with all supported versions of Oracle Database and Oracle Grid Infrastructure.

Compliance Checks for Oracle RAC Extended Clusters

AHF adds support for running compliance checks against Oracle RAC Extended Clusters.

An Oracle RAC Extended Cluster consists of nodes that are located in multiple locations called sites.

When you deploy an Oracle Standalone Cluster, you can also choose to configure the cluster as an Oracle RAC Extended Cluster. You can extend an Oracle RAC cluster across two, or more, geographically separate sites, each equipped with its own storage. In the event that one of the sites fails, the other site acts as an active standby.

AHF can now run compliance checks to verify the configuration of RAC Extended Clusters. These checks can be run with the command:

```
ahfctl compliance -includeprofile extended
```

For more information, see *About Oracle Extended Clusters*.

Related Topics

- About Oracle Extended Clusters

Insights Helps Explain Why Events Occurred

AHF Insights now provides the ability to drill into **Major Events**, showing the CPU and I/O stats, providing context for why the event occurred.

The AHF Insights **Operating System Analysis** -> **Report** -> **Summary Timeline** shows when problems occurred and correlates them with the timing of lifecycle events such as Database start or stop.

The **Summary Timeline** has now been enhanced to include useful context data such as CPU and I/O OS metrics under the **Major Events** section.

With this addition AHF Insights shows not only what happened and where, but also why.

Related Topics

- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Insights Timeline Makes Problem Analysis and Resolution Easier

AHF Insights timeline chart and table now dynamically adjust time ranges and allow to copy results as plain text.

The AHF Insights **Timeline** chart can be zoomed to focus on just the events of interest. The below event table now filters dynamically based on the chart zoom. A new copy button capturing everything from the filtered event table as plain text – making problem event analysis and documentation super easy.

Related Topics

- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Insights into Disk Space Problems

AHF Insights shows the number of disk space problems detected and color-codes disks based on their usage.

The AHF Insights **Home** dashboard now highlights on the **Space Analysis** panel, the number of disk space problems detected. Drilling down onto the Space Analysis Report includes a new color-coded view of all the usage of all disks.

This makes detecting and and understanding disk space usage problems fast and easy.

Related Topics

- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Latest Python and Java Third-Parties

AHF has upgraded the versions of Python and Java third-party software to fix Common Vulnerabilities and Exposures (CVEs).

AHF 24.1 has upgraded the versions of many third party libraries in both Python and Java. The following CVEs are all fixed:

- https://nvd.nist.gov/vuln/detail/CVE-2023-49083
- https://nvd.nist.gov/vuln/detail/CVE-2023-48795
- https://nvd.nist.gov/vuln/detail/CVE-2023-46308

For more information, see .*Third-Party License Information*

Related Topics

- Third-Party License Information

Deprecated Oracle Trace File Analyzer Masking Feature

Deprecated `tfactl set redact=mask|sanitize` in release 24.1

Related Topics

- Deprecated Oracle Trace File Analyzer Masking in Release 24.1
  Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 24.1 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Oracle Orachk Specific Best Practice Checks

- Verify loopback interface MTU size

Oracle Exachk Specific Best Practice Checks

- Exadata Critical Issue EX83
- Exadata Critical Issue EX84

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.11

- Upgraded Java Version
  AHF 23.11.0 is shipped with Java version 11.0.21.
- Option to View Operating System and Database Parameter Values
  AHF 23.11 includes a new command option `tfactl param` to view the values of operating system and database parameters specified.
- Database Anomalies Advisor
  AHF Insights adds the Database Anomalies Advisor, which shows database anomalies, their cause, and recommended actions.
- AHF Support for Oracle Linux 9
  AHF adds support for OL9 for both Intel-64/AMD-64 (x86_64) and Arm (aarch64)
- AHF Insights Space Usage Analytics for Diagnostic Destinations
  A new section **Space Analysis** has been added in release 23.11 that renders **Disk Utilization** and **Diagnostice Space Usage** data in visual and tabular format.
- Get Insights from Exawatcher Data
  AHF Insights now includes `Exawatcher` data.
- Insights Timeline Includes Patch Information
  AHF Insights timeline now includes details about when patches were applied.

Upgraded Java Version

AHF 23.11.0 is shipped with Java version 11.0.21.

Option to View Operating System and Database Parameter Values

AHF 23.11 includes a new command option `tfactl param` to view the values of operating system and database parameters specified.

> **Note:**
>
> `tfactl run param` will be deprecated in a future release. It will be replaced by `tfactl param`.

For more information, see:

- *tfactl run*
- *tfactl param*

Related Topics

- tfactl run
  Use the `tfactl run` command to run the requested action (can be inventory or scan or any support tool).
- tfactl param
  Use the `tfactl param` command to view the values of operating system and database parameters specified.

Database Anomalies Advisor

AHF Insights adds the Database Anomalies Advisor, which shows database anomalies, their cause, and recommended actions.

AHF detects database anomalies and identifies the cause and corrective action. This is now made available via AHF Insights in the new Database Anomalies Advisor.

The Database Anomalies Advisor shows a summary timeline of anomalies for hosts and database instances. Findings can be drilled into to understand the cause and recommendation action.

To view the Database Anomalies Advisor and it’s recommendations, run `ahf analysis create --type insights`, open the resulting report, and click Database Anomalies Advisor.

Related Topics

- Database Anomalies Advisor
  AHF detects database anomalies and identifies the cause and corrective action.
- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.

AHF Support for Oracle Linux 9

AHF adds support for OL9 for both Intel-64/AMD-64 (x86_64) and Arm (aarch64)

Oracle Linux is an optimized and secure operating environment for application development and deployment. Oracle Linux 9 provides kernel, performance, and security enhancements.

AHF is now supported on Oracle Linux 9 on both Intel-64/AMD-64 (x86_64) and Arm (aarch64).

For more information, see Announcing Oracle Linux 9 general availability .

AHF Insights Space Usage Analytics for Diagnostic Destinations

A new section **Space Analysis** has been added in release 23.11 that renders **Disk Utilization** and **Diagnostice Space Usage** data in visual and tabular format.

You can view the directory structure and space consumed by directories and files in a visual and tree format across all diagnostic directories and nodes.

Related Topics

- Space Analysis
- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.
- tfactl get
  Use the `tfactl get` command to view the details of various Oracle Trace File Analyzer configuration settings.

Get Insights from Exawatcher Data

AHF Insights now includes `Exawatcher` data.

`Exawatcher` is an Exadata specific tool that collects performance data from Exadata storage cells. Previously, `Exawatcher` data was not available within AHF Insights.

AHF Insights now includes `Exawatcher` data, in the same easy to explore interface as all other diagnostic data.

Related Topics

- Operating System Issues
- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Insights Timeline Includes Patch Information

AHF Insights timeline now includes details about when patches were applied.

AHF Insights provides a bird’s eye view of your entire system, with the ability to spot problems, drill into the root cause and understand how to resolve.

When triaging issues, it can be useful to understand when patches were applied.

The AHF Insights Timeline now shows datapoints highlighting when new patches were applied. In addition, several other usability improvements have been added:

- The timeline can be viewed in a Database Faceted format.
- Operating System Issues data has been rounded to 2 decimal places in the Report section tables.
- Node names in the drop-downs selections are sorted alphabetically.

AHF Release 23.10

- Using the exadcli Utility to Collect Cell Metric Data for Guest VMs (domUs)
  `exadcli` enables you to issue an ExaCLI command to be run on multiple remote nodes. Remote nodes are referenced by their host name or IP address.
- Option to Set a Custom Port to Upload Diagnostics
  Starting with AHF 23.10, you can configure a custom port while setting `ahfctl setupload` parameters.
- Option to Include Profiles While Running AHF Compliance Checks
  Starting with AHF 23.10, you can use `-includeprofile` to specify a comma-delimited list of profiles to add profile specific checks to the existing checks list.
- AHF Insights Support for Larger Collection Intervals
  Starting with 23.10, you can generate Insights report for time period of 12 hours.
- AHF Insights User Experience Improvement
  Report tab in the Operating System Issues section has been revamped to provide a seemless experience.
- Terminal Releases of AHF for Old Platforms
  Several old Operating Systems are approaching their end of life, as a result AHF is announcing terminal releases.
- New GoldenGate Diagnostic Collection Component
  AHF diagcollect now includes a new component for GoldenGate.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.10 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Using the exadcli Utility to Collect Cell Metric Data for Guest VMs (domUs)

`exadcli` enables you to issue an ExaCLI command to be run on multiple remote nodes. Remote nodes are referenced by their host name or IP address.

For more information, see *Using the exadcli Utility to Collect Cell Metric Data for Guest VMs (domUs)*.

Related Topics

- Using the exadcli Utility to Collect Cell Metric Data for Guest VMs (domUs)
  `exadcli` enables you to run an ExaCLI command on multiple remote nodes. Remote nodes are referenced by their host name or IP address.

Option to Set a Custom Port to Upload Diagnostics

Starting with AHF 23.10, you can configure a custom port while setting `ahfctl setupload` parameters.

If you do not specify a port, then 443 is used by default. You can set a port number in the range of 0 - 65353.

Related Topics

- ahfctl setupload
  Use the `ahfctl setupload` command to set upload parameters.
- ahfctl getupload
  Use the `ahfctl getupload` command to fetch the details of configured upload parameters.
- Automatically Upgrading Oracle Autonomous Health Framework to the Latest Version
  AHF Automatic Upgrade enables you to upgrade AHF on the fly without manually downloading `ahf_setup` and upgrading it.

Option to Include Profiles While Running AHF Compliance Checks

Starting with AHF 23.10, you can use `-includeprofile` to specify a comma-delimited list of profiles to add profile specific checks to the existing checks list.

```
ahfctl compliance -includeprofile profile1, profile2...
```

```
orachk -includeprofile profile1, profile2...
```

```
exachk -includeprofile profile1, profile2...
```

> **Note:**
>
> You cannot:
>
> - use `-includeprofile` and `-profile` options together
> - use `-includeprofile` and `-excludeprofile` options together

Use the `-profile` option to specify a comma-delimited list of profiles to run only the checks in the specified profiles.

Use the `-excludeprofile` option to specify a comma-delimited list of profiles to exclude from the compliance check run.

Related Topics

- ahfctl compliance
- Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options
  Review the list of Compliance Framework (Oracle Orachk and Oracle Exachk) command-line options.
- Controlling the Scope of Checks
  Use the list of commands to control the scope of checks.

- Using Profiles with Oracle Autonomous Health Framework
  Profiles are logical groupings of related checks. These related checks are grouped by a particular role, a task, or a technology.

AHF Insights Support for Larger Collection Intervals

Starting with 23.10, you can generate Insights report for time period of 12 hours.

In addition, improvements have been made to the **Operating System Issues** section. You will now be able to view the data in problematic time ranges in plots with more data points.

The problematic time ranges will have the following reading intervals:

- 5 seconds for ranges less than 1 minute
- 30 seconds for ranges more than 1 minute

The number of data points for plots under **Operating System Issues** section are dynamic for optimal time taken to generate report.

The data points for time ranges greater than 4 hours are reduced and have the following reading intervals:

- 1 minute for intervals up to 4 hours
- 3 minutes for intervals greater than 4 hours and less than 12 hours
- 5 minutes for intervals greater than 12 hours.

Related Topics

- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.
- Operating System Issues

AHF Insights User Experience Improvement

Report tab in the Operating System Issues section has been revamped to provide a seemless experience.

With Report view, explore the findings in a drop-down fashion with a full widescreen view.

You can:

- view the Event information in a subplot within the Summary Timeline Gantt Chart
- explore the top ranked metrics in tables under a problem finding in a visual format
- view the metrics associated with the prblem finding in a visual format
- drill down into the detailed state of the system at a specific problematic point in time under 'Problematic Snapshots' section. Problem specific system snapshots are organized into dropdowns ordered by problem timestamp

Related Topics

- Operating System Issues

Terminal Releases of AHF for Old Platforms

Several old Operating Systems are approaching their end of life, as a result AHF is announcing terminal releases.

For more information, see *Unsupported platforms*.

Related Topics

- Supported Platforms
  You can use Oracle Autonomous Health Framework with all supported versions of Oracle Database and Oracle Grid Infrastructure.

New GoldenGate Diagnostic Collection Component

AHF diagcollect now includes a new component for GoldenGate.

AHF has a long-standing ability to collect Golden Gate diagnostics via an SRDC (Service Request Data Collection). However, the Golden Gate SRDC collected logs irrespective of the timeframe and copied all the files matching the file pattern. This resulted in collecting extra logs, which were not required for diagnostics.

Golden Gate has now been added as a new diagcollect component, allowing AHF to discover the Golden Gate directories, inventory the files and store it in BDB. This enables collections based on timeframe which results in only necessary log collection and faster, smaller diagnostic collections.

To use the goldengate component, run:

```
tfactl diagcollect -goldengate -last 1h -noclassify
```

Related Topics

- Using On-Demand Diagnostic Collections
  Run Oracle Trace File Analyzer on demand using `tfactl` command-line tool.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.10 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Best Practice Checks Common to Both Oracle Orachk and Oracle Exachk

Oracle Orachk Specific Best Practice Checks

Oracle Exachk Specific Best Practice Checks

- Oracle High Availability Services Automatic Startup Configuration
- CHECK FOR EXADATA CRITICAL ISSUE EX80
- CHECK FOR EXADATA CRITICAL ISSUE EX81
- CHECK FOR EXADATA CRITICAL ISSUE EX82
- CHECK FOR EXADATA CRITICAL ISSUE DB52
- Verify number of inactive patches for database home

- Verify number of inactive patches for Grid Infrastructure home

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.9

- Enhancement to Controlling the Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.
- Easier to Manage Audit Dump Logs
  AHF Managelogs feature adds ability to manage audit dump logs.
- Enhancement to ahfctl setupgrade and ahfctl unsetupgrade to Store or Remove autoupdate Configurations
  A new option `-autoupdate` has been added to `ahfctl setupgrade` and `ahfctl unsetupgrade`.
- Faster Creation of Diagnostic Collections with Insights Reports
  AHF TFA collections, which include Insights reports are now created faster.
- Quicker Grid Infrastructure Problem Resolution with CVU Diagnostics
  Cluster Verification Utility (CVU) diagnostic files are included in AHF diagnostic collections.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.9 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Enhancement to Controlling the Behavior of Oracle Orachk or Oracle Exachk Daemon

AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

Command	Description

`exachk -autostart reset`
`orachk -autostart reset`
`ahfctl compliance -autostart reset`
	Starts and loads the default schedulers.

`exachk -autostop unset`
`orachk -autostop unset`
`ahfctl compliance -autostop unset`
	Removes all default unmodified schedulers.

Related Topics

- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.
- (Recommended) Installing on Linux or Unix as root User in Daemon Mode
  To obtain the fullest capabilities of Oracle Autonomous Health Framework, install it as `root`.
- Automatic Compliance Checking
  Use the daemon to configure automatic compliance check runs at scheduled intervals.
- Starting and Stopping the Daemon
  Start and stop the daemon and force the daemon to stop a compliance check run.
- Configuring the Daemon for Automatic Start
  Installing Oracle Autonomous Health Framework as `root` on Linux or Solaris automatically sets up and runs the Oracle Orachk or Oracle Exachk daemon.
- Controlling the Behavior of the Daemon
  Use the list of commands to control the behavior of the daemon.
- Running Auto Start
  Use the list of commands to start or stop auto start.
- ahfctl compliance

Easier to Manage Audit Dump Logs

AHF Managelogs feature adds ability to manage audit dump logs.

The AHF Managelogs feature purges logs from default locations like the Grid Infrastructure and all Database Automatic Diagnostic Repository (ADR) destinations.

To do this purging Managelogs uses the Database Automatic Diagnostic Repository (ADR), however ADR does not manage audit dump files. As a result, audit dump files can grow and consume too much space.

The Managelogs feature has been expanded to optionally also include management of audit dump files for Grid Infrastructure and Database.

Configure automatic log purging

- Configure auto purge:

  ```
  tfactl set manageLogsAutoPurge=ON
  ```

- Include audit dumps:

  ```
  tfactl set managelogs.adump=ON
  ```

- Set the frequency of purging (defaults to 60 mins)

  ```
  tfactl set manageLogsAutoPurgeInterval=<n>
  ```

- Configure how old logs must be for them to be purged (default 30 days):

  ```
  tfactl set manageLogsAutoPurgePolicyAge=<d|h>
  ```

Purge logs on-demand

- Enable audit dumps:

```
tfactl set managelogs.adump=ON
```

- Check the usage for audit dump destination

```
tfactl managelogs -show usage
```

- Check variation for audit dump destination

```
tfactl managelogs -show variation
```

- Purge audit dump files along with other destinations managed by managelogs:

```
tfactl managelogs -purge
```

Related Topics

- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.
- tfactl managelogs
  Use the `tfactl managelogs` command to manage Automatic Diagnostic Repository log and trace files.

Enhancement to ahfctl setupgrade and ahfctl unsetupgrade to Store or Remove autoupdate Configurations

A new option `-autoupdate` has been added to `ahfctl setupgrade` and `ahfctl unsetupgrade`.

- To store `autoupdate` configurations, run, for example,

```
ahfctl setupgrade -autoupgrade on -swstage /opt/oracle.ahf -
frequency 1 -autoupdate on
```

- To turn on `autoupdate` configurations, run:

```
ahfctl setupgrade -autoupdate on
```

- To turn off `autoupdate` configurations, run:

```
ahfctl setupgrade -autoupdate off
```

- To unset `autoupdate` configurations, run:

```
ahfctl unsetupgrade -autoupdate
```

Related Topics

- ahfctl setupgrade
  Use the `ahfctl setupgrade` command to set upgrade parameters.
- ahfctl unsetupgrade
  Use the `ahfctl unsetupgrade` command to unset upgrade parameters.

Faster Creation of Diagnostic Collections with Insights Reports

AHF TFA collections, which include Insights reports are now created faster.

AHF Insights reports can be generated stand-alone using the command `ahf analysis create --type insights`. Alternatively, a TFA diagnostic collection can be created with an AHF Insights report included by adding the `-insight` option to the existing `-diagcollect` command.

This creation of the AHF Insights report often requires analysis of existing zipped diagnostics. Unzipping and processing the collections is CPU intensive and can be slow.

This process of analyzing the diagnostic collection to generate the AHF Insights report has been streamlined and performance improved. Timings will vary based on the type of collection being performed and the systems involved.

An example baseline from testing shows the following improvement, on the time taken to generate the included AHF Insights report:

- **23.8:** `tfactl diagcollect -asm -crs- os -tns -insight -last 1h` >> 6.8 seconds
- **23.9:** `tfactl diagcollect -asm -crs- os -tns -insight -last 1h` >> 1 second

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.
- Explore Diagnostic Insights
  Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

Quicker Grid Infrastructure Problem Resolution with CVU Diagnostics

Cluster Verification Utility (CVU) diagnostic files are included in AHF diagnostic collections.

As CVU (Cluster Verification Utility) diagnostic files contain periodic Grid Infrastructure configuration information and critical diagnostic reports they are often required for diagnosis of Grid Infrastructure problems.

AHF now collects all files under the following CVU directories:

- `<GI_BASE>/crsdata/<node>/cvu/diagnostics/cvu_diag_report.txt`
- `<GI_BASE>/crsdata/@global/cvu/baseline/cvures/cvusnapshot*.zip`

To include the CVU diagnostic files add the `-cvu` component to the `diagcollect` command.

For example:

```
tfactl diagcollect -cvu -last 1h -noclassify
```

By default, AHF will include CVU in CRS or Database collections for example, both these automatically include CVU diagnostics:

- `tfactl diagcollect -crs -last 1h -noclassify`
- `tfactl diagcollect -database orcl -last 1h -noclassify`

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.
- Using On-Demand Diagnostic Collections
  Run Oracle Trace File Analyzer on demand using `tfactl` command-line tool.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.9 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Oracle Orachk Specific Best Practice Checks

- Check asmappl.config consistency across nodes for ODA
- Verify clusterware ADVM volume resources configuration
- Verify printk logging configuration

Oracle Exachk Specific Best Practice Checks

- Verify RoCE cabling and switch ports assignment
- Check file `S_CRSCONFIG_<`*`NODE`*`>_ENV.TXT` for consistent limit values across all nodes in the cluster
- Verify DSA authentication is not supported for SSH equivalency

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.8

- Easier to Manage Best Practice Compliance
  AHF compliance checks from Oracle Orachk and Oracle Exachk are now fully integrated into AHF Insights Best Practice section.
- Enhancements to the AHF Insights Interface Design and Usability
  AHF 23.8 includes the following enhancements to the user interface to make it more intuitive and easier to use.

- Upload AHF Insights Report Automatically to Object Store or Pre-Authenticated URL (PAR)
  Upload AHF Insights report automatically if Object Store is configured as part of AHF or Pre-Authenticated URL (PAR) for centralized monitoring.
- Automate the Generation of AHF Insights Reports Using AHF Cron
  Schedule cron jobs to generate AHF Insights report.
- Guided Resolution of Database Performance Problems Caused by Noisy Neighbors
  AHF Balance no-longer requires a GI Home and now works with any Oracle Home.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.8 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Easier to Manage Best Practice Compliance

AHF compliance checks from Oracle Orachk and Oracle Exachk are now fully integrated into AHF Insights Best Practice section.

AHF has thousands of Best Practice Compliance Checks, which are run automatically by AHF Oracle Orachk and Oracle Exachk. The results of these checks are viewable in HTML reports and output in JSON and XML for consumption into other tools. In addition, all Best Practice Compliance Checks are fully integrated into AHF Insights for running on-demand.

AHF Insights makes it easy to quickly see the Health Score, understand where systems are out of compliance and then take the necessary corrective action.

With this enhancement, you can:

- Explore the best practice data in a visual format.
- Filter best practices across different status through visualization and Status status drop-down.
- Search checks from all sections of best practice report.
- View the best practice report in a vertical fashion.
- See the health score with a visual distribution of checks that have failed.

Continue to use the Oracle Orachk / Oracle Exachk commands for automated scheduled runs, but for on-demand compliance investigation, generate an AHF Insights report:

```
ahf analysis create --type insights
```

For more information, see Compliance Checking with Oracle Orachk and Oracle Exachk and Best Practice Issues.

Enhancements to the AHF Insights Interface Design and Usability

AHF 23.8 includes the following enhancements to the user interface to make it more intuitive and easier to use.

> **Note:**
>
> `plotly.js` dependency on CDN has been removed for customers using AHF Insights in restrictive environments.

You can now:

- Copy data in text format into the clipboard to post it into SR body while raising a service request.
  Copy button is included in the following sections of the report:
  - Cluster
  - Databases
  - Database Servers
  - Storage Servers
  - Fabric Switches
  - Recommended Software
- Spot the disks that have anomalies. In the **Operating System Issues** tab, under **Local IO**, click **Disk** to view **Disk Metrics**. Disks that have anomalies are marked with an **X** mark.
- Explore process aggregate from operating system details in a more intuitive way.
  - Demarcated process aggregates per the instance group like Databases, ASM, APX (Apex), IOS, Clusterware, and so on.
  - Legends specific to individual category rather than single legend for all categories.

Related Topics

- Introduction to AHF Insights
  AHF Insights provides a bird's eye view of the entire system with the ability to further drill down for root cause analysis.
- Cluster
- Databases
- Database Servers
- Storage Servers
- Fabric Switches
- Recommended Software
- Operating System Issues

Upload AHF Insights Report Automatically to Object Store or Pre-Authenticated URL (PAR)

Upload AHF Insights report automatically if Object Store is configured as part of AHF or Pre-Authenticated URL (PAR) for centralized monitoring.

Uploading AHF Insights reports helps Oracle Cloud Operations to identify, investigate, track, and resolve system health issues and divergences in best practice configurations quickly and effectively.

Oracle Autonomous Database on Dedicated Exadata Infrastructure and Oracle SaaS

To set REST endpoints (Object Store's), run:

```
ahfctl setupload -name oss -type https -user <user> -url <object_store> -
password
```

To upload AHF Insights report to Object Store, run:

```
ahf analysis create --type insights
```

.

Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D) and Oracle Base Database Service

To upload AHF Insights report to PAR location, run:

```
tfactl diagcollect -insight -last 1h -par <par_url>
```

```
tfactl insight -last 1h -par <par_url>
```

Related Topics

- ahfctl setupload
  Use the `ahfctl setupload` command to set upload parameters.
- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.
- tfactl insight
  Use the `tfactl insight` command to generate AHF Insights report from across nodes in the AHF cluster.
- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

Automate the Generation of AHF Insights Reports Using AHF Cron

Schedule cron jobs to generate AHF Insights report.

> **Note:**
>
> The AHF Insights report will be generated every Monday at 3 a.m.

- To get cron details:

  ```
  tfactl get cron
  ```

  ```
  # tfactl get cron
    .----------------------------------------------.
    |                <hostname>                    |
    +--------------------------------------+-------+
    | Configuration Parameter              | Value |
    +--------------------------------------+-------+
    | Enable/disable the TFA cron ( cron ) | OFF   |
    '--------------------------------------+-------'
  ```

- To enable cron:

  ```
  tfactl set cron=on
  ```

  ```
  # tfactl set cron=on
    Successfully set cron=ON
    .----------------------------------------------.
    |                <hostname>                    |
    +--------------------------------------+-------+
    | Configuration Parameter              | Value |
    +--------------------------------------+-------+
    | Enable/disable the TFA cron ( cron ) | ON    |
    '--------------------------------------+-------'
  ```

- To reload cron with modifications:

  ```
  tfactl refreshconfig modifycron -enable true -id <ID> -validFor all
  ```

  ```
  # tfactl refreshconfig modifycron -enable true -id id001 -validFor
  all
  modifycron() completed successfully.
  ```

- To list existing cron details:

  ```
  # tfactl refreshconfig listcrons
  ```

  ```
  # tfactl refreshconfig listcrons
    TFA CRON item:
    Name:     id001
    Command:  ahf analysis create --type insights --last 5m
    Schedule: 0 3 * * 1
  ```

- To turn off cron:

```
# tfactl set cron=off
```

```
# tfactl set cron=off
  Successfully set cron=OFF
  .----------------------------------------------.
  |                <hostname>                    |
  +--------------------------------------+-------+
  | Configuration Parameter              | Value |
  +--------------------------------------+-------+
  | Enable/disable the TFA cron ( cron ) | OFF   |
  '--------------------------------------+-------'
```

Related Topics

- tfactl get
  Use the `tfactl get` command to view the details of various Oracle Trace File Analyzer configuration settings.
- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.
- tfactl refreshconfig
  Use the `tfactl refreshconfig` command to refresh and list Oracle Trace File Analyzer cron jobs.
- tfactl refreshconfig modifycron
  Use the `tfactl refreshconfig modifycron` command to modify the Oracle Trace File Analyzer cron entry.

Guided Resolution of Database Performance Problems Caused by Noisy Neighbors

AHF Balance no-longer requires a GI Home and now works with any Oracle Home.

Database CPU use is limited by the database `CPU_COUNT` parameter. When these limits add up to more than the number of CPUs on a machine, noisy-neighbor problems are possible.

AHF Balance analyzes database CPU configuration and historical CPU usage data from Enterprise Manager. The high-level results of this analysis are shown in the Oracle Orachk / Oracle Exachk MAA Score Card.

Further reports can be run to:

- Get an overview of possible noisy neighbors across the fleet.
- See detailed information about a specific database.
- Generate a corrective action plan.

To use AHF Balance:

- Configure AHF Balance to analyze historical CPU usage from Enterprise Manager’s repository database:

  ```
  ahf configuration set --type impact --connect-string <EM-DATABASE-
  CONNECT-STRING> --user-name <USER-NAME>
  ```

  > **Note:**
  >
  > Ensure that the connect string does not contain any spaces.

- Run a fleet-wide analysis to create a detailed AHF Balance report to understand noisy neighbors and the improvements possible by changing `CPU_COUNT` settings:

  ```
  ahf analysis create --type impact --scope fleet --name <FLEET_NAME>
  ```

- Run a cluster-level analysis to get a detailed corrective action plan:

  ```
  ahf analysis create --type impact --scope cluster --name
  cluster_name
  ```

For more information, see Data Source.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.8 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Best Practice Checks Common to Both Oracle Orachk and Oracle Exachk

- Verify health of data dictionary for multitenant database
- Verify health of data dictionary for non-multitenant database

Oracle Orachk Specific Best Practice Checks

- Oracle Database recommendation for audit settings
- Oracle Database unified auditing recommendation

Oracle Exachk Specific Best Practice Checks

- Check for `CachedBy` and `CachingPolicy GridDisks` attributes
- Check for tainted kernel by non-Oracle modules and third-party security software installed from package

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.7

- Easier Patch Management with AHF Insights
  AHF Insights now includes a new patching section showing Database and GI patches
- AHF Insights Go Mobile
  AHF Insights is now mobile responsive and optimized for ease of reading.
- Easier Operation on Exadata Dom0
  On Exadata Dom0, AHF installations can be converted from standalone (extract) to typical, and `/EXAVMIMAGES` is now used for the default data directory.
- Faster Redaction of Diagnostic Collections
  Diagnostic collections can now be redacted faster by increasing the CPU allocation to ACR.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.7 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Easier Patch Management with AHF Insights

AHF Insights now includes a new patching section showing Database and GI patches

Managing patches can be difficult. It requires the ability to:

- Keep track of which individual patches are applied, to which hosts, and when.
- Spot where you’ve got gaps in patches.
- Understand which bugs the various patches fix.

AHF Insights now makes this a whole lot easier with the new **Patching Information** section. The Patching Information section shows Database and GI patches per host and Oracle Home, providing easy understanding of which patches are applied and where. There’s also a new patch timeline, which visualizes patch information showing when patches were applied. Gaps or inconsistencies in patching are highlighted across nodes for the same home. Bugs and relevant patch information can be quickly searched and viewed via interactive reports.

Related Topics

- Patch Information

AHF Insights Go Mobile

AHF Insights is now mobile responsive and optimized for ease of reading.

People rely on AHF Insights to get a top-down system view, see when problems occur, understand the causes, and how to fix them. Now, AHF Insights can be viewed on a mobile phone. Navigate system topology, drill into problems, and get recommendations from anywhere when on the go. To view graphs just tilt to landscape to get full screen metric immersion.

In addition, AHF Insights has several improvements to make it easier to use and faster to find important information. Various AHF Insights sections have now been optimized to provide default viewing options, which make it even easier and faster to explore data.

- The Cluster Section now shows Database homes ordered by Database Version and Database Homes are expanded by default.
- The Database Section shows CDB names sorted alphabetically by default.

- The Operating System Issues Section has rearranged and added new data labels and the IO and Network details can now be configured.

Related Topics

- Cluster
- Databases
- Operating System Issues

Easier Operation on Exadata Dom0

On Exadata Dom0, AHF installations can be converted from standalone (extract) to typical, and `/EXAVMIMAGES` is now used for the default data directory.

AHF provides multiple installation methods:

- **Standalone**: Extracts only the AHF bits.
- **Typical**: Performs full install including configuring scheduling for important features like compliance checking.

Previously, to change an AHF installation from standalone to typical required an uninstall followed by a fresh install. Now, any upgrades on Exadata Dom0 of a Standalone installation will prompt to convert to Typical and any installation will prompt to start the scheduler if it's not already running. Existing AHF installations can be converted from Standalone to Typical during scripted upgrades by using the `-upgradetotypical` option.

On Exadata Dom0 the default installation location of `/opt` can get quickly filled by collections.

Now, fresh AHF installations on Exadata Dom0 use `/EXAVMIMAGES` as the default data directory. Additionally, auto upgrades as either root or a user within the Platinum role will automatically move the data directory to be under `/EXAVMIMAGES`.

For more information, see Convert AHF Standalone (default) Installation to Typical Installation.

Faster Redaction of Diagnostic Collections

Diagnostic collections can now be redacted faster by increasing the CPU allocation to ACR.

AHF ships with ACR (Adaptive Classification and Redaction) for the purposes of sanitizing sensitive data. Redaction involves scanning the full contents of every file within a collection, so is very CPU intensive. For this reason, there are certain limits put in place within AHF to ensure excessive CPU is not used.

All AHF processes run under a CGroups setting, which caps the maximum CPU usage at the lower of either 4 CPUs or 75% of available CPUs. Additionally, there is a specific cap on ACR to only use a maximum of 20% of available CPU.

In some environments, however, customers have large CPU resources and want to use more CPU so redaction can be completed quickly. This can now be accomplished with this two-phase process:

Firstly, increase the AHF CGroup limit above the normal 75% limit by using the `-force` option:

```
ahfctl setresourcelimit -resource cpu -value <cpu_count> -force
```

For more information about setting resource limit, see ahfctl setresourcelimit.

Secondly, use the `-acrprocesscount` option to set the number of ACR processes that will be used within the diagnostic collection command:

```
tfactl diagcollect <option> <-sanitize | -mask> -acrprocesscount <cpu_count>
```

For example, `tfactl diagcollect -last 5m -acrprocesscount 3 -sanitize`

For more information on redaction of AHF collections, see Sanitizing Sensitive Information in Oracle Trace File Analyzer Collections and tfactl diagcollect.

> **Caution:**
>
> Most customers should not perform redaction in a production environment. Instead, set up a staging server for ACR.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.7 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Oracle Orachk Specific Best Practice Checks

- Verify number of inactive patches for Grid Infrastructure home
- Verify number of inactive patches for database home

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.6

- Top-Down View of Network Abnormalities Across the System
  AHF Insights metrics section now includes Aggregated NICs data as part of the Network section.
- View Process Metrics for All Hosts at a Glance
  AHF Insights adds a new Process metrics tab.
- Capture Up-To-The-Minute Insights Data
  AHF Insights can now collect fresh data without using the cache.
- AHF Provides Complete Support for the X10M Platform
  AHF now provides complete support for Oracle Exadata X10M.

- AHF for ARM
  AHF provides built-in support for ARM architectures in the cloud and on-premises.
- Dynamically Change the Diagnostic Storage Location for AHF Without Reinstallation
  AHF command-line option to move installed AHF data directory to a different location.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.6 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Top-Down View of Network Abnormalities Across the System

AHF Insights metrics section now includes Aggregated NICs data as part of the Network section.

Understanding the cause of network issues often meant trawling through different log files and trying to spot that one line that was different.

AHF now brings together all relevant data from the network interface card into one easy-to-understand screen, showing:

- Receive Rate
- Transmit Rate
- Total Space
- Error Rate
- Received Packet Count
- Transmitted Packet Count
- Errored Received Datagram Count
- Error Rate for Transmitted Packets
- Drop Rate for Received Packets

Each graph shows data of one type across all sources, easily enabling visualization of abnormalities. To explore the NICs data: **Operating System Issues** > **Metrics** > **Network** > **Aggregated NICS**.

For more information about Operating System Issues, see Operating System Issues.

For more information about AHF Insights, watch: Exadata Master Class: Maximize System Performance with Autonomous Health Framework Insights.

View Process Metrics for All Hosts at a Glance

AHF Insights adds a new Process metrics tab.

When triaging operating system issues, it's useful to understand various process metrics such as real-time process count or number of blocked processes.

AHF surfaces all process metrics in one screen under the **Metrics Process** tab.

The **Process** section shows:

- Process Count

- Blocked Process Count
- Real-Time Process Count
- D State Process Count
- Process on CPU Count
- Total File Descriptors

Data for each host is overlaid on the same chart, enabling easy comparison. To explore the Process data: **Operating System Issues** > **Metrics** > **Process**.

For more information about Operating System Issues, see Operating System Issues.

Capture Up-To-The-Minute Insights Data

AHF Insights can now collect fresh data without using the cache.

To make Insights data collection fast, AHF caches important information. Sometimes, however, it's useful to capture all data fresh at the time of collection.

AHF Insights can now be generated using the `--refresh` option to avoid the use of cache. When the refresh option is used collection time will be longer as everything is collected on-demand as requested.

To generate AHF Insights without caching, run the command:

```
ahf analysis create --type insights --refresh
```

For more information, see ahf analysis.

AHF Provides Complete Support for the X10M Platform

AHF now provides complete support for Oracle Exadata X10M.

In June, Oracle released the latest Exadata X10M platform.

AHF EXAchk compliance checks have been extended to provide X10M support.

This new support covers the new database server system model, the new Exadata smart flash cache size and new Exadata versions.

Specific checks updated include:

1. Verify Exadata Smart Flash Cache is created.
2. Verify RAID disk controller CacheVault capacitor condition [Storage Server].
3. Exadata storage server system model number.
4. Exadata software validation on storage server and database server for platinum certification.
5. Verify Exadata Smart Flash Cache is created.
6. Verify RAID disk controller CacheVault capacitor condition [Storage Server].
7. Exadata storage server system model number.
8. Exadata software validation on storage server and database server for platinum certification.

AHF Insights then visualizes the results of these compliance checks along with a complete bird's-eye view of the Platform.

AHF for ARM

AHF provides built-in support for ARM architectures in the cloud and on-premises.

Oracle Database on ARM provides customers with:

- Predictable performance at a lower cost
- Energy-efficient and sustainable design
- Flexible VM shapes to size to workloads
- Cloud automation tools to simplify management
- Free credits for open source developers, research universities, industry partners, and customers

AHF now provides native support for ARM. On-premise AHF downloads for ARM are available on the AHF download page.

Read more about Oracle Database for ARM in the Cloud and On-premise.

Dynamically Change the Diagnostic Storage Location for AHF Without Reinstallation

AHF command-line option to move installed AHF data directory to a different location.

AHF stores all compliance results, diagnostic collections as well as AHF logs within the AHF data directory. Overtime as systems change it may be useful to move that data directory to a different location.

Previously, moving the data directory required an uninstall and reinstall of AHF using a different `data_dir` path. AHF has now made it easier to move the data directory without the need to uninstall.

Use the new command: `ahfctl movedatadir <`*`new_directory`*`>`.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.6 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Oracle Orachk Specific Best Practice Checks

- Verify number of inactive patches for database home

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.5

- AHF Insights New Features and Performance Improvements
  AHF Insights now includes several new features and performance improvements.
- AHF Print Collections Improvements
  AHF now makes it easier to understand any diagnostic collections, which are queued for execution.
- Diagnostic Collection Improvements
  AHF now makes it easier to list the contents of nested diagnostic collections or to list the contents of multiple zip files from the same collection.
- Optimization of AHF Compliance Results and Log Storage
  Cleanup of AHF compliance results and log data has been improved.

AHF Insights New Features and Performance Improvements

AHF Insights now includes several new features and performance improvements.

- The pertinent charts are annotated to highlight anomalies detected.
- The newly added System Overview section presents key metrics from the following areas:
  - OS
  - CPU
  - Memory
  - Network
  - I/O
- For easy comparison, Cluster-Wide OS charts are now available with metrics from multiple cluster nodes overlayed in the same chart.
- A new Configuration Section has been added for viewing CPU and Memory configuration details.
- Chart size and rendering performance has been improved.
- Insights visualizations size has been reduced by 45%, which significantly reduces the size of overall Insights report.
- The user interface now performs deferred rendering of visualizations that improves the page load time and user experience.

AHF Print Collections Improvements

AHF now makes it easier to understand any diagnostic collections, which are queued for execution.

When a collection is requested, AHF will review available resources and may queue that collection for execution later when more resources are available.

A new print collections option has been added to show the status of any queued collections:

```
tfactl print collections -status queued
```

Related Topics

- tfactl print
  Use the `tfactl print` command to print information from the Berkeley DB (BDB).

Diagnostic Collection Improvements

AHF now makes it easier to list the contents of nested diagnostic collections or to list the contents of multiple zip files from the same collection.

- To list the contents of diagnostic collection including any nested zip files, use:

  ```
  tfactl collection list-contents -collectionzip zip
  ```

- To list the contents of all zip files within a specific collection, use:

  ```
  tfactl collection list-contents -collectionname collection-name
  ```

Related Topics

- tfactl collection
  Use the `tfactl collection` command to manage Oracle Trace File Analyzer collections.

Optimization of AHF Compliance Results and Log Storage

Cleanup of AHF compliance results and log data has been improved.

Results and log data management has been available for many releases:

- Automatic retention: `COLLECTION_RETENTION=`*n*
- On-demand retention: `user_collection_retention=`*n*

AHF now includes a new option `-purge_size` to specify the retention size to manage results and log data.

For example, to purge compliance data larger than 1024 MB, use:

```
ahfctl compliance -purge_size 1024
```

Related Topics

- collection_retention
  Set the `collection_retention` daemon option to purge health check collection results that are older than a specified number of days.
- ahfctl compliance

AHF Release 23.4

- Insights into Oracle Database Appliance (ODA) and Generic Oracle RAC Systems
  AHF Insights now runs on ODA and generic Oracle RAC systems in addition to its previous support for Exadata.

- Tracking and Reporting of System Level Changes
  The tfactl changes command has been enhanced to now report system level changes in the following areas:
- Support JSON Payload as Options for tfactl Commands
  Cloud Operations need to be able to easily request Oracle Trace File Analyzer collections from the OneView interface and be able to support new AHF collection features without having to request changes to cloud agent code.
- New Options for Understanding the Status of Diagnostic Collections
  New `tfactl print collections -status` options hav been added to understand the status of AHF diagnostic collections if they are successful, failed, or still running.
- Oracle Orachk Support to Send Email Attachments as JSON
  Starting in release 23.4, Oracle Orachk supports sending email attachments in JSON format instead of HTML when specified.
- Unified AHF Command-Line Interface Enhancements
  Review the list of enhancements made to AHF CLI in release 23.4.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.4 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Insights into Oracle Database Appliance (ODA) and Generic Oracle RAC Systems

AHF Insights now runs on ODA and generic Oracle RAC systems in addition to its previous support for Exadata.

AHF Insights provides a bird's-eye view of an entire system. The rich interface showcases:

- Environment topology
- Configuration
- Database and System Kernel parameters
- Compliance management and drift tracking including recommended RU's
- Timeline of sequence of events
- Visual highlighting of anomalies in system metrics
- Root causes for issues and fixes for some anomalous cases

Operating System information on systems prior to 19.3 is not supported.

AHF Insights reports can be generated using the command: `ahf analysis create --type insights`.

To get started with AHF Insights see Introduction to AHF Insights.

Tracking and Reporting of System Level Changes

The tfactl changes command has been enhanced to now report system level changes in the following areas:

- Oracle Database parameters set to non-default values
- Oracle Home installations

- Oracle Home patch installation
- Operating system parameters that are relevant to Oracle Grid Infrastructure and Oracle Database installations
- Operating system patches

Command output displays both current and previous values. Change results can also be generated in JSON format by adding the `-json` option. Changes are reported on a per-node basis by default but can be controlled using the `-node` option. Output it limited to a maximum of 30-day period.

For more information, see tfactl changes.

Support JSON Payload as Options for tfactl Commands

Cloud Operations need to be able to easily request Oracle Trace File Analyzer collections from the OneView interface and be able to support new AHF collection features without having to request changes to cloud agent code.

By supporting the use of JSON to provide a list of arguments for all `tfactl` commands that json can be constructed by the requestor and simply be passed through the cloud agent to AHF.

New Collection options can be supported immediately by the initial request without the need to request Cloud agent clode changes.

This feature simply extracts the json provided and expands it to call in to the current tfactl command line interface.

New Options for Understanding the Status of Diagnostic Collections

New `tfactl print collections -status` options hav been added to understand the status of AHF diagnostic collections if they are successful, failed, or still running.

The `tfactl print collections` command has been enhanced to provide three new options:

- `tfactl print collections -status FAILED`: Prints failed collections.
- `tfactl print collections -status QUEUED`: Prints collections that are queued and yet to start.
- `tfactl print collections -status COMPLETED`: Prints completed collections.

For more information, see tfactl print.

Oracle Orachk Support to Send Email Attachments as JSON

Starting in release 23.4, Oracle Orachk supports sending email attachments in JSON format instead of HTML when specified.

Use the `-attachment_type` option or set the `RAT_ATTACHMENT_TYPE` environment variable to send email attachments in JSON format. This feature is intended to use with the following two Oracle Orachk email notification methods:

- together with the `-sendemail` option
- through the `NOTIFICATION_EMAIL` and `AUTORUN_FLAGS` configuration in the autoruns

- **What's included in the attached JSON files?**
  - The attachments for manual runs include the `orachk_summary.json` and `orachk_valid_results.json` files.
  - For scheduled runs, the `diff` JSON file is also attached together with files mentioned above.
- **How to specify the attachment type for a manual run?**
  - Using the `-attachment_type` option:

    ```
    orachk -sendemail user@domain.com -attachment_type json
    ```

  - Or, setting the RAT environment variable instead:

    ```
    export RAT_ATTACHMENT_TYPE=json
    ```

- **How to specify the attachment type as JSON for scheduled runs?**
  You must
  - configure `NOTIFICATION_EMAIL` value for the corresponding `autorun` entry, for example:

    ```
    orachk -set 'NOTIFICATION_EMAIL=user@domain.com' -id autostart_client
    ```

  - configure `AUTORUN_FLAGS` value for the corresponding `autorun` entry, for example:

    ```
    orachk -set 'AUTORUN_FLAGS=<previous autorun flags> -attachment_type
    json' -id autostart_client
    ```

Unified AHF Command-Line Interface Enhancements

Review the list of enhancements made to AHF CLI in release 23.4.

- `ahf software get-latest-mrp-level`: Get the latest MRP level to see if the metadata needs to be updated.

  ```
  ahf software get-latest-mrp-level
  19.18
      Database: Database MRP 19.18.0.0.230418
      GI      : GI MRP 19.18.0.0.230418
  19.17
      Database: Database MRP 19.17.0.0.230418
      GI      : GI MRP 19.17.0.0.230418
  ```

  For more information, see ahf software.
- `--clusters clu1 clu2 clu3`: Specify a space-delimited list of clusters to include in the AHF Balance fleet scope of the analysis.

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --clusters
  clu1 clu2 clu3
  ```

  For more information, see ahf analysis

- `--refresh`: Create analysis report with the most recent data from AHF Insights sources.

  ```
  ahf analysis create --type insights --refresh
  ```

  For more information, see ahf analysis

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.4 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Best Practice Checks Common to Both Oracle Orachk and Oracle Exachk

- AHF Balance check for CPU contention between databases
- AHF CPU oversubscription check

Oracle Orachk Specific Best Practice Checks

- Validate database listener service configuration with clusterware

Oracle Exachk Specific Best Practice Checks

- Validate KMS configuration for database encryption
- Compare instance name between CRS and cloud registration file

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.3

- Enable Database SRDCs for the Platinum Role
  Starting in release 23.3, database SRDCs can be run by users with `platinum` role on the system in the `dba` group.
- Unified AHF Command-Line Interface Monthly Recommended Patches (MRP) Support
  In release 23.3, the unified AHF command-line interface has been enhanced to report Monthly Recommended Patches (MRP) information.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.3 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Enable Database SRDCs for the Platinum Role

Starting in release 23.3, database SRDCs can be run by users with `platinum` role on the system in the `dba` group.

When an AHF user has been granted the required AHF role, they can request a subset of database-specific SRDCs to be executed even if they are not in the `dba` group for that database. Only the AHF owner (`root`) can grant the role.

Predominantly, in the Platinum environment, diagnostic requests are executed on the customer's system through the Platinum Gateway as the `orarom` user. The specific user may not be `orarom`, but in most cases it is and this user may be granted the `platinum` AHF role.

When a user with the `platinum` role (initial implementation) requests an SRDC collection that requires normally to be run as a user in the `dba` group and is within a limited whitelist, the request will not be rejected. Instead, the request will be executed as the DB owner or Grid owner as appropriate.

This solves the case where the Platinum team are not able to gather some diagnostics automatically through their gateway due to their user not being added to the `dba` group for all of a customers databases.

Unified AHF Command-Line Interface Monthly Recommended Patches (MRP) Support

In release 23.3, the unified AHF command-line interface has been enhanced to report Monthly Recommended Patches (MRP) information.

In November 2022, Oracle introduced Monthly Recommended Patches (MRP). MRP provides customers with frequent access to recommended and well-tested patch collections. For more information, see *Introducing Monthly Recommended Patches (MRPs) and FAQ (Doc ID 2898740.1)*.

It is difficult for the customers to determine which MRP level and patches they have installed. The AHF command-line now provides a command to query the MRP level and installed patches.

To get the MRP level for the specified Oracle Home:

```
ahf software get-mrp-level --oracle-home TEXT
```

To compare MRP level against the specified Oracle Home to determine installed and missing patches:

```
ahf software compare-mrp-level --oracle-home TEXT --mrp-level TEXT
```

For more information, see *ahf software*.

Related Topics

- Introducing Monthly Recommended Patches (MRPs) and FAQ (Doc ID 2898740.1)
- ahf observer
  Use the `ahf observer` command to retrieve status of AHF components.
- ahf software
  Use the `ahf software` command to retrieve the details of AHF software and Monthly Recommended Patches (MRP).

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.3 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Oracle Orachk Specific Best Practice Checks

- Verify important bug fixes on long term recent releases

Oracle Exachk Specific Best Practice Checks

- Verify symbolic link for cloud registration file
- Verify database TDE wallet configuration
- Verify TNS configuration and connectivity to database using SYS credentials

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.2

- AHF Balance
  Intelligent Workload Advisor (IWA) introduced in AHF release 22.3 has been renamed as AHF Balance in release 23.2.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.2 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

AHF Balance

Intelligent Workload Advisor (IWA) introduced in AHF release 22.3 has been renamed as AHF Balance in release 23.2.

Related Topics

- Resolve Noisy Neighbor Issues
  AHF Balance is a command-line utility that analyzes historical CPU consumption data and Database Resource Manager (DBRM) settings for the set of databases running in a cluster.
- Running Unified AHF CLI Administration Commands

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.2 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Oracle Exachk Specific Best Practice Checks

- Verify important bug fixes on long term recent releases

- Exadata Critical Issue EX78

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

AHF Release 23.1

- New Status in Oracle Orachk/Oracle Exachk Report
  In release 23.1, a new check status of **Undetermined** has been introduced into the Oracle Orachk/Oracle Exachk reports.
- Compare Configuration Across Two Different systems
  Starting in release 23.1, you can compare configuration across two different systems.
- Machine Readable Output Option for AHFCTL Commands
  In release 23.1, JSON output option has been added to a number of AHFCTL commands to allow other software to easily integrate with AHF.
- AHF SQLAgent Connection Pooling
  The `SQL Agent` reduces the number of connections AHF makes to the database.
- New Oracle Orachk and Oracle Exachk Best Practice Checks
  Release 23.1 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

New Status in Oracle Orachk/Oracle Exachk Report

In release 23.1, a new check status of **Undetermined** has been introduced into the Oracle Orachk/Oracle Exachk reports.

Previously, if a check failed for an unexpected reason, such as permission denied or unable to find a resource, it would be marked as failed. This led to false negatives. These types of check failures now result in the check status being marked as **Undetermined**. Note that **Undetermined** checks carry the same weight in the Health Score Calculation as skipped checks.

Compare Configuration Across Two Different systems

Starting in release 23.1, you can compare configuration across two different systems.

For example:

- Primary vs Standby
- Test vs Production
- Heathy vs Unhealthy system

Run Oracle Orachk/Oracle Exachk on both systems and then pass both resulting zip to the `-diff` option to show configuration sections:

1. Different values for same configuration/parameter
2. Unique values found only in first system

3. Unique values found only in second system
4. Common values in both systems

Use the new configuration comparison as follows:

```
orachk -diff {compliance collection zip1} {compliance collection zip2}
-force -showallcomparison


exachk -diff {compliance collection zip1} {compliance collection zip2}
-force -showallcomparison
```

Machine Readable Output Option for AHFCTL Commands

In release 23.1, JSON output option has been added to a number of AHFCTL commands to allow other software to easily integrate with AHF.

For example:

- `ahfctl switch -status -json`
- `ahfctl statusahf -json`
- `ahfctl upgradehistory -json`
- `ahfctl queryupdate -json`

AHF SQLAgent Connection Pooling

The `SQL Agent` reduces the number of connections AHF makes to the database.

Previously, when TFAC ran an SQL query to gather metrics and health data, an SQL*Plus sub-process was created. This sub-process allocated resources to establish a database connection, which was then used to execute one single SQL query. Upon completion of the SQL query, the connection was closed and the sub-process was terminated.

The new SQL Agent creates a sub-process that keeps the database connections open through the life-time of AHF. A communication channel is opened between AHF and the SQL Agent, so the database connections can be reused and serve all SQL query execution requests from AHF.

By reducing the number of connections, resource consumption such as CPU and Memory are decreased along with the number of audit connection logs.

New Oracle Orachk and Oracle Exachk Best Practice Checks

Release 23.1 includes the following new Oracle Orachk and Oracle Exachk best practice checks.

Best Practice Checks Common to Both Oracle Orachk and Oracle Exachk

- EM Status
- Verify important bug fixes on long term recent releases

Oracle Orachk Specific Best Practice Checks

- Validate password file sharing

Oracle Exachk Specific Best Practice Checks

- AHF CPU oversubscription check
- Verify CPU configuration across all virtual machines in a cluster
- Check file system usage in cloud environments
- Verify the status of `dbcs-agent` and `dbcs-admin` processes

All checks can be explored in more detail via the Health Check Catalogs:

Related Topics

- Oracle Orachk Health Check Catalog
- Oracle Exachk Health Check Catalog

1 Overview

Oracle Autonomous Health Framework is a collection of components that analyzes the diagnostic data collected, and proactively identifies issues before they affect the health of your clusters or your Oracle Real Application Clusters (Oracle RAC) databases.

Most of the Oracle Autonomous Health Framework components are already available in Oracle Database 12*c* release 1 (12.1).

- Oracle Autonomous Health Framework Problem and Solution Space
  Oracle Autonomous Health Framework (AHF) maximizes availability and performance by enforcing best practices, capturing data at first failure, monitoring the whole system (server, database, I/O, and network) to proactively discover issues and notify the user and provide timely bug resolution by suggesting fixes automatically after failure.
- Components of Autonomous Health Framework
  This section describes the diagnostic components that are part of Oracle Autonomous Health Framework.

1.1 Oracle Autonomous Health Framework Problem and Solution Space

Oracle Autonomous Health Framework (AHF) maximizes availability and performance by enforcing best practices, capturing data at first failure, monitoring the whole system (server, database, I/O, and network) to proactively discover issues and notify the user and provide timely bug resolution by suggesting fixes automatically after failure.

System administrators can use most of the components in Oracle Autonomous Health Framework interactively during installation, patching, and upgrading. Database administrators can use Oracle Autonomous Health Framework to diagnose operational runtime issues and mitigate the impact of these issues.

- Availability Issues
  Availability issues are runtime issues that threaten the availability of software stack.
- Performance Issues
  Performance issues are runtime issues that threaten the performance of the system.

1.1.1 Availability Issues

Availability issues are runtime issues that threaten the availability of software stack.

Availability issues can result from either software issues (Oracle Database, Oracle Grid Infrastructure, operating system) or the underlying hardware resources (CPU, Memory, Network, Storage).

The components within Oracle Autonomous Health Framework address the following availability issues:

Examples of Server Availability Issues

Server availability issues can cause a server to be evicted from the cluster and shut down all the database instances that are running on the server.

Examples of such issues are:

- **Issue:** Network congestion on the private interconnect can cause time-critical internode or storage I/O to have excessive latency or dropped packets. This type of failure typically builds up and can be detected early, and corrected or relieved.

  Solution: If a change in the server configuration causes this issue, then Cluster Verification Utility (CVU) detects it if the issue persists for more than an hour. However, Oracle Cluster Health Advisor detects the issue within minutes and presents corrective actions.

- **Issue:** Network failures on the private interconnect caused by a pulled cable or failed network interface card (NIC) can immediately result in evicted nodes.

  Solution: Although these types of network failures cannot be detected early, the cause can be narrowed down by using Cluster Health Monitor and Oracle Trace File Analyzer to pinpoint the time of the failure and the network interfaces involved.

Examples of Database Availability Issues

Database availability issues can cause an Oracle database or one of the instances of the database to become unresponsive and thus unavailable to users.

Examples of such issues are:

- **Issue:** Runaway queries or delays can deny critical database resources such as locks, latches, or CPU to other sessions. Denial of critical database resources results in database or an instance of a database being non-responsive to applications.

  Solution: Blocker Resolver detects and automatically resolves these types of delayss. Also, Oracle Cluster Health Advisor detects, identifies, and notifies the database administrator of such delays and provides an appropriate corrective action.

- **Issue:** Denial-of-service (DoS) attacks, vulnerabilities, or simply software bugs can cause a database or a database instance to be unresponsive.

  Solution: Proactive recommendations of known issues and their resolutions provided by Oracle Orachk can prevent such occurrences. If these issues are not prevented, then automatic collection of logs by Oracle Trace File Analyzer, in addition to data collected by Cluster Health Monitor, can speed up the correction of these issues.

- **Issue:** Configuration changes can cause database outages that are difficult to troubleshoot. For example, incorrect permissions on the `oracle.bin` file can prevent session processes from being created.

  Solution: Use Cluster Verification Utility and Oracle Orachk to speed up identification and correction of these types of issues. You can generate a diff report using Oracle Orachk to see a baseline comparison of two reports and a list of differences. You can also view configuration reports created by Cluster Verification Utility to verify whether your system meets the criteria for an Oracle installation.

1.1.2 Performance Issues

Performance issues are runtime issues that threaten the performance of the system.

Performance issues can result from either software issues (bugs, configuration problems, data contention, and so on) or client issues (demand, query types, connection management, and so on).

Server and database performance issues are intertwined and difficult to separate. It is easier to categorize them by their origin: database server or client.

Examples of Database Server Performance Issues

- **Issue:** Deviations from best practices in configuration can cause database server performance issues.

  Solution: Oracle Orachk detects configuration issues when Oracle Orachk runs periodically and notifies the database administrator of the appropriate corrective settings.
- **Issue:** A session can cause other sessions to slow down waiting for the blocking session to release its resource or complete its work.

  Solution: Blocker Resolver detects these chains of sessions and automatically terminates the root holder session to relieve the bottleneck.
- **Issue:** Unresolved known issues or unpatched bugs can cause database server performance issues.

  Solution: These issues can be detected through the automatic Oracle Orachk reports and flagged with associated patches or workarounds. Oracle Orachk is regularly enhanced to include new critical issues, either in existing products or in new product areas.

Examples of Performance Issues Caused by Database Client

- **Issue:** Misconfigured parameters such as SGA and PGA allocation, number of sessions or processes, CPU counts, and so on, can cause database performance degradation.

  Solution: Oracle Orachk and Oracle Cluster Health Advisor detect the settings and consequences respectively and notify you automatically with recommended corrective actions.

1.2 Components of Autonomous Health Framework

This section describes the diagnostic components that are part of Oracle Autonomous Health Framework.

- Introduction to Oracle Autonomous Health Framework Configuration Audit Tools
  Oracle Orachk and Oracle Exachk provide a lightweight and non-intrusive health check framework for the Oracle stack of software and hardware components.
- Introduction to Oracle Trace File Analyzer
  Oracle Trace File Analyzer is a utility for targeted diagnostic collection that simplifies diagnostic data collection for Oracle Clusterware, Oracle Grid Infrastructure, and Oracle Real Application Clusters (Oracle RAC) systems, in addition to single instance, non-clustered databases.

- Introduction to AHF Insights
  AHF Insights provides a bird's eye view of the entire system with the ability to further drill down for root cause analysis.
- Introduction to Oracle Cluster Health Advisor
  Oracle Cluster Health Advisor continuously monitors cluster nodes and Oracle RAC databases for performance and availability issue precursors to provide early warning of problems before they become critical.
- Introduction to AHF Scope
  AHF Scope is a standalone, interactive, real-time capable front-end to Oracle Cluster Health Advisor (CHA). AHF Scope requires a very small foot-print on the monitored system.
- Introduction to AHF Balance
  AHF Balance is a command-line utility that analyzes historical CPU consumption data and Database Resource Manager (DBRM) settings for the set of databases running in a cluster.
- Introduction to Cluster Health Monitor
  Cluster Health Monitor is a component of Oracle Grid Infrastructure, which continuously monitors and stores Oracle Clusterware and operating system resources metrics.
- Introduction to Blocker Resolver
  Blocker Resolver is an Oracle Real Application Clusters (Oracle RAC) environment feature that autonomously resolves delays and keeps the resources available.

1.2.1 Introduction to Oracle Autonomous Health Framework Configuration Audit Tools

Oracle Orachk and Oracle Exachk provide a lightweight and non-intrusive health check framework for the Oracle stack of software and hardware components.

Oracle Orachk and Oracle Exachk:

- Automates risk identification and proactive notification before your business is impacted
- Runs health checks based on critical and reoccurring problems
- Presents high-level reports about your system health risks and vulnerabilities to known issues
- Enables you to drill-down specific problems and understand their resolutions
- Enables you to schedule recurring health checks at regular intervals
- Sends email notifications and diff reports while running in daemon mode
- Integrates the findings into Oracle Health Check Collections Manager and other tools of your choice
- Runs in your environment with no need to send anything to Oracle

You have access to Oracle Orachk and Oracle Exachk as a value add-on to your existing support contract. There is no additional fee or license required to run Oracle Orachk and Oracle Exachk.

Use Oracle Exachk for Oracle Engineered Systems except for Oracle Database Appliance. For all other systems, use Oracle Orachk.

Run health checks for Oracle products using the command-line options.

1.2.2 Introduction to Oracle Trace File Analyzer

Oracle Trace File Analyzer is a utility for targeted diagnostic collection that simplifies diagnostic data collection for Oracle Clusterware, Oracle Grid Infrastructure, and Oracle Real Application Clusters (Oracle RAC) systems, in addition to single instance, non-clustered databases.

Enabled by default, Oracle Trace File Analyzer:

- Provides comprehensive first failure diagnostics collection
- Efficiently collects, packages, and transfers diagnostic data to Oracle Support
- Reduces round trips between customers and Oracle

Oracle Trace File Analyzer reduces the time required to obtain the correct diagnostic data, which eventually saves your business money.

For more information, see *Oracle Autonomous Health Framework Checks and Diagnostics User's Guide*.

New Attention Log for Efficient Critical Issue Resolution

Diagnosability of database issues is enhanced through a new attention log, as well as classification of information written to database trace files. The new attention log is written in a structured format (XML or JSON) that is much easier to process or interpret and only contains information that requires attention from an administrator. The contents of trace files now contains information that enables much easier classification of trace messages, such as for security and sensitivity.

Enhanced diagnosability features simplify database administration and improve data security.

For more information, see Attention Log

1.2.3 Introduction to AHF Insights

AHF Insights provides a bird's eye view of the entire system with the ability to further drill down for root cause analysis.

> **Note:**
>
> Starting in AHF 23.8, `plotly.js` dependency on CDN has been removed for customers using AHF Insights in restrictive environments.

Previously, results from different AHF components were not available in a single dashboard making it challenging to combine and correlate. To mitigate this, AHF Insights provides a web-based graphical user interface, which does not require a web server to host the web pages, for all diagnostic data collectors and analyzers that are part of AHF Kit.

AHF performs a contextual diagnostic collection for a given period to analyze the performance of database systems. The collection includes diagnostic data from various AHF features such as:

- Configuration
- Environment Topology
- Metrics
- Logs

This diagnostic data collected from the system passes through AHF Insights, which in turn produces an offline report with analysis in the following areas:

- System Configuration
- System State
- Anomalies in the Operating System
- Best Practices Compliance
- System Traces
- Root cause for issues and fixes in some of the anomalous cases

To get started, run the following command:

```
ahf analysis create --type insights
```

Example 1-1   ahf analysis create --type insights

```
[root@node02 ~]# tfactl print status

.-----------------------------------------------------------------------
-------------------------.
| Host   | Status of TFA | PID    | Port | Version    | Build
ID              | Inventory Status |
+-----------------+---------------+--------+------+------------
+----------------------+----------+
| node02 | RUNNING       | 134679 | 5000 | 22.3.0.0.0 |
22300020221031131221 | COMPLETE         |
| node01 | RUNNING       | 128438 | 5000 | 22.3.0.0.0 |
22300020221031131221 | COMPLETE         |
'-----------------+---------------+--------+------+------------
+----------------------+----------'


[root@node02 ~]# ahf analysis create --type insights --last 2h
Starting analysis and collecting data for insights
Collecting data for AHF Insights (This may take a few minutes per node)
AHF Insights report is being generated for the last 2h
From Date : 11/20/2022 01:16:41 UTC - To Date : 11/20/2022 03:17:15 UTC
Report is generated at : /opt/oracle.ahf/data/repository/
collection_Sun_Nov_20_03_16_36_UTC_2022_node_all/cgexa-
ogmn12_insights_2022_11_20_03_18_13.zip
```

1.2.4 Introduction to Oracle Cluster Health Advisor

Oracle Cluster Health Advisor continuously monitors cluster nodes and Oracle RAC databases for performance and availability issue precursors to provide early warning of problems before they become critical.

Oracle Cluster Health Advisor does the following:

- Detects node and database performance problems
- Provides early-warning alerts and corrective action
- Supports on-site calibration to improve sensitivity

In Oracle Database 12c release 2 (12.2.0.1), Oracle Cluster Health Advisor supports the monitoring of two critical subsystems of Oracle Real Application Clusters (Oracle RAC): the database instance and the host system. Oracle Cluster Health Advisor determines and tracks the health status of the monitored system. It periodically samples a wide variety of key measurements from the monitored system.

Over a hundred database and cluster node problems have been modeled, and the specific operating system and Oracle Database metrics that indicate the development or existence of these problems have been identified. This information is used to construct a trained, calibrated model that is based on a normal operational period of the target system.

Oracle Cluster Health Advisor runs an analysis multiple times a minute. Oracle Cluster Health Advisor estimates an expected value of an observed input based on the default model. Oracle Cluster Health Advisor then performs anomaly detection for each input based on the difference between observed and expected values. If sufficient inputs associated with a specific problem are abnormal, then Oracle Cluster Health Advisor raises a warning and generates an immediate targeted diagnosis and corrective action.

Oracle Cluster Health Advisor models are conservative to prevent false warning notifications. However, the default configuration may not be sensitive enough for critical production systems. Therefore, Oracle Cluster Health Advisor provides an onsite model calibration capability to use actual production workload data to form the basis of its default setting and increase the accuracy and sensitivity of node and database models.

You can also use Oracle Cluster Health Advisor to diagnose and triage past problems. Specify the past dates through the command-line interface CHACTL, AHF Insights, or AHF Scope.

1.2.5 Introduction to AHF Scope

AHF Scope is a standalone, interactive, real-time capable front-end to Oracle Cluster Health Advisor (CHA). AHF Scope requires a very small foot-print on the monitored system.

AHF Scope is invoked using the `ahfscope` script available in the `/opt/oracle.ahf/ahfscope/bin/` directory. AHF Scope is designed primarily for cluster or database experts. It is capable of handling large amounts of data efficiently. Its layout and mode of operation is designed for functional efficiency. Most of the operations can be executed using a positional pointer and Hot Keys, or a floating menu available at the cursor position.

If Grid Infrastructure Management Repository (GIMR) is configured, AHF Scope will connect directly to GIMR using a JDBC connection, and read the current data in real-time. AHF Scope can also operate locally with no connection to GIMR using a data archive extracted from GIMR.

Note:

GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c. For more information, see Removing Grid Infrastructure Management Repository.

1.2.6 Introduction to AHF Balance

AHF Balance is a command-line utility that analyzes historical CPU consumption data and Database Resource Manager (DBRM) settings for the set of databases running in a cluster.

It assists in understanding the history of CPU-based noisy neighbor problems and recommends appropriate DBRM settings to minimize the risk of noisy neighbor problems.

1.2.7 Introduction to Cluster Health Monitor

Cluster Health Monitor is a component of Oracle Grid Infrastructure, which continuously monitors and stores Oracle Clusterware and operating system resources metrics.

Enabled by default, Cluster Health Monitor:

- Assists node eviction analysis
- Logs all process data locally
- Enables you to define pinned processes
- Listens to CSS and GIPC events
- Categorizes processes by type
- Supports plug-in collectors such as `traceroute`, `netstat`, `ping`, and so on
- Provides CSV output for ease of analysis

Cluster Health Monitor serves as a data feed for other Oracle Autonomous Health Framework components such as Oracle Cluster Health Advisor.

1.2.8 Introduction to Blocker Resolver

Blocker Resolver is an Oracle Real Application Clusters (Oracle RAC) environment feature that autonomously resolves delays and keeps the resources available.

Enabled by default, Blocker Resolver:

- Reliably detects database delays and deadlocks
- Autonomously resolves database delays and deadlocks
- Logs all detections and resolutions
- Provides SQL interface to configure sensitivity (Normal/High) and trace file sizes

A database delays when a session blocks a chain of one or more sessions. The blocking session holds a resource such as a lock or latch that prevents the blocked sessions from progressing. The chain of sessions has a root or a final blocker session, which blocks all the other sessions in the chain. Blocker Resolver resolves these issues autonomously by detecting and resolving the delays.

2
Get Started

2.1 Supported Platforms

You can use Oracle Autonomous Health Framework with all supported versions of Oracle Database and Oracle Grid Infrastructure.

Run Oracle Autonomous Health Framework on engineered systems such as, Oracle Database Applicance, and Oracle Exadata and Zero Data Loss Recovery Appliance.

Oracle Autonomous Health Framework supports the following operating systems. Use a Java Runtime Edition of version 1.8.

- Linux OEL
- Linux RedHat
- Linux SuSE
- zLinux
- Oracle Solaris SPARC
- Oracle Solaris x86-64
- AIX
- HP-UX
- Microsoft Windows 64-bit
- Microsoft Windows Server 2012 R2 and above

Note:

Only 32-bit platforms are supported for 32-bit EBS environments using the command `orachk compliance -ebs32bit`.

Important:

AHF is not supported on Microsoft Windows 7 and 10.

Oracle Autonomous Health Framework is shipped with Oracle Grid Infrastructure since versions 11.2.0.4 and 12.1.0.2. However, this installation does not include many of the Oracle Database tools. Oracle releases new versions of Oracle Autonomous Health Framework several times a year. These new releases include new features and bug fixes.

Ensure that you get the latest Oracle Autonomous Health Framework with Oracle Database support tools bundle from My Oracle Support note 2550798.1.

Unsupported platforms

AHF has stopped support for the following platforms. You cannot install AHF 23.9.0 or higher on these platforms.

- Solaris Sparc 5.10
- Solaris Intel
- AIX 6.x
- Linux 6 (RHEL6 and OEL6)

The terminal release for Solaris Sparc 5.10, Solaris Intel, and AIX 6.x is AHF 23.6.3 and it is available for download at My Oracle Support note 2550798.1.

The terminal release for Linux 6 (RHEL6 and OEL6) is AHF 23.10.0 and it is available for download at My Oracle Support note 2550798.1. AHF will not provide further release for this platform and customers will not be able to upgrade AHF after 23.10.0.

The terminal release for AIX 7.1 and Solaris 11.3 is 23.8.1 and it is available for download at My Oracle Support note 2550798.1.

Related Topics

- https://support.oracle.com/rs?type=doc&id=2550798.1

2.2 Recommended Browsers

With popular browsers such as Chrome, Firefox, or Safari, you can view both the new and old Oracle Orachk / Oracle Exachk HTML report layouts.

The reports are rendered best in the newest and last 5 prior versions of these browsers:

- Microsoft Internet Explorer (latest, latest minus 5)
- Microsoft Edge (latest, latest minus 5)

- Google Chrome (latest, latest minus 5)
- Mozilla Firefox (latest, latest minus 5)
- Apple Safari (latest, latest minus 5)

2.3 Scope of Oracle Stack Supported

Oracle Autonomous Health Framework performs compliance checks for the entire range of Oracle products from hardware, to Oracle Database, middleware, and applications.

Oracle Autonomous Health Framework proactively scans for top known problems (based on prioritization of reported issues) within an Oracle system.

The scope of Oracle Autonomous Health Framework increases with new releases. The following lists the current products on which you can use Oracle Autonomous Health Framework.

- **Oracle Engineered Systems**
  - Oracle Big Data Appliance
  - Oracle Exadata Database Machine Version 2 and later
  - Zero Data Loss Recovery Appliance
  - Oracle Private Cloud Appliance
- **Oracle Database Appliance**
- **Oracle ASR**
- **Oracle Database**
  - Single-instance Oracle Database
  - Oracle Grid Infrastructure and Oracle RAC
  - Maximum Availability Architecture (MAA) validation
  - Upgrade Readiness validation
  - Oracle GoldenGate
  - Application Continuity
- **Enterprise Manager Cloud Control (12c and 13c)**
  - Management Repository
  - Management Agents
  - Oracle Management Service (OMS), version 12.1.0.1 and later on Linux only
- **Oracle Identity and Access Management**
  - Oracle Identity Manager (11.1.2.2.x and 11.1.2.3.x)
  - Oracle Access Manager (11.1.2.2.x and 11.1.2.3.x)
  - Oracle Unified Directory (11.1.2.2.x and 11.1.2.3.x)
- **Oracle Hardware Systems**
  - Oracle Solaris
  - Oracle Solaris Cluster
  - Oracle Systems configuration for Oracle Middleware and Oracle Applications

  - Oracle ZFS Storage Appliance
  - Oracle Virtual Networking
- **Oracle Siebel**
  - Oracle Siebel verification of the database configuration for stability, best practices, and performance optimization (Siebel 8.1.1.11 connecting to Oracle Database 11.2.0.4.)
- **Oracle PeopleSoft**
  - Oracle PeopleSoft verification of database best practices

Related Topics

- https://support.oracle.com/rs?type=doc&id=1070954.1

2.4 Prerequisites

Review the prerequisites to install and use Oracle Autonomous Health Framework on various supported platforms.

- Compliance Framework (Oracle Orachk and Oracle Exachk) Prerequisites
  Review the list of prerequisites to run Oracle Orachk and Oracle Exachk.
- Oracle Trace File Analyzer Prerequisites
  Review the list of prerequisites to run Oracle Trace File Analyzer.

2.4.1 Compliance Framework (Oracle Orachk and Oracle Exachk) Prerequisites

Review the list of prerequisites to run Oracle Orachk and Oracle Exachk.

- Storage Servers that are Configured to Deny SSH Access
  The following discussion applies to any Oracle engineered system that uses Oracle Exadata storage servers.
- Running Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance
  Review the list of additional prerequisites for running Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance.
- Running Oracle Autonomous Health Framework in Non-English Environments
  Set globalization environment variables to run Oracle Autonomous Health Framework in non-English environments.

2.4.1.1 Storage Servers that are Configured to Deny SSH Access

The following discussion applies to any Oracle engineered system that uses Oracle Exadata storage servers.

Optionally, you can prevent SSH access, also known as **locking** or **locked**. All Oracle Exachk functions involving locked storage servers are run with standard `exacli` commands from the database server upon which Oracle Exachk is launched. To temporarily unlock the storage servers that Oracle Exachk finds locked, provide the user name and credentials that you specified when configuring `exacli` to lock/unlock storage servers.

See Configuring Security for Oracle Exadata System Software in the Exadata System Software User's Guide.

Oracle Exachk does not operate upon the storage server attribute `accessLevelPerm`. If you have set that attribute to `remoteLoginDisabled` before an Oracle Exachk run, then it will remain unchanged during and after the Oracle Exachk run.

Oracle Exachk operates only upon the storage server attribute `accessLevelTemp`. For example, starting with the storage servers locked with `remoteLoginDisabled`:

```
ssh randomceladm01
ssh: connect to host randomceladm01 port 22: Connection refused

ssh randomceladm02
ssh: connect to host randomceladm02 port 22: Connection refused

ssh randomceladm03
ssh: connect to host randomceladm03 port 22: Connection refused

exachk -unlockcells all
Enter exacli user name: celluser
Is EXACLI password same on all Storage Servers?[y/n][y] y
Enter password for EXACLI user celluser to unlock Storage Server
192.168.178.225:
.  .  .  .  .  .  .  .  .  .  .
Storage cell 192.168.178.225 successfully unlocked
Storage cell 192.168.178.226 successfully unlocked
Storage cell 192.168.178.227 successfully unlocked

ssh randomceladm03
Last login: Tue Mar  6 12:32:36 2018 from randomadm01.us.oracle.com

ssh randomceladm02
Last login: Tue Mar  6 12:32:09 2018 from randomadm01.us.oracle.com

ssh randomceladm01
Last login: Tue Mar  6 12:18:57 2018 from randomadm01.us.oracle.com

exacli -c celluser@randomceladm01
Password: ************
exacli celluser@randomceladm01> list cell attributes
accessLevelPerm,accessLevelTemp
remoteLoginDisabled
((accesslevel=remoteLoginEnabled,starttime=2018-03-06T13:49:15-08:00,
endtime=2018-03-06T14:39:15-08:00,duration=50m,reason=Running Exachk))

As can be seen from the example, Oracle EXAchk implements a temporary window
with a default expiration time of 50 minutes, to cover the period that
Oracle EXAchk
may be executing on the storage server.
In normal operation, this temporary window is closed with "-lockcells"
during the exachk cleanup routine.
If exachk is blocked from the cleanup routine, say because of "kill -9",
the temporary window will expire in it's own good time.
```

```
The following example shows the typical Oracle EXAchk execution
sequence starting with the storage servers locked.
You can see by the commands at the end that "remoteLoginDisabled" is
still set and there is no temporary window:

exachk -c X4-2 -profile storage
...
...
Copying plug-ins
. .
Enter exacli user name: celluser
Is EXACLI password same on all Storage Servers?[y/n][y]
Enter password for EXACLI user celluser to unlock Storage Server
192.168.178.225:
.  .  .  .  .  .  .  .  .  .  .  .  .
Node randomcel01 is configured for ssh user equivalency for root user
Node randomcel02 is configured for ssh user equivalency for root user
Node randomcel03 is configured for ssh user equivalency for root user
.  .  .  .  .  .  .  .  .  .  .  .  .
...
...
Starting to run root privileged commands in background on STORAGE
SERVER randomcel01 (192.168.178.225)
Starting to run root privileged commands in background on STORAGE
SERVER randomcel02 (192.168.178.226)
Starting to run root privileged commands in background on STORAGE
SERVER randomcel03 (192.168.178.227)
Collections from STORAGE SERVER:
------------------------------------------------------------
Collecting - Exadata Critical Issue EX10
...
...
Detailed report (html) -  /root/vern_wagman/exachk_122014/production/
lock_doc/exachk_randomclient01_030618_140319/
exachk_randomclient01_030618_140319.html
UPLOAD [if required] - /root/vern_wagman/exachk_122014/production/
lock_doc/exachk_randomclient01_030618_140319.zip

ssh randomceladm01
ssh: connect to host randomceladm01 port 22: Connection refused

exacli -c celluser@randomceladm01
Password: ************
exacli celluser@randomceladm01> list cell attributes
accessLevelPerm,accessLevelTemp
         remoteLoginDisabled
```

2.4.1.2 Running Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance

Review the list of additional prerequisites for running Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance.

- Storage Servers

- InfiniBand Switches

Related Topics

- Compliance Framework (Oracle Orachk and Oracle Exachk) Prerequisites
  Review the list of prerequisites to run Oracle Orachk and Oracle Exachk.

2.4.1.2.1 Storage Servers

On the database, if you configure passwordless SSH equivalency for the user that launched Oracle Autonomous Health Framework to the `root` user on each storage server, then Oracle Autonomous Health Framework uses SSH equivalency credentials to complete the storage server checks.

You can run Oracle Autonomous Health Framework from the Oracle Exadata storage server, if there is no SSH connectivity from the database to the storage server.

To lock and unlock cells, use the `-unlockcells` and `-lockcells` options for Oracle Exadata and Zero Data Loss Recovery Appliance.

```
exachk -unlockcells all | -cells [comma-delimited list of cell names or cell
IPs]
```

```
exachk -lockcells all | -cells [comma-delimited list of cell names or cell
IPs]
```

Once the cells have been unlocked, if they are not locked again within the default timeout of 50 minutes, then they will be automatically locked again. You can adjust the timeout period using the `RAT_CELLUNLOCK_TIMEOUT` environment variable.

For example to change the timeout to 2 hours:

```
export RAT_CELLUNLOCK_TIMEOUT=120m
```

```
exachk -unlockcells all
```

2.4.1.2.2 InfiniBand Switches

On the database, if you configure passwordless SSH equivalency for the user that launched Oracle Autonomous Health Framework to the `nm2user` user on each InfiniBand switch, then Oracle Autonomous Health Framework uses SSH equivalency credentials to complete the InfiniBand switch checks.

If you have not configured passwordless SSH equivalency, then Oracle Autonomous Health Framework prompts you for the `nm2user` user password on each of the InfiniBand switches.

2.4.1.3 Running Oracle Autonomous Health Framework in Non-English Environments

Set globalization environment variables to run Oracle Autonomous Health Framework in non-English environments.

Oracle Autonomous Health Framework supports only English language. However, you can run Oracle Autonomous Health Framework by setting the globalization environment variables.

- To run Oracle Autonomous Health Framework in a non-English environment, set the environment variable `NLS_LANG` to `AMERICAN_AMERICA.[NLS_CHARACTERSET]`.

  For example:

  ```
  export NLS_LANG=AMERICAN_AMERICA.JA16SJISTILDE
  ```

  For more information on setting globalization environment variables, see *Setting Up a Globalization Support Environment* in the *Oracle Database Globalization Support Guide*.

Related Topics

- Oracle Database Globalization Support Guide

2.4.2 Oracle Trace File Analyzer Prerequisites

Review the list of prerequisites to run Oracle Trace File Analyzer.

- Perl Modules
  Review the list of Perl modules used by Oracle Trace File Analyzer.

2.4.2.1 Perl Modules

Review the list of Perl modules used by Oracle Trace File Analyzer.

```
B
Carp
Config
Cwd
Data::Dumper
Date::Calc
Date::Format
Date::Manip
Date::Parse
Encode
English
Exporter
Fcntl
File::Basename
File::Copy
File::Find
File::Path
File::Spec::Functions
```

```
File::Spec
File::Temp
FindBin
Getopt::Long
Getopt::Std
IO::File
IO::Handle
IPC::Open2
IPC::Open2
IPC::Open3
JSON
List::Util
Math::BigInt
Net::Domain
Net::Ping
POSIX
Pod::Usage
Socket
Storable
Sys::Hostname
Term::ANSIColor
Term::ReadLine
Text::ASCIITable
Text::ParseWords
Text::Wrap
Time::Local
Time::Piece
Tokenizer
Win32::Service
Win32
locale
strict
threads::shared
threads
warnings
```

- To find the version number of Perl installed on your system, see 3 quick ways to find out the version number of an installed Perl module from the terminal.
- To check if a module is installed on your system:

  ```
  # perldoc -l Socket
  /usr/lib64/perl5/vendor_perl/Socket.pm
  #
  # perldoc -l Sys::Hostname
  /usr/lib64/perl5/Sys/Hostname.pm
  #
  # perldoc -l XML::Simple
  No documentation found for "XML::Simple".
  #
  ```

- To check the version of a module that is installed on your system:

  ```
  # perldoc -m Socket | grep 'VERSION.*='
  our $VERSION = '2.010';
  ```

```
#
# perldoc -m Sys::Hostname | grep 'VERSION.*='
$VERSION = '1.16';
#
# perldoc -m XML::Simple | grep 'VERSION.*='
No module found for "XML::Simple".
#
```

2.5 Installing, Upgrading, Patching, and Uninstalling Oracle Autonomous Health Framework

Learn to install, upgrade, patch, and use Oracle Autonomous Health Framework on various supported platforms.

- Installing Oracle Autonomous Health Framework
  Learn to install Oracle Autonomous Health Framework on Linux, Unix, and Microsoft Windows operating systems.
- Upgrading Oracle Autonomous Health Framework
  Learn to upgrade Oracle Autonomous Health Framework on Linux, Unix, and Microsoft Windows operating systems.
- Patching Oracle Autonomous Health Framework
  Learn to patch Oracle Autonomous Health Framework automatically or on demand.
- Uninstalling Oracle Autonomous Health Framework
  To uninstall Oracle Autonomous Health Framework, run the `uninstall` command as `root`, or install user.

2.5.1 Installing Oracle Autonomous Health Framework

Learn to install Oracle Autonomous Health Framework on Linux, Unix, and Microsoft Windows operating systems.

> **Note:**
>
> Starting in AHF version 23.7.0, AHF full installers are shipped with Java 11.

- Prerequisites for Configuring Oracle Autonomous Health Framework
  Review the prerequisites to configure Oracle Autonomous Health Framework.
- Installing Oracle Autonomous Health Framework on Linux
  Install Oracle Autonomous Health Framework as `root` to obtain the fullest capabilities. Oracle Autonomous Health Framework has reduced capabilities when you install it as a non-root user.
- Installing AHF on Microsoft Windows
  Install Oracle Trace File Analyzer as a Microsoft Windows service. Run the AHF compliance framework (Oracle Orachk/Oracle Exachk) on-demand.

- Installing AHF on Oracle Big Data Appliance
  Run the `ahf_setup` command to run Oracle Autonomous Health Framework on the Oracle Big Data Appliance.
- Installing AHF on Oracle Exadata Dom0
  To run AHF scheduler on Oracle Exadata dom0, follow these steps:
- Group Permissions for Oracle Exachk Results Directories and Files
- Configure MOS Upload While Installing or Upgrading AHF
  Use the `-setupmos` or `-nosetupmos` command options to configure MOS upload while installing or upgrading AHF.

2.5.1.1 Prerequisites for Configuring Oracle Autonomous Health Framework

Review the prerequisites to configure Oracle Autonomous Health Framework.

- **Minimum disk storage space for AHF Software directory:** at least 3 GB
  AHF Software directory is `ahf_loc` (`ahf_home`) flag value where AHF software is placed, for example, `/opt/oracle.ahf`.
- **Minimum disk storage space for AHF Data directory:** at least 5 GB
  However, it is advisable to set based on the customer environment and requirements. For example, when a cluster has many nodes or many databases running or if the customers want to keep reports/collections for longer period.

  AHF Data directory is `data_dir` (`ahf_data`) flag value where AHF data and collections are generated, for example, `/u01/oracle/grid/oracle.ahf/data` or `/opt/oracle.ahf/data`
- **Minimum disk storage space for /tmp location:** at least 2 GB

2.5.1.2 Installing Oracle Autonomous Health Framework on Linux

Install Oracle Autonomous Health Framework as `root` to obtain the fullest capabilities. Oracle Autonomous Health Framework has reduced capabilities when you install it as a non-root user.

- (Recommended) Installing on Linux or Unix as root User in Daemon Mode
  To obtain the fullest capabilities of Oracle Autonomous Health Framework, install it as `root`.
- Installing on Linux or UNIX as Non-root User in Non-Daemon Mode
  If you are unable to install as `root`, then install Oracle Autonomous Health Framework as the Oracle home owner.
- Running AHF on SELinux Enabled Systems
  To run AHF on SELinux enabled systems, use this procedure.

2.5.1.2.1 (Recommended) Installing on Linux or Unix as root User in Daemon Mode

To obtain the fullest capabilities of Oracle Autonomous Health Framework, install it as `root`.

> **Note:**
>
> Perl version 5.10 or later is required to install Oracle Autonomous Health Framework.

Oracle Autonomous Health Framework maintains Access Control Lists (ACLs) to determine which users are allowed access. By default, the `GRID_HOME` owner and `ORACLE_HOME` owners have access to their respective diagnostics. No other users can perform diagnostic collections.

If Oracle Autonomous Health Framework is already installed, then reinstalling performs an upgrade to the existing location.

To install as `root`:

1. Download the Oracle Autonomous Health Framework zipped file, copy the downloaded file to the required machine, and then unzip the file.
2. To ensure that the environment has been set correctly, enter the following commands:

   ```
   umask
   env | more
   ```

   Verify that the `umask` command displays a value of `22`, `022`, or `0022`.
3. Run the `ahf_setup` command:

   ```
   ahf_setup
   ```

   If you plan to run only Oracle Orachk or Oracle Exachk and do not want to run any Oracle Trace File Analyzer processes, then use the install option of `-extract -notfasetup`.

The installation prompts you to do a local or cluster installation.

Cluster installation requires passwordless SSH user equivalency for `root` to all cluster nodes. If you have not already configured passwordless SSH user equivalency, then the installation optionally sets up passwordless SSH user equivalency and then removes at the end.

If you do not wish to use passwordless SSH, then you install Oracle Autonomous Health Framework on each host using a local installation. Run the `tfactl syncnodes` command to generate and deploy relevant SSL certificates.

Oracle Clusterware does not manage Oracle Autonomous Health Framework because Oracle Autonomous Health Framework must be available if Oracle Clusterware stops working.

The installation configures Oracle Autonomous Health Framework for auto-start. The implementation of auto-start is platform-dependent. Linux uses `init`, or an `init` replacement, such as `upstart` or `systemd` and Microsoft Windows uses a Windows service.

Installing Oracle Autonomous Health Framework as `root` on Linux or Solaris automatically sets up and runs the Oracle Orachk or Oracle Exachk daemon.

The daemon runs a full local Oracle Orachk check once every week at 3 AM, and a partial run of the most impactful checks at 2 AM every day through the `oratier1` or `exatier1` profiles. The daemon automatically purges the `oratier1` or `exatier1` profile run that runs daily, after a week. The daemon also automatically purges the full local run after 2 weeks. You can change the daemon settings after enabling auto start.

To remove auto start:

- `orachk -autostop`
- `exachk -autostop`

To remove all default unmodified schedulers:

- `orachk -autostop unset`
- `exachk -autostop unset`

To auto start, run:

- `orachk -autostart`
- `orachk -autostart`

The installer prompts you to specify one or more email addresses of the recipients who can receive diagnostic notifications. Oracle Autonomous Health Framework notifies the recipients with the results of Oracle Orachk and Oracle Exachk compliance checking, or when Oracle Autonomous Health Framework detects significant faults.

To start and load the default schedulers:

- `orachk -autostart reset`
- `exachk -autostart reset`

Related Topics

- Oracle Autonomous Health Framework Installation Command-Line Options
  Understand the options that you can supply to the Oracle Autonomous Health Framework installer script to customize the installation.
- Securing Access to Diagnostic Collections
  Running `tfactl` commands is restricted to authorized users.
- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

2.5.1.2.2 Installing on Linux or UNIX as Non-root User in Non-Daemon Mode

If you are unable to install as `root`, then install Oracle Autonomous Health Framework as the Oracle home owner.

Note:

- Perl version 5.10 or later is required to install Oracle Autonomous Health Framework.
- You cannot perform cluster-wide installation as a non-root user.

Oracle Autonomous Health Framework has reduced capabilities when you install it as the non-root user in non-daemon mode. Therefore, you cannot complete the following tasks:

- Automate diagnostic collections
- Collect diagnostics from remote hosts
- Collect files that are not readable by the Oracle home owner, for example, `/var/log/messages`, or certain Oracle Grid Infrastructure logs

To install as the Oracle home owner, use the `-ahf_loc` option, and optionally specify the `-notfasetup` option to prevent the running of any Oracle Trace File Analyzer processes.

```
ahf_setup -ahf_loc install_dir [-notfasetup]
```

For more information, run `ahf_setup -h`.

2.5.1.2.3 Running AHF on SELinux Enabled Systems

To run AHF on SELinux enabled systems, use this procedure.

SELinux Modes

- **Disabled**: SElinux is disabled.
- **Permissive**: SELinux prints warnings instead of enforcing.
- **Enforcing**: SELinux security policy is enforced.

You can enable or disable SELinux. When enabled, SELinux can run in either **enforcing** or **permissive** modes. To check the status of SELinux, run the `getenforce` or `sestatus` commands. The `getenforce` command returns **Enforcing**, **Permissive**, or **Disabled**.

```
/usr/sbin/getenforce
Permissive
```

The `sestatus` command returns the SELinux status and the SELinux policy being used:

```
/usr/sbin/sestatus
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: permissive
```

```
Mode from config file: permissive
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 31
```

Installing AHF in Permissive or Enforcing Mode

AHF installer loads the policy and sets relevant contexts.

Installing AHF in Disabled Mode

AHF is installed successfully. However, later if you switch the mode to **Permissive** or **Enforcing**, then SELinux starts blocking the AHF processes.

To run AHF, load the SELinux policy:

```
ahfctl loadpolicy
Checking if policy exists
Please wait while the policy is being loaded, it might take couple of
minutes.
Successfully loaded SELinux policy
Restarting TFA...
```

To check if the policy is loaded successfully, run the following command:

```
/usr/sbin/semodule -l | grep inittfa-policy
```

To unload the SELinux policy:

```
ahfctl unloadpolicy
Please wait while the policy is being removed, it might take couple of
minutes.
Successfully removed Contexts and Policy
```

2.5.1.3 Installing AHF on Microsoft Windows

Install Oracle Trace File Analyzer as a Microsoft Windows service. Run the AHF compliance framework (Oracle Orachk/Oracle Exachk) on-demand.

> **Note:**
>
> You cannot install Oracle Autonomous Health Framework into a directory if there is a space in the name of the directory, for example, `Program Files`.
>
> Strawberry Perl for Windows version 5.30 or later (OR) Perl 5 version 28 binaries located in Grid home, and .NET Framework version 4.0.30319 or later

> **Note:**
>
> AHF Notification Email and MOS functionalities are not supported on Microsoft Windows systems. AHF will not prompt you with the following messages while installing on Windows systems.
>
> ```
> Do you want to add AHF Notification Email IDs ? [Y]|N :
> Do you want AHF to store your My Oracle Support Credentials for 
> Automatic
> Upload ? Y|[N] :
> ```

1. Copy the downloaded zip file to a temporary location on a required machine, and then unzip it.
2. Open a command prompt as administrator, and then run the installer script by specifying a Perl home and the location where you want to install Oracle Autonomous Health Framework, for example:

   ```
   installahf.bat -perlhome D:\oracle\product\12.2.0\dbhome_1\perl -
   ahf_loc c:\AHF
   ```

   You can also run `installahf.bat -perlhome D:\oracle\product\12.2.0\dbhome_1\perl` and provide AHF location during installation when the installer prompts.
3. To install AHF on Oracle Grid Infrastructure:

   ```
   installahf.bat -crshome crshome_path
   ```

For clusterwide AHF setup, perform a local installation on each host, and then run the `tfactl syncnodes` command to generate and deploy relevant SSL certificates.

Related Topics

- Determine which .NET Framework versions are installed

2.5.1.4 Installing AHF on Oracle Big Data Appliance

Run the `ahf_setup` command to run Oracle Autonomous Health Framework on the Oracle Big Data Appliance.

1. Download the Oracle Autonomous Health Framework zipped file to a directory on the Oracle Big Data Appliance, as `root` user.
2. Run the `ahf_setup` command and you can optionally specify the `-extract` option.

   ```
   ahf_setup -ahf_loc install_dir
   ```

   For more information, run `ahf_setup -help`.

2.5.1.5 Installing AHF on Oracle Exadata Dom0

To run AHF scheduler on Oracle Exadata dom0, follow these steps:

- **Standalone:** Extracts only the AHF bits.
- **Typical:** Performs full install including configuring scheduling for important features like compliance checking.

AHF in Standalone (default) Mode on Exadata dom0

To install AHF in standalone (default) mode on dom0:

```
# ./ahf_setup

AHF Installer for Platform Linux Architecture x86_64

AHF Installation Log : /tmp/ahf_install_242000_45942_2024_02_27-22_19_10.log

Starting Autonomous Health Framework (AHF) Installation

AHF Version: 24.2.0 Build Date: 202402262228

Default AHF Location : /opt/oracle.ahf

Do you want to install AHF at [/opt/oracle.ahf] ? [Y]|N :

AHF Location : /opt/oracle.ahf

AHF Data Directory : /EXAVMIMAGES/oracle.ahf/data

Extracting AHF to /opt/oracle.ahf

Setting up AHF CLI and SDK

AHF is deployed at /opt/oracle.ahf

EXAchk is available at /opt/oracle.ahf/bin/exachk

AHF binaries are available in /opt/oracle.ahf/bin

Do you want to start TFA and EXAchk schedulers Y|[N] :

AHF is successfully Installed

Moving /tmp/ahf_install_242000_45942_2024_02_27-22_19_10.log to /EXAVMIMAGES/
oracle.ahf/data/scam02db01/diag/ahf/
```

Convert AHF Standalone (default) Installation to Typical Installation

To convert AHF Standalone (default) installation to Typical installation:

```
# ./ahf_setup -upgradetotypical -silent
```

```
AHF Installer for Platform Linux Architecture x86_64

AHF Installation Log : /tmp/
ahf_install_242000_123646_2024_02_27-22_50_39.log

Starting Autonomous Health Framework (AHF) Installation

AHF Version: 24.2.0 Build Date: 202402262228

AHF Location : /opt/oracle.ahf

Installed AHF Version: 24.1.1 Build Date: 202402210742

AHF Data Directory : /EXAVMIMAGES/oracle.ahf/data

Extracting AHF to /opt/oracle.ahf

Setting up AHF CLI and SDK

AHF is deployed at /opt/oracle.ahf

EXAchk is available at /opt/oracle.ahf/bin/exachk

AHF binaries are available in /opt/oracle.ahf/bin

Configuring TFA Services

Discovering Nodes and Oracle Resources

Successfully generated certificates.

Starting TFA Services
Created symlink from /etc/systemd/system/multi-user.target.wants/
oracle-tfa.service to /etc/systemd/system/oracle-tfa.service.
Created symlink from /etc/systemd/system/graphical.target.wants/oracle-
tfa.service to /etc/systemd/system/oracle-tfa.service.

.-----------------------------------------------------------------------
-----------.
| Host       | Status of TFA | PID    | Port | Version    | Build
ID              |
+------------+---------------+--------+------+------------
+------------------------+
| scam02db01 | RUNNING       | 143538 | 5000 | 24.2.0.0.0 |
24020002024022622853 |
'------------+---------------+--------+------+------------
+------------------------'

Running TFA Inventory...

Adding default users to TFA Access list...

.-----------------------------------------------------------------.
|                  Summary of AHF Configuration                  |
+-----------------+-----------------------------------------------+
| Parameter       | Value                                        |
+-----------------+----------------------------------------------+
| AHF Location    | /opt/oracle.ahf                              |
| TFA Location    | /opt/oracle.ahf/tfa                          |
| Exachk Location | /opt/oracle.ahf/exachk                       |
| Data Directory  | /EXAVMIMAGES/oracle.ahf/data                 |
| Repository      | /EXAVMIMAGES/oracle.ahf/data/repository      |
| Diag Directory  | /EXAVMIMAGES/oracle.ahf/data/scam02db01/diag |
'-----------------+----------------------------------------------'

Starting EXAchk Scheduler from AHF

AHF is successfully Installed

Moving /tmp/ahf_install_242000_123646_2024_02_27-22_50_39.log to /
EXAVMIMAGES/oracle.ahf/data/scam02db01/diag/ahf/
```

The `-silent` option is used to avoid user prompt.

AHF is upgraded from Standalone to Typical and the Standalone data directory `/opt` is moved to `/EXAVMIMAGES`.

AHF Scheduler on Local Exadata dom0 - Install Locally and Synchronize at the End

To run AHF scheduler on Exadata dom0:

```
# ./ahf_setup -scheduler

AHF Installer for Platform Linux Architecture x86_64

AHF Installation Log : /tmp/ahf_install_242000_240604_2024_02_27-22_32_31.log

Starting Autonomous Health Framework (AHF) Installation

AHF Version: 24.2.0 Build Date: 202402262228

AHF Location : /opt/oracle.ahf

AHF Data Directory : /EXAVMIMAGES/oracle.ahf/data

Do you want to add AHF Notification Email IDs ? [Y]|N : N

Extracting AHF to /opt/oracle.ahf

Setting up AHF CLI and SDK

Configuring TFA Services

Discovering Nodes and Oracle Resources

Successfully generated certificates.

Starting TFA Services

.----------------------------------------------------------------------------
```

```
-----.
| Host       | Status of TFA | PID    | Port | Version    | Build
ID               |
+------------+---------------+--------+------+------------
+------------------------+
| scam02db01 | RUNNING       | 254226 | 5000 | 24.2.0.0.0 |
240200020240226222853 |
'------------+---------------+--------+------+------------
+------------------------'

Running TFA Inventory...

Adding default users to TFA Access list...

.----------------------------------------------------------------.
|                  Summary of AHF Configuration                  |
+-----------------+----------------------------------------------+
| Parameter       | Value                                        |
+-----------------+----------------------------------------------+
| AHF Location    | /opt/oracle.ahf                              |
| TFA Location    | /opt/oracle.ahf/tfa                          |
| Exachk Location | /opt/oracle.ahf/exachk                       |
| Data Directory  | /EXAVMIMAGES/oracle.ahf/data                 |
| Repository      | /EXAVMIMAGES/oracle.ahf/data/repository      |
| Diag Directory  | /EXAVMIMAGES/oracle.ahf/data/scam02db01/diag |
'-----------------+----------------------------------------------'

Starting EXAchk Scheduler from AHF

AHF binaries are available in /opt/oracle.ahf/bin

AHF is successfully Installed

Do you want AHF to store your My Oracle Support Credentials for
Automatic Upload ? Y|[N] :

Moving /tmp/ahf_install_242000_240604_2024_02_27-22_32_31.log to /
EXAVMIMAGES/oracle.ahf/data/scam02db01/diag/ahf/
```

This will install AHF scheduler only on local dom0. After installing AHF scheduler on all the dom0s, run the `tfactl syncnodes -nodes` *comma-delimited-list-of-remote-dom0s* command on any one of the nodes to synchronize Oracle Trace File Analyzer.

```
# tfactl syncnodes -nodes node2
Current Node List in TFA :
1. node1
Node List in Cluster :
1. node2
Node List to sync TFA Certificates :
     1  node2
Syncing TFA Certificates on node2 :
TFA_HOME on node2 : /opt/oracle.ahf/tfa
DATA_DIR on node2 : /opt/oracle.ahf/data/node2/tfa
Shutting down TFA on node2...
```

```
Copying TFA Certificates to node2...
Copying SSL Properties to node2...
Sleeping for 5 seconds...
Starting TFA on node2...
Trying to add node2 to TFA...
.----------------------------------------------------------------------------
--------------------------.
| Host           | Status of TFA | PID    | Port | Version    | Build
ID             | Inventory Status |
+---------------+---------------+--------+------+------------
+----------------------+------------------+
| node1          | RUNNING       | 148216 | 5000 | 22.1.0.0.0 |
22100020220411155753 | COMPLETE          |
| node2          | RUNNING       |  95897 | 5000 | 22.1.0.0.0 |
22100020220405120331 | COMPLETE          |
'---------------+---------------+--------+------+------------
+----------------------+------------------'
```

AHF Scheduler on all Exadata dom0 - Recommended

To run AHF scheduler on all Exadata dom0 and synchronize the nodes: `ahf_setup -scheduler -nodes` *`comma-delimited-list-of-remote-dom0s`*.

```
# ahf_setup -scheduler -nodes node2
AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/ahf_install_221000_239748_2022_04_05-05_08_14.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 22.1.0 Build Date: 202204051203
Default AHF Location : /opt/oracle.ahf
Do you want to install AHF at [/opt/oracle.ahf] ? [Y]|N :
AHF Location : /opt/oracle.ahf
AHF Data Directory stores diagnostic collections and metadata.
AHF Data Directory requires at least 5GB (Recommended 10GB) of free space.
Please Enter AHF Data Directory : /opt/oracle.ahf
AHF Data Directory : /opt/oracle.ahf/data
Do you want to add AHF Notification Email IDs ? [Y]|N : n
AHF will also be installed/upgraded on these Cluster Nodes :
1. node2
The AHF Location and AHF Data Directory must exist on the above nodes
AHF Location : /opt/oracle.ahf
AHF Data Directory : /opt/oracle.ahf/data
Extracting AHF to /opt/oracle.ahf
Configuring TFA Services
Discovering Nodes and Oracle Resources
Successfully generated certificates.
Starting TFA Services
Created symlink from /etc/systemd/system/multi-user.target.wants/oracle-
tfa.service to /etc/systemd/system/oracle-tfa.service.
Created symlink from /etc/systemd/system/graphical.target.wants/oracle-
tfa.service to /etc/systemd/system/oracle-tfa.service.

.----------------------------------------------------------------------------
-------.
| Host           | Status of TFA | PID    | Port | Version    | Build
ID             |
+---------------+---------------+--------+------+------------
+----------------------+
| node1          | RUNNING       | 261388 | 5000 | 22.1.0.0.0 |
22100020220405120331 |
'---------------+---------------+--------+------+------------
+----------------------'

Running TFA Inventory...
Adding default users to TFA Access list...

.------------------------------------------------------------.
|                Summary of AHF Configuration                |
+-----------------+------------------------------------------+
| Parameter       | Value                                    |
+-----------------+------------------------------------------+
| AHF Location    | /opt/oracle.ahf                          |
| TFA Location    | /opt/oracle.ahf/tfa                      |
| Exachk Location | /opt/oracle.ahf/exachk                   |
| Data Directory  | /opt/oracle.ahf/data                     |
| Repository      | /opt/oracle.ahf/data/repository          |
| Diag Directory  | /opt/oracle.ahf/data/node1/diag     |
'-----------------+------------------------------------------'

Starting exachk scheduler from AHF ...
AHF install completed on node1
Installing AHF on Remote Nodes :
AHF will be installed on node2, Please wait.
Installing AHF on node2 :
[node2] Copying AHF Installer
[node1] Running AHF Installer
[node2] Syncing TFA Certificates
[node2] Restarting TFA

.-----------------------------------------------------------------------
-------------------------------.
| Host          | Status of TFA | PID    | Port | Version    | Build
ID             | Inventory Status |
+---------------+---------------+--------+------+------------
+----------------------+------------------+
| node1          | RUNNING       | 261388 | 5000 | 22.1.0.0.0 |
22100020220405120331 | COMPLETE         |
| node2          | RUNNING       | 113878 | 5000 | 22.1.0.0.0 |
22100020220405120331 | COMPLETE         |
'---------------+---------------+--------+------+------------
+----------------------+------------------'

AHF binaries are available in /opt/oracle.ahf/bin
AHF is successfully installed
Do you want AHF to store your My Oracle Support Credentials for
Automatic Upload ? Y|[N] : n
Moving /tmp/ahf_install_221000_239748_2022_04_05-05_08_14.log to /opt/
oracle.ahf/data/node1/diag/ahf/
```

For more information about managing CPU and memory resources on dom0, see *Running AHFCTL Commands to Limit CPU and Memory Usage*.

Related Topics

- Running AHFCTL Commands to Limit CPU and Memory Usage
  You need root access to ahfctl, or sudo access to run getresourcelimit, setresourcelimit, unsetresourcelimit commands.

2.5.1.6 Group Permissions for Oracle Exachk Results Directories and Files

> **Note:**
>
> Not applicable to Microsoft Windows.

1. During AHF installation, the installer runs the $ORACLE_HOME/bin/osdbagrp command to get the default operating system group and grants 750 permission to the default operating system group till the user_root directory.

   ```
   # cat install.properties | grep EXACHK_DATA_DIR
   EXACHK_DATA_DIR=/opt/oracle.ahf/data/adcs/exachk


   # ls -l /opt/oracle.ahf/data/adcs/exachk | grep user_root
   drwxr-x--t 4 root dba  4096 May 18 14:34 user_root
   ```

2. Each time either orachk or exachk is run,

   - The default operating system group is set with permission 750 on the output directory and the directories within it.

     ```
     # ls -l /opt/oracle.ahf/data/adcs/exachk/user_root | grep output
     drwxr-x--t 5 root dba  4096 May 22 08:27 output
     ```

   - The default operating system group is set with permission 750 on the upload directory.

     ```
     # ls -lrt /opt/oracle.ahf/data/adcs/exachk/user_root/output/
     <collection_dir> | grep upload
     drwxr-x--- 2 root dba  4096 May 23 06:32 upload
     ```

   - The default operating system group is set with permission 640 on all of the JSON files within the upload direcoty.

     ```
     # ls -lrt /opt/oracle.ahf/data/adcs/exachk/user_root/output/
     exachk_adcs_rac19c_052322_063119/upload | grep .*.json
     -rw-r----- 1 root dba  3068 May 23 06:32 exachk_summary.json
     -rw-r----- 1 root dba  2463 May 23 06:32
     adcs_exachk_valid_results.json
     -rw-r----- 1 root dba  5675 May 23 06:32 check_env.json
     ```

3. Use the `ahfctl setosgroup` command to change the default operating system group any time you want. This group change will reflect on the `user_root` directory. Similarly, the respective runs will have the new group.

   ```
   ahfctl setosgroup [-h] [-group GROUP]
   ```

   For example, to set the default operating system group to *dba*, run the `ahfctl setosgroup -group` *`dba`* command.
4. Use the `ahfctl getosgroup` command to get the default operating system group configured.

   ```
   $ ahfctl getosgroup
   os_group: dba
   ```

2.5.1.7 Configure MOS Upload While Installing or Upgrading AHF

Use the `-setupmos` or `-nosetupmos` command options to configure MOS upload while installing or upgrading AHF.

> **Note:**
>
> If you have already configured MOS upload on the cluster nodes, then you will not be prompted to enter MOS upload configuration details.

Installing AHF without using the -setupmos or -nosetupmos command options:

Local: `./ahf_setup -local`

Cluster-wide: `./ahf_setup`

You will be prompted to confirm if you want to configure MOS upload. If you enter `Y` to confirm configuration, then you will be prompted to enter MOS configuration details, name, user, password, and URL. After successful AHF installation, run the `ahfctl getupload` command to validate MOS upload configuration.

If you install AHF cluster-wide and configure MOS upload, then the MOS upload configuration will automatically be synchronized to other nodes in the cluster.

Installing AHF using the -setupmos command option:

Local: `./ahf_setup -local -setupmos`

Cluster-wide: `./ahf_setup -setupmos`

You will be prompted to enter MOS configuration details, name, user, password, and URL. After successful AHF installation, run the `ahfctl getupload` command to validate MOS upload configuration.

If you install AHF cluster-wide and configure MOS upload, then the MOS upload configuration will automatically be synchronized to other nodes in the cluster.

Installing AHF using the -nosetupmos command option:

Local: `./ahf_setup -local -nosetupmos`

Cluster-wide: `../ahf_setup -nosetupmos`

You will not be prompted to enter MOS upload configuration details.

Upgrading AHF without using the -setupmos or -nosetupmos command options:

Local: `./ahf_setup -local`

Cluster-wide: `./ahf_setup`

You will be prompted to confirm if you want to configure MOS upload. If you enter `Y` to confirm configuration, then you will be prompted to enter MOS configuration details, name, user, password, and URL. After successful AHF installation, run the `ahfctl getupload` command to validate MOS upload configuration.

If you upgrade AHF cluster-wide and configure MOS upload, then the MOS upload configuration will automatically be synchronized to other nodes in the cluster.

2.5.2 Upgrading Oracle Autonomous Health Framework

Learn to upgrade Oracle Autonomous Health Framework on Linux, Unix, and Microsoft Windows operating systems.

> **Note:**
>
> Starting in AHF version 23.7.0, AHF full installers are shipped with Java 11.

- Maintaining Oracle Autonomous Health Framework to the Latest Version
  Oracle releases a new version of Oracle Autonomous Health Framework every month.
- Automatically Upgrading Oracle Autonomous Health Framework to the Latest Version
  AHF Automatic Upgrade enables you to upgrade AHF on the fly without manually downloading `ahf_setup` and upgrading it.
- Upgrading AHF on Local File System, ACFS, and NFS
  You can upgrade AHF on local file system, Oracle Advanced Cluster File System (Oracle ACFS), and Network File System (NFS).

2.5.2.1 Maintaining Oracle Autonomous Health Framework to the Latest Version

Oracle releases a new version of Oracle Autonomous Health Framework every month.

Applying standard Release Update Revisions (RURs) automatically updates Oracle Autonomous Health Framework. However, the Release Update Revisions (RURs) do not contain the rest of the Oracle Database support tools bundle updates. Download the latest version of Oracle Autonomous Health Framework with Oracle Database support tools bundle from My Oracle Support note 2550798.1.

Upgrading is similar to first-time installation. As `root`, use the `ahf_setup` script. If Oracle Autonomous Health Framework is already installed, then the installer updates the existing installation. When already installed, a cluster upgrade does not need SSH. The cluster upgrade uses the existing daemon secure socket communication between hosts.

```
$ ahf_setup
```

Related Topics

- https://support.oracle.com/rs?type=doc&id=2550798.1

2.5.2.2 Automatically Upgrading Oracle Autonomous Health Framework to the Latest Version

AHF Automatic Upgrade enables you to upgrade AHF on the fly without manually downloading `ahf_setup` and upgrading it.

> **Note:**
>
> You need AHF installed user privileges to run the upgrade commands.

Autoupgrade Support Matrix

Autoupgrade is supported on:

- Linux
- Solaris
- AIX

> **Note:**
>
> - `openssl` is needed for all platforms to support `autoupgrade`. If `openssl` is not present, then `autoupgrade` exits gracefully.
> - If you are not using the default port (443), then you must configure a custom port using the ahfctl setupload command to upgrade AHF successfully.

Autoupgrade is NOT supported on:

- HP-UX
- Microsoft Windows
- Standalone (Extract) installations of AHF (except Exadata dom0)

Autoupgrade of AHF by non-root user is supported only if the existing installation was done by the same user and the installation type is typical (full). For example, if user "X" has installed AHF, then autoupgrade cannot be performed by user "Y".

Upgrade AHF Automatically:

Oracle Trace File Analyzer scheduler automatically upgrades AHF if it finds a new version of AHF either at Software stage location or at Rest Endpoints (Object Store).

Oracle Trace File Analyzer scheduler is scheduled to run on a weekly time interval to check if a new version of AHF is present at AHF Software stage or at Rest Endpoints (Object Store). If a new version of AHF is found, then Oracle Trace File Analyzer scheduler will automatically upgrade AHF to the latest version without changing any of the saved configurations.

Upgrade AHF with `upgrade` option:

With this option, you can upgrade AHF irrespective of number of old days. If a new version of AHF is present either at Software stage location or at Rest Endpoints (Object Store), then AHF will be upgraded. If a new version of AHF is not found at these two places, then download AHF from MOS to Software stage, and then upgrade.

```
ahfctl upgrade
```

Set the following attributes in the `ahf.properties` file using command-line options:

```
ahfctl setupgrade -autoupgrade <on/off> -swstage path
```

To disable autoupgrade:

```
ahfctl setupgrade -autoupgrade off
```

Or

```
ahfctl unsetupgrade -autoupgrade
```

To unset autoupgrade parameters:

```
ahfctl unsetupgrade
[-all]
[-swstage]
[-autoupgrade]
[-servicename]
[-frequency]
```

To get autoupgrade configurations parameters:

```
ahfctl getupgrade -all
```

Note:

To get best results out of autoupgrade, run the latest AHF version.

Example 2-1 Set autoupgrade parameters with valid inputs

```
ahfctl setupgrade -swstage /scratch/ahf_stage -autoupgrade on -frequency 21
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
```

Example 2-2 Set all autoupgrade parameters with valid inputs

```
ahfctl setupgrade -all
Enter autoupgrade flag <on/off> : on
Enter software stage location : /scratch/ahf_stage
Enter auto upgrade frequency : 30
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
```

Example 2-3 Turn off autoupgrade

Oracle Trace File Analyzer scheduler will not run automatic upgrade.

```
ahfctl setupgrade -autoupgrade off
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
```

Example 2-4 Print upgrade entries

```
ahfctl getupgrade -all
autoupgrade : off
autoupgrade.swstage : /scratch/ahf_stage
autoupgrade.frequency : 30
autoupgrade.servicename : [not set]
```

Example 2-5 Unset all upgrade parameters

```
ahfctl unsetupgrade -all
AHF upgrade parameters successfully removed
Successfully synced AHF configuration
```

Example 2-6 Unset a single parameter

```
ahfctl unsetupgrade -swstage
Software stage location successfully removed
Successfully synced AHF configuration
```

Example 2-7 Invalid Frequency

```
ahfctl setupgrade -frequency 0
Invalid autoupgrade frequency. Use frequency between 1 and 30
```

Example 2-8 AHF is older than 180 days

```
ahfctl getupload
Autonomous Health Framework is older than 180 days. please use "ahfctl
upgrade" to upgrade to latest version of AHF
continue running original command ...
ahfctl upgrade
Starting download of Autonomous Health Framework from: https://
updates.oracle.com/Orion/Services/download/AHF-LINUX_v20.2.3.zip?
```

```
aru=23858854&patch_file=AHF-LINUX_v20.2.3.zip
...
Upgrading Autonomous Health Framework
...
```

Example 2-9   AHF is older than 365 days

```
ahfctl getupload
Autonomous Health Framework is older than 360 days. please use "ahfctl
upgrade" to latest version of AHF
ahfctl upgrade
Starting download of Autonomous Health Framework from: https://
updates.oracle.com/Orion/Services/download/AHF-LINUX_v20.2.3.zip?
aru=23858854&patch_file=AHF-LINUX_v20.2.3.zip
...
Upgrading Autonomous Health Framework
...
```

Example 2-10   New version of AHF is available at software stage location

```
ahfctl upgrade
AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/ahf_install_211000_31931_2021_03_29-06_54_58.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 21.1.0 Build Date: 202103290252
AHF is already installed at /opt/oracle.ahf
Installed AHF Version: 21.1.0 Build Date: 202103290200
Upgrading /opt/oracle.ahf
Shutting down AHF Services
Shutting down TFA
. . . . .
. . .
Successfully shutdown TFA..
Starting AHF Services
Starting TFA..
Waiting up to 100 seconds for TFA to be started..
. . . . .
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands
No new directories were added to TFA
INFO: Starting exachk scheduler in background. Details for the process can
be found at /u01/app/grid/oracle.ahf/data/busm01client01/diag/exachk/
compliance_start_290321_065650.log
AHF is sucessfully upgraded to latest version
.----------------------------------------------------------------------.
| Host | TFA Version | TFA Build ID | Upgrade Status |
+----------------+-------------+----------------------+-----------------+
| node01      | 21.1.0.0.0 | 21100020210329025257 | UPGRADED |
| node02      | 21.1.0.0.0 | 21100020210329020041 | UPGRADED |
'----------------+-------------+----------------------+-----------------'
Moving /tmp/ahf_install_211000_31931_2021_03_29-06_54_58.log to /u01/app/
grid/oracle.ahf/data/busm01client01/diag/ahf/
```

```
Please upgrade AHF on the below mentioned nodes as well using ahfctl
upgrade
node02
```

Example 2-11 Set REST endpoints using setupload command

```
ahfctl setupload -name ahf_upgrade_loc -type https -url 'https://IP
Address/rest/tfa-processor/download?
osName=LINUX&ahfVersion=%2720.2%27'
-https_token "X-TFA-Authorization: <>"
-header Content-Type:application/json
```

> **Note:**
>
> The name of config must always be ahf_upgrade_loc. This name indicates that the config is for AHF download.

You can ovewrite `ahf_upgrade_loc` using `ahfctl setupgrade -autoupgrade_servicename` *`new name`*

At rest endpoints, AHF downloads the AHF installer zip if newer version is available.

Example 2-12 Set REST endpoints with a custom port using setupload command

```
ahfctl setupload -name ahf_upgrade_loc -type https -url 'https://IP
Address/rest/tfa-processor/download?
osName=LINUX&ahfVersion=%2720.2%27'
-https_token "X-TFA-Authorization: <>"
-header Content-Type:application/json -port <port number>
```

Example 2-13 Set REST endpoints (Object Store's) using setupload command

```
ahfctl setupload
-name ahf_upgrade_loc
-type https
-user testuser
-url https://host.domain/v1/id5igemtjzlt/tfa_bucket -password
```

At Object store, you can keep either `ahf_setup` or zip. First, AHF tries to download `ahf_setup`. If `ahf_setup` is not available, then AHF searches for AHF installer zip.

1. Configure object storage endpoint:

   ```
   ahfctl setupload -name upload_end_point -type https
   Enter upload_end_point.https.user: john.doe@acme.com
   Enter upload_end_point.https.password:
   Enter upload_end_point.https.url: https://
   swiftobjectstorage.acme.com/v1/dbaasimage/CAIPING
   Successfully synced AHF configuration
   ```

2. Configure setupgrade with the name of your upload configuration:

   ```
   ahfctl setupgrade -servicename upload_end_point
   Successfully synced AHF configuration
   AHF autoupgrade parameters successfully updated
   ```

3. Run the `ahfctl upgrade` command:

   ```
   ahfctl upgrade
   Upload configuration check for: upload_end_point.
   Parameters are configured correctly to upload.

   AHF-LINUX_v21.1.0.zip successfully downloaded at /opt/oracle.ahf
   /opt/oracle.ahf/AHF-LINUX_v21.1.0.zip successfully extracted at /opt/
   oracle.ahf

   AHF software signature has been validated successfully
   ```

Example 2-14 Set mos upload configuration

```
ahfctl setupload -name mosconf1 -type https
Enter mosconf1.https.user : john.doe@acme.com
Enter mosconf1.https.password :
Enter mosconf1.https.url : https://transport.oracle.com/upload/issue
Successfully synced AHF configuration
Upload configuration set for: mosconf1
type: https
mosconf1.https.user: john.doe@acme.com
mosconf1.https.password: ******
mosconf1.https.url: https://transport.oracle.com/upload/issue
Service upload parameters successfully stored.
AHF will continue to upload the collections to the Service until unset using
tfactl unsetserviceupload [-all]
```

Related Topics

- ahfctl setupgrade
  Use the `ahfctl setupgrade` command to set upgrade parameters.
- ahfctl unsetupgrade
  Use the `ahfctl unsetupgrade` command to unset upgrade parameters.
- ahfctl getupgrade
  Use the `ahfctl getupgrade` command to fetch upgrade config from the `ahf.properties` file.
- ahfctl upgrade
  Use the `ahfctl upgrade` command to upgrade AHF to a new version.
- ahfctl setupload
  Use the `ahfctl setupload` command to set upload parameters.

2.5.2.3 Upgrading AHF on Local File System, ACFS, and NFS

You can upgrade AHF on local file system, Oracle Advanced Cluster File System (Oracle ACFS), and Network File System (NFS).

Local File System

If the stage location is a local file system and if the AHF installer zip file exists in the stage location, then after upgrading, the installer removes the AHF installer zip file and all the extracted items from the stage location.

1. Configure the auto upgrade parameters.

```
ahfctl setupgrade -all

Enter autoupgrade flag <on/off> : on
Enter software stage location : /opt/local
Enter auto upgrade frequency : 30
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
refreshConfig() completed successfully.
```

2. Check if the AHF installer zip file exists in the stage location.

```
ls /opt/local
AHF-LINUX_v22.1.0.zip
```

> **Note:**
>
> Oracle Trace File Analyzer scheduler calls `ahfctl upgrade -nomos` at a given frequency, in this example, auto-upgrade will happen every 30 days at 3 AM. You can also initiate automatic upgrade from the command-line using the `ahfctl upgrade` command.

3. Run the upgrade command.

```
ahfctl upgrade
AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/
ahf_install_221000_139332_2022_03_09-02_09_42.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 22.1.0 Build Date: 202203081742
AHF is already installed at /opt/oracle.ahf
Installed AHF Version: 22.1.0 Build Date: 202203081714
Upgrading /opt/oracle.ahf
Shutting down AHF Services
Nothing to do !
Shutting down TFA
Removed symlink /etc/systemd/system/multi-user.target.wants/oracle-
tfa.service.
Removed symlink /etc/systemd/system/graphical.target.wants/oracle-
tfa.service.
```

```
Successfully shutdown TFA..
Starting AHF Services
Starting TFA..
Waiting up to 100 seconds for TFA to be started..
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands
No new directories were added to TFA
Directory /u01/app/grid/crsdata/scao05adm07/trace/chad was already added
to TFA Directories.
INFO: Starting exachk scheduler in background. Details for the process
can be found at /u01/app/grid/oracle.ahf/data/scao05adm07/diag/exachk/
compliance_start_090322_021151.log
AHF is successfully upgraded to latest version
.--------------------------------------------------------------------.
| Host        | TFA Version | TFA Build ID         | Upgrade Status |
+-------------+-------------+----------------------+----------------+
| scao05adm07 |  22.1.0.0.0 | 22100020220308174218 | UPGRADED       |
| scao05adm08 |  22.1.0.0.0 | 22100020220308171448 | UPGRADED       |
'-------------+-------------+----------------------+----------------'
Moving /tmp/ahf_install_221000_139332_2022_03_09-02_09_42.log to /u01/app/
grid/oracle.ahf/data/scao05adm07/diag/ahf/
Please upgrade AHF on the below mentioned nodes as well using ahfctl
upgrade
scao05adm08
```

4. Validate if AHF installer zip and the extracted files are removed from the stage location.

```
ls -lart /opt/local
drwxr-xr-x   2 root     root            2 Mar  9 02:32 .
drwxr-xr-x  25 root     sys            28 Mar  9 02:32 ..
```

Oracle Advanced Cluster File System (Oracle ACFS)

If the stage location is ACFS and if the AHF installer zip file exists in the stage location, then after upgrading, the installer removes the AHF installer zip file and retains all the extracted binaries in the stage location so that the other nodes can consume them.

1. Configure the auto upgrade parameters.

```
ahfctl setupgrade -all
Enter autoupgrade flag <on/off> : on
Enter software stage location : /acfs01
Enter auto upgrade frequency : 30
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
refreshConfig() completed successfully.
```

2. Check if the AHF installer zip file exists in the stage location.

```
ls -lart /acfs01
total 387862
-rw-r--r--+  1 root root       1520 Apr 30  2020 README.txt
-rw-r--r--+  1 root root        625 Nov  1 15:15 oracle-tfa.pub
```

```
-rw-r--r--+  1 root root        384 Jan  4 22:45 ahf_setup.dat
-rwxr-xr-x+  1 root root  392587026 Mar  9 01:55 ahf_setup
```

3. Run the upgrade command.

```
ahfctl upgrade
AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/
ahf_install_221000_139332_2022_03_09-02_09_42.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 22.1.0 Build Date: 202203081742
AHF is already installed at /opt/oracle.ahf
Installed AHF Version: 22.1.0 Build Date: 202203081714
Upgrading /opt/oracle.ahf
Shutting down AHF Services
Nothing to do !
Shutting down TFA
Removed symlink /etc/systemd/system/multi-user.target.wants/oracle-
tfa.service.
Removed symlink /etc/systemd/system/graphical.target.wants/oracle-
tfa.service.
Successfully shutdown TFA..
Starting AHF Services
Starting TFA..
Waiting up to 100 seconds for TFA to be started..
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands
No new directories were added to TFA
Directory /u01/app/grid/crsdata/scao05adm07/trace/chad was already
added to TFA Directories.
INFO: Starting exachk scheduler in background. Details for the
process can be found at /u01/app/grid/oracle.ahf/data/scao05adm07/
diag/exachk/compliance_start_090322_021151.log
AHF is successfully upgraded to latest version
.-----------------------------------------------------------------
.
| Host        | TFA Version | TFA Build ID         | Upgrade Status
|
+-------------+-------------+----------------------+----------------
+
| scao05adm07 |  22.1.0.0.0 | 22100020220308174218 | UPGRADED
|
| scao05adm08 |  22.1.0.0.0 | 22100020220308171448 | UPGRADED
|
'-------------+-------------+----------------------
+----------------'
Moving /tmp/ahf_install_221000_139332_2022_03_09-02_09_42.log
to /u01/app/grid/oracle.ahf/data/scao05adm07/diag/ahf/
Please upgrade AHF on the below mentioned nodes as well using
ahfctl upgrade
scao05adm08
```

4. Validate the AHF installer zip is removed and the extracted binaries are retained.

```
ls -lart /acfs01
-rw-r--r--+  1 root root       1520 Apr 30  2020 README.txt
-rw-r--r--+  1 root root        625 Nov  1 15:15 oracle-tfa.pub
-rw-r--r--+  1 root root        384 Jan  4 22:45 ahf_setup.dat
-rwxr-xr-x+  1 root root  392587026 Mar  9 01:55 ahf_setup
```

Network File System (NFS)

- If the stage location is NFS and if the AHF installer zip file exists in the stage location, then the installer asks the user to extract it.
- If the stage location has AHF binaries in the extracted form, then after upgrading, the installer retains the extracted AHF binaries as is.
- If the stage location has AHF installer zip file, then after upgrading, the installer removes the AHF installer zip file.

1. Configure the auto upgrade parameters.

```
ahfctl setupgrade -all
Enter autoupgrade flag <on/off> : on
Enter software stage location : /export/sheisey_R/ahf_stage
Stage location /export/sheisey_R/ahf_stage file system type is NFS. User
needs to unzip AHF zip placed at NFS file system.
Enter auto upgrade frequency : 30
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
refreshConfig() completed successfully.
```

2. Check if the AHF installer zip file or AHF binaries in the extracted form exists in the stage location.

```
ls -lart /export/sheisey_R/ahf_stage
-rw-r--r--    1 root root  389105013 Feb  3 06:08 AHF-LINUX_v22.1.0.zip
-rw-r--r--+  1 root root       1520 Apr 30  2020 README.txt
-rw-r--r--+  1 root root        625 Nov  1 15:15 oracle-tfa.pub
-rw-r--r--+  1 root root        384 Jan  4 22:45 ahf_setup.dat
-rwxr-xr-x+  1 root root  392587026 Mar  9 01:55 ahf_setup
```

3. Run the upgrade command.

```
ahfctl upgrade
AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/
ahf_install_221000_139332_2022_03_09-02_09_42.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 22.1.0 Build Date: 202203081742
AHF is already installed at /opt/oracle.ahf
Installed AHF Version: 22.1.0 Build Date: 202203081714
Upgrading /opt/oracle.ahf
Shutting down AHF Services
Nothing to do !
Shutting down TFA
Removed symlink /etc/systemd/system/multi-user.target.wants/oracle-
```

```
tfa.service.
Removed symlink /etc/systemd/system/graphical.target.wants/oracle-
tfa.service.
Successfully shutdown TFA..
Starting AHF Services
Starting TFA..
Waiting up to 100 seconds for TFA to be started..
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands
No new directories were added to TFA
Directory /u01/app/grid/crsdata/scao05adm07/trace/chad was already
added to TFA Directories.
INFO: Starting exachk scheduler in background. Details for the
process can be found at /u01/app/grid/oracle.ahf/data/scao05adm07/
diag/exachk/compliance_start_090322_021151.log
AHF is successfully upgraded to latest version
.-----------------------------------------------------------------
.
| Host        | TFA Version | TFA Build ID         | Upgrade Status
|
+-------------+-------------+----------------------+----------------
+
| scao05adm07 |  22.1.0.0.0 | 22100020220308174218 | UPGRADED
|
| scao05adm08 |  22.1.0.0.0 | 22100020220308171448 | UPGRADED
|
'-------------+-------------+----------------------
+----------------'
Moving /tmp/ahf_install_221000_139332_2022_03_09-02_09_42.log
to /u01/app/grid/oracle.ahf/data/scao05adm07/diag/ahf/
Please upgrade AHF on the below mentioned nodes as well using
ahfctl upgrade
scao05adm08
```

4. Validate if the AHF installer zip is removed and the extracted binaries are retained.

```
ls -lart /export/sheisey_R/ahf_stage
-rw-r--r--+  1 root root      1520 Apr 30  2020 README.txt
-rw-r--r--+  1 root root       625 Nov  1 15:15 oracle-tfa.pub
-rw-r--r--+  1 root root       384 Jan  4 22:45 ahf_setup.dat
-rwxr-xr-x+  1 root root  392587026 Mar  9 01:55 ahf_setup
```

2.5.3 Patching Oracle Autonomous Health Framework

Learn to patch Oracle Autonomous Health Framework automatically or on demand.

- Running AHFCTL Update Commands to Automatically Patch Oracle Autonomous Health Framework
  You need AHF install user privileges to run the `update`, `setupdate`, `getupdate`, and `unsetupdate` commands.

- Running AHFCTL Update Commands to Apply AHF Metadata and Framework Updates
  You need AHF install user privileges to run these commands.

2.5.3.1 Running AHFCTL Update Commands to Automatically Patch Oracle Autonomous Health Framework

You need AHF install user privileges to run the `update`, `setupdate`, `getupdate`, and `unsetupdate` commands.

- ahfctl update
  Use the `ahfctl update` command to apply AHF updates automatically.
- ahfctl setupdate
  Use the `ahfctl setupdate` command to set update parameters.
- ahfctl getupdate
  Use the `ahfctl getupdate` command to get update parameters.
- ahfctl unsetupdate
  Use the `ahfctl unsetupdate` command to unset update parameters.
- How to Apply an Update
  Configure AHF to automatically download new compliance checks and SRDCs from MOS (My Oracle Support) or a REST Endpoint.

2.5.3.1.1 ahfctl update

Use the `ahfctl update` command to apply AHF updates automatically.

Note:

You need AHF install user privileges to run the `ahfctl update` command.

Caution:

Make sure to test the metadata on a pre-production system before copying the downloaded file to the production-mounted filesystem.

1. Configure automatic download on a staging server.
2. Test the downloaded metadata on a pre-production system.
3. Configure auto-update on all production systems.
4. Copy the test metadata zip on production mounted file systems to automatically apply the update.

Syntax

```
ahfctl update
[-h]
[-nomos]
[-debug]
```

Parameters

Table 2-1   ahfctl update Command Parameters

Parameter	Description
`-nomos`	Specify not to configure MOS.
`-debug`	Specify the `-debug` option to enable debugging.

Example 2-15   New AHF metadate update is available at software stage location

```
ahfctl update
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220607 from 20220516
Please copy ahf_data_20220607.zip and run the command 'ahfctl
applyupdate -updatefile ahf_data_20220607.zip' on the below mentioned
nodes
scao05adm08
```

Example 2-16   REST Endpoints parameters are configured and a new AHF metadata update is available at the REST Endpoint

```
ahfctl update
Applying AHF metedata update...
AHF update zip is not available at stage location /opt/rajeev
Upload configuration check for: ahf_update_loc.
Parameters are configured correctly to upload.
ahf_data_20220607.zip successfully downloaded at /opt/rajeev
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220607 from 20220601
Please copy ahf_data_20220607.zip and run the command 'ahfctl
applyupdate -updatefile ahf_data_20220607.zip' on the below mentioned
nodes
scao05adm08
```

2.5.3.1.2 ahfctl setupdate

Use the `ahfctl setupdate` command to set update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl setupdate` command.

Syntax

```
ahfctl setupdate
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupdate AUTOUPDATE]
[-servicename SERVICENAME]
[-fstype FSTYPE]
[-frequency FREQUENCY]
```

Parameters

Table 2-2 ahfctl setupdate Command Parameters

Parameter	Description
`-all`	Specify to configure all parameters.
`-swstage` *`SWSTAGE`*	Specify the software stage location, for example, `/opt/oracle.ahf`.
`-autoupdate` *`AUTOUPDATE`*	Specify to enable or disable autoupdate. Default: `on`. Valid values: `on`| `off`.
`-servicename` *`SERVICENAME`*	Specify the name of the REST download service. Default: `ahf_update_loc`.
`-fstype` *`FSTYPE`*	Specify the stage location file system type, for example, `nfs/acfs/local`.
`-frequency` *`FREQUENCY`*	Specify the autoupdate frequency in days in the range (1,30), for example, 15.
`-debug`	Specify the `-debug` option to enable debugging.

Example 2-17 Set update configuration

```
ahfctl setupdate -swstage /opt/oracle.ahf -autoupdate on
```

Example 2-18 Set all update parameters

```
ahfctl setupdate -all
Enter autoupdate flag <on/off> : on
Enter software stage location : /scratch/ahf_stage
Enter auto update frequency : 30
AHF autoupdate parameters successfully updated
Successfully synced AHF configuration
```

Example 2-19 Disable autoupdate

```
ahfctl setupdate -autoupdate off
AHF autoupdate parameters successfully updated
Successfully synced AHF configuration
```

2.5.3.1.3 ahfctl getupdate

Use the `ahfctl getupdate` command to get update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl getupdate` command.

Syntax

```
ahfctl getupdate
[-h]
[-all]
[-debug]
```

Parameters

Table 2-3 ahfctl getupdate Command Parameters

Parameter	Description
`-all`	Specify to get all parameters.
`-debug`	Specify the `-debug` option to enable debugging.

Example 2-20 Get all update parameters

```
ahfctl getupdate -all
autoupdate : on
autoupdate.swstage : /opt/oracle.ahf
autoupdate.frequency : 30
autoupdate.servicename : [not set]
autoupdate.fstype : [not set]
```

2.5.3.1.4 ahfctl unsetupdate

Use the `ahfctl unsetupdate` command to unset update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl unsetupdate` command.

Syntax

```
ahfctl setupdate
[-h]
[-all]
[-swstage SWSTAGE]
```

```
[-autoupdate AUTOUPDATE]
[-servicename SERVICENAME]
[-fstype FSTYPE]
[-frequency FREQUENCY]
```

Parameters

Table 2-4 ahfctl setupdate Command Parameters

Parameter	Description
`-all`	Specify to unset all parameters.
`-swstage` *`SWSTAGE`*	Specify to unset the software stage location.
`-autoupdate` *`AUTOUPDATE`*	Specify to unset the autoupdate flag.
`-servicename` *`SERVICENAME`*	Specify to uset the REST download service name.
`-fstype` *`FSTYPE`*	Specify to unset the stage location file system type.
`-frequency` *`FREQUENCY`*	Specify to unser the autoupdate frequency.
`-debug`	Specify the `-debug` option to enable debugging.

Example 2-21 Unset a single update parameter

```
ahfctl unsetupdate -swstage
Software stage location successfully removed
Successfully synced AHF configuration
```

Example 2-22 Unset all update configuration

```
ahfctl unsetupdate -all
AHF update parameters successfully removed
Successfully synced AHF configuration
```

2.5.3.1.5 How to Apply an Update

Configure AHF to automatically download new compliance checks and SRDCs from MOS (My Oracle Support) or a REST Endpoint.

1. Configure MOS credentials.

   For example:

   ```
   ahfctl setupload -name mosconf1 -type https
   Enter mosconf1.https.user : john.doe@acme.com
   Enter mosconf1.https.password :
   Enter mosconf1.https.url : https://transport.oracle.com/upload/issue
   ```

2. Configure auto update.

For example:

```
ahfctl setupdate -autoupdate on -swstage /my/staging/path -
frequency 1
```

3. Apply update when you're ready.

```
ahfctl update
```

2.5.3.2 Running AHFCTL Update Commands to Apply AHF Metadata and Framework Updates

You need AHF install user privileges to run these commands.

> **Note:**
>
> To configure AHF auto-update refer to:
>
> - ahfctl update
> - ahfctl setupdate
> - ahfctl getupdate
> - ahfctl unsetupdate

- ahfctl applyupdate
  Use the `ahfctl applyupdate` command to update metadata and framework files on the local node from the `zip` file provided.
- ahfctl queryupdate
  Use the `ahfctl queryupdate` command to check if an update was applied. To get a list of all the metadata and framework updates applied, use the `-all` option. To query a metadata or framework update with a specific update ID, use the `–updateid` option.
- ahfctl rollbackupdate
  Use the `ahfctl rollbackupdate` command to rollback the updates with a specific update ID applied to the local node. If you do not specify the update ID, then AHF rolls back to the previous state by default.
- ahfctl deleteupdatebackup
  Use the `ahfctl deleteupdatebackup` command to delete the backup directories used for AHF update.

2.5.3.2.1 ahfctl applyupdate

Use the `ahfctl applyupdate` command to update metadata and framework files on the local node from the `zip` file provided.

> **Note:**
>
> - You need AHF install user privileges to run the `ahfctl applyupdate` command.
> - You must apply metadata and framework updates to all cluster nodes.

Syntax

```
ahfctl applyupdate [-h] [-debug] [-updatefile UPDATEFILE]
```

Parameters

Table 2-5 ahfctl applyupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updatefile` *`UPDATEFILE`*	Specify the name of the `zip` file. The existing metadata and framework files will be replaced with the files in the `zip` file. Download the `zip` file from My Oracle Support note 2550798.1.

Example 2-23 ahfctl applyupdate

```
# ahfctl applyupdate -updatefile /tmp/ahf_data_20220203.zip
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220203 from 20211220
```

Related Topics

- https://support.oracle.com/epmos/faces/DocContentDisplay?id=2550798.1

2.5.3.2.2 ahfctl queryupdate

Use the `ahfctl queryupdate` command to check if an update was applied. To get a list of all the metadata and framework updates applied, use the `-all` option. To query a metadata or framework update with a specific update ID, use the `-updateid` option.

> **Note:**
>
> To verify if the metadata and framework updates were applied to all nodes in a cluster, run the `ahfctl queryupdate` command as the AHF install user on each cluster node.

Syntax

```
ahfctl queryupdate [-h] [-debug] [-updateid UPDATEID] [-all] [-json]
```

Parameters

Table 2-6 ahfctl queryupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	To query framework update with a specific update ID. Specify `-updateid` *`UPDATEID`* option to query framework updates. **Note:** To query metadata updates, please use the `-all` option.
`-all`	Lists all applied metadata and framework updates.
`-json`	Specify this option to get the output in JSON format.

Example 2-24 ahfctl queryupdate

```
# ahfctl queryupdate -all
AHF Metadata Update: 20220203
Status: Applied
Applied on: Fri Feb 4 00:47:00 2022


# ahfctl queryupdate -all
AHF Framework update: PATCH_22.2.4.1
Status: Applied
Fixes: 34716496
Applied on: Wed Nov 30 15:14:56 2022
```

34716496 is the updateid for AHF framework update applied.

```
ahfctl queryupdate -updateid 34716496
AHF Framework update: PATCH_22.2.4.1
Status: Applied
Fixes: 34716496
Applied on: Wed Nov 30 15:14:56 2022
1:53
AHF framework updated files:
/opt/oracle.ahf/ahf/lib/ahfcomponents.py
/opt/oracle.ahf/ahf/lib/ahfctl.py
/opt/oracle.ahf/exachk/messages/framework_messages.json
/opt/oracle.ahf/exachk/lib/ahf_metadata.py
```

2.5.3.2.3 ahfctl rollbackupdate

Use the `ahfctl rollbackupdate` command to rollback the updates with a specific update ID applied to the local node. If you do not specify the update ID, then AHF rolls back to the previous state by default.

> **Note:**
>
> To rollback the metadata and framework updates applied to all nodes in a cluster, you must run the `ahfctl rollbackupdate` command as the AHF install user on each cluster node.

Syntax

```
ahfctl rollbackupdate [-h] [-debug] [-updateid UPDATEID]
```

Parameters

Table 2-7 ahfctl rollbackupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	Specify update ID, for example, Bug ID, Build ID, that you want to rollback.

Example 2-25 ahfctl rollbackupdate

```
# ahfctl rollbackupdate -updateid 20220203
Data files with timestamp 20220203 identified. Rolling back the files to
Production version 20211220
Rolled back the data files 20220203 to Production version 20211220
```

2.5.3.2.4 ahfctl deleteupdatebackup

Use the `ahfctl deleteupdatebackup` command to delete the backup directories used for AHF update.

Note:

- To delete the backup directories on all nodes in a cluster, you must run the `ahfctl deleteupdatebackup` command as the AHF install user on each cluster node.
- You must not delete the backup directories randomly. Oracle recommends deleting the backup directories in the same order the updates were applied. If you delete the backup directories associated with a specific timestamp, then you will not be able to roll back to the state before the updates with that specific timestamp were applied.
- Upgrading AHF using the `ahf_setup` script automatically deletes the backup directories of the previous AHF versions.
- Oracle recommended to delete the AHF update backup directories only when there's a need to free up space on the system. You cannot delete the AHF update backup directory of the current running timestamp/update because once the backup directory is deleted for the specific timestamp, rolling back the update to specific timestamp/update is not possible.
  For example: AHF Updates applied in order is: 20230901 -> 20231001 -> 20231101 (Current latest update). You can delete update backups for 20230901 and 20231001 but not the 20231101.

Syntax

```
ahfctl deleteupdatebackup [-h] [-debug] [-updateid UPDATEID] [-silent]
```

Parameters

Table 2-8 ahfctl deleteupdatebackup Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	Deletes the backup directories with the specified timestamp.
`-silent`	Skips user confirmation for delete backup directories.

Example 2-26 ahfctl deletebackup

```
# ahfctl deleteupdatebackup -updateid 20220130
Deleted metadata backup directory for: /opt/oracle.ahf/data/
work/.exachk_patch_directory/.20220130_metadata_bkp
```

2.5.4 Uninstalling Oracle Autonomous Health Framework

To uninstall Oracle Autonomous Health Framework, run the `uninstall` command as `root`, or install user.

Run `ahfctl uninstall` to uninstall AHF.

Running the command:

- Stops Oracle Orachk
- Stops Oracle Trace File Analyzer
- Deletes the Oracle Autonomous Health Framework installation directory

Example 2-27

```
ahfctl uninstall -deleterepo -silent
Starting AHF Uninstall
AHF will be uninstalled on: node1

Stopping AHF service on local node node1...
Sleeping for 10 seconds...

Stopping TFA Support Tools...

Removing AHF setup on node1:
Removing /opt/oracle.ahf/rpms
Removing /opt/oracle.ahf/jre
Removing /opt/oracle.ahf/common
Removing /opt/oracle.ahf/bin
Removing /opt/oracle.ahf/python
Removing /opt/oracle.ahf/analyzer
Removing /opt/oracle.ahf/tfa
Removing /opt/oracle.ahf/orachk
Removing /opt/oracle.ahf/ahf
Removing /opt/oracle.ahf/data/node1
Removing /opt/oracle.ahf/install.properties
Removing /opt/oracle.ahf/data/repository
Removing /opt/oracle.ahf/data
Removing /opt/oracle.ahf
```

2.6 Start Using Oracle Autonomous Health Framework

- Understanding the Directory Structure
  Review the list of key Oracle Autonomous Health Framework directories.
- Configuring Oracle Trace File Analyzer and Oracle Orachk/Oracle Exachk to Use the Same Notification Addresses
  Configure notification emails to notify the recepients the results of Oracle Orachk and Oracle Exachk compliance checking, or when Oracle Trace File Analyzer detects significant faults.

- Oracle Trace File Analyzer Command-Line and Shell Options
  The `tfactl` tool functions as a command-line interface, shell interface, and menu interface.
- Manage Oracle Trace File Analyzer and Oracle Orachk Daemons Using systemctl Commands
  Run the `systemctl` commands as `root` user on an Oracle Linux server. You can also start/stop Oracle Trace File Analyzer daemon using the `tfactl shutdown` and `tfactl start` commands.
- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

2.6.1 Understanding the Directory Structure

Review the list of key Oracle Autonomous Health Framework directories.

Table 2-9 Key Oracle Autonomous Health Framework Directories

Directory	Description
AHF_LOC	Directory where Oracle Autonomous Health Framework is installed.
AHF_LOC/python	Python home directory.
AHF_LOC/orachk	Oracle Orachk home directory.
AHF_LOC/jre	JRE home directory.
AHF_LOC/common	Oracle Autonomous Health Framework common directory that contains libraries, ACR, ORDS, and so on.
AHF_LOC/bin	Directory that contains Oracle Autonomous Health Framework binaries including the command-line interface `tfactl` and `orachk`.
AHF_LOC/analyzer	Oracle Autonomous Health Framework Analyzer directory.
AHF_LOC/data	Oracle Autonomous Health Framework data directory contains data generated by Oracle Autonomous Health Framework components such as configuration files, Berkeley DB (BDB), Index data, and so on.
AHF_LOC/tfa	Oracle Trace File Analyzer home directory.
DATA_DIR	Directory where Oracle Autonomous Health Framework stores diagnostic collections and Metadata.
DATA_DIR/repository	Directory where Oracle Autonomous Health Framework stores diagnostic collections.
DATA_DIR/*HOST*/diag	This directory contains logs from all components.

2.6.2 Configuring Oracle Trace File Analyzer and Oracle Orachk/Oracle Exachk to Use the Same Notification Addresses

Configure notification emails to notify the recepients the results of Oracle Orachk and Oracle Exachk compliance checking, or when Oracle Trace File Analyzer detects significant faults.

Use the `ahfnotificationaddress` option to configure Oracle Trace File Analyzer and Oracle Orachk/Oracle Exachk to use the same notification addresses.

1. Specify a space-delimited list of email addresses.

   ```
   # tfactl set ahfnotificationaddress="id1 id2..."
   ```

   You use the `tfactl set ahfnotificationaddress` command to set or update the existing list of email addresses.

   If you specify the email addresses while installing Oracle Autonomous Health Framework, then Oracle Autonomous Health Framework persists those email addresses in the `install.properties` file. Oracle Orachk and Oracle Exachk pick those email addresses from the `install.properties` file, and then updates the `NOTIFICATION_EMAIL` property for scheduled jobs. However, if you explicitly specify email addresses while creating jobs, then Oracle Orachk and Oracle Exachk override the email addresses in the `install.properties` file. By default, Oracle Trace File Analyzer does not set notification emails using the email addresses in the `install.properties` file; instead, you will have to explicitly specify the email addresses.

   ```
   # tfactl set ahfnotificationaddress="test-user1@example.com test-
   user1@example.com"
   Successfully set the AHF Notification Address
   ```

   Run the `orachk -get NOTIFICATION_EMAIL` and `exachk -get NOTIFICATION_EMAIL` commands to view the list of notification email addresses set for Oracle Orachk and Oracle Exachk scheduled jobs.

2. To get the list of notification emails:

   ```
   # tfactl get ahfnotificationaddress
   ```

   Fetches and displays the list of notification email IDs from the `install.properties` file.

   ```
   # tfactl get ahfnotificationaddress
   AHF Notification Address : test-user1@example.com test-user1@example.com
   ```

3. To unset notification emails:

   ```
   # tfactl unset ahfnotificationaddress
   ```

Removes the notification email IDs from the install.properties file.

```
# tfactl unset ahfnotificationaddress
Successfully unset the AHF Notification Address
```

Related Topics

- NOTIFICATION_EMAIL
  Set the NOTIFICATION_EMAIL daemon option to send email notifications to the recipients you specify.
- Configuring Email Notification Details
  Configure Oracle Trace File Analyzer to send an email to the registered email address after an automatic collection completes.
- Getting Existing Options for the Daemon
  Query the values that you set for the daemon options.

Configuring Oracle Trace File Analyzer and Oracle Orachk/Oracle Exachk to Use Different Notification Addresses

For Oracle Orachk/Oracle Exachk:

Specify a comma-delimited list of email addresses, as follows:

```
$ orachk -set
"NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany.co
m"


$ exachk -set
"NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany.co
m"
```

Optionally, you can specify the name of the profile. If you do not specify, then id=DEFAULT. For example:

```
$ orachk -id dba -set
"NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany.co
m"


$ exachk -id dba -set
"NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany.co
m"
```

For Oracle Trace File Analyzer:

To set the notification email for a specific ORACLE_HOME, include the operating system owner in the command:

```
$ tfactl set notificationAddress=os_user:email
```

To set the notification email for any ORACLE_HOME:

```
$ tfactl set notificationAddress=email
```

2.6.3 Oracle Trace File Analyzer Command-Line and Shell Options

The tfactl tool functions as a command-line interface, shell interface, and menu interface.

Table 2-10 Oracle Trace File Analyzer Interfaces

Interface	Command	How to use
Command-line	`$ tfactl` *`command`*	Specify all command options at the command line.
Shell interface	`$ tfactl`	Set and change the context and then run commands from within the shell.
Menu Interface	`$ tfactl` *`menu`*	Select the menu navigation options and then choose the command that you want to run.

Using tfactl, you can:

- Run administration commands
- Collect diagnostic data
- Analyze diagnostic data collection

Running tfactl commands depends upon the level of access you have to tfactl. Run the administration commands as root or sudo. Or, run a subset of commands as:

- An Oracle Database home owner or Oracle Grid Infrastructure home owner.
- A member of OS DBA or ASM groups.

To grant other users access to tfactl:

```
tfactl access
```

To use tfactl as a command-line tool:

```
tfactl [command][options]
```

To use tfactl as a shell interface, enter tfactl, and then run the commands as needed:

```
$ tfactl
tfactl>
```

Append the -help option to any of the tfactl commands to obtain command-specific help.

```
$ tfactl [command] -help
```

Related Topics

- Running the Installer Script
  Run the installer script to install Oracle Autonomous Health Framework or to just extract the content of the installer package.
- Running Oracle Trace File Analyzer Administration Commands
  You need `root` access to `tfactl`, or `sudo` access to run all administration commands.
- Running Oracle Trace File Analyzer Summary and Analysis Commands
  Use these commands to view the summary of deployment and status of Oracle Trace File Analyzer, and changes and events detected by Oracle Trace File Analyzer.
- Running Oracle Trace File Analyzer Diagnostic Collection Commands
  Run the diagnostic collection commands to collect diagnostic data.

2.6.4 Manage Oracle Trace File Analyzer and Oracle Orachk Daemons Using systemctl Commands

Run the `systemctl` commands as `root` user on an Oracle Linux server. You can also start/stop Oracle Trace File Analyzer daemon using the `tfactl shutdown` and `tfactl start` commands.

```
systemctl status oracle-tfa.service
systemctl start oracle-tfa.service
systemctl stop oracle-tfa.service
```

```
# systemctl status oracle-tfa.service
oracle-tfa.service - Oracle Trace File Analyzer
Loaded: loaded (/etc/systemd/system/oracle-tfa.service; enabled;
vendor preset: disabled)
Active: inactive (dead) since Fri 2021-01-29 18:50:51 PST; 24s ago
Process: 79935 ExecStart=/etc/init.d/init.tfa run >/dev/null 2>&1
</dev/null (code=killed, signal=TERM)
Main PID: 79935 (code=killed, signal=TERM)
Jan 29 15:47:46 den02mwa systemd[1]: Started Oracle Trace File
Analyzer.
Jan 29 15:47:47 den02mwa init.tfa[79935]: Starting TFA..
Jan 29 15:47:48 den02mwa init.tfa[79935]: Starting TFA out of init,
Should be running in 10 seconds
Jan 29 15:47:48 den02mwa init.tfa[79935]: Successfully updated jvmXmx
to 128 in TFA...
Jan 29 15:47:56 den02mwa init.tfa[79935]: OSWatcher is already
deployed at /opt/oracle.ahf/tfa/ext/oswbb
Jan 29 15:47:56 den02mwa init.tfa[79935]: Cannot find valid Non root
user to run OSWatcher
Jan 29 18:50:41 den02mwa systemd[1]: Stopping Oracle Trace File
Analyzer...
Jan 29 18:50:41 den02mwa init.tfa[79935]: Telemetry not enabled - Not
Starting Adapter
```

```
Jan 29 18:50:51 den02mwa systemd[1]: Stopped Oracle Trace File Analyzer.


# tfactl start
Starting TFA..
Created symlink /etc/systemd/system/multi-user.target.wants/oracle-
tfa.service -> /etc/systemd/system/oracle-tfa.service.
Created symlink /etc/systemd/system/graphical.target.wants/oracle-
tfa.service -> /etc/systemd/system/oracle-tfa.service.
Waiting up to 100 seconds for TFA to be started..
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands


# tfactl shutdown
Shutting down TFA
Removed /etc/systemd/system/multi-user.target.wants/oracle-tfa.service.
Removed /etc/systemd/system/graphical.target.wants/oracle-tfa.service.
Successfully shutdown TFA..
```

2.6.5 Behavior of Oracle Orachk or Oracle Exachk Daemon

AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

Command	Description

`exachk -autostart reset`
`orachk -autostart reset`
`ahfctl compliance -autostart reset`
	Starts and loads the default schedulers.

`exachk -autostop unset`
`orachk -autostop unset`
`ahfctl compliance -autostop unset`
	Removes all default unmodified schedulers.

Daemon behavior until AHF 23.8

The behavior of `exachk -autostart`, `orachk -autostart`, `ahfctl compliance -autostart`, and `ahfctl upgrade` are the same. The table below illustrates different scenarios of schedulers and their behavior before and after autostart and upgrade.

Before autostart/upgrade	After autostart/upgrade
Default schedulers	Default schedulers
User-defined + default schedulers	User-defined
Only user-defined	Only user-defined
User-defined + modified default schedulers	User-defined + modified default schedulers
2 default schedulers: One modified default and the other is not	Only modified default scheduler
Only one default scheduler out of 2 default schedulers	Both default schedulers

Before autostart/upgrade	After autostart/upgrade
No schedulers	No schedulers

The table below illustrates different scenarios of schedulers and their behavior before and after `exachk -autostart`, `orachk -autostart`, and `ahfctl compliance -autostart`.

Before autostop	After autostop
Default schedulers	No schedulers
User-defined + default schedulers	User-defined schedulers only
Only user-defined	Only user-defined
User-defined + modified default schedulers	User-defined + modified default schedulers
2 default schedulers: One modified default and the other is not	Only modified default scheduler
Only one default scheduler out of 2 default schedulers	No scheduler
No scheduler	No scheduler

Daemon behavioral changes in AHF 23.9

The behavior of `exachk -autostart`, `orachk -autostart`, `ahfctl compliance -autostart`, and `ahfctl upgrade` remains the same as in AHF 23.8. There will be no changes to the scheduler entries be it default schedulers or user-defined schedulers.

Before autostart/upgrade or autostop and then autostart	After autostart/upgrade or autostop and then autostart
Default schedulers	Default schedulers
User-defined + default schedulers	User-defined + default schedulers
Only user-defined	Only user-defined
User-defined + modified default schedulers	User-defined + modified default schedulers
2 default schedulers: One modified default and the other is not	2 default schedulers: One modified default and the other is not
Only one default scheduler out of 2 default schedulers	Only one default scheduler out of 2 default schedulers
No schedulers	No schedulers

The table below illustrates the behavior after `autostart reset`.

Before -autostart reset	After -autostart reset
Default schedulers	Default schedulers
User-defined + default schedulers	Default schedulers
Only user-defined	Default schedulers
User-defined + modified default schedulers	Default schedulers
2 default schedulers: One modified default and the other is not	Default schedulers
Only one default scheduler out of 2 default schedulers	Default schedulers

Before -autostart reset	After -autostart reset
No schedulers	Default schedulers

The table below illustrates the behavior when `autostop unset` is run and then `autostart`.

Before -autostop unset and then autostart	After -autostop unset and then autostart
Default schedulers	No schedulers
User-defined + default schedulers	User-defined
Only user-defined	Only user-defined
User-defined + modified default schedulers	User-defined + modified default schedulers
2 default schedulers: One modified default and the other is not	Only modified default scheduler
Only one default scheduler out of 2 default schedulers	No schedulers
No schedulers	No schedulers

Use Cases

Use case	Outcome
`-autostop` and then `-autostart`	`autostop` will only deconfigure the compliance and autostart will start the compliance and load all the schedulers that were present before `autostop`.
`-autostop unset` and then `-autostart`	`autostop unset` will deconfigure the compliance and remove all the default unmodified schedulers and `autostart` will start the compliance and load the user-defined schedulers and modified default schedulers if they exist.
`-autostop` and then `-autostart reset`	`autostop` will only deconfigure the compliance and `autostart reset` will start the compliance and only load the default schedulers.
`-autostop unset` and then `-autostart reset`	`autostop unset` will deconfigure the compliance and remove all the default unmodified schedulers and `autostart reset` will start the compliance and only load the default schedulers.

Example 2-28 exachk -autostop unset, exachk -autostart reset, and exachk -get all

```
# exachk -autostop unset
Removing exachk cache discovery....
Successfully completed exachk cache discovery removal.
Successfully copied Daemon Store to Remote Nodes

# exachk -autostart reset
Successfully copied Daemon Store to Remote Nodes
exachk is using TFA Scheduler. TFA PID: 113253
Daemon log file location is : /opt/oracle.ahf/data/test-server/exachk/
user_root/output/exachk_daemon.log

# exachk -get all
```

```
------------------------------------------------------------
Scheduled runs:
------------------------------------------------------------
ID: exachk.autostart_client_exatier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile exatier1 -dball -showpass -
tag autostart_client_exatier1 -readenvconfig
AUTORUN_SCHEDULE  =  3 2 * * 1,2,3,4,5,6
COLLECTION_RETENTION  =  7
------------------------------------------------------------
------------------------------------------------------------
ID: exachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
AUTORUN_SCHEDULE  =  3 3 * * 0
COLLECTION_RETENTION  =  14
------------------------------------------------------------
```

Example 2-29   exachk -autostop unset and exachk -get all

```
# exachk -autostop unset
Removing exachk cache discovery....
Successfully completed exachk cache discovery removal.
Successfully copied Daemon Store to Remote Nodes

# exachk -get all
No scheduler for any ID
```

Example 2-30   exachk -autostart reset and exachk -get all

```
# exachk -autostart reset
Successfully copied Daemon Store to Remote Nodes
exachk is using TFA Scheduler. TFA PID: 113253
Daemon log file location is : /opt/oracle.ahf/data/test-server/exachk/
user_root/output/exachk_daemon.log

# exachk -get all
------------------------------------------------------------
Scheduled runs:
------------------------------------------------------------
ID: exachk.autostart_client_exatier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile exatier1 -dball -showpass -
tag autostart_client_exatier1 -readenvconfig
AUTORUN_SCHEDULE  =  3 2 * * 1,2,3,4,5,6
COLLECTION_RETENTION  =  7
------------------------------------------------------------
------------------------------------------------------------
ID: exachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
AUTORUN_SCHEDULE  =  3 3 * * 0
```

```
COLLECTION_RETENTION  =  14
------------------------------------------------------------
```

3

Run Compliance Checks

- Compliance Checking with Oracle Orachk and Oracle Exachk
  Oracle Orachk and Oracle Exachk share a common compliance check framework and a large portion of their features and tasks are common.
- Oracle Health Check Collections Manager for Oracle Application Express 20.2+
  Oracle Health Check Collections Manager is a companion application to Oracle Autonomous Health Framework that gives you an enterprise-wide view of your compliance check collection data.

3.1 Compliance Checking with Oracle Orachk and Oracle Exachk

Oracle Orachk and Oracle Exachk share a common compliance check framework and a large portion of their features and tasks are common.

- Getting Started with Running Compliance Checks
  Review these topics to get started with Oracle Autonomous Health Framework compliance checking.
- Running Compliance Checks Automatically
  Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.
- Running Compliance Checks On-Demand
  Usually, compliance checks run at scheduled intervals. However, Oracle recommends that you run compliance checks on-demand when needed.
- Running Compliance Checks in Silent Mode
  Run compliance checks automatically by scheduling them with the Automated Daemon Mode operation.
- Understanding and Managing Reports and Output
  Oracle Orachk and Oracle Exachk generate a detailed HTML report with findings and recommendations.
- Running Subsets of Checks
  Run a subset of compliance checks where necessary.
- Understanding Oracle Exachk specifics for Oracle Exadata and Zero Data Loss Recovery Appliance
  Understand the features and learn to perform tasks specific to Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance.
- Integrating Compliance Check Results with Other Tools
  Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager and other third-party tools.

- Using Oracle Orachk to Confirm System Readiness for Implementing Application Continuity
  Application Continuity Checking for Application Continuity enables you to deploy Application Continuity easily and transparently.
- Running Oracle ZFS Storage Appliance Compliance Checks
  Learn to run the compliance checks for Oracle ZFS Storage Appliances.
- Using Oracle Exachk on Oracle Big Data Appliance
  Understand the features and learn to perform tasks specific to Oracle Exachk on Oracle Big Data Appliance.
- Easily Manage Cell, Switches, Databases and exacli Passwords
  Learn to manage passwords for cells, switches, databases, and `exacli` using the following commands:
- Using the exadcli Utility to Collect Cell Metric Data for Guest VMs (domUs)
  `exadcli` enables you to run an ExaCLI command on multiple remote nodes. Remote nodes are referenced by their host name or IP address.
- Query AHF Message Codes to Understand More About the Context and Next Steps
  You can now query Oracle Orachk and Oracle Exachk check details using a four digit code representing the check.

3.1.1 Getting Started with Running Compliance Checks

Review these topics to get started with Oracle Autonomous Health Framework compliance checking.

- Running Oracle Orachk or Oracle Exachk as a Non-Root User
  You can optionally run Oracle Orachk or Oracle Exachk as a non-root user.
- Non-Root Users Running Root Privileged Checks on Database Servers
  Non-root user can run `root` privileged checks on the database servers without requiring `root` password or `sudo`.
- Automatic Compliance Checking
  Use the daemon to configure automatic compliance check runs at scheduled intervals.
- Email Notification and Report Overview
  The following sections provide a brief overview about email notifications and sections of the HTML report output.
- Recommended On-Demand Usage
  This section summarizes the scenarios that Oracle recommends running compliance checks on-demand.
- Running Compliance Checks on a Remote Node
  Run compliance checks on remote nodes using RSA/DSA SSH private and public keys.
- Creating, Modifying, and Deleting User-Defined Profiles
  Specify a comma-delimited list of check IDs to create and modify custom profiles.
- Sanitizing Sensitive Information in the Diagnostic Collections
  Oracle Autonomous Health Framework uses Adaptive Classification and Redaction (ACR) to sanitize sensitive data.

- Problem Repair Automation Options
  Starting in release 19.3, Oracle Orachk and Oracle Exachk have the capability to automatically fix problems when found.
- Integration of Oracle DBSAT into Oracle Autonomous Health Framework
  DBSAT is a lightweight utility that will not impair system performance in a measurable way.
- Integration of AutoUpgrade utility into Oracle Autonomous Health Framework
  The `AutoUpgrade` utility identifies issues before upgrades, performs pre- and postupgrade actions, deploys upgrades, performs postupgrade actions, and starts the upgraded Oracle Database.

3.1.1.1 Running Oracle Orachk or Oracle Exachk as a Non-Root User

You can optionally run Oracle Orachk or Oracle Exachk as a non-root user.

When you have installed AHF as `root` and if non-root users run Oracle Orachk or Oracle Exachk and want to change the directory to their own output location, then the non-user will not be able to browse any directory using `ls -l` in the path before their own output location. However, they can directly `cd` to the output location.

```
$ cd /u01/app/crsusr/oracle.ahf/data/host_name/
$ ls -ltra
ls: cannot open directory .: Permission denied
$ cd orachk


$ ls
ls: cannot open directory .: Permission denied
$ cd user_racusr
$ ls -l
total 7456
-r-xr-xr-x 1 root root 6836 Jun 1 13:37 cgrep
rw-rr- 1 root root 5481 Jun 1 13:37 cgrep.pyc
drwxr-xr-x 7 racusr oinstall 274432 Jun 1 14:05
orachk_host_name_ratcdb_060120_133414
rr---- 1 racusr oinstall 7323951 Jun 1 14:05
orachk_host_name_ratcdb_060120_133414.zip
drwx-----T 2 racusr root 4096 Jun 1 14:05 output
drwx-----T 4 racusr root 4096 Jun 1 14:05 work
```

Non-root users can copy the path of Oracle Orachk run result and `cd` directly there, or copy the result. Alternatively, they can run the `ahfctl showrepo` command and it will show them the correct location where their results are available.

```
$ ahfctl showrepo

<<output truncated>>
orachk repository: /u01/app/crsusr/oracle.ahf/data/host_name/orachk/
user_racusr/output
```

Related Topics

- ahfctl showrepo
  Use the `ahfctl showrepo` command to get the repository locations of Oracle Autonomous Health Framework components.

3.1.1.2 Non-Root Users Running Root Privileged Checks on Database Servers

Non-root user can run `root` privileged checks on the database servers without requiring `root` password or `sudo`.

The Oracle Trace File Analyzer daemon must be running on all database servers in cluster.

1. As `root` user, grant permission to non-root users to run `root` privileged checks using the `tfactl access grant -user *user_name* -role privileged-compliance-checks` command.
2. Ensure that the non-root user has been assigned to the granted role and promotion is set to n/a.

```
tfactl access lsusers
.-------------------------------------------.
|            TFA Users in Node1             |
+-----------+---------+----------+----------+
| User Name | Status  | Promoted | Roles    |
+-----------+---------+----------+----------+
| dbusr     | Allowed | false    | n/a      |
| giusr     | Allowed | true     | n/a      |
| orarom    | Allowed | n/a      | platinum |
'-----------+---------+----------+----------'
```

Once the non-root user has been assigned to `privileged-compliance-checks` role, non-root user can run Oracle Orachk with the `-runasroot` option to run `root` privileged checks.

3.1.1.3 Automatic Compliance Checking

Use the daemon to configure automatic compliance check runs at scheduled intervals.

Installing Oracle Autonomous Health Framework as `root` on Linux or Solaris automatically sets up Oracle Orachk or Oracle Exachk to use the Oracle Trace File Analyzer scheduler daemon.

The daemon runs a full local Oracle Orachk check once every week at 3 AM, and a partial run of the most impactful checks at 2 AM every day through the `oratier1` or `exatier1` profiles. The daemon automatically purges the `oratier1` or `exatier1` profile run that runs daily, after a week. The daemon also automatically purges the full local run after 2 weeks. You can change the daemon settings after enabling auto start.

To remove auto start, run:

- `orachk -autostop`
- `exachk -autostop`

To remove all default unmodified schedulers:

- `orachk -autostop unset`
- `exachk -autostop unset`

> **Note:**
>
> - Daemon mode is supported only on the Linux and Solaris operating systems.
> - If you have an Oracle Engineered System, then in addition to the following usage steps, follow the system-specific instructions.

1. Set the daemon properties.

   At a minimum, set `AUTORUN_SCHEDULE` and `NOTIFICATION_EMAIL`.

   For example, to set the tool to run at 3 AM every Sunday and email the results to *some.body@example.com*, run the following command:

   ```
   $ exachk -set "AUTORUN_SCHEDULE=3 * *
   0 ;NOTIFICATION_EMAIL=some.body@example.com"
   ```

   ```
   $ orachk -set "AUTORUN_SCHEDULE=3 * *
   0 ;NOTIFICATION_EMAIL=some.body@example.com"
   ```

   Optionally, you can specify the name of the profile. If you do not specify, then `id=DEFAULT`.

   For example:

   ```
   $ exachk -id dba -set "AUTORUN_SCHEDULE=3 * *
   0;NOTIFICATION_EMAIL=some.body@example.com"
   ```

   ```
   $ orachk -id dba -set "AUTORUN_SCHEDULE=3 * *
   0;NOTIFICATION_EMAIL=some.body@example.com"
   ```

2. Configure the compliance check daemon as described in "*Running Compliance Checks Automatically*".
3. Start the daemon as the `root` user.

   - `orachk -autostart`
   - `exachk -autostart`

   To start and load the default schedulers:

   - `orachk -autostart reset`
   - `exachk -autostart reset`

> **Note:**
>
> You must log in as the `root` user to run the `-autostart` and `-autostop` commands. Non-root users cannot run the TFA Scheduler.

```
$ orachk -autostart
Commands -autostart and -autostop can not be run as non root user.
Switch to root user and try again.


$ orachk -autostop
Commands -autostart and -autostop can not be run as non root user.
Switch to root user and try again.
```

Related Topics

- Running Compliance Checks Automatically
  Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.
- Using Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance
  Usage of Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance depends on other considerations such as virtualization, parallel run, and so on.

Running Oracle Orachk or Oracle Exachk Scheduler With the Oracle Trace File Analyzer Daemon

Oracle Orachk or Oracle Exachk scheduler is run by the Oracle Trace File Analyzer daemon.
Oracle Trace File Analyzer scheduler:

- Decides which is the master node.
- Picks the Oracle Orachk or Oracle Exachk entries only on the master node.
- Runs only on the master node.
- Runs Oracle Orachk or Oracle Exachk clusterwide.
- Consolidates all the output on the master node.
- Enters which is the master node in the logs.
- Notifies through email that points to the master node where the report output is stored.

Example 3-1 Default configuration of Oracle Oracle Orachk/Oracle Exachk scheduler and daemon information

```
# orachk -autostatus
Master node = testserver
orachk daemon version = 221000
Install location = /opt/oracle.ahf/orachk
Started at = Wed Jun 22 20:56:51 UTC 2022
Scheduler type = TFA Scheduler
Scheduler PID:  1766980
```

```
------------------------------------------------------------
ID: orachk.autostart_client_oratier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile oratier1 -dball -showpass -tag
autostart_client_oratier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  3 2 * * 1,2,3,4,5,6
------------------------------------------------------------

------------------------------------------------------------
ID: orachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  3 3 * * 0
------------------------------------------------------------

Next auto run starts on Jun 23, 2022 02:03:00
ID:orachk.AUTOSTART_CLIENT_ORATIER1
```

Related Topics

- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

3.1.1.4 Email Notification and Report Overview

The following sections provide a brief overview about email notifications and sections of the HTML report output.

- First Email Notification
  After completing compliance check runs, the daemon emails the assessment report as an HTML attachment to all users that you have specified in the `NOTIFICATION_EMAIL` list.
- What does the Compliance Check Report Contain?
  Compliance check reports contain the health status of each system grouped under different sections of the report.
- Subsequent Email Notifications
  For the subsequent compliance check runs after the first email notification, the daemon emails the summary of differences between the most recent runs.
- Generating a Diff Report
  The diff report attached to the previous email notification shows a summary of differences between the most recent runs.

3.1.1.4.1 First Email Notification

After completing compliance check runs, the daemon emails the assessment report as an HTML attachment to all users that you have specified in the `NOTIFICATION_EMAIL` list.

3.1.1.4.2 What does the Compliance Check Report Contain?

Compliance check reports contain the health status of each system grouped under different sections of the report.

The HTML report output contains the following:

- Health score
- Summary of compliance check runs
- Table of contents
- Controls for report features
- Findings
- Recommendations

Details of the report output are different on each system. The report is dynamic, and therefore the tools display certain sections only if applicable.

System Health Score and Summary

System Health Score and Summary report provide:

- A high-level health score based on the number of passed or failed checks
- A summary of compliance check run includes:
  - Name, for example, Cluster Name
  - Version of the operating system kernel
  - Path, version, name of homes, for example, CRS, DB, and EM Agent
  - Version of the component checked, for example, Exadata
  - Number of nodes checked, for example, database server, storage servers, InfiniBand switches
  - Version of Oracle Orachk and Oracle Exachk
  - Name of the collection output
  - Date and time of collection
  - Duration of the check
  - Name of the user who ran the check, for example, `root`
  - How long the check is valid

Table of Contents and Report Feature

The **Table of Contents** section provides links to major sections in the report:

- Database Server
- Storage Server
- InfiniBand Switch
- Cluster Wide
- Maximum Availability Architecture (MAA) Scorecard

- Infrastructure Software and Configuration Summary
- Findings needing further review
- Platinum Certification
- System-wide Automatic Service Request (ASR) compliance check
- Skipped Checks
- Top 10 Time Consuming Checks

The **Report Feature** section enables you to:

- Filter checks based on their statuses
- Select the regions
- Expand or collapse all checks
- View check IDs
- Remove findings from the report
- Get a printable view

Report Findings

The **Report Findings** section displays the result of each compliance check grouped by technology components, such as Database Server, Storage Server, InfiniBand Switch, and Cluster Wide.

Each section shows:

- Check status (`FAIL`, `WARNING`, `INFO`, or `PASS`)
- Type of check
- Check message
- Where the check was run
- Link to expand details for further findings and recommendation

Click **View** for more information about the compliance check results and the recommendations.

- What to do to solve the problem
- Where the recommendation applies
- Where the problem does not apply
- Links to relevant documentation or My Oracle Support notes
- Example of data on which the recommendation is based

Maximum Availability Architecture (MAA) Score Card

Maximum Availability Architecture (MAA) Score Card displays the recommendations for the software installed on your system.

The details include:

- Outage Type
- Status of the check
- Description of the problem

- Components found
- Host location
- Version of the components compared to the recommended version
- Status based on comparing the version found to the recommended version

Related Topics

- Understanding and Managing Reports and Output
  Oracle Orachk and Oracle Exachk generate a detailed HTML report with findings and recommendations.

3.1.1.4.3 Subsequent Email Notifications

For the subsequent compliance check runs after the first email notification, the daemon emails the summary of differences between the most recent runs.

Specify a list of comma-delimited email addresses in the `NOTIFICATION_EMAIL` option.

The email notification contains:

- System Health Score of this run compared to the previous run
- Summary of number of checks that were run and the differences between runs
- Most recent report result as attachment
- Previous report result as attachment
- Diff report as attachment

3.1.1.4.4 Generating a Diff Report

The diff report attached to the previous email notification shows a summary of differences between the most recent runs.

To identify the changes since the last run:

- Run the following command:

  ```
  $ orachk -diff report_1 report_2
  ```

  Review the diff report to see a baseline comparison of the two reports and then a list of differences.

Related Topics

- Comparing Two Reports
  Oracle Autonomous Health Framework automatically compare the two most recent HTML reports and generate a third diff report, when run in automated daemon mode.
- Managing the Report Output
  Use the list of commands to manage compliance checks report output.

3.1.1.5 Recommended On-Demand Usage

This section summarizes the scenarios that Oracle recommends running compliance checks on-demand.

Apart from scheduled compliance check runs, run compliance checks on-demand by running the following commands:

```
$ orachk
```

```
$ exachk
```

Oracle recommends that you run compliance checks in the following on-demand scenarios:

- Pre- or post-upgrades
- Machine relocations from one subnet to another
- Hardware failure or repair
- Problem troubleshooting
- In addition to go-live testing

While running pre- or post-upgrade checks, Oracle Autonomous Health Framework automatically detects the databases that are registered with Oracle Clusterware and presents the list of databases to check.

Run the pre-upgrade checks during the upgrade planning phase. Oracle Autonomous Health Framework prompts you for the version to which you are planning to upgrade:

```
$ orachk –u –o pre
```

```
$ exachk –u –o pre
```

After upgrading, run the post-upgrade checks:

```
$ orachk –u –o post
```

```
$ exachk –u –o post
```

Related Topics

- Running Compliance Checks On-Demand
  Usually, compliance checks run at scheduled intervals. However, Oracle recommends that you run compliance checks on-demand when needed.

3.1.1.6 Running Compliance Checks on a Remote Node

Run compliance checks on remote nodes using RSA/DSA SSH private and public keys.

1. Generate RSA/DSA SSH private and public keys on each of the remote nodes as `root` user.
2. Add the content of the above generated public key to the `authorized_keys` file for each of the remote nodes.

For example:

```
cat $HOME/.ssh/id_dsa.pub >> $HOME/.ssh/authorized_keys
```

3. Copy the private keys of all the remote nodes where you want to run the checks, for example, in the *PRIVATEKEYDIR* directory.
4. Rename each of the private keys as id_*encryption*.*remote_hostname*.*remote_user*.

   Where:

   - *remote_user* is the Linux user who created the key
   - *encryption* can be RSA/DSA
   - *remote_host* is the hostname (not FQDN) of the remote node

   For example:

   ```
   id_dsa.node1.root
   ```

   ```
   id_rsa.node2.oradb
   ```

Ensure that passwordless SSH between the local node and remote node is present. ssh -i id_*encryption*.*remote_host*.*remote_user* *remote_user*@*remote_host* must be able to log in to the *remote_host* without any password.

- Synchronous Remote Run
- Asynchronous Remote Run

3.1.1.6.1 Synchronous Remote Run

This is a blocking-call. Outputs the stdout of the remote run. User gets the prompt or control only when the remote run is completed. Once completed, the collection will be available at the working directory.

```
# orachk -remotehost remote_host remote_args -remoteuser remote_user -
remotedestdir remote_dest_dir -identitydir PRIVATEKEYDIR
```

```
# exachk -remotehost remote_host remote_args -remoteuser remote_user -
remotedestdir remote_dest_dir -identitydir PRIVATEKEYDIR
```

For example:

```
orachk -remotehost node2 -profile asm -remoteuser root -remotedestdir /
scratch/user/ -identitydir /scratch/user/privatekeys/
```

```
exachk -remotehost node1 -localonly -c X4-2,MAA -remoteuser oracle -
remotedestdir /scratch/user/ -identitydir /scratch/user/privatekeys/
```

```
$ orachk -remotehost node2 -profile asm -remoteuser root -remotedestdir /
scratch/user1/ -identitydir .privatekeys/

Starting orachk run on node2. For more detail about run check /scratch/user1/
orachkremote/orachk_node2_112818_040034_run.log

Clusterware stack is running from /scratch/app/11.2.0.4/grid. Is this the
correct Clusterware Home?[y/n][y]

Checking ssh user equivalency settings on all nodes in cluster for root
```

3.1.1.6.2 Asynchronous Remote Run

This is a non-blocking-call. Oracle Orachk and Oracle Exachk initiate the remote run, display a `_run.log` file, and give control to the user. Check the `_run.log` file to ensure the completion of the remote run. Once completed, the collection will be available at the working directory

```
# orachk -remotehost remote_host remote_args -remoteuser remote_user -
remotedestdir remote_dest_dir  -identitydir PRIVATEKEYDIR -asynch
```

```
# exachk -remotehost remote_host remote_args -remoteuser remote_user -
remotedestdir remote_dest_dir -identitydir PRIVATEKEYDIR -asynch
```

Where:

- *remote_host* is the host name of the remote node.
- *remote_args* are the arguments that needs to be passed to the Oracle Orachk and Oracle Exachk run in the remote node.
- *remote_user* is the remote user who runs Oracle Orachk and Oracle Exachk.
- *remote_dest_dir* is the remote directory where `orachk.zip` or `exachk.zip` is extracted.
- *PRIVATEKEYDIR* is the directory contains the private keys of the remote nodes in the specified format.

> **Note:**
>
> If you use DSA keys, then set the `RAT_SSH_ENCR` environment variable to `dsa` before running the Oracle Orachk and Oracle Exachk remote run commands.

For example:

```
orachk -remotehost node2 -remoteuser oradb -remotedestdir /scratch/
user/ -identitydir /scratch/user/privatekeys/ -asynch
```

```
exachk -remotehost node1 -cells node1 -c X4-2,MAA -remoteuser root -
remotedestdir /scratch/user/ -identitydir /scratch/user/privatekeys/ -
asynch
```

```
$ orachk -remotehost node2 -localonly -remoteuser root -
identitydir .privatekeys/ -asynch

Starting orachk run on node2. For more detail about run check /scratch/
user1/orachkremote/orachk_node2_112818_041037_run.log
```

Private key files

```
$ ls PRIVATEKEYDIR/
id_dsa.node1.oracle    id_dsa.node4.root    id_dsa.node6.oracle
id_dsa.node8.root    id_dsa.node11.oracle
id_dsa.node2.root      id_dsa.node5.oracle  id_dsa.node6.root
id_dsa.node9.root
id_dsa.node3.root      id_dsa.node5.root    id_dsa.node7.root
id_dsa.node10.oracle
```

3.1.1.7 Creating, Modifying, and Deleting User-Defined Profiles

Specify a comma-delimited list of check IDs to create and modify custom profiles.

Specify valid check IDs and descriptive unique profile name.

1. To create a profile:

   ```
   orachk -createprofile profile_name check_ids
   ```

   ```
   exachk -createprofile profile_name check_ids
   ```

   ```
   orachk -createprofile customprofile1
   E94AC6ACDA502F3BE04312C0E50A290A,
   F01E3FEDBD2B243EE04312C0E50A4DC5,
   F02293F7261D1BCAE04312C0E50A4118,
   F9370B4F5707076DE04312C0E50A78AE

   Validating checks...

   Profile customprofile1 created successfully...
   ```

   Oracle Orachk and Oracle Exachk validate profile names and check IDs before creating the profile and print appropriate messages if any discrepancies found.

Oracle Orachk and Oracle Exachk create the profiles only if the profile names are unique and check IDs are valid.

2. To modify a profile:

```
orachk -modifyprofile profile_name check_ids
```

```
exachk -modifyprofile profile_name check_ids
```

```
exachk -modifyprofile customprofile1 21B57D4065DDEA3DE0530D98EB0A8205,
39128FBB540C098AE0530D98EB0AFB1A,
9AD8AF3966FB3027E040E50A1EC0308F,
019F5085951978CAE05313C0E50A4FCB

Validating checks...

Modifying profile customprofile1...

Profile customprofile1 modified successfully...


Added Checks:
21B57D4065DDEA3DE0530D98EB0A8205
9AD8AF3966FB3027E040E50A1EC0308F
019F5085951978CAE05313C0E50A4FCB
--------------------------------
Removed Checks:
39128FBB540C098AE0530D98EB0AFB1A
```

You cannot modify the profile name. You can only add to or remove check IDs form the profile.
If the check IDs are in the profile, then Oracle Orachk and Oracle Exachk remove them from the profile.

If the check IDs are not in the profile, then Oracle Orachk and Oracle Exachk add them to the profile.

3. To delete a profile:

```
orachk -deleteprofile profile_name
```

```
exachk -deleteprofile profile_name
```

```
orachk -deleteprofile customprofile1

Deleting profile customprofile1...

Profile customprofile1 deleted successfully...
```

Oracle Orachk and Oracle Exachk delete the profile by removing the profile entry ID from the `profiles.dat` file, and deleting the corresponding `profiles.prf` file.

3.1.1.8 Sanitizing Sensitive Information in the Diagnostic Collections

Oracle Autonomous Health Framework uses Adaptive Classification and Redaction (ACR) to sanitize sensitive data.

> **Note:**
>
> The `-sanitize` parameter has been deprecated and removed in 23.3. Oracle recommends using the `ahfctl redact` command instead.

After collecting copies of diagnostic data, Oracle Orachk and Oracle Exachk use Adaptive Classification and Redaction (ACR) to sanitize sensitive data in the collections. ACR uses a machine learning based engine to redact a pre-defined set of entity types in a given set of files. ACR also sanitizes or masks entities that occur in path names.

- Sanitization replaces a sensitive value with random characters.
- Masking replaces a sensitive value with a series of asterisks ("*").

ACR currently sanitizes the following entity types:

- Host names
- IP addresses
- MAC addresses
- Oracle Database names
- Tablespace names
- Service names
- Ports
- Operating system user names

ACR also masks Personally Identifiable Information (PII), that is, user data from the database appearing in block and redo dumps. There is no separate command for it.

To sanitize sensitive information:

```
orachk -sanitize comma_delimited_list_of_collection_IDs
```

or

```
exachk -sanitize comma_delimited_list_of_collection_IDs
```

Block dumps before redaction:

```
14A533F40 00000000 00000000 00000000 002C0000 [...............,.]
14A533F50 35360C02 30352E30 31322E37 380C3938 [..650.507.2189.8]
14A533F60 31203433 37203332 2C303133 360C0200 [34 123 7310,...6]
```

Block dumps after redaction:

```
14A533F40 ******** ******** ******** ******** [****************]
14A533F50 ******** ******** ******** ******** [****************]
14A533F60 ******** ******** ******** ******** [****************]
```

Redo dumps before redaction:

```
col 74: [ 1] 80
col 75: [ 5] c4 0b 19 01 1f
col 76: [ 7] 78 77 06 16 0c 2f 26
```

Redo dumps after redaction:

```
col 74: [ 1] **
col 75: [ 5] ** ** ** ** **
col 76: [ 7] ** ** ** ** ** ** **
```

To print the reverse map of sanitized elements:

```
orachk -rmap all|comma_delimited_list_of_element_IDs
```

or

```
exachk -rmap all|comma_delimited_list_of_element_IDs
```

Sanitizing Sensitive Information in Oracle Orachk or Oracle Exachk Output

> **Note:**
>
> The `-sanitize` parameter has been deprecated and removed in 23.3. Oracle recommends using the `ahfctl redact` command instead.

1. If you specify a file name that does not follow the naming convention:

   For example:

   ```
   $ orachk -sanitize orachk_invalid.html
   /scratch/testuser/may31/orachk_invalid.html is not a valid orachk
   collection
   ```

2. If you specify a file that does not exist:

   For example:

   ```
   $ orachk -sanitize /tmp/orachk_invalid.html
   /tmp/orachk_invalid.html does not exist
   ```

3. If you sanitize a file that exists with valid Oracle Autonomous Health Framework naming convention, but the file is not generated by Oracle Autonomous Health Framework:

   For example:

   ```
   $ orachk -sanitize orachk_invalidcollection.zip
   orachk is sanitizing /scratch/testuser/may31/
   orachk_invalidcollection.zip. Please
   wait...
   ACR error occurred while sanitizing orachk collection
   ```

4. To sanitize a file with relative path:

   For example:

   ```
   $ orachk -sanitize new/orachk_node061919_053119_001343.zip
   orachk is sanitizing
   /scratch/testuser/may31/new/orachk_node061919_053119_001343.zip.
   Please wait...

   Sanitized collection is:
   /scratch/testuser/may31/orachk_aydv061919_053119_001343.zip


   $ orachk -sanitize .orachk_node061919_053119_001343.zip
   orachk is sanitizing
   /scratch/testuser/may31/.orachk_node061919_053119_001343.zip.
   Please wait...

   Sanitized collection is:
   /scratch/testuser/may31/orachk_aydv061919_053119_001343.zip
   ```

5. To sanitize Oracle Autonomous Health Framework debug log:

   For example:

   ```
   $ orachk -sanitize new/orachk_debug_053119_023653.log
   orachk is sanitizing /scratch/testuser/may31/new/
   orachk_debug_053119_023653.log.
   Please wait...

   Sanitized collection is: /scratch/testuser/may31/
   orachk_debug_053119_023653.log
   ```

6. To run full sanity check:

   For example:

   ```
   $ orachk -localonly -profile asm -sanitize -silentforce

   Detailed report (html) -
   /scratch/testuser/may31/orachk_node061919_053119_04448/
   orachk_node061919_053119_04448.html

   orachk is sanitizing /scratch/testuser/may31/
   ```

```
orachk_node061919_053119_04448.
Please wait...

Sanitized collection is: /scratch/testuser/may31/
orachk_aydv061919_053119_04448

UPLOAD [if required] - /scratch/testuser/may31/
orachk_node061919_053119_04448.zip
```

7. To print the reverse map of sanitized elements:

   For example:

```
orachk -rmap pu406jKxg,kEvGFDT
_____________________________________________________________________________
______
| Entity Type | Substituted Entity Name | Original Entity Name |
_____________________________________________________________________________
______
| dbname      | XTT_MANUR                | ASM_POWER             |
| dbname      | fcb63u2                  | rac12c2               |
_____________________________________________________________________________
______


orachk -rmap all
```

Setting up Staging Server for Adaptive Classification and Redaction (ACR)

Adaptive Classification and Redaction (ACR) is a CPU intensive task as it examines data in each file to redact sensitive entities. ACR spawns multiple processes to redact the files across these processes. Whenever an ACR process is scheduled on a CPU, it may utilise the CPU fully (can reach ~100% CPU utilisation). But, since ACR does not run at an elevated priority, it does not starve other processes on the system. However, since ACR is sharing the resources with other processes running on the production environment, it can affect those processes. Hence, to not affect the processes and applications on the production environment, it is recommended to set up a staging server dedicated for redacting the collections using ACR.

For more information about setting up staging server for Adaptive Classification and Redaction (ACR), see My Oracle Support note 2882798.1.

Related Topics

- https://support.oracle.com/rs?type=doc&id=2882798.1

3.1.1.9 Problem Repair Automation Options

Starting in release 19.3, Oracle Orachk and Oracle Exachk have the capability to automatically fix problems when found.

Certain checks have a repair command associated with them. To see what the repair command actually does, run the `-showrepair` command.

```
orachk -showrepair check_id
```

```
exachk -showrepair check_id
```

To run the repair commands include one of the following options:

```
orachk -repair all
```

```
orachk -repair check_id,[check_id,check_id...]
```

```
orachk -repair file
```

```
exachk -repair all
```

```
exachk -repair check_id,[check_id,check_id...]
```

```
exachk -repair file
```

- *check_id*: Refers to specific checks that you want to repair. Specify a check ID or a list of comma-delimited list of check IDs.
- *file*: A text file that contains a list of check IDs. Add one check ID per line.
  For example:

  ```
  check ID1
  check ID2
  check IDn
  ```

3.1.1.10 Integration of Oracle DBSAT into Oracle Autonomous Health Framework

DBSAT is a lightweight utility that will not impair system performance in a measurable way.

The Oracle Database Security Assessment Tool (Oracle DBSAT):

- Analyzes database configurations
- Users and their entitlements
- Security policies
- Identifies where sensitive data resides to uncover security risks (not executed in Oracle Autonomous Health Framework)

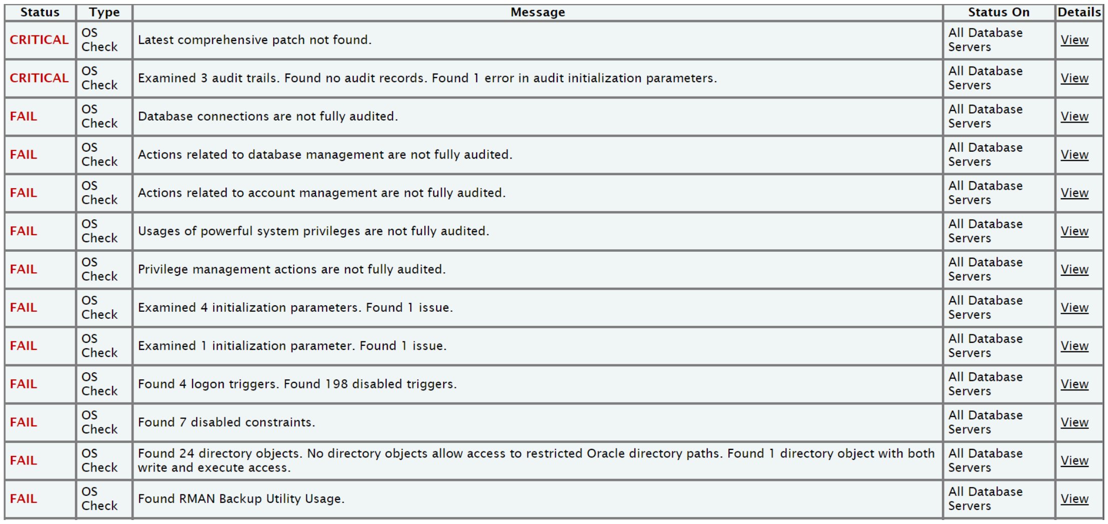
- Improves the security posture of Oracle Databases within your organization

Oracle Autonomous Health Framework always includes the latest DBSAT and runs DBSAT on all databases if you use the `-security` profile. For example, `# orachk -profile security`.

You can use Oracle DBSAT report findings to:

- Fix immediate short-term risks
- Implement a comprehensive security strategy
- Support your regulatory compliance program
- Promote security best practices

Figure 3-1 Oracle Database Security Assessment Report



Status	Type	Message	Status On	Details
CRITICAL	OS Check	Latest comprehensive patch not found.	All Database Servers	View
CRITICAL	OS Check	Examined 3 audit trails. Found no audit records. Found 1 error in audit initialization parameters.	All Database Servers	View
FAIL	OS Check	Database connections are not fully audited.	All Database Servers	View
FAIL	OS Check	Actions related to database management are not fully audited.	All Database Servers	View
FAIL	OS Check	Actions related to account management are not fully audited.	All Database Servers	View
FAIL	OS Check	Usages of powerful system privileges are not fully audited.	All Database Servers	View
FAIL	OS Check	Privilege management actions are not fully audited.	All Database Servers	View
FAIL	OS Check	Examined 4 initialization parameters. Found 1 issue.	All Database Servers	View
FAIL	OS Check	Examined 1 initialization parameter. Found 1 issue.	All Database Servers	View
FAIL	OS Check	Found 4 logon triggers. Found 198 disabled triggers.	All Database Servers	View
FAIL	OS Check	Found 7 disabled constraints.	All Database Servers	View
FAIL	OS Check	Found 24 directory objects. No directory objects allow access to restricted Oracle directory paths. Found 1 directory object with both write and execute access.	All Database Servers	View
FAIL	OS Check	Found RMAN Backup Utility Usage.	All Database Servers	View

For more information, see *Oracle Database Security Assessment Report*.

Related Topics

- Oracle Database Security Assessment Report

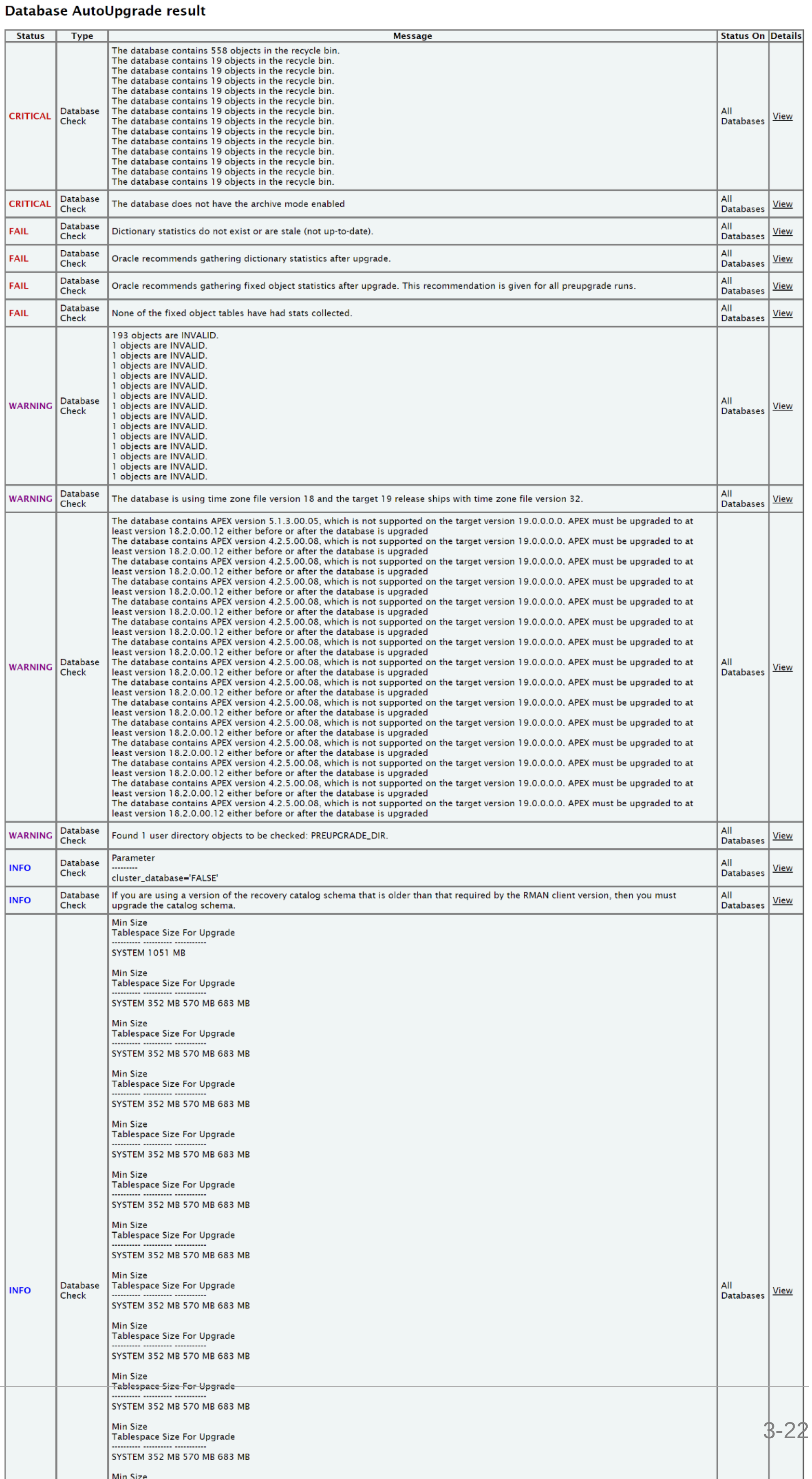
3.1.1.11 Integration of AutoUpgrade utility into Oracle Autonomous Health Framework

The `AutoUpgrade` utility identifies issues before upgrades, performs pre- and postupgrade actions, deploys upgrades, performs postupgrade actions, and starts the upgraded Oracle Database.

Before the upgrade, in Analyze mode, the `AutoUpgrade` utility performs read-only analysis of databases before upgrade, so that it can identify issues that require fixing.

When you run Oracle Orachk in pre-upgrade mode, Oracle Orachk in turn runs the `AutoUpgrade` utility to check if each database is ready to upgrade or not.

Figure 3-2   Database AutoUpgrade Result



Database AutoUpgrade result

Status	Type	Message	Status On	Details
CRITICAL	Database Check	The database contains 558 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin. The database contains 19 objects in the recycle bin.	All Databases	View
CRITICAL	Database Check	The database does not have the archive mode enabled	All Databases	View
FAIL	Database Check	Dictionary statistics do not exist or are stale (not up-to-date).	All Databases	View
FAIL	Database Check	Oracle recommends gathering dictionary statistics after upgrade.	All Databases	View
FAIL	Database Check	Oracle recommends gathering fixed object statistics after upgrade. This recommendation is given for all preupgrade runs.	All Databases	View
FAIL	Database Check	None of the fixed object tables have had stats collected.	All Databases	View
WARNING	Database Check	193 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID. 1 objects are INVALID.	All Databases	View
WARNING	Database Check	The database is using time zone file version 18 and the target 19 release ships with time zone file version 32.	All Databases	View
WARNING	Database Check	The database contains APEX version 5.1.3.00.05, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded The database contains APEX version 4.2.5.00.08, which is not supported on the target version 19.0.0.0.0. APEX must be upgraded to at least version 18.2.0.00.12 either before or after the database is upgraded	All Databases	View
WARNING	Database Check	Found 1 user directory objects to be checked: PREUPGRADE_DIR.	All Databases	View
INFO	Database Check	Parameter --------- cluster_database='FALSE'	All Databases	View
INFO	Database Check	If you are using a version of the recovery catalog schema that is older than that required by the RMAN client version, then you must upgrade the catalog schema.	All Databases	View
INFO	Database Check	Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 1051 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size Tablespace Size For Upgrade ---------- ---------- ----------- SYSTEM 352 MB 570 MB 683 MB Min Size	All Databases	View

For more information, see *Using AutoUpgrade for Oracle Database Upgrades*.

Related Topics

- Using AutoUpgrade for Oracle Database Upgrades

3.1.2 Running Compliance Checks Automatically

Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.

> **Note:**
>
> Daemon mode is supported only on the Linux and Solaris operating systems.

Configure the daemon to:

- Schedule recurring compliance checks at regular interval
- Send email notifications when the compliance check runs complete, clearly showing any differences since the last run
- Purge collection results after a pre-determined period
- Check and send email notification about stale passwords
- Store multiple profiles for automated compliance check runs
- Restart automatically if the *server* or *node* where it is running restarts

> **Note:**
>
> While running, the daemon answers all the prompts required by subsequent on-demand compliance checks.
>
> To run on-demand compliance checks, do not use the daemon process started by others. Run on-demand compliance checks within the same directory where you have started the daemon.

If you change the system configuration such as adding or removing *servers* or *nodes*, then restart the daemon.

- Setting and Getting Options for the Daemon
  Set the daemon options before you start the daemon. Reset the daemon options anytime after starting the daemon.
- Starting and Stopping the Daemon
  Start and stop the daemon and force the daemon to stop a compliance check run.
- Querying the Status and Next Planned Daemon Run
  Query the status and next automatic run schedule of the running daemon.
- Configuring the Daemon for Automatic Start
  Installing Oracle Autonomous Health Framework as `root` on Linux or Solaris automatically sets up and runs the Oracle Orachk or Oracle Exachk daemon.

- Configuring the Daemon for Automatic Restart
  By default, you must manually restart the daemon if you restart the *server* or *node* on which the daemon is running.

Related Topics

- Starting and Stopping the Daemon
  Start and stop the daemon and force the daemon to stop a compliance check run.
- Querying the Status and Next Planned Daemon Run
  Query the status and next automatic run schedule of the running daemon.
- Configuring the Daemon for Automatic Restart
  By default, you must manually restart the daemon if you restart the *server* or *node* on which the daemon is running.

Related Topics

- Running Compliance Checks On-Demand
  Usually, compliance checks run at scheduled intervals. However, Oracle recommends that you run compliance checks on-demand when needed.

3.1.2.1 Setting and Getting Options for the Daemon

Set the daemon options before you start the daemon. Reset the daemon options anytime after starting the daemon.

To set the daemon options:

Set the daemon options using the `-set` option.

Set an option as follows:

```
$ orachk -set "option_1=option_1_value"
```

```
$ exachk -set "option_1=option_1_value"
```

Set multiple options using the *name=value* format separated by semicolons as follows:

```
$ orachk -set
"option_1=option_1_value;option_2=option_2_value;option_n=option_n_valu
e"
```

```
$ exachk -set
"option_1=option_1_value;option_2=option_2_value;option_n=option_n_valu
e"
```

- AUTORUN_SCHEDULE
  Schedule recurring compliance check runs using the `AUTORUN_SCHEDULE` daemon option.
- AUTORUN_FLAGS
  The `AUTORUN_FLAGS` daemon option determines how compliance checks are run.

- NOTIFICATION_EMAIL
  Set the `NOTIFICATION_EMAIL` daemon option to send email notifications to the recipients you specify.
- collection_retention
  Set the `collection_retention` daemon option to purge health check collection results that are older than a specified number of days.
- PASSWORD_CHECK_INTERVAL
  The `PASSWORD_CHECK_INTERVAL` daemon option defines the frequency, in hours, for the daemon to validate the passwords entered when the daemon was started the first time.
- Setting Multiple Option Profiles for the Daemon
  Use only one daemon process for each server. Do not start a single daemon on multiple databases in a cluster, or multiple daemons on the same database.
- Getting Existing Options for the Daemon
  Query the values that you set for the daemon options.

Related Topics

- Controlling the Behavior of the Daemon
  Use the list of commands to control the behavior of the daemon.

3.1.2.1.1 AUTORUN_SCHEDULE

Schedule recurring compliance check runs using the `AUTORUN_SCHEDULE` daemon option.

To schedule recurring compliance check runs:

Set the `AUTORUN_SCHEDULE` option, as follows:

```
AUTORUN_SCHEDULE=minute hour day month day_of_week
```

Where:

- *`minute`*

  Valid values: 0-59 (Optional. If omitted, then 0 is used)

  Allowed special characters: * , - /
- *`hour`* is 0–23

  Valid values: 0–23

  Allowed special characters: * , - /
- *`day`*

  Valid values: 1–31

  Allowed special characters: * , -
- *`month`*

  Valid values: 1–12 or JAN–DEC

  Allowed special characters: * , -
- *`day_of_week`*

  Valid values: 0–6 or SUN–SAT

Allowed special characters: * , -

Asterisk (*): Use the asterisk (*) as a wildcard to specify multiple values separated by commas.

Comma (,): Use commas to separate items of a list. For example, using "MON,WED,FRI" in the 5th field (day of week) means Mondays, Wednesdays and Fridays.

Dash (-): Use dash to define ranges.

Slash (/): Use slashes combined with ranges to specify step values. For example, */5 in the minutes field indicates every 5 minutes (see note below about frequencies). It is shorthand for the more verbose form 5,10,15,20,25,30,35,40,45,50,55,00.

> **Note:**
>
> Frequencies, in general, cannot be expressed; only step values, which evenly divide their range express accurate frequencies.
>
> - **For minutes:** /2, /3, /4, /5, /6, /10, /12, /15, /20 and /30 because 60 is evenly divisible by those numbers
> - **For hours:** /2, /3, /4, /6, /8 and /12

Table 3-1   AUTORUN_SCHEDULE

Example	Result
`"AUTORUN_SCHEDULE=0,15,30,45 * * * *"`	Runs every 15 minutes.
`"AUTORUN_SCHEDULE=* * * *"`	Runs every hour.
`"AUTORUN_SCHEDULE=3 * * 0"`	Runs at 3 AM every Sunday.
`"AUTORUN_SCHEDULE=2 * * 1, 3, 5"`	Runs at 2 AM on Monday, Wednesday, and Friday.
`"AUTORUN_SCHEDULE=4 1 * *"`	Runs at 4 AM on the first day of every month.
`"AUTORUN_SCHEDULE=8,20 * * 1, 2, 3, 4, 5"`	Runs at 8 AM and 8 PM every Monday, Tuesday, Wednesday, Thursday, and Friday.
`"AUTORUN_SCHEDULE=*/5 2-4 * JAN 2"`	Runs every 5 minutes at 2,3,4 AM every Tuesday in the month of January.
`"AUTORUN_SCHEDULE=*/1 * * * *"`	Runs every minute.
`"AUTORUN_SCHEDULE=*/5 0-7 * 8 *"`	Runs every 5 minutes at 12,1,2,3,4,5,6,7 AM every day in the month of August.

Example 3-2 AUTORUN_SCHEDULE

```
$ orachk -set "AUTORUN_SCHEDULE=3 * * 0"
```

```
$ exachk -set "AUTORUN_SCHEDULE=3 * * 0"
```

Optionally, you can specify the name of the profile. If you do not specify, then `id=DEFAULT`.

For example:

```
$ orachk -id dba -set "AUTORUN_SCHEDULE=3 * * 0"
```

```
$ exachk -id dba -set "AUTORUN_SCHEDULE=3 * * 0"
```

3.1.2.1.2 AUTORUN_FLAGS

The `AUTORUN_FLAGS` daemon option determines how compliance checks are run.

To configure how compliance checks should run:

Set the `AUTORUN_FLAGS` option as follows:

```
AUTORUN_FLAGS=flags
```

Where:

- *flags* can be any combination of valid command-line flags.

Table 3-2 AUTORUN_FLAGS

Example	Result
`"AUTORUN_FLAGS=-profile dba"`	Runs only the `dba` profile checks.
`"AUTORUN_FLAGS=-profile sysadmin -tag syadmin"`	Runs only the `dba` profile checks and tags the output with the value `sysadmin`.
`-excludeprofile ebs`	Runs all checks except the checks in the `ebs` profile.

Example 3-3 AUTORUN_FLAGS

```
$ orachk -set "AUTORUN_FLAGS=-profile sysadmin -tag sysadmin"
```

```
$ exachk -set "AUTORUN_FLAGS=-profile sysadmin -tag sysadmin"
```

3.1.2.1.3 NOTIFICATION_EMAIL

Set the `NOTIFICATION_EMAIL` daemon option to send email notifications to the recipients you specify.

The daemon notifies the recipients each time a health check run completes or when the daemon experiences a problem.

To configure email notifications:

1. Specify a comma-delimited list of email addresses, as follows:

   ```
   $ orachk -set
   "NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany
   .com"
   ```

   ```
   $ exachk -set
   "NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany
   .com"
   ```

   Optionally, you can specify the name of the profile. If you do not specify, then `id=DEFAULT`.

   For example:

   ```
   $ orachk -id dba -set
   "NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany
   .com"
   ```

   ```
   $ exachk -id dba -set
   "NOTIFICATION_EMAIL=some.person@acompany.com,another.person@acompany
   .com"
   ```

2. Test the email notification configuration using the `-testemail` option, as follows:

   ```
   $ orachk -testemail all
   ```

   ```
   $ exachk -testemail all
   ```

After the first health check run, the daemon notifies the recipients with report output attached.

For the subsequent health check runs after the first email notification, the daemon emails the summary of differences between the most recent runs to all recipients specified in the `NOTIFICATION_EMAIL` list.

Related Topics

- PASSWORD_CHECK_INTERVAL
  The PASSWORD_CHECK_INTERVAL daemon option defines the frequency, in hours, for the daemon to validate the passwords entered when the daemon was started the first time.

3.1.2.1.4 collection_retention

Set the collection_retention daemon option to purge health check collection results that are older than a specified number of days.

To configure collection retention period:

1. Set the collection_retention option for automatic retention or the user_collection_retention option for on-demand retention, as follows:

   ```
   collection_retention=number_of_days
   ```

   ```
   user_collection_retention=number_of_days
   ```

   If you do not set this option, then the daemon does not purge the stale collections.
2. Set the collection_retention or user_collection_retention option to an appropriate number of days based on:
   - Frequency of your scheduled collections
   - Size of the collection results
   - Available disk space

For example:

```
$ orachk -set "collection_retention=60"
```

```
$ exachk -set "collection_retention=60"
```

```
$ orachk -set "user_collection_retention=60"
```

```
$ exachk -set "user_collection_retention=60"
```

To Control Collection Retention Using Size

Set the size in MB using the environment variable RAT_PURGE_SIZE. When the health check collections consume the size specified, then Oracle Orachk starts purging the old collections, and retains the space specified using RAT_PURGE_SIZE.

For example:

```
$export RAT_PURGE_SIZE=4096
```

3.1.2.1.5 PASSWORD_CHECK_INTERVAL

The `PASSWORD_CHECK_INTERVAL` daemon option defines the frequency, in hours, for the daemon to validate the passwords entered when the daemon was started the first time.

If an invalid password is found due to a password change, then the daemon stops, makes an entry in the daemon log, and then sends an email notification message to the recipients specified in the `NOTIFICATION_EMAIL` option.

To configure password validation frequency:

1. Set the `PASSWORD_CHECK_INTERVAL` option, as follows:

   ```
   PASSWORD_CHECK_INTERVAL=number_of_hours
   ```

   If you do not set the `PASSWORD_CHECK_INTERVAL` option, then the daemon cannot actively check password validity and fails the next time the daemon tries to run after a password change. Using the `PASSWORD_CHECK_INTERVAL` option enables you to take corrective action and restart the daemon with the correct password rather than having failed collections.
2. Set the `PASSWORD_CHECK_INTERVAL` option to an appropriate number of hours based on:
   - Frequency of your scheduled collections
   - Password change policies

For example:

```
$ orachk -set "PASSWORD_CHECK_INTERVAL=1"
```

```
$ exachk -set "PASSWORD_CHECK_INTERVAL=1"
```

Related Topics

- NOTIFICATION_EMAIL
  Set the `NOTIFICATION_EMAIL` daemon option to send email notifications to the recipients you specify.

3.1.2.1.6 Setting Multiple Option Profiles for the Daemon

Use only one daemon process for each server. Do not start a single daemon on multiple databases in a cluster, or multiple daemons on the same database.

The daemon does not start, if the daemon detects another Oracle Autonomous Health Framework daemon process running locally.

Define multiple different run profiles using the same daemon. Defining multiple different run profiles enables you to run multiple different compliance checks with different daemon options, such as different schedules, email notifications, and automatic run flags. The daemon manages all profiles.

Define daemon option profiles using the `-id id` option before the `-set` option, where *id* is the name of the profile.

```
$ orachk -id id -set "option=value"
```

```
$ exachk -id id -set "option=value"
```

To set multiple option profiles for the daemon:

For example, if the database administrator wants to run checks within the `dba` profile and the system administrator wants to run checks in the `sysadmin` profile, then configure the daemon using the profiles option.

1. Define the database administrator profile as follows:

```
$ orachk -id dba -set "NOTIFICATION_EMAIL=dba@example.com;\
   AUTORUN_SCHEDULE=4,8,12,16,20 * * *;AUTORUN_FLAGS=-profile dba -tag
dba;\
   collection_retention=30"

Created notification_email for ID[dba]
Created autorun_schedule for ID[dba]
Created autorun_flags for ID[dba]
Created collection_retention for ID[dba]
```

```
$ exachk -id dba -set "NOTIFICATION_EMAIL=dba@example.com;\
   AUTORUN_SCHEDULE=4,8,12,16,20 * * *; AUTORUN_FLAGS=-profile dba -tag
dba;\
   collection_retention=30"

Created notification_email for ID[dba]
Created autorun_schedule for ID[dba]
Created autorun_flags for ID[dba]
Created collection_retention for ID[dba]
```

2. Define the system administrator profile as follows:

```
$ orachk -id sysadmin -set "NOTIFICATION_EMAIL=sysadmin@example.com;\
   AUTORUN_SCHEDULE=3 * * 1,3,5; AUTORUN_FLAGS=-profile sysadmin -tag
sysadmin;\
   collection_retention=60"

Created notification_email for ID[sysadmin]
Created autorun_schedule for ID[sysadmin]
Created autorun_flags for ID[sysadmin]
Created collection_retention for ID[sysadmin]
```

```
$ exachk -id sysadmin -set "NOTIFICATION_EMAIL=sysadmin@example.com;\
   AUTORUN_SCHEDULE=3 * * 1,3,5; AUTORUN_FLAGS=-profile sysadmin -tag
sysadmin;\
   collection_retention=60"
```

```
Created notification_email for ID[sysadmin]
Created autorun_schedule for ID[sysadmin]
Created autorun_flags for ID[sysadmin]
Created collection_retention for ID[sysadmin]
```

Related Topics

- Controlling the Behavior of the Daemon
  Use the list of commands to control the behavior of the daemon.

3.1.2.1.7 Getting Existing Options for the Daemon

Query the values that you set for the daemon options.

To query the values, use `[-id` *`ID`*`] -get` *`option`* `|` *`all`*.

Where:

- *`ID`* is a daemon option profile.
- *`option`* is a specific daemon option you want to retrieve.
- *`all`* returns values of all options.

To get existing options for the daemon:

1. To get a specific daemon option: `-get` *`option`*

```
$ orachk -get NOTIFICATION_EMAIL

ID: orachk.default
------------------------------------------
notification_email = some.body@example.com


$ exachk -get NOTIFICATION_EMAIL

ID: exachk.default
------------------------------------------
notification_email = some.body@example.com
```

2. To query multiple daemon option profiles: `-get` *`option`*:

```
$ orachk -get NOTIFICATION_EMAIL

ID: orachk.default
------------------------------------------
notification_email = some.body@example.com

ID: dba
------------------------------------------
notification_email = dba@example.com

ID: sysadmin
```

```
------------------------------------------
notification_email = sysadmin@example.com


$ exachk -get NOTIFICATION_EMAIL

ID: exachk.default
------------------------------------------
notification_email = some.person@example.com

ID: dba
------------------------------------------
notification_email = dba@example.com

ID: sysadmin
------------------------------------------
notification_email = sysadmin@example.com
```

3. To limit the request to a specific daemon option profile: `-id` *`ID`* `-get` *`option`*

   To get the `NOTIFICATION_EMAIL` for a daemon profile called `dba`:

```
$ orachk -id dba -get NOTIFICATION_EMAIL

ID: dba
------------------------------------------
notification_email = dba@example.com


$ exachk -id dba -get NOTIFICATION_EMAIL

ID: dba
------------------------------------------
notification_email = dba@example.com
```

4. To get all options set: `-get all`

```
$ orachk -get all

ID: orachk.default
------------------------------------------
notification_email = some.body@example.com
autorun_schedule = 3 * * 0
collection_retention = 30
password_check_interval = 1


$ exachk -get all

ID: exachk.default
------------------------------------------
notification_email = some.body@example.com
autorun_schedule = 3 * * 0
```

```
collection_retention = 30
password_check_interval = 1
```

5. To query all daemon option profiles: `-get all`

```
$ orachk -get all

ID: orachk.default
------------------------------------------
notification_email = some.body@example.com
autorun_schedule = 3 * * 0
collection_retention = 30
password_check_interval = 12

ID: dba
------------------------------------------
notification_email = dba@example.com
autorun_schedule = 4,8,12,16,20 * * *
autorun_flags = -profile dba -tag dba
collection_retention = 30
password_check_interval = 1

ID: sysadmin
------------------------------------------
notification_email = sysadmin@example.com
autorun_schedule = 3 * * 1,3,5
autorun_flags = -profile sysadmin -tag sysadmin
collection_retension = 60
password_check_interval = 1


$ exachk -get all

ID: exachk.default
------------------------------------------
notification_email = some.body@example.com
autorun_schedule = 3 * * 0
collection_retention = 30
password_check_interval = 1

ID: dba
------------------------------------------
notification_email = dba@example.com
autorun_schedule = 4,8,12,16,20 * * *
autorun_flags = -profile dba -tag dba
collection_retention = 30
password_check_interval = 1

ID: sysadmin
------------------------------------------
notification_email = sysadmin@example.com
autorun_schedule = 3 * * 1,3,5
autorun_flags = -profile sysadmin -tag sysadmin
```

```
collection_retension = 60
password_check_interval = 1
```

6. To limit the request to a specific daemon option profile: `-id` *`ID`* `-get all`

   To get all the options set for a daemon profile called `dba`:

   ```
   $ orachk -id dba -get all

   ID: dba
   ------------------------------------------
   notification_email = dba@example.com
   autorun_schedule = 4,8,12,16,20 * * *
   autorun_flags = -profile dba -tag dba
   collection_retention = 30
   password_check_interval = 1
   ```

   ```
   $ exachk -id dba -get all

   ID: dba
   ------------------------------------------
   notification_email = dba@example.com
   autorun_schedule = 4,8,12,16,20 * * *
   autorun_flags = -profile dba -tag dba
   collection_retention = 30
   password_check_interval = 1
   ```

3.1.2.2 Starting and Stopping the Daemon

Start and stop the daemon and force the daemon to stop a compliance check run.

To start and stop the daemon:

1. To start the daemon:

   ```
   $ orachk -autostart
   ```

   ```
   $ orachk -autostart reset
   ```

   ```
   $ exachk -autostart
   ```

   ```
   $ exachk -autostart reset
   ```

   The tools prompt you to provide required information during startup.

2. To stop the daemon:

   ```
   $ orachk -autostop
   ```

   ```
   $ orachk -autostop unset
   ```

   ```
   $ exachk -autostop
   ```

   ```
   $ exachk -autostop unset
   ```

   If a compliance check run is progress when you run the stop command, then the daemon indicates so and continues running.

3. To force the daemon to stop a compliance check run:

   ```
   $ orachk -autostop
   ```

   ```
   $ orachk -autostop unset
   ```

   ```
   $ exachk -autostop
   ```

   ```
   $ exachk -autostop unset
   ```

The daemon stops the compliance check run and then confirms when it is done. If necessary, then stop the daemon using the `-autostop` option.

The window allows to setup a value to randomize the execution hour and minute to be set for each daemon schedule. By default, `exachk` sets 2:03 AM for `exatier` profile entry, and 3:03 AM for full run entry.

Regarding the hour, when using the window, if you setup `autostart` with a window of 5, and considering `exachk` uses 2 AM as default hour, that means that `exachk` will pick a value between 2AM +/-5 hours, that is, any hour between 9 PM and 7 AM. If the `autostart` window is 1, then hour value could be 1 AM, 2 AM, or 3 AM.

Regarding the minute, when using `autorun` window, the minute will be a randomized value between 0 and 59.

Note that the window applies only to the action of setting up the entry. It is not meant as a window applied for every time the scheduled entry runs. If the entry is setup to run at, let's say, 4:15 AM, then it will run at that time the days scheduled.

Use cases:

1. **Using the `RAT_AUTORUN_WINDOW` variable from the environment before installing AHF**

When AHF is installed running the `ahf_setup` file, if the `RAT_AUTORUN_WINDOW` is set, then `exachk` scheduler will pick `RAT_AUTORUN_WINDOW` value and apply the window to the `exachk` scheduler entries.

```
# export RAT_AUTORUN_WINDOW=5
#  ./ahf_setup -ahf_loc /opt/oracle.ahf -data_dir /opt/oracle.ahf -
silent
# orachk -get all
------------------------------------------------------------
ID: orachk.autostart_client_oratier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile oratier1 -dball -showpass -tag
autostart_client_oratier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  20 1 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
ID: orachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  15 3 * * 0
------------------------------------------------------------


# export RAT_AUTORUN_WINDOW=5
# ./ahf_setup -ahf_loc /opt/oracle.ahf -data_dir /opt/oracle.ahf -
silent
# exachk -get all
------------------------------------------------------------
ID: exachk.autostart_client_exatier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile exatier1 -dball -showpass -tag
autostart_client_exatier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  20 1 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
ID: exachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  15 3 * * 0
------------------------------------------------------------
```

As seen above, the hour values belong to the window, and the minute value is a random value between 0 and 59.

2. **Using the `-autorun_window` *`<value>`* option while installing AHF**
   The `-autorun_window` can be specified as an option when running `ahf_setup`.

```
# ./ahf_setup -ahf_loc /opt/oracle.ahf -data_dir /opt/oracle.ahf -silent -
autorun_window 5
# orachk -get all
```

```
------------------------------------------------------------
ID: orachk.autostart_client_oratier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile oratier1 -dball -showpass -
tag autostart_client_oratier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  24 6 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
ID: orachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  29 6 * * 0
------------------------------------------------------------
```

```
# ./ahf_setup -ahf_loc /opt/oracle.ahf -data_dir /opt/oracle.ahf -
silent -autorun_window 5
# exachk -get all
------------------------------------------------------------
ID: exachk.autostart_client_exatier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile exatier1 -dball -showpass -
tag autostart_client_exatier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  24 6 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
ID: exachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  29 6 * * 0
------------------------------------------------------------
```

> **Note:**
>
> If `RAT_AUTORUN_WINDOW` is defined, and `-autorun_window` is passed, then the `-autorun_window` command-line option has more priority and the environment variable value will be ignored.

When the RAT variable is set at install time, it will be stored automatically on the `orachk` and `exachk` environment file:

```
# cat `orachk -showenvfile`
RAT_AUTORUN_WINDOW=5


# cat `exachk -showenvfile`
RAT_AUTORUN_WINDOW=5
```

So the subsequent `autostop` and `autostart` commands will make use of the existent variable value in the environment file (when defined). Entry can be manually deleted from the file anytime.

3. **Using the existing `RAT_AUTORUN_WINDOW` value defined in `orachk`/`exachk` environment file**
   As mentioned above, if the value exists in the environment file, then an `autostart` command will automatically read the value and apply the window:

```
# orachk -autostart
.
.
Applying execution time window of (+/-) 5 hours
Applying execution time window of (+/-) 5 hours
Successfully copied Daemon Store to Remote Nodes
.  .  .
orachk is using TFA Scheduler. TFA PID: 3964931

# orachk -get all
------------------------------------------------------------
ID: orachk.autostart_client_oratier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile oratier1 -dball -showpass -tag
autostart_client_oratier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  42 23 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
ID: orachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  31 0 * * 0
------------------------------------------------------------


>># exachk -autostart
.
.
Applying execution time window of (+/-) 5 hours
Applying execution time window of (+/-) 5 hours
Successfully copied Daemon Store to Remote Nodes
.  .  .
exachk is using TFA Scheduler. TFA PID: 3964931

# exachk -get all
------------------------------------------------------------
ID: exachk.autostart_client_exatier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile exatier1 -dball -showpass -tag
autostart_client_exatier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  42 23 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
```

```
ID: exachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  31 0 * * 0
------------------------------------------------------------
```

4. **Using the `-autorun_window` option when calling `exachk -autostart`**

```
# orachk -autostart -autorun_window 4
.
.
Applying execution time window of (+/-) 4 hours
Applying execution time window of (+/-) 4 hours
Successfully copied Daemon Store to Remote Nodes
.  .  .
orachk is using TFA Scheduler. TFA PID: 3964931

# orachk -get all
------------------------------------------------------------
ID: orachk.autostart_client_oratier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile oratier1 -dball -showpass -
tag autostart_client_oratier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  45 5 * * 1,2,3,4,5,6
------------------------------------------------------------
------------------------------------------------------------
ID: orachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  24 6 * * 0
------------------------------------------------------------


# exachk -autostart -autorun_window 4
.
.

Applying execution time window of (+/-) 4 hours
Applying execution time window of (+/-) 4 hours
Successfully copied Daemon Store to Remote Nodes

.  .  .
exachk is using TFA Scheduler. TFA PID: 3964931

# exachk -get all
------------------------------------------------------------
ID: exachk.autostart_client_exatier1
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -profile exatier1 -dball -showpass -
tag autostart_client_exatier1 -readenvconfig
COLLECTION_RETENTION  =  7
AUTORUN_SCHEDULE  =  45 5 * * 1,2,3,4,5,6
```

```
------------------------------------------------------------
------------------------------------------------------------
ID: exachk.autostart_client
------------------------------------------------------------
AUTORUN_FLAGS  =  -usediscovery -tag autostart_client -readenvconfig
COLLECTION_RETENTION  =  14
AUTORUN_SCHEDULE  =  24 6 * * 0
------------------------------------------------------------
```

> **Note:**
>
> Passing a value of 0 to the autorun window option, will disable the window even if the environment variable is set in the environment or in the `exachk .env` file.

Related Topics

- Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands in 22.2
  Starting with the AHF 22.2 (2022-09-14), commands to run the Oracle Orachk or Oracle Exachk scheduler without the Oracle Trace File Analyzer daemon are deprecated. These commands are completely removed in AHF 23.8 (2023-08-28).

3.1.2.3 Querying the Status and Next Planned Daemon Run

Query the status and next automatic run schedule of the running daemon.

To query the status and next planned daemon run:

1. To check if the daemon is running:

   ```
   $ orachk -autostatus
   ```

   ```
   $ exachk -autostatus
   ```

   If the daemon is running, then the daemon confirms and displays the PID.

2. To query more detailed information about the daemon:

   ```
   $ orachk -autostatus
   ```

   ```
   $ exachk -autostatus
   ```

   The daemon responds with the following information:

   - Node on which the daemon is installed
   - Version
   - Install location
   - Time when the daemon was started

3. To query the next scheduled compliance check run:

   ```
   $ orachk -autostatus
   ```

   ```
   $ exachk -autostatus
   ```

   The daemon responds with details of schedule.

   If you have configured multiple daemon option profiles, then the output shows whichever is scheduled to run next.

Related Topics

- Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands in 22.2
  Starting with the AHF 22.2 (2022-09-14), commands to run the Oracle Orachk or Oracle Exachk scheduler without the Oracle Trace File Analyzer daemon are deprecated. These commands are completely removed in AHF 23.8 (2023-08-28).

3.1.2.4 Configuring the Daemon for Automatic Start

Installing Oracle Autonomous Health Framework as `root` on Linux or Solaris automatically sets up and runs the Oracle Orachk or Oracle Exachk daemon.

To configure the daemon to stop or start automatically:

Run these commands as `root`.

1. To remove auto start configuration:
   - `$ orachk -autostop`
   - `$ exachk -autostop`

   To remove all default unmodified schedulers:
   - `orachk -autostop unset`
   - `exachk -autostop unset`
2. To configure the daemon to start automatically:
   - `$ orachk -autostart`
   - `$ exachk -autostart`

   To start and load the default schedulers:
   - `orachk -autostart reset`
   - `exachk -autostart reset`

   The daemon runs a full local Oracle Orachk check once every week at 3 AM, and a partial run of the most impactful checks at 2 AM every day through the `oratier1` or `exatier1` profiles. The daemon automatically purges the `oratier1` or `exatier1` profile run that runs daily, after a week. The daemon also automatically purges the full local run after 2 weeks. You can change the daemon settings after enabling auto start.
   - `$ orachk -autostart -monthly`

- `$ exachk -autostart -monthly`

  Use the `-monthly` option to configure the daemon to run a full local Oracle Orachk once every month, and a partial run of the most important checks at 2 AM every day through the `oratier1` or `exatier1` profiles.

Related Topics

- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

3.1.2.5 Configuring the Daemon for Automatic Restart

By default, you must manually restart the daemon if you restart the *server* or *node* on which the daemon is running.

However, if you use the automatic restart option, the daemon restarts automatically after the *server* or *node* reboot.

Configure the daemons to auto restart as `root`.

To configure the daemon to restart automatically:

1. To configure the daemon to restart automatically:

   ```
   $ orachk -initsetup
   ```

   ```
   $ exachk -initsetup
   ```

   The tool prompts you to provide the required information during startup.

   > **Note:**
   >
   > Stop the daemon before running `-initsetup`, if the daemon is already running.

2. To query automatic restart status of the daemon:

   ```
   $ orachk -initcheck
   ```

   ```
   $ exachk -initcheck
   ```

3. To remove automatic restart configuration:

   ```
   $ orachk -initrmsetup
   ```

   ```
   $ exachk -initrmsetup
   ```

Related Topics

- Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands in 22.2
  Starting with the AHF 22.2 (2022-09-14), commands to run the Oracle Orachk or Oracle Exachk scheduler without the Oracle Trace File Analyzer daemon are deprecated. These commands are completely removed in AHF 23.8 (2023-08-28).

3.1.3 Running Compliance Checks On-Demand

Usually, compliance checks run at scheduled intervals. However, Oracle recommends that you run compliance checks on-demand when needed.

Examples of when you must run compliance checks on-demand:

- Pre- or post-upgrades
- Machine relocations from one subnet to another
- Hardware failure or repair
- Problem troubleshooting
- In addition to go-live testing

To start on-demand compliance check runs, log in to the system as an appropriate user, and then run an appropriate tool. Specify the options to direct the type of run that you want.

```
$ orachk
```

```
$ exachk
```

> **Note:**
>
> To avoid problems while running the tool from terminal sessions on a network attached workstation or laptop, consider running the tool using VNC. If there is a network interruption, then the tool continues to process to completion. If the tool fails to run, then re-run the tool. The tool does not resume from the point of failure.

Output varies depending on your environment and options used:

- The tool starts discovering your environment
- If you have configured passwordless SSH equivalency, then the tool does not prompt you for passwords
- If you have not configured passwordless SSH for a particular component at the required access level, then the tool prompts you for password
- If the daemon is running, then the commands are sent to the daemon process that answers all prompts, such as selecting the database and providing passwords

- If the daemon is not running, then the tool prompts you for required information, such as which database you want to run against, the required passwords, and so on
- The tool investigates the status of the discovered components

> **Note:**
>
> If you are prompted for passwords, then the Expect utility runs when available. In this way, the passwords are gathered at the beginning, and the Expect utility supplies the passwords when needed at the root password prompts. The Expect utility being supplying the passwords enables the tool to continue without the need for further input. If you do not use the Expect utility, then closely monitor the run and enter the passwords interactively as prompted.
>
> Without the Expect utility installed, you must enter passwords many times depending on the size of your environment. Therefore, Oracle recommends that you use the Expect utility.

While running pre- or post-upgrade checks, Oracle Orachk and Oracle Exachk automatically detect databases that are registered with Oracle Clusterware and presents the list of databases to check.

Run the pre-upgrade checks during the upgrade planning phase. Oracle Orachk and Oracle Exachk prompt you for the version that you are planning to upgrade:

```
$ orachk -u -o pre
```

```
$ exachk -u -o pre
```

After upgrading, run the post-upgrade checks:

```
$ orachk -u -o post
```

```
$ exachk -u -o post
```

1. The tool starts collecting information across all the relevant components, including the remote nodes.
2. The tool runs the compliance checks against the collected data and displays the results.
3. After completing the compliance check run, the tool points to the location of the detailed HTML report and the `.zip` file that contains more output.

- Running On-Demand With or Without the Daemon
  When running on-demand, if the daemon is running, then the daemon answers all prompts where possible including the passwords.
- Sending Results by Email
  Optionally email the HTML report to one or more recipients using the `-sendemail` option.

- How Long Should It Take to Run Oracle Exachk?
  The elapsed time for an Oracle Exachk run varies based on the cluster size, number of Oracle Databases that are running, hardware type and configuration, overall system load, and so on.

Related Topics

- Running Compliance Checks Automatically
  Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.
- Upgrade Readiness Mode (Oracle Clusterware and Oracle Database Upgrade Checks)
  You can use Upgrade Readiness Mode to obtain an Upgrade Readiness Assessment.
- Expect - Expect - Home Page

3.1.3.1 Running On-Demand With or Without the Daemon

When running on-demand, if the daemon is running, then the daemon answers all prompts where possible including the passwords.

To run health checks on-demand with or without the daemon:

1. To run health checks on-demand if the daemon is running, then use:

   ```
   $ orachk
   ```

   ```
   $ exachk
   ```

2. To avoid connecting to the daemon process, meaning the tool to interactively prompt you as required, use the `-nodaemon` option.

   ```
   $ orachk -nodaemon
   ```

   ```
   $ exachk -nodaemon
   ```

> **Note:**
>
> Daemon mode is supported only on the Linux and Solaris operating systems.

> **Note:**
>
> If you are running database pre-upgrade checks (`-u -o pre`) and if the daemon is running, then you must use the `-nodaemon` option.

Related Topics

- Upgrade Readiness Mode (Oracle Clusterware and Oracle Database Upgrade Checks)
  You can use Upgrade Readiness Mode to obtain an Upgrade Readiness Assessment.

3.1.3.2 Sending Results by Email

Optionally email the HTML report to one or more recipients using the `-sendemail` option.

To send health check run results by email:

1. Specify the recipients in the `NOTIFICATION_EMAIL` environment variable.

   ```
   $ orachk -sendemail "NOTIFICATION_EMAIL=email_recipients"
   ```

   ```
   $ exachk -sendemail "NOTIFICATION_EMAIL=email_recipients"
   ```

   Where *email_recipients* is a comma-delimited list of email addresses.
2. Verify the email configuration settings using the `-testemail` option.

Related Topics

- NOTIFICATION_EMAIL
  Set the `NOTIFICATION_EMAIL` daemon option to send email notifications to the recipients you specify.

3.1.3.3 How Long Should It Take to Run Oracle Exachk?

The elapsed time for an Oracle Exachk run varies based on the cluster size, number of Oracle Databases that are running, hardware type and configuration, overall system load, and so on.

The elapsed times presented here are only for example purposes because the experience with each configuration is unique.

Table 3-3 Oracle Autonomous Health Framework Run Time

Hardware Configuration	Oracle Database Configuration	Run Time (minutes)
X2-2 1/4 rack	No Oracle Databases	16
X2-2 1/4 rack	Three Oracle Databases	24m7.884s
X4-2 1/4 rack	Three Oracle Databases	22m51.497s
X4-2 1/4 rack	Eight Oracle Databases	35
X4-8 full rack	One Oracle Database	17
X5-2 1/4 rack dom0	Not applicable	22m41.228s
X5-2 1/4 rack domU	One CDB with one PDB per server	9
X6-2 1/4 rack dom0	Not applicable	22m20.827s
X6-2 1/4 rack domU	One CDB with 50 PDBs per server	56
X7-2 1/4 rack	One CDB with one PDB per server	17
X7-8 full rack	One CDB with one PDB per server	17

3.1.4 Running Compliance Checks in Silent Mode

Run compliance checks automatically by scheduling them with the Automated Daemon Mode operation.

> **Note:**
>
> Silent mode operation is maintained for backwards compatibility for the customers who were using it before the daemon mode was available. Silent mode is limited in the checks it runs and Oracle does not actively enhance it any further.

Running compliance checks in silent mode using the `-s` option does not run any checks on the storage servers and switches.

Running compliance checks in silent mode using the `-S` option excludes checks on database server that require `root` access. Also, does not run any checks on the storage servers and database servers.

To run compliance checks silently, configure passwordless SSH equivalency. It is not required to run remote checks, such as running against a single-instance database.

When compliance checks are run silently, output is similar to that described in On-Demand Mode Operation.

> **Note:**
>
> If not configured to run in silent mode operation on an Oracle Engineered System, then the tool does not perform storage server or InfiniBand switch checks.

Including Compliance Checks that Require root Access

Run as `root` or configure `sudo` access to run compliance checks in silent mode and include checks that require `root` access.

To run compliance checks including checks that require `root` access, use the `-s` option followed by other required options:

```
$ orachk -s
```

```
$ exachk -s
```

Excluding Compliance Checks that Require root Access

To run compliance checks excluding checks that require `root` access, use the `-S` option followed by other required options:

```
$ orachk -S
```

```
$ exachk -S
```

3.1.5 Understanding and Managing Reports and Output

Oracle Orachk and Oracle Exachk generate a detailed HTML report with findings and recommendations.

- Temporary Files and Directories
  While running compliance checks, Oracle Orachk and Oracle Exachk create temporary directories and files for the purposes of data collection and assessment, and then delete them upon completion of compliance check runs.
- Output Files and Directories
  Oracle Orachk and Oracle Exachk create an output directory that contains various files for you to examine.
- HTML Report Output
- Tagging Reports
  The compliance check HTML report is typically named: `orachk_`*`hostname_database_date_timestamp`*`.html` or `exachk_`*`hostname_database_date_timestamp`*`.html`.
- Tracking File Attribute Changes and Comparing Snapshots
  Use the Oracle Orachk and Oracle Exachk `-fileattr` option and command flags to record and track file attribute settings, and compare snapshots.
- Comparing Two Reports
  Oracle Autonomous Health Framework automatically compare the two most recent HTML reports and generate a third diff report, when run in automated daemon mode.
- Merging Reports
  Merging reports is useful in role-separated environments where different users are run different subsets of checks and then you want to view everything as a whole.
- Maintaining Temporary Files and Directories
  Oracle Orachk and Oracle Exachk create a number of temporary files and directories while running compliance checks.
- Consuming Multiple Results in Other Tools
  Optionally integrate compliance check results into various other tools.

Related Topics

- Integrating Compliance Check Results with Other Tools
  Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager and other third-party tools.

3.1.5.1 Temporary Files and Directories

While running compliance checks, Oracle Orachk and Oracle Exachk create temporary directories and files for the purposes of data collection and assessment, and then delete them upon completion of compliance check runs.

By default, Oracle Orachk and Oracle Exachk create temporary files and directories in the /opt/oracle.SupportTools/exachk or /opt/oracle.SupportTools/orachk directories if they exist, or in the $HOME directory of the user who runs the tool.

Change this temporary working directory by setting the environment variable RAT_TMPDIR=tmp_directory before using the tools:

```
$ export RAT_TMPDIR=/tmp
$ orachk
```

```
$ export RAT_TMPDIR=/tmp
$ exachk
```

If you are using sudo access for root, and change the RAT_TMPDIR=tmp_directory, then you must also reflect this change in the /etc/sudoers file.

The /etc/sudoers file on each server must contain the entry for the root script in the new temporary directory location:

```
oracle ALL=(root) NOPASSWD:/tmp/root_orachk.sh
```

```
oracle ALL=(root) NOPASSWD:/tmp/root_exachk.sh
```

Alternatively, you can change the location of the directory used for creating the root script only by setting the environment variable.

```
export RAT_ROOT_SH_DIR=/mylocation
```

Add an entry in the /etc/sudoers file as follows:

```
oracle ALL=(root) NOPASSWD:/mylocation/root_orachk.sh
```

Note:

Any directory specified in RAT_TMPDIR must exist on the hosts for all cluster nodes.

3.1.5.2 Output Files and Directories

Oracle Orachk and Oracle Exachk create an output directory that contains various files for you to examine.

The name format of the output directory is:

```
utility_name host_name database date time_stamp
```

where,

- *utility* is either `orachk` or `exachk`
- *host_name* is the host name of the node on which Oracle Orachk or Oracle Exachk was run
- *database* is the name of the database or one of the databases against which compliance checks were performed, if applicable
- *date* is the date the compliance check was run
- *timestamp* is the time the compliance check was run

By default, Oracle Orachk and Oracle Exachk create output in the directory from where they are run. To change the location of the output directory, use the `-output` option as follows:

```
$ orachk -output output_dir
```

```
$ exachk -output output_dir
```

Alternatively, set the output directory using the `RAT_OUTPUT` environment variable as follows:

```
$ export RAT_OUTPUT=output_dir
$ orachk
```

```
$ export RAT_OUTPUT=output_dir
$ exachk
```

The contents of this directory is available in a zip file with the same name.

After completing the compliance checks, Oracle Orachk and Oracle Exachk report the location of this zip file and the HTML report file.

```
...
Detailed report (html) - /orahome/oradb/orachk/
orachk_myhost_rdb11204_041816_055429/
orachk_myhost_rdb11204_041816_055429.html


UPLOAD(if required) - /orahome/oradb/orachk/
orachk_myhost_rdb11204_041816_055429.zip


$ ls -la
total 61832
drwxr-xr-x   4 oradb oinstall     4096 Apr 18 05:55 .
drwx------ 34 oradb oinstall     4096 Apr 18 05:58 ..
drwxr--r--   3 oradb oinstall     4096 Mar 28 17:36 .cgrep
-rw-r--r--   1 oradb oinstall  4692868 Mar 28 17:35 CollectionManager_App.sql
```

```
-rw-r--r--  1 oradb oinstall 41498425 Apr 18 05:54 collections.dat
-rwxr-xr-x  1 oradb oinstall  2730651 Mar 28 17:35 orachk
drwxr-xr-x  7 oradb oinstall     4096 Apr 18 05:55
orachk_myhost_rdb11204_041816_055429
-rw-r--r--  1 oradb oinstall    36141 Apr 18 05:55
orachk_myhost_rdb11204_041816_055429.zip
-rw-r--r--  1 oradb oinstall  9380260 Mar 28 19:02 orachk.zip
-rw-r--r--  1 oradb oinstall     3869 Mar 28 17:36 readme.txt
-rw-r--r--  1 oradb oinstall  4877997 Apr 18 05:54 rules.dat
-rw-r--r--  1 oradb oinstall    40052 Mar 28 17:35
sample_user_defined_checks.xml
-rw-r--r--  1 oradb oinstall     2888 Mar 28 17:35
user_defined_checks.xsd
-rw-r--r--  1 oradb oinstall      425 Mar 28 17:36 UserGuide.txt
```

The output directory contains several other directories and the main HTML report file.

```
$ cd orachk_myhost_rdb11204_041816_055429
$ ls -la
total 60
drwxr-xr-x 7 oradb oinstall  4096 Apr 18 05:55 .
drwxr-xr-x 4 oradb oinstall  4096 Apr 18 05:55 ..
drwxr-xr-x 2 oradb oinstall  4096 Apr 18 05:55 log
-rw-r--r-- 1 oradb oinstall 30815 Apr 18 05:55
orachk_myhost_rdb11204_041816_055429.html
drwxr-xr-x 4 oradb oinstall  4096 Apr 18 05:55 outfiles
drwxr-xr-x 2 oradb oinstall  4096 Apr 18 05:55 reports
drwxr-xr-x 2 oradb oinstall  4096 Apr 18 05:55 scripts
drwxr-xr-x 2 oradb oinstall  4096 Apr 18 05:55 upload
```

Oracle Oracle Orachk and Oracle Exachk each creates an output directory containing the following information depending on which tool you use:

Table 3-4 Output Files and Directories

Output	Description
log (directory)	Contains several log files recording details about the compliance check, including: **Oracle Orachk:** • orachk.log: Main log for the compliance check. • orachk_error.log: std_error log for the compliance check. • orachk_debug_*date*_*time*.log: Debug output when run with -debug, which is useful for troubleshooting. **Oracle Exachk:** • exachk.log: Main log for the compliance check. • exachk_error.log: std_error log for the compliance check. • exachk_debug_*date*_*time*.log: Debug output when run with -debug, which is useful for troubleshooting.
outfiles (directory)	Contains several the collection results.

Table 3-4 (Cont.) Output Files and Directories

Output	Description
`reports (directory)`	Contains subreports used to build the main report.
`scripts (directory)`	Contains scripts used during collection.
`upload (directory)`	Contains files to upload collection results to a database for the Oracle Health Check Collections Manager to consume, integrate the results into your own application, or integrate into other utilities.
`orachk_*.html`	**Oracle Orachk:** Main HTML report output using the same name format as the output directory: `orachk_`*`host_name_database_date_timestamp`*`.html`.
`exachk_*.html`	**Oracle Exachk:** Main HTML report output using the same name format as the output directory: `exachk_`*`host_name_database_date_timestamp`*`.html`.

Related Topics

- Integrating Compliance Check Results with Other Tools
  Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager and other third-party tools.
- How to Capture Debug Output
  Follow these procedures to capture debug information.

3.1.5.3 HTML Report Output

The compliance check HTML report contains the following:

- High level health score
- Summary of the run
- Table of contents that provides easy access to findings
- Findings and recommendations to resolve the issues

- System Health Score and Summary
  Oracle Orachk and Oracle Exachk calculate a high-level System Health Score based on the number of passed or failed compliance checks.
- HTML Report Table of Contents and Features
  The **Table of Contents** provides links to each of the major sections within the HTML report.
- HTML Report Findings
  Report findings are grouped by Oracle Stack component.
- Maximum Availability Architecture (MAA) Scorecard
  The Maximum Availability Architecture (MAA) Scorecard is displayed after the Findings group.

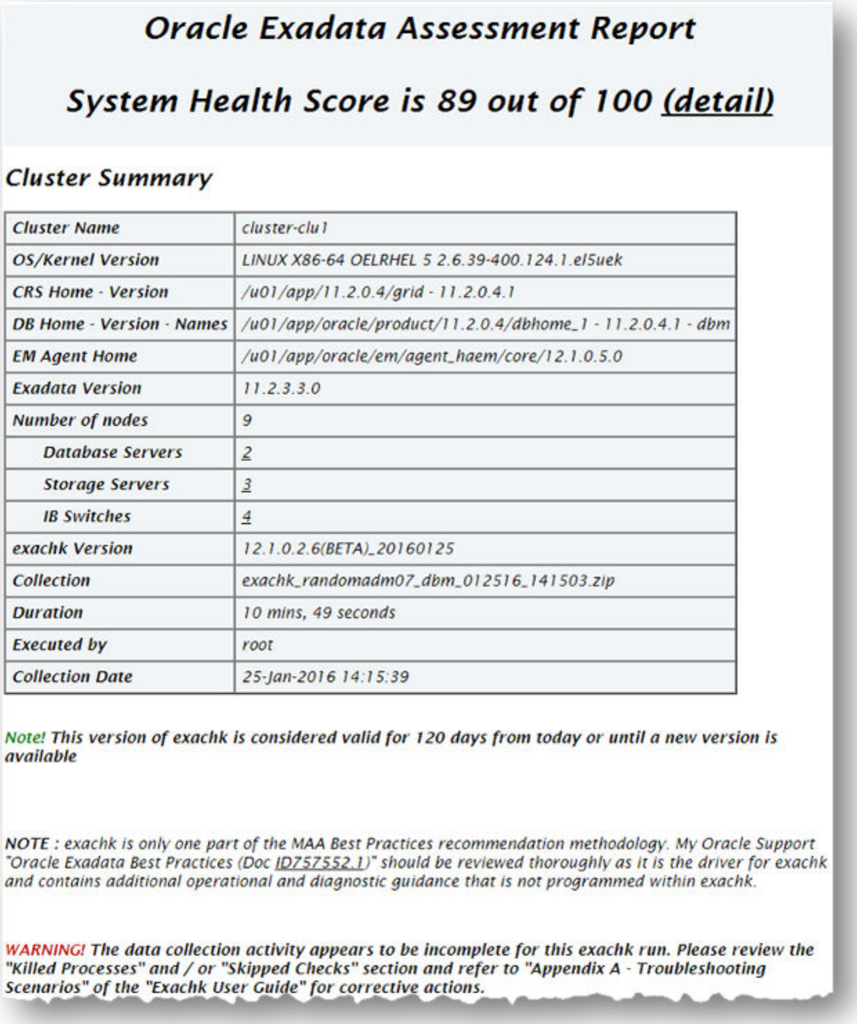
- Findings Needing Further Review
  Issues that compliance checks have only a partial view and need user reviews to determine if they are relevant are displayed in the **Findings needing further review** section.
- Platinum Certification
  The **Platinum Certification** section shows a list of compliance status items for the Oracle Platinum service.
- Viewing Clusterwide Linux Operating System Compliance Check (VMPScan)
  On Linux systems, view a summary of the VMPScan report in the Clusterwide Linux Operating System Health check (VMPScan) section of the compliance check report.
- "Systemwide Automatic Service Request (ASR) healthcheck" Section
  `asrexacheck` is designed to check and test ASR configurations to ensure that communication to the ASR Manager is possible.
- File Attribute Changes
  The **File Attribute Changes** section is shown in the report only when Oracle Orachk and Oracle Exachk is run with the `-fileattr` option.
- Skipped Checks
  Any checks that were not able to be run and skipped for some reason are shown in the **Skipped Checks** section.
- Component Elapsed Times
  The **Component Elapsed Times** gives a breakdown of time required to check various components.
- Top 10 Time Consuming Checks
  The **Top 10 Time Consuming Checks** section shows the slowest 10 checks that were run.
- How to Find a Check ID
  Each compliance check has a unique 32 character ID.
- How to Remove Checks from an Existing HTML Report
  Hide individual findings from the report using **Remove findings** .

3.1.5.3.1 System Health Score and Summary

Oracle Orachk and Oracle Exachk calculate a high-level System Health Score based on the number of passed or failed compliance checks.

A summary of the run shows, where and when it was run, which version was used, how long it took, which user it was run as, and so on.

Figure 3-3   System Health Score and Summary



Oracle Exadata Assessment Report

System Health Score is 89 out of 100 (detail)

Cluster Summary

Cluster Name	cluster-clu1
OS/Kernel Version	LINUX X86-64 OELRHEL 5 2.6.39-400.124.1.el5uek
CRS Home - Version	/u01/app/11.2.0.4/grid - 11.2.0.4.1
DB Home - Version - Names	/u01/app/oracle/product/11.2.0.4/dbhome_1 - 11.2.0.4.1 - dbm
EM Agent Home	/u01/app/oracle/em/agent_haem/core/12.1.0.5.0
Exadata Version	11.2.3.3.0
Number of nodes	9
Database Servers	2
Storage Servers	3
IB Switches	4
exachk Version	12.1.0.2.6(BETA)_20160125
Collection	exachk_randomadm07_dbm_012516_141503.zip
Duration	10 mins, 49 seconds
Executed by	root
Collection Date	25-Jan-2016 14:15:39

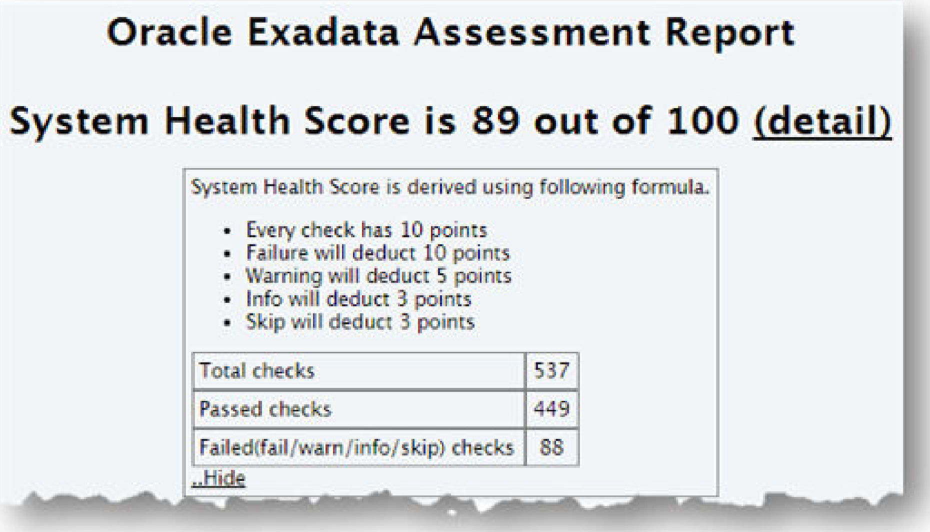
Note! This version of exachk is considered valid for 120 days from today or until a new version is available

NOTE : exachk is only one part of the MAA Best Practices recommendation methodology. My Oracle Support "Oracle Exadata Best Practices (Doc ID757552.1)" should be reviewed thoroughly as it is the driver for exachk and contains additional operational and diagnostic guidance that is not programmed within exachk.

WARNING! The data collection activity appears to be incomplete for this exachk run. Please review the "Killed Processes" and / or "Skipped Checks" section and refer to "Appendix A - Troubleshooting Scenarios" of the "Exachk User Guide" for corrective actions.

Click the **detail** link to expand the **System Health Score** section to view details of how this is calculated.

Figure 3-4   System Health Score Detail



Oracle Exadata Assessment Report

System Health Score is 89 out of 100 (detail)

System Health Score is derived using following formula.

- Every check has 10 points
- Failure will deduct 10 points
- Warning will deduct 5 points
- Info will deduct 3 points
- Skip will deduct 3 points

Total checks	537
Passed checks	449
Failed(fail/warn/info/skip) checks	88

..Hide

To generate an HTML report without the **System Health Score** section, use the `–noscore` option:

```
$ orachk -noscore
```

```
$ exachk -noscore
```

Related Topics

- Managing the Report Output
  Use the list of commands to manage compliance checks report output.

3.1.5.3.2 HTML Report Table of Contents and Features

The **Table of Contents** provides links to each of the major sections within the HTML report.

The next section in the HTML report after the summary is the **Table of Contents** and **Report Features**:

- The **Table of Contents** provides links to each of the major sections within the HTML report
  - What is shown in the Table of Contents will depend on the Oracle Stack components found during the compliance check run.
- The **Report Features** allow you to:
  - Filter checks based on their statuses.
  - Select the regions.

- Expand or collapse all checks.
- View check IDs.
- Remove findings from the report.
- Get a printable view.

By default, passed checks are hidden. To view, select the **Pass** check box under **Show Checks with the following status**. To exclude passed checks from the HTML report, use the `-nopass` option:

```
$ orachk -nopass
```

```
$ exachk -nopass
```

Figure 3-5   Report Table of Contents and Features

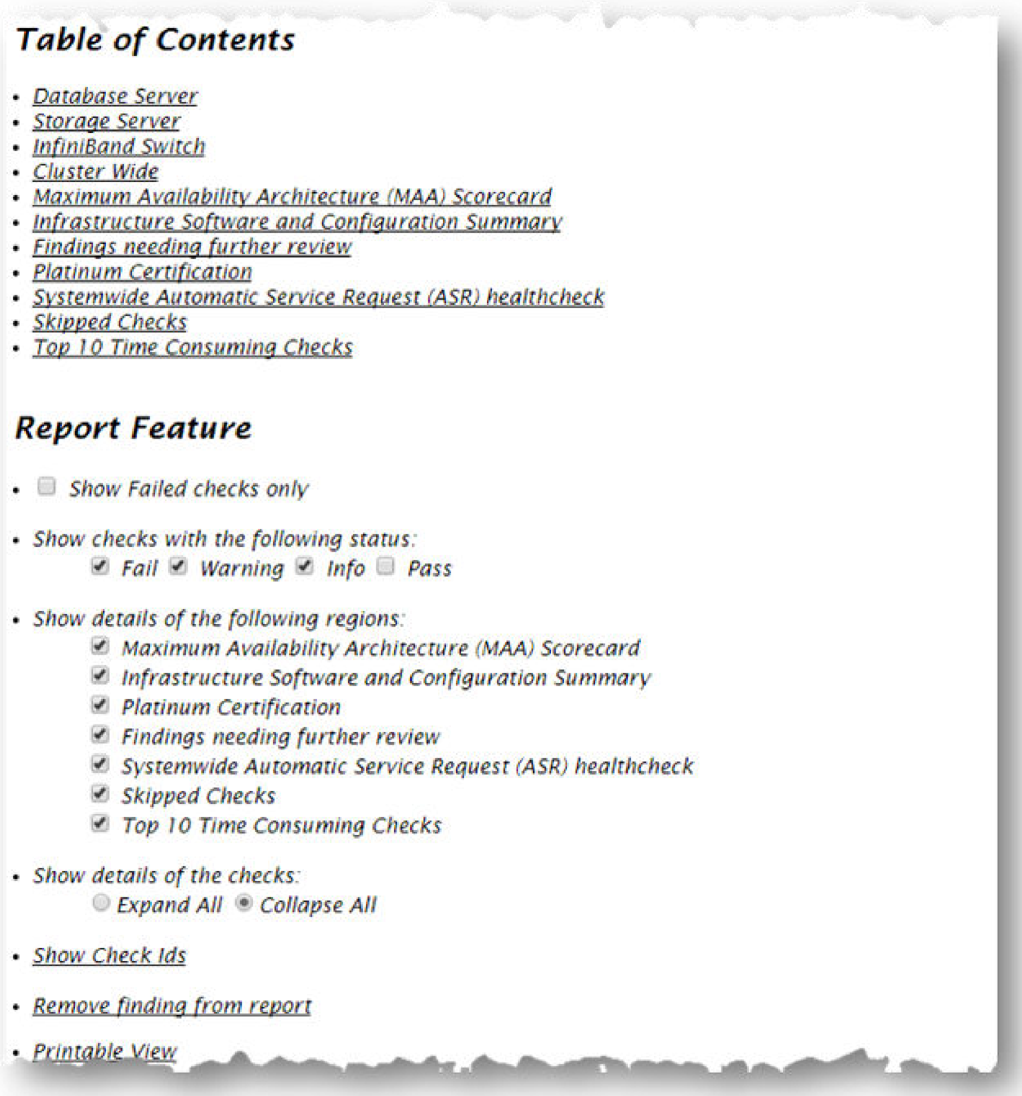


Table of Contents

- Database Server
- Storage Server
- InfiniBand Switch
- Cluster Wide
- Maximum Availability Architecture (MAA) Scorecard
- Infrastructure Software and Configuration Summary
- Findings needing further review
- Platinum Certification
- Systemwide Automatic Service Request (ASR) healthcheck
- Skipped Checks
- Top 10 Time Consuming Checks

Report Feature

- □ Show Failed checks only
- Show checks with the following status:
  ☑ Fail ☑ Warning ☑ Info □ Pass
- Show details of the following regions:
  ☑ Maximum Availability Architecture (MAA) Scorecard
  ☑ Infrastructure Software and Configuration Summary
  ☑ Platinum Certification
  ☑ Findings needing further review
  ☑ Systemwide Automatic Service Request (ASR) healthcheck
  ☑ Skipped Checks
  ☑ Top 10 Time Consuming Checks
- Show details of the checks:
  ○ Expand All ● Collapse All
- Show Check Ids
- Remove finding from report
- Printable View

Related Topics

- How to Find a Check ID
  Each compliance check has a unique 32 character ID.
- How to Remove Checks from an Existing HTML Report
  Hide individual findings from the report using **Remove findings** .
- Managing the Report Output
  Use the list of commands to manage compliance checks report output.

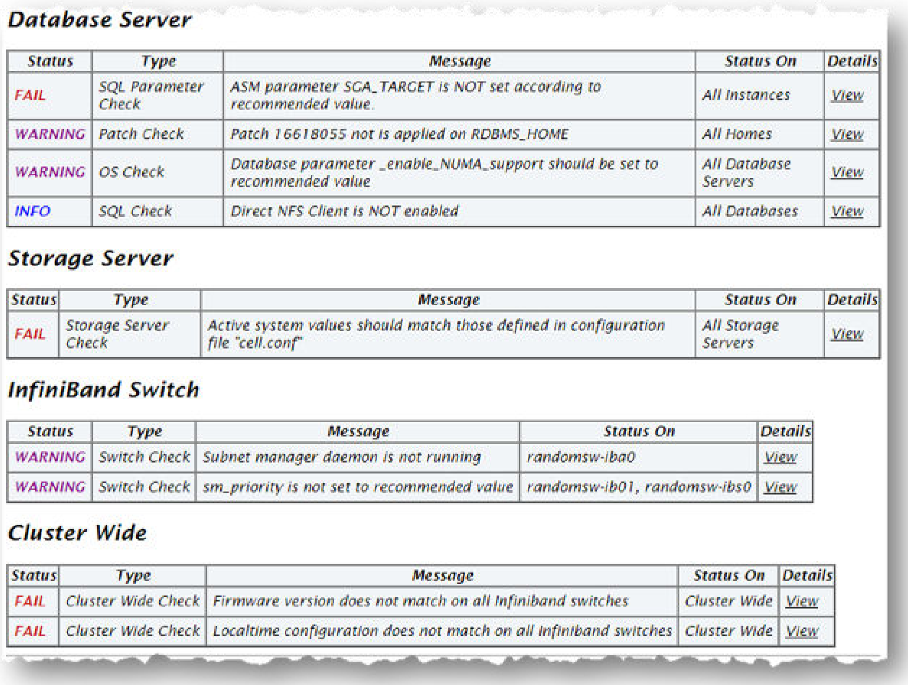
3.1.5.3.3 HTML Report Findings

Report findings are grouped by Oracle Stack component.

Findings include:

- Status of check (`FAIL`, `WARNING`, `INFO`, or `PASS`)
- Type of check
- Check message
- Location where the check was run
- Link to expand details for further findings and recommendations

Figure 3-6   Report Findings



Database Server

Status	Type	Message	Status On	Details
FAIL	SQL Parameter Check	ASM parameter SGA_TARGET is NOT set according to recommended value.	All Instances	View
WARNING	Patch Check	Patch 16618055 not is applied on RDBMS_HOME	All Homes	View
WARNING	OS Check	Database parameter _enable_NUMA_support should be set to recommended value	All Database Servers	View
INFO	SQL Check	Direct NFS Client is NOT enabled	All Databases	View

Storage Server

Status	Type	Message	Status On	Details
FAIL	Storage Server Check	Active system values should match those defined in configuration file "cell.conf"	All Storage Servers	View

InfiniBand Switch

Status	Type	Message	Status On	Details
WARNING	Switch Check	Subnet manager daemon is not running	randomsw-iba0	View
WARNING	Switch Check	sm_priority is not set to recommended value	randomsw-ib01, randomsw-ibs0	View

Cluster Wide

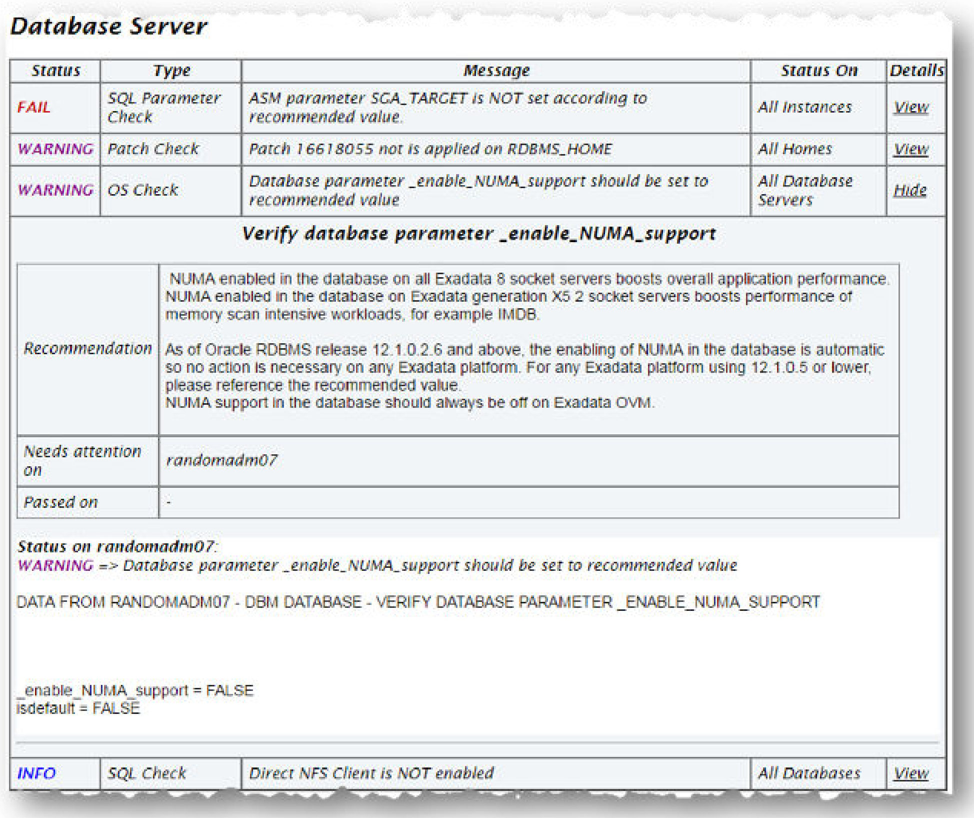
Status	Type	Message	Status On	Details
FAIL	Cluster Wide Check	Firmware version does not match on all Infiniband switches	Cluster Wide	View
FAIL	Cluster Wide Check	Localtime configuration does not match on all Infiniband switches	Cluster Wide	View

Click **view details** to view the findings and the recommendations.

- Solution to solve the problem

- Applicable recommendations
- Where the problem does not apply
- Links to relevant documentation or My Oracle Support notes
- Example of data the recommendation is based on

Figure 3-7   View Report Findings



Database Server

Status	Type	Message	Status On	Details
FAIL	SQL Parameter Check	ASM parameter SGA_TARGET is NOT set according to recommended value.	All Instances	View
WARNING	Patch Check	Patch 16618055 not is applied on RDBMS_HOME	All Homes	View
WARNING	OS Check	Database parameter _enable_NUMA_support should be set to recommended value	All Database Servers	Hide

Verify database parameter _enable_NUMA_support

Recommendation	NUMA enabled in the database on all Exadata 8 socket servers boosts overall application performance. NUMA enabled in the database on Exadata generation X5 2 socket servers boosts performance of memory scan intensive workloads, for example IMDB. As of Oracle RDBMS release 12.1.0.2.6 and above, the enabling of NUMA in the database is automatic so no action is necessary on any Exadata platform. For any Exadata platform using 12.1.0.5 or lower, please reference the recommended value. NUMA support in the database should always be off on Exadata OVM.
Needs attention on	randomadm07
Passed on	-

Status on randomadm07:
WARNING => Database parameter _enable_NUMA_support should be set to recommended value

```
DATA FROM RANDOMADM07 - DBM DATABASE - VERIFY DATABASE PARAMETER _ENABLE_NUMA_SUPPORT



_enable_NUMA_support = FALSE
isdefault = FALSE
```

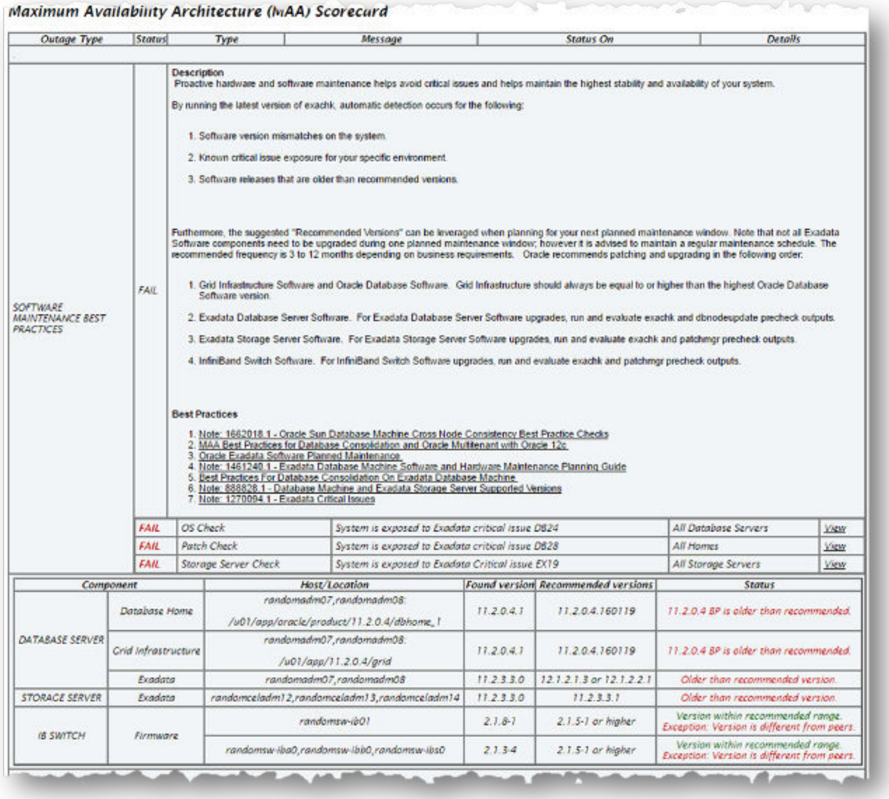
INFO	SQL Check	Direct NFS Client is NOT enabled	All Databases	View

3.1.5.3.4 Maximum Availability Architecture (MAA) Scorecard

The Maximum Availability Architecture (MAA) Scorecard is displayed after the Findings group.

The MAA Scorecard provides a set of best practices for maximum availability architecture. It also shows results related to maximum availability, such as the installed software versions checked for noncurrent software, and use of incompatible features.

Figure 3-8   Maximum Availability Architecture (MAA) Scorecard



Maximum Availability Architecture (MAA) Scorecard

Outage Type	Status	Type	Message	Status On	Details
SOFTWARE MAINTENANCE BEST PRACTICES	FAIL				

Description

Proactive hardware and software maintenance helps avoid critical issues and helps maintain the highest stability and availability of your system.

By running the latest version of exachk, automatic detection occurs for the following:

1. Software version mismatches on the system.
2. Known critical issue exposure for your specific environment.
3. Software releases that are older than recommended versions.

Furthermore, the suggested "Recommended Versions" can be leveraged when planning for your next planned maintenance window. Note that not all Exadata Software components need to be upgraded during one planned maintenance window; however it is advised to maintain a regular maintenance schedule. The recommended frequency is 3 to 12 months depending on business requirements.   Oracle recommends patching and upgrading in the following order:

1. Grid Infrastructure Software and Oracle Database Software. Grid Infrastructure should always be equal to or higher than the highest Oracle Database Software version.
2. Exadata Database Server Software. For Exadata Database Server Software upgrades, run and evaluate exachk and dbnodeupdate precheck outputs.
3. Exadata Storage Server Software. For Exadata Storage Server Software upgrades, run and evaluate exachk and patchmgr precheck outputs.
4. InfiniBand Switch Software. For InfiniBand Switch Software upgrades, run and evaluate exachk and patchmgr precheck outputs.

Best Practices

1. Note: 1662018.1 - Oracle Sun Database Machine Cross Node Consistency Best Practice Checks
2. MAA Best Practices for Database Consolidation and Oracle Multitenant with Oracle 12c
3. Oracle Exadata Software Planned Maintenance
4. Note: 1461240.1 - Exadata Database Machine Software and Hardware Maintenance Planning Guide
5. Best Practices For Database Consolidation On Exadata Database Machine
6. Note: 888828.1 - Database Machine and Exadata Storage Server Supported Versions
7. Note: 1270094.1 - Exadata Critical Issues

Status	Type	Message	Status On	Details
FAIL	OS Check	System is exposed to Exadata critical issue DB24	All Database Servers	View
FAIL	Patch Check	System is exposed to Exadata critical issue DB28	All Homes	View
FAIL	Storage Server Check	System is exposed to Exadata Critical issue EX19	All Storage Servers	View

Component		Host/Location	Found version	Recommended versions	Status
DATABASE SERVER	Database Home	randomadm07,randomadm08: /u01/app/oracle/product/11.2.0.4/dbhome_1	11.2.0.4.1	11.2.0.4.160119	11.2.0.4 BP is older than recommended.
	Grid Infrastructure	randomadm07,randomadm08: /u01/app/11.2.0.4/grid	11.2.0.4.1	11.2.0.4.160119	11.2.0.4 BP is older than recommended.
	Exadata	randomadm07,randomadm08	11.2.3.3.0	12.1.2.1.3 or 12.1.2.2.1	Older than recommended version.
STORAGE SERVER	Exadata	randomceladm12,randomceladm13,randomceladm14	11.2.3.3.0	11.2.3.3.1	Older than recommended version.
IB SWITCH	Firmware	randomsw-ib01	2.1.8-1	2.1.5-1 or higher	Version within recommended range. Exception: Version is different from peers.
		randomsw-iba0,randomsw-ibb0,randomsw-ibs0	2.1.3-4	2.1.5-1 or higher	Version within recommended range. Exception: Version is different from peers.

To generate an HTML report without the **MAA Scorecard** section, use the `-m` option:

```
$ orachk -m
```

```
$ exachk -m
```

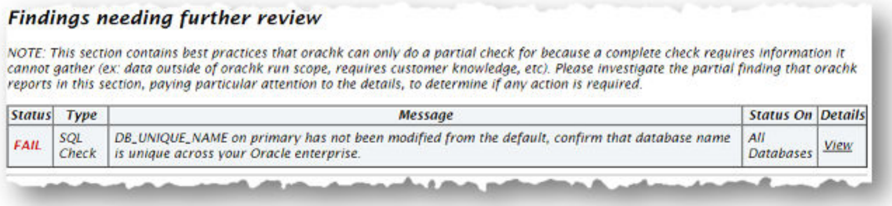
Related Topics

- Controlling the Scope of Checks
  Use the list of commands to control the scope of checks.

3.1.5.3.5 Findings Needing Further Review

Issues that compliance checks have only a partial view and need user reviews to determine if they are relevant are displayed in the **Findings needing further review** section.

Figure 3-9   Findings needing further review



Findings needing further review

NOTE: This section contains best practices that orachk can only do a partial check for because a complete check requires information it cannot gather (ex: data outside of orachk run scope, requires customer knowledge, etc). Please investigate the partial finding that orachk reports in this section, paying particular attention to the details, to determine if any action is required.

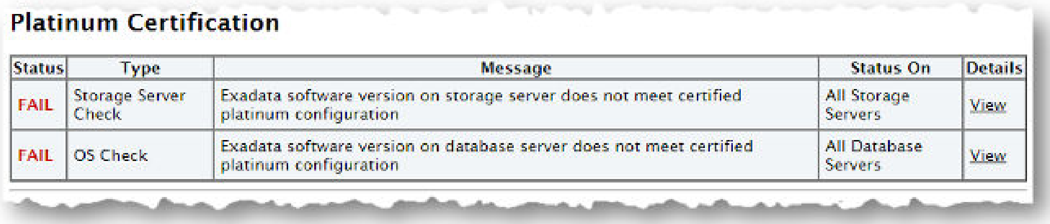
Status	Type	Message	Status On	Details
FAIL	SQL Check	DB_UNIQUE_NAME on primary has not been modified from the default, confirm that database name is unique across your Oracle enterprise.	All Databases	View

3.1.5.3.6 Platinum Certification

The **Platinum Certification** section shows a list of compliance status items for the Oracle Platinum service.

For the existing Platinum customers it is a review. For customers not yet participating in Oracle Platinum, it is an indication of readiness to participate in Oracle Platinum.

Figure 3-10   Platinum Certification



Platinum Certification

Status	Type	Message	Status On	Details
FAIL	Storage Server Check	Exadata software version on storage server does not meet certified platinum configuration	All Storage Servers	View
FAIL	OS Check	Exadata software version on database server does not meet certified platinum configuration	All Database Servers	View

Note:

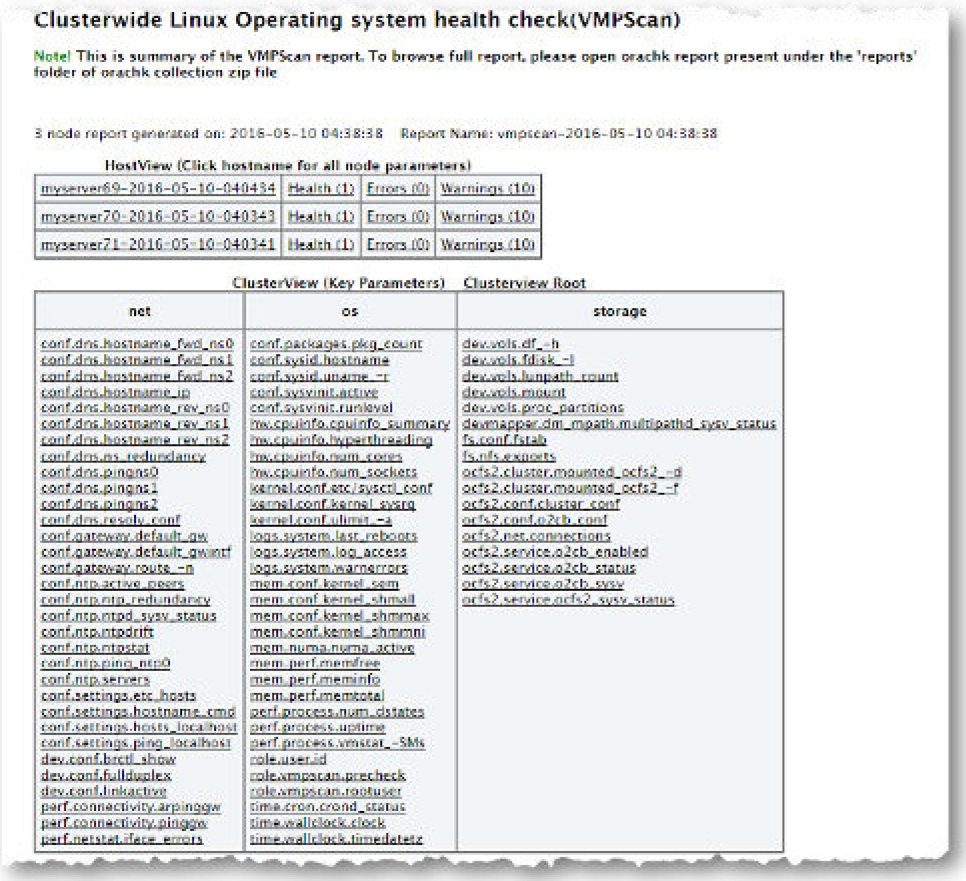
This section is seen when compliance checks are run on Oracle Engineered Systems.

3.1.5.3.7 Viewing Clusterwide Linux Operating System Compliance Check (VMPScan)

On Linux systems, view a summary of the VMPScan report in the Clusterwide Linux Operating System Health check (VMPScan) section of the compliance check report.

The full VMPScan report is also available within the `*collection*/reports` and `*collection*/outfiles/vmpscan` directory.

Figure 3-11   Clusterwide Linux Operating System Health Check (VMPScan)



Clusterwide Linux Operating system health check(VMPScan)

Note! This is summary of the VMPScan report. To browse full report, please open orachk report present under the 'reports' folder of orachk collection zip file

3 node report generated on: 2016-05-10 04:38:38   Report Name: vmpscan-2016-05-10 04:38:38

HostView (Click hostname for all node parameters)

myserver69-2016-05-10-040434	Health (1)	Errors (0)	Warnings (10)
myserver70-2016-05-10-040343	Health (1)	Errors (0)	Warnings (10)
myserver71-2016-05-10-040341	Health (1)	Errors (0)	Warnings (10)

ClusterView (Key Parameters)   Clusterview Root

net	os	storage
conf.dns.hostname_fwd_ns0	conf.packages.pkg_count	dev.vols.df_-h
conf.dns.hostname_fwd_ns1	conf.sysid.hostname	dev.vols.fdisk_-l
conf.dns.hostname_fwd_ns2	conf.sysid.uname_-r	dev.vols.lunpath_count
conf.dns.hostname_ip	conf.sysvinit.active	dev.vols.mount
conf.dns.hostname_rev_ns0	conf.sysvinit.runlevel	dev.vols.proc_partitions
conf.dns.hostname_rev_ns1	hw.cpuinfo.cpuinfo_summary	devmapper.dm_mpath.multipathd_sysv_status
conf.dns.hostname_rev_ns2	hw.cpuinfo.hyperthreading	fs.conf.fstab
conf.dns.ns_redundancy	hw.cpuinfo.num_cores	fs.nfs.exports
conf.dns.pingns0	hw.cpuinfo.num_sockets	ocfs2.cluster.mounted_ocfs2_-d
conf.dns.pingns1	kernel.conf.etc/sysctl_conf	ocfs2.cluster.mounted_ocfs2_-f
conf.dns.pingns2	kernel.conf.kernel_sysrq	ocfs2.conf.cluster_conf
conf.dns.resolv_conf	kernel.conf.ulimit_-a	ocfs2.conf.o2cb_conf
conf.gateway.default_gw	logs.system.last_reboots	ocfs2.net.connections
conf.gateway.default_gwintf	logs.system.log_access	ocfs2.service.o2cb_enabled
conf.gateway.route_-n	logs.system.warnerrors	ocfs2.service.o2cb_status
conf.ntp.active_peers	mem.conf.kernel_sem	ocfs2.service.o2cb_sysv
conf.ntp.ntp_redundancy	mem.conf.kernel_shmall	ocfs2.service.ocfs2_sysv_status
conf.ntp.ntpd_sysv_status	mem.conf.kernel_shmmax	
conf.ntp.ntpdrift	mem.conf.kernel_shmmni	
conf.ntp.ntpstat	mem.numa.numa_active	
conf.ntp.ping_ntp0	mem.perf.memfree	
conf.ntp.servers	mem.perf.meminfo	
conf.settings.etc_hosts	mem.perf.memtotal	
conf.settings.hostname_cmd	perf.process.num_dstates	
conf.settings.hosts_localhost	perf.process.uptime	
conf.settings.ping_localhost	perf.process.vmstat_-SMs	
dev.conf.brctl_show	role.user.id	
dev.conf.fullduplex	role.vmpscan.precheck	
dev.conf.linkactive	role.vmpscan.rootuser	
perf.connectivity.arpinggw	time.cron.crond_status	
perf.connectivity.pinggw	time.wallclock.clock	
perf.netstat.iface_errors	time.wallclock.timedatetz	

Note:

The VMPScan report is included only when Oracle Orachk is run on Linux systems.

3.1.5.3.8 "Systemwide Automatic Service Request (ASR) healthcheck" Section

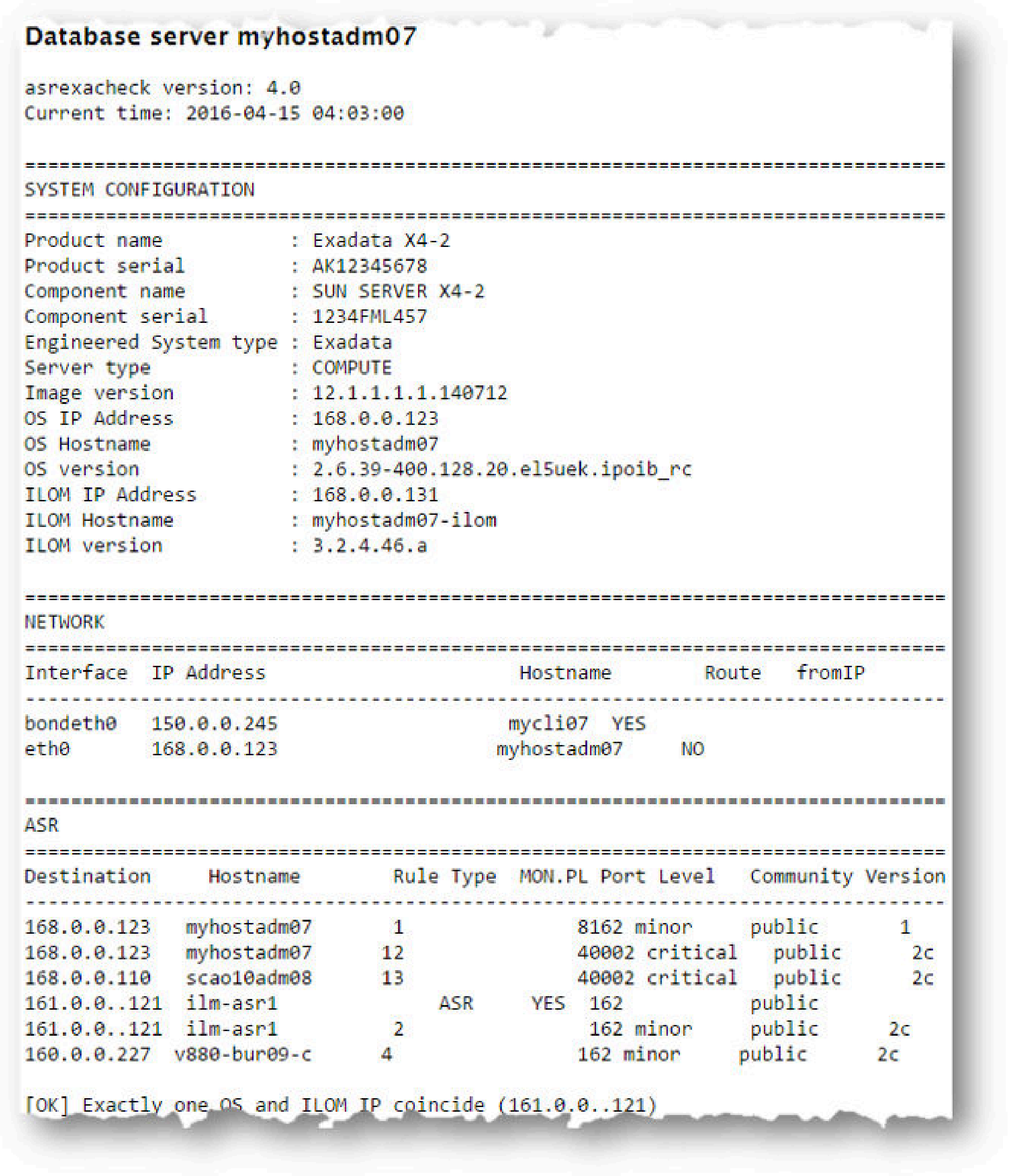
`asrexacheck` is designed to check and test ASR configurations to ensure that communication to the ASR Manager is possible.

This is a non-invasive script that checks configurations only and does not write to any system or configuration files. The script checks for known configuration issues and any previous hardware faults that may not have been reported by ASR due to a misconfiguration on the BDA.

This section is included in the report only when the compliance checks are run on Oracle Engineered Systems.

The following is a sample of the **Systemwide Automatic Service Request (ASR) healthcheck** section truncated for brevity:

Figure 3-12   Systemwide Automatic Service Request (ASR) healthcheck



```
Database server myhostadm07

asrexacheck version: 4.0
Current time: 2016-04-15 04:03:00

================================================================================
SYSTEM CONFIGURATION
================================================================================
Product name           : Exadata X4-2
Product serial         : AK12345678
Component name         : SUN SERVER X4-2
Component serial       : 1234FML457
Engineered System type : Exadata
Server type            : COMPUTE
Image version          : 12.1.1.1.1.140712
OS IP Address          : 168.0.0.123
OS Hostname            : myhostadm07
OS version             : 2.6.39-400.128.20.el5uek.ipoib_rc
ILOM IP Address        : 168.0.0.131
ILOM Hostname          : myhostadm07-ilom
ILOM version           : 3.2.4.46.a

================================================================================
NETWORK
================================================================================
Interface  IP Address                      Hostname        Route   fromIP
--------------------------------------------------------------------------------
bondeth0   150.0.0.245                    mycli07  YES
eth0       168.0.0.123                   myhostadm07     NO

================================================================================
ASR
================================================================================
Destination     Hostname        Rule Type  MON.PL Port Level   Community Version
--------------------------------------------------------------------------------
168.0.0.123   myhostadm07       1               8162 minor     public       1
168.0.0.123   myhostadm07      12               40002 critical   public      2c
168.0.0.110   scao10adm08      13               40002 critical   public      2c
161.0.0..121  ilm-asr1              ASR     YES  162           public
161.0.0..121  ilm-asr1          2                162 minor     public      2c
160.0.0.227  v880-bur09-c      4                162 minor     public      2c

[OK] Exactly one OS and ILOM IP coincide (161.0.0..121)
```

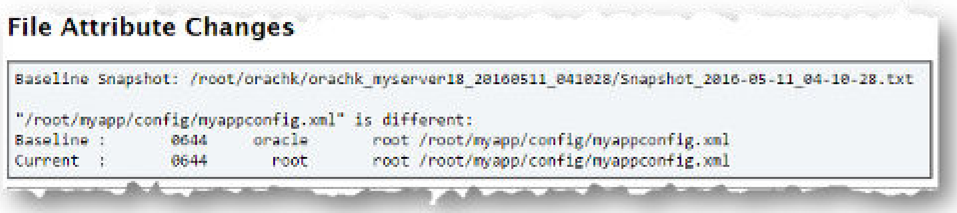
Related Topics

- https://support.oracle.com/rs?type=doc&id=2103715.1

3.1.5.3.9 File Attribute Changes

The **File Attribute Changes** section is shown in the report only when Oracle Orachk and Oracle Exachk is run with the `-fileattr` option.

Figure 3-13   File Attribute Changes



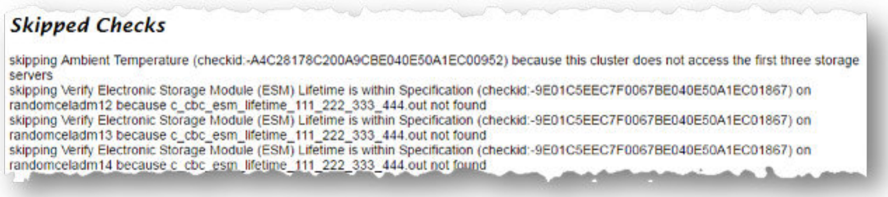
File Attribute Changes

```
Baseline Snapshot: /root/orachk/orachk_myserver18_20160511_041028/Snapshot_2016-05-11_04-10-28.txt

"/root/myapp/config/myappconfig.xml" is different:
Baseline :       0644     oracle       root /root/myapp/config/myappconfig.xml
Current  :       0644       root       root /root/myapp/config/myappconfig.xml
```

3.1.5.3.10 Skipped Checks

Any checks that were not able to be run and skipped for some reason are shown in the **Skipped Checks** section.

Figure 3-14   Skipped Checks



Skipped Checks

```
skipping Ambient Temperature (checkid:-A4C28178C200A9CBE040E50A1EC00952) because this cluster does not access the first three storage
servers
skipping Verify Electronic Storage Module (ESM) Lifetime is within Specification (checkid:-9E01C5EEC7F0067BE040E50A1EC01867) on
randomceladm12 because c_cbc_esm_lifetime_111_222_333_444.out not found
skipping Verify Electronic Storage Module (ESM) Lifetime is within Specification (checkid:-9E01C5EEC7F0067BE040E50A1EC01867) on
randomceladm13 because c_cbc_esm_lifetime_111_222_333_444.out not found
skipping Verify Electronic Storage Module (ESM) Lifetime is within Specification (checkid:-9E01C5EEC7F0067BE040E50A1EC01867) on
randomceladm14 because c_cbc_esm_lifetime_111_222_333_444.out not found
```

Related Topics

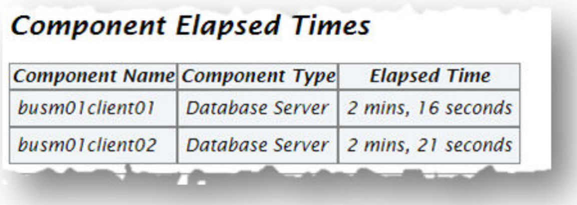
- Slow Performance, Skipped Checks, and Timeouts
  Follow these procedures to fix slow performance and other issues.

3.1.5.3.11 Component Elapsed Times

The **Component Elapsed Times** gives a breakdown of time required to check various components.

This can be useful when diagnosing performance problems.

Figure 3-15   Component Elapsed Times



Component Elapsed Times

Component Name	Component Type	Elapsed Time
busm01client01	Database Server	2 mins, 16 seconds
busm01client02	Database Server	2 mins, 21 seconds

Related Topics

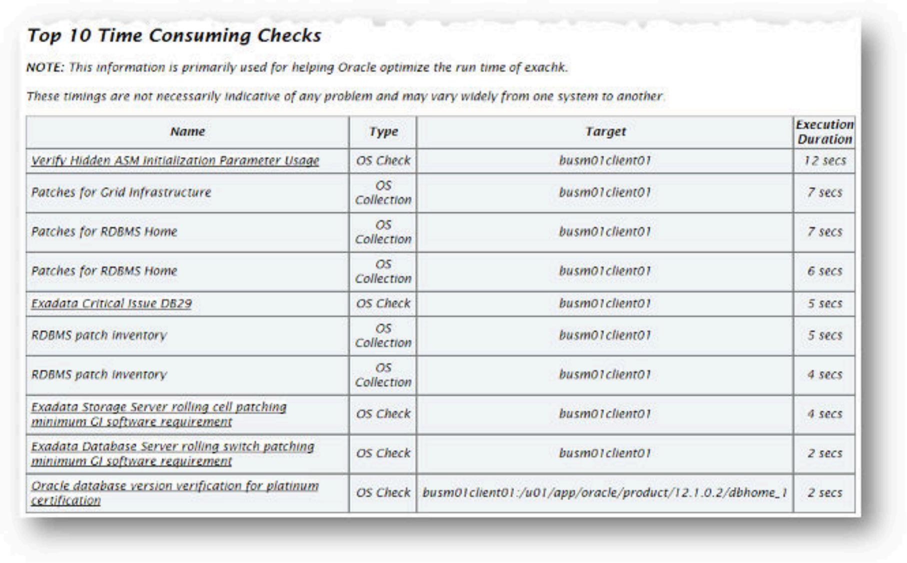
- Slow Performance, Skipped Checks, and Timeouts
  Follow these procedures to fix slow performance and other issues.

3.1.5.3.12 Top 10 Time Consuming Checks

The **Top 10 Time Consuming Checks** section shows the slowest 10 checks that were run.

This can be useful when diagnosing performance problems.

Figure 3-16 Top 10 Time Consuming Checks



Top 10 Time Consuming Checks

NOTE: This information is primarily used for helping Oracle optimize the run time of exachk.

These timings are not necessarily indicative of any problem and may vary widely from one system to another.

Name	Type	Target	Execution Duration
Verify Hidden ASM Initialization Parameter Usage	OS Check	busm01client01	12 secs
Patches for Grid Infrastructure	OS Collection	busm01client01	7 secs
Patches for RDBMS Home	OS Collection	busm01client01	7 secs
Patches for RDBMS Home	OS Collection	busm01client01	6 secs
Exadata Critical Issue DB29	OS Check	busm01client01	5 secs
RDBMS patch inventory	OS Collection	busm01client01	5 secs
RDBMS patch inventory	OS Collection	busm01client01	4 secs
Exadata Storage Server rolling cell patching minimum GI software requirement	OS Check	busm01client01	4 secs
Exadata Database Server rolling switch patching minimum GI software requirement	OS Check	busm01client01	2 secs
Oracle database version verification for platinum certification	OS Check	busm01client01:/u01/app/oracle/product/12.1.0.2/dbhome_1	2 secs

Related Topics

- Slow Performance, Skipped Checks, and Timeouts
  Follow these procedures to fix slow performance and other issues.
- Oracle Orachk Sample Report
- Oracle Exachk Sample Report

3.1.5.3.13 How to Find a Check ID

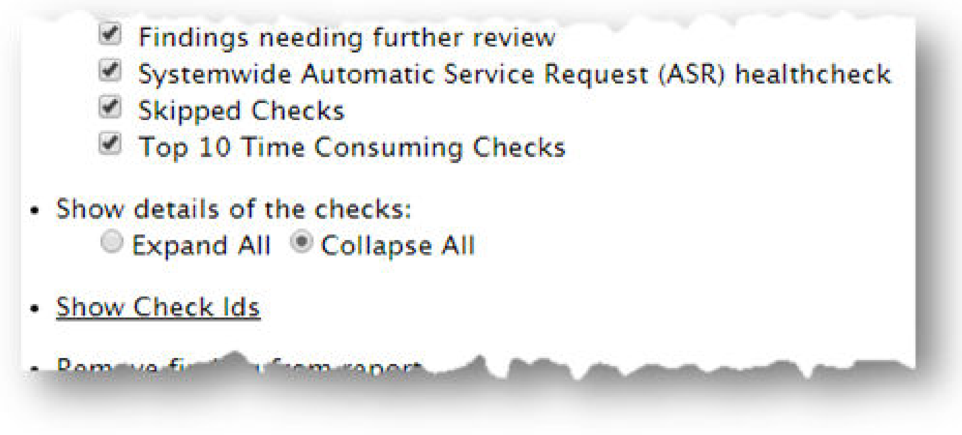
Each compliance check has a unique 32 character ID.

You may want to find a check id while:

- Communicating to Oracle or your own internal teams about a specific check
- Excluding or only running one or more checks

To find a particular check id using a generated report, click the **Show Check Ids** link.

Figure 3-17   Show Check Ids

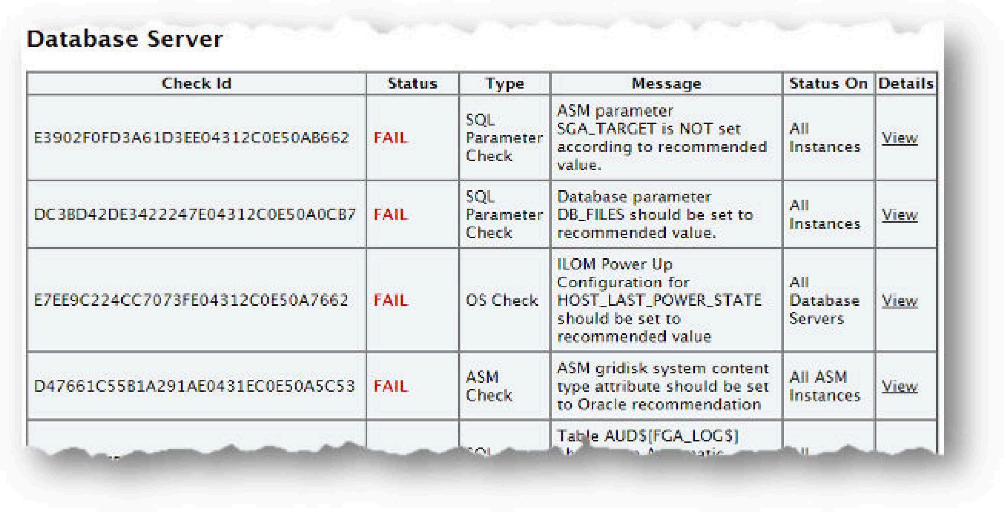


☑ Findings needing further review
☑ Systemwide Automatic Service Request (ASR) healthcheck
☑ Skipped Checks
☑ Top 10 Time Consuming Checks

- Show details of the checks:
  ○ Expand All ● Collapse All
- Show Check Ids
- Remove fi from report

The findings will then display an extra column to the left with the Check Id.

Figure 3-18   Show Check Ids



Database Server

Check Id	Status	Type	Message	Status On	Details
E3902F0FD3A61D3EE04312C0E50AB662	FAIL	SQL Parameter Check	ASM parameter SGA_TARGET is NOT set according to recommended value.	All Instances	View
DC3BD42DE3422247E04312C0E50A0CB7	FAIL	SQL Parameter Check	Database parameter DB_FILES should be set to recommended value.	All Instances	View
E7EE9C224CC7073FE04312C0E50A7662	FAIL	OS Check	ILOM Power Up Configuration for HOST_LAST_POWER_STATE should be set to recommended value	All Database Servers	View
D47661C55B1A291AE0431EC0E50A5C53	FAIL	ASM Check	ASM gridisk system content type attribute should be set to Oracle recommendation	All ASM Instances	View
			Table AUD$[FGA_LOG$]		

Related Topics

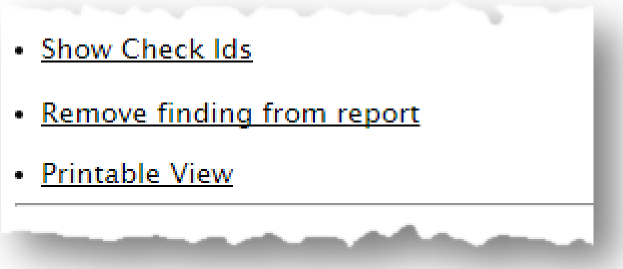
- [Running Subsets of Checks](#)
  Run a subset of compliance checks where necessary.

3.1.5.3.14 How to Remove Checks from an Existing HTML Report

Hide individual findings from the report using **Remove findings** .

Click **Remove finding from report**.

Figure 3-19   Remove Findings from Report



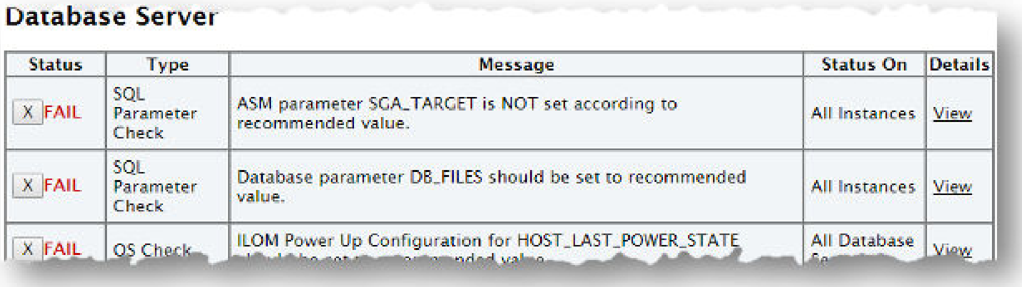
- Show Check Ids
- Remove finding from report
- Printable View

A button with an X appears next to each finding.

Click X to hide the finding. This does not remove the finding from the source of the HTML report it simply hides it. If the HTML report is reloaded the finding will appear again.

To permanently hide the finding use your browser's **Save Page** option to save the report once the finding is hidden.

Figure 3-20   Remove Findings from Report



Database Server

Status	Type	Message	Status On	Details
X FAIL	SQL Parameter Check	ASM parameter SGA_TARGET is NOT set according to recommended value.	All Instances	View
X FAIL	SQL Parameter Check	Database parameter DB_FILES should be set to recommended value.	All Instances	View
X FAIL	OS Check	ILOM Power Up Configuration for HOST_LAST_POWER_STATE	All Database	View

If there are findings that you never want to see in the report, then they can be excluded altogether so the checks are never run in the first place.

Related Topics

- Running Subsets of Checks
  Run a subset of compliance checks where necessary.

3.1.5.4 Tagging Reports

The compliance check HTML report is typically named:
`orachk_hostname_database_date_timestamp.html` or
`exachk_hostname_database_date_timestamp.html`.

You can include other tags in the HTML report name to facilitate differentiation and identification.

Include a custom tag in the HTML report name as follows:

```
$ orachk -tag tag_name
```

```
$ exachk -tag tag_name
```

The resulting HTML report name is similar to the following:

```
orachk_host_name_database_date_timestamp_tag_name.html
```

```
exachk_host_name_database_date_timestamp_tag_name.html
```

3.1.5.5 Tracking File Attribute Changes and Comparing Snapshots

Use the Oracle Orachk and Oracle Exachk `-fileattr` option and command flags to record and track file attribute settings, and compare snapshots.

Changes to the attributes of files such as owner, group, or permissions can cause unexpected consequences. Proactively monitor and mitigate the issues before your business gets impacted.

- Using the File Attribute Check With the Daemon
  You must have Oracle Grid Infrastructure installed and running before you use `-fileattr`.
- Taking File Attribute Snapshots
  By default, Oracle Grid Infrastructure homes and all the installed Oracle Database homes are included in the snapshots.
- Including Directories to Check
  Include directories in the file attribute changes check.
- Excluding Directories from Checks
  Exclude directories from file attribute changes checks.
- Rechecking Changes
  Compare the new snapshot with the previous one to track changes.
- Designating a Snapshot As a Baseline
  Designate a snapshot as a baseline to compare with other snapshots.
- Restricting System Checks
  Restrict Oracle Orachk and Oracle Exachk to perform only file attribute changes checks.
- Removing Snapshots
  Remove the snapshots diligently.

3.1.5.5.1 Using the File Attribute Check With the Daemon

You must have Oracle Grid Infrastructure installed and running before you use `-fileattr`.

To use file attribute check with the daemon:

1. Start the daemon.

   ```
   orachk -d start
   ```

2. Start the client run with the `-fileattr` options.

   ```
   orachk -fileattr start -includedir "/root/myapp,/etc/oratab" -
   excludediscovery
   ```

   ```
   orachk -fileattr check -includedir "/root/myapp,/etc/oratab" -
   excludediscovery
   ```

3. Specify the output directory to store snapshots with the `-output` option.

   ```
   orachk -fileattr start -output "/tmp/mysnapshots"
   ```

4. Specify a descriptive name for the snapshot with the `-tag` option to identify your snapshots.

   For example:

   ```
   orachk -fileattr start -tag "BeforeXYZChange"
     Generated snapshot directory-
     orachk_myserver65_20160329_052056_ BeforeXYZChange
   ```

3.1.5.5.2 Taking File Attribute Snapshots

By default, Oracle Grid Infrastructure homes and all the installed Oracle Database homes are included in the snapshots.

To take file attribute snapshots:

To start the first snapshot, run the `-fileattr start` command.

```
orachk -fileattr start
```

```
exachk -fileattr start
```

Example 3-4 orachk -fileattr start

```
orachk -fileattr start
CRS stack is running and CRS_HOME is not set. Do you want to set CRS_HOME
to /u01/app/11.2.0.4/grid?[y/n][y]
Checking ssh user equivalency settings on all nodes in cluster
Node mysrv22 is configured for ssh user equivalency for oradb user
```

```
Node mysrv23 is configured for ssh user equivalency for oradb user

List of directories(recursive) for checking file attributes:
/u01/app/oradb/product/11.2.0/dbhome_11202
/u01/app/oradb/product/11.2.0/dbhome_11203
/u01/app/oradb/product/11.2.0/dbhome_11204
orachk has taken snapshot of file attributes for above directories
at: /orahome/oradb/orachk/orachk_mysrv21_20160504_041214
```

3.1.5.5.3 Including Directories to Check

Include directories in the file attribute changes check.

To include directories to check:

Run the file attribute changes check command with the `-includedir` *`directories`* option.

Where, *`directories`* is a comma-delimited list of directories to include in the check.

For example:

```
orachk -fileattr start -includedir "/home/oradb,/etc/oratab"
```

```
exachk -fileattr start -includedir "/home/oradb,/etc/oratab"
```

Example 3-5   orachk -fileattr start -includedir

```
orachk -fileattr start -includedir "/root/myapp/config/"
CRS stack is running and CRS_HOME is not set. Do you want to set
CRS_HOME to /u01/app/12.2.0/grid?[y/n][y]
Checking for prompts on myserver18 for oragrid user...
Checking ssh user equivalency settings on all nodes in cluster
Node myserver17 is configured for ssh user equivalency for root user
List of directories(recursive) for checking file attributes:
/u01/app/12.2.0/grid
/u01/app/oradb/product/12.2.0/dbhome_1
/u01/app/oradb2/product/12.2.0/dbhome_1
/root/myapp/config/
orachk has taken snapshot of file attributes for above directories
at: /root/orachk/orachk_ myserver18_20160511_032034
```

3.1.5.5.4 Excluding Directories from Checks

Exclude directories from file attribute changes checks.

To exclude directories from checks:

Run the file attribute changes check command to exclude directories that you do not list in the `-includedir` discover list by using the `-excludediscovery` option.

Example 3-6 orachk -fileattr start -includedir -excludediscovery

```
orachk -fileattr start -includedir "/root/myapp/config/" -excludediscovery
CRS stack is running and CRS_HOME is not set. Do you want to set CRS_HOME
to /u01/app/12.2.0/grid?[y/n][y]
Checking for prompts on myserver18 for oragrid user...
Checking ssh user equivalency settings on all nodes in cluster
Node myserver17 is configured for ssh user equivalency for root user
List of directories(recursive) for checking file attributes:
/root/myapp/config/
orachk has taken snapshot of file attributes for above directories at: /root/
orachk/orachk_myserver18_20160511_032209
```

3.1.5.5.5 Rechecking Changes

Compare the new snapshot with the previous one to track changes.

To recheck changes:

Run the file attribute changes check command with the `check` option to take a new snapshot, and run a normal health check collection.

The `-fileattr check` command compares the new snapshot with the previous snapshot.

For example:

```
orachk -fileattr check
```

```
exachk -fileattr check
```

> **Note:**
>
> To obtain an accurate comparison between the snapshots, you must use `-fileattr check` with the same options that you used with the previous snapshot collection that you obtained with `-fileattr start`.
>
> For example, if you obtained your first snapshot by using the options `-includedir "/somedir" -excludediscovery` when you ran `-fileattr start`, then you must include the same options with `-fileattr check` to obtain an accurate comparison.

Example 3-7 orachk -fileattr check -includedir -excludediscovery

```
orachk -fileattr check -includedir "/root/myapp/config" -excludediscovery
CRS stack is running and CRS_HOME is not set. Do you want to set CRS_HOME
to /u01/app/12.2.0/grid?[y/n][y]
Checking for prompts on myserver18 for oragrid user...
Checking ssh user equivalency settings on all nodes in cluster
Node myserver17 is configured for ssh user equivalency for root user
 List of directories(recursive) for checking file attributes:
/root/myapp/config
Checking file attribute changes...
```

```
.
"/root/myapp/config/myappconfig.xml" is different:
Baseline :       0644     oracle       root /root/myapp/config/
myappconfig.xml
Current  :       0644       root       root /root/myapp/config/
myappconfig.xml
...
```

Results of the file attribute changes are reflected in the **File Attribute Changes** section of the HTML output report.

3.1.5.5.6 Designating a Snapshot As a Baseline

Designate a snapshot as a baseline to compare with other snapshots.

To designate a snapshot as a baseline:

Run the file attribute changes check command with the `-baseline` *`path_to_snapshot`* option.

The `-baseline` *`path_to_snapshot`* command compares a specific baseline snapshot with other snapshots, if you have multiple different baselines to check.

```
orachk -fileattr check -baseline path_to_snapshot
```

```
exachk -fileattr check -baseline path_to_snapshot
```

Example 3-8 orachk -fileattr check

```
orachk -fileattr check -baseline "/tmp/Snapshot"
```

3.1.5.5.7 Restricting System Checks

Restrict Oracle Orachk and Oracle Exachk to perform only file attribute changes checks.

By default, `-fileattr check` also performs a full health check run.

To restrict system checks:

Run the file attribute changes check command with the `-fileattronly` option.

```
orachk -fileattr check -fileattronly
```

```
exachk -fileattr check -fileattronly
```

3.1.5.5.8 Removing Snapshots

Remove the snapshots diligently.

To remove snapshots:

Run the file attribute changes check command with the `remove` option:

```
orachk -fileattr remove
```

```
exachk -fileattr remove
```

Example 3-9   orachk -fileattr remove

```
orachk -fileattr remove
CRS stack is running and CRS_HOME is not set. Do you want to set CRS_HOME
to /u01/app/12.2.0/grid?[y/n][y]y
Checking for prompts on myserver18 for oragrid user...
Checking ssh user equivalency settings on all nodes in cluster
Node myserver17 is configured for ssh user equivalency for root user

List of directories(recursive) for checking file attributes:
/u01/app/12.2.0/grid
/u01/app/oradb/product/12.2.0/dbhome_1
/u01/app/oradb2/product/12.2.0/dbhome_1
Removing file attribute related files...
...
```

3.1.5.6 Comparing Two Reports

Oracle Autonomous Health Framework automatically compare the two most recent HTML reports and generate a third diff report, when run in automated daemon mode.

To generate a diff HTML report, use the `-diff` option:

```
$ orachk -diff report_1 report_2
```

```
$ exachk -diff report_1 report_2
```

where, *`report_1`* and *`report_2`* are the path and name of any of the following:

- HTML reports
- Output directories
- Output zip files

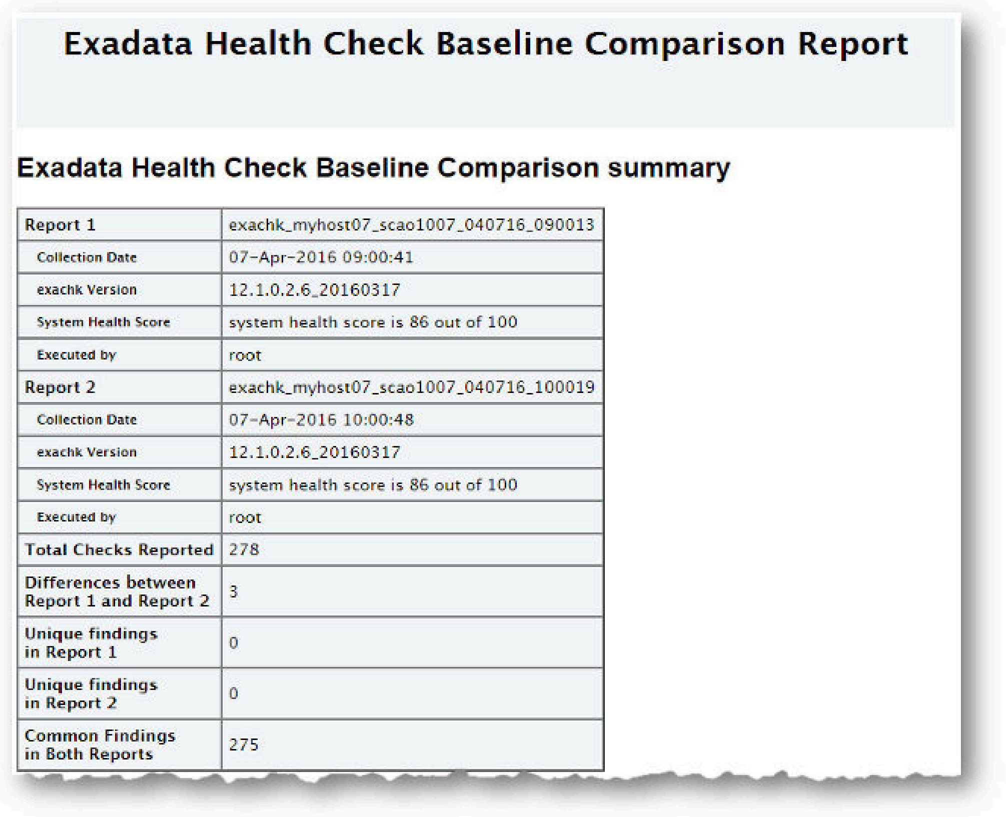
The diff output lists a summary of changes found and the location of the new diff HTML report.

```
$exachk -diff exachk_myhost07_scao1007_040716_090013.zip
exachk_myhost07_scao1007_040716_100019.zip
```

```
Summary
Total   : 278
Missing : 0
New     : 0
Changed : 3
Same    : 275
Check comparison is complete. The comparison report can be viewed
in: /opt/oracle.SupportTools/exachk/
exachk_040716090013_040716100019_diff.html
```

The diff HTML report shows a summary of both compared reports.

Figure 3-21   Health Check Baseline Comparison Report



Exadata Health Check Baseline Comparison Report

Exadata Health Check Baseline Comparison summary

Report 1	exachk_myhost07_scao1007_040716_090013
Collection Date	07-Apr-2016 09:00:41
exachk Version	12.1.0.2.6_20160317
System Health Score	system health score is 86 out of 100
Executed by	root
Report 2	exachk_myhost07_scao1007_040716_100019
Collection Date	07-Apr-2016 10:00:48
exachk Version	12.1.0.2.6_20160317
System Health Score	system health score is 86 out of 100
Executed by	root
Total Checks Reported	278
Differences between Report 1 and Report 2	3
Unique findings in Report 1	0
Unique findings in Report 2	0
Common Findings in Both Reports	275

The **Table of Contents** provides quick access to the major sections in the report. You can also access various check Ids listed in the **Show Check Ids** section.

Figure 3-22   Table of Contents

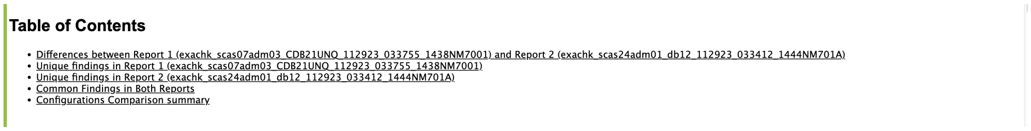
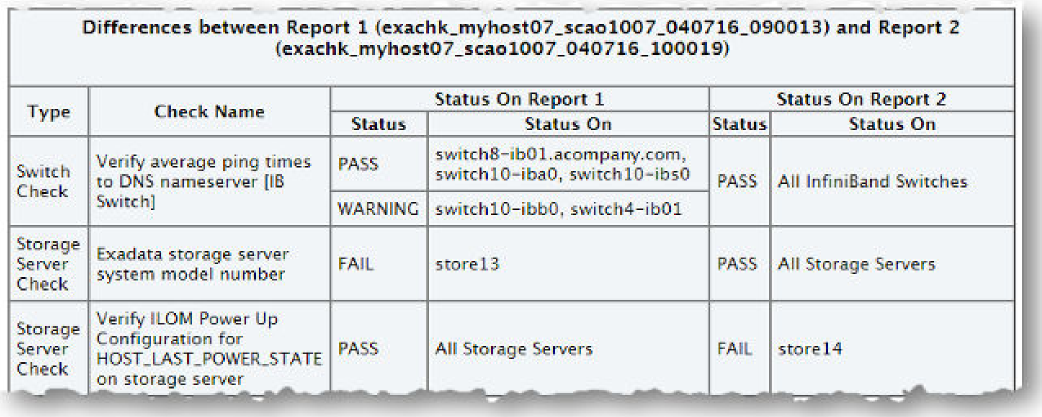


Table of Contents

- Differences between Report 1 (exachk_scas07adm03_CDB21UNQ_112923_033755_1438NM7001) and Report 2 (exachk_scas24adm01_db12_112923_033412_1444NM701A)
- Unique findings in Report 1 (exachk_scas07adm03_CDB21UNQ_112923_033755_1438NM7001)
- Unique findings in Report 2 (exachk_scas24adm01_db12_112923_033412_1444NM701A)
- Common Findings in Both Reports
- Configurations Comparison summary

The **Differences between Report 1 and Report 2** section shows what checks have different results.

Figure 3-23   Difference Between Reports

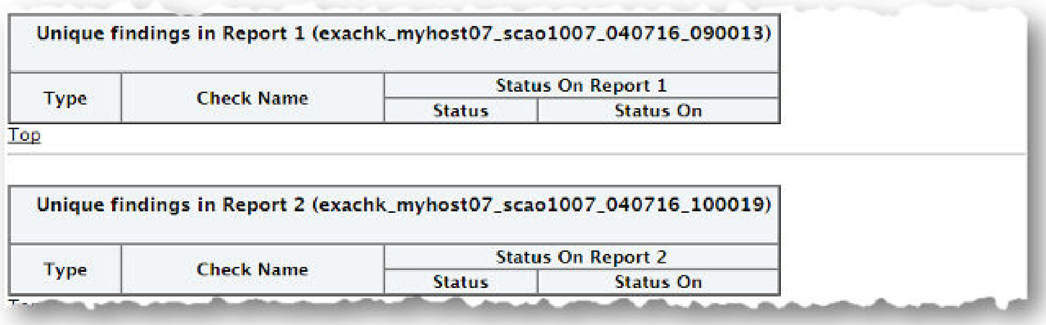


Differences between Report 1 (exachk_myhost07_scao1007_040716_090013) and Report 2 (exachk_myhost07_scao1007_040716_100019)

Type	Check Name	Status On Report 1		Status On Report 2	
		Status	Status On	Status	Status On
Switch Check	Verify average ping times to DNS nameserver [IB Switch]	PASS	switch8-ib01.acompany.com, switch10-iba0, switch10-ibs0	PASS	All InfiniBand Switches
		WARNING	switch10-ibb0, switch4-ib01		
Storage Server Check	Exadata storage server system model number	FAIL	store13	PASS	All Storage Servers
Storage Server Check	Verify ILOM Power Up Configuration for HOST_LAST_POWER_STATE on storage server	PASS	All Storage Servers	FAIL	store14

The **Unique findings** section shows any check findings that were unique to either of the reports

Figure 3-24   Unique Findings



Unique findings in Report 1 (exachk_myhost07_scao1007_040716_090013)

Type	Check Name	Status On Report 1	
		Status	Status On

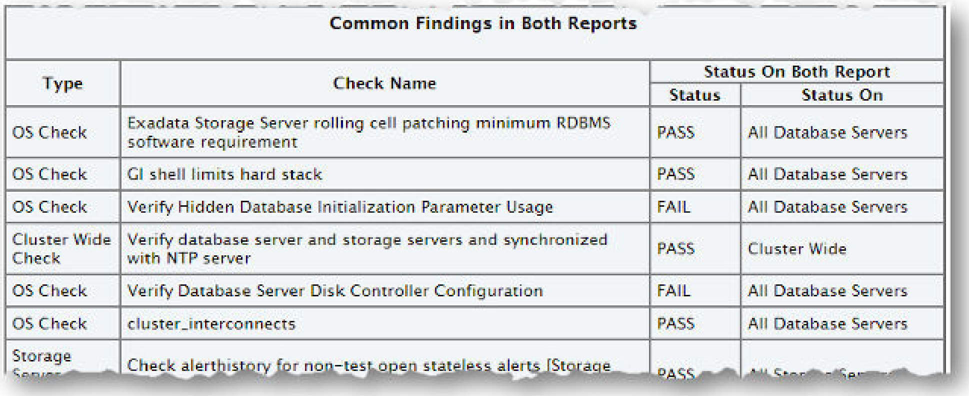
Top

Unique findings in Report 2 (exachk_myhost07_scao1007_040716_100019)

Type	Check Name	Status On Report 2	
		Status	Status On

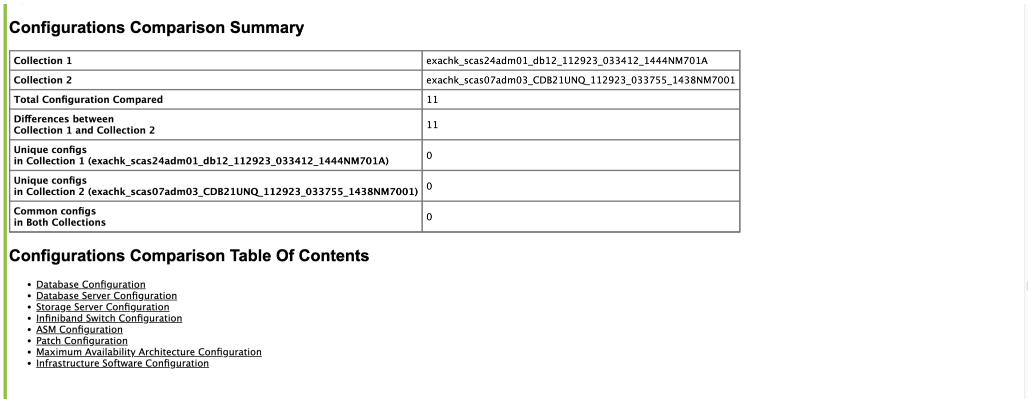
The **Common Findings in Both Reports** section shows all the check results that had the same results in both the reports.

Figure 3-25 Common Findings in Both Reports



Common Findings in Both Reports			
Type	Check Name	Status On Both Report	
		Status	Status On
OS Check	Exadata Storage Server rolling cell patching minimum RDBMS software requirement	PASS	All Database Servers
OS Check	GI shell limits hard stack	PASS	All Database Servers
OS Check	Verify Hidden Database Initialization Parameter Usage	FAIL	All Database Servers
Cluster Wide Check	Verify database server and storage servers and synchronized with NTP server	PASS	Cluster Wide
OS Check	Verify Database Server Disk Controller Configuration	FAIL	All Database Servers
OS Check	cluster_interconnects	PASS	All Database Servers
Storage Server	Check alerthistory for non-test open stateless alerts [Storage	PASS	All Storage Ser

The **Configurations Comparison** section contains comparison for various system configurations. Each sub-section under **Configurations Comparison** contains the differences, common configs and unique configs from each collection.

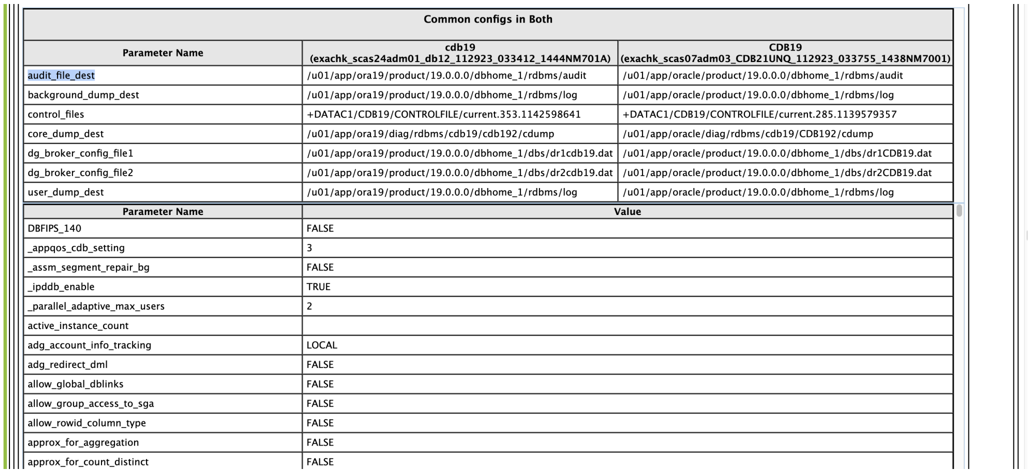


Configurations Comparison Summary

Collection 1	exachk_scas24adm01_db12_112923_033412_1444NM701A
Collection 2	exachk_scas07adm03_CDB21UNQ_112923_033755_1438NM7001
Total Configuration Compared	11
Differences between Collection 1 and Collection 2	11
Unique configs in Collection 1 (exachk_scas24adm01_db12_112923_033412_1444NM701A)	0
Unique configs in Collection 2 (exachk_scas07adm03_CDB21UNQ_112923_033755_1438NM7001)	0
Common configs in Both Collections	0

Configurations Comparison Table Of Contents

- Database Configuration
- Database Server Configuration
- Storage Server Configuration
- Infiniband Switch Configuration
- ASM Configuration
- Patch Configuration
- Maximum Availability Architecture Configuration
- Infrastructure Software Configuration



Common configs in Both		
Parameter Name	**cdb19 (exachk_scas24adm01_db12_112923_033412_1444NM701A)**	**CDB19 (exachk_scas07adm03_CDB21UNQ_112923_033755_1438NM7001)**
audit_file_dest	/u01/app/ora19/product/19.0.0.0/dbhome_1/rdbms/audit	/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/audit
background_dump_dest	/u01/app/ora19/product/19.0.0.0/dbhome_1/rdbms/log	/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/log
control_files	+DATAC1/CDB19/CONTROLFILE/current.353.1142598641	+DATAC1/CDB19/CONTROLFILE/current.285.1139579357
core_dump_dest	/u01/app/ora19/diag/rdbms/cdb19/cdb192/cdump	/u01/app/oracle/diag/rdbms/cdb19/CDB192/cdump
dg_broker_config_file1	/u01/app/ora19/product/19.0.0.0/dbhome_1/dbs/dr1cdb19.dat	/u01/app/oracle/product/19.0.0.0/dbhome_1/dbs/dr1CDB19.dat
dg_broker_config_file2	/u01/app/ora19/product/19.0.0.0/dbhome_1/dbs/dr2cdb19.dat	/u01/app/oracle/product/19.0.0.0/dbhome_1/dbs/dr2CDB19.dat
user_dump_dest	/u01/app/ora19/product/19.0.0.0/dbhome_1/rdbms/log	/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/log

Parameter Name	Value
DBFIPS_140	FALSE
_appqos_cdb_setting	3
_assm_segment_repair_bg	FALSE
_ipddb_enable	TRUE
_parallel_adaptive_max_users	2
active_instance_count	
adg_account_info_tracking	LOCAL
adg_redirect_dml	FALSE
allow_global_dblinks	FALSE
allow_group_access_to_sga	FALSE
allow_rowid_column_type	FALSE
approx_for_aggregation	FALSE
approx_for_count_distinct	FALSE

3.1.5.7 Merging Reports

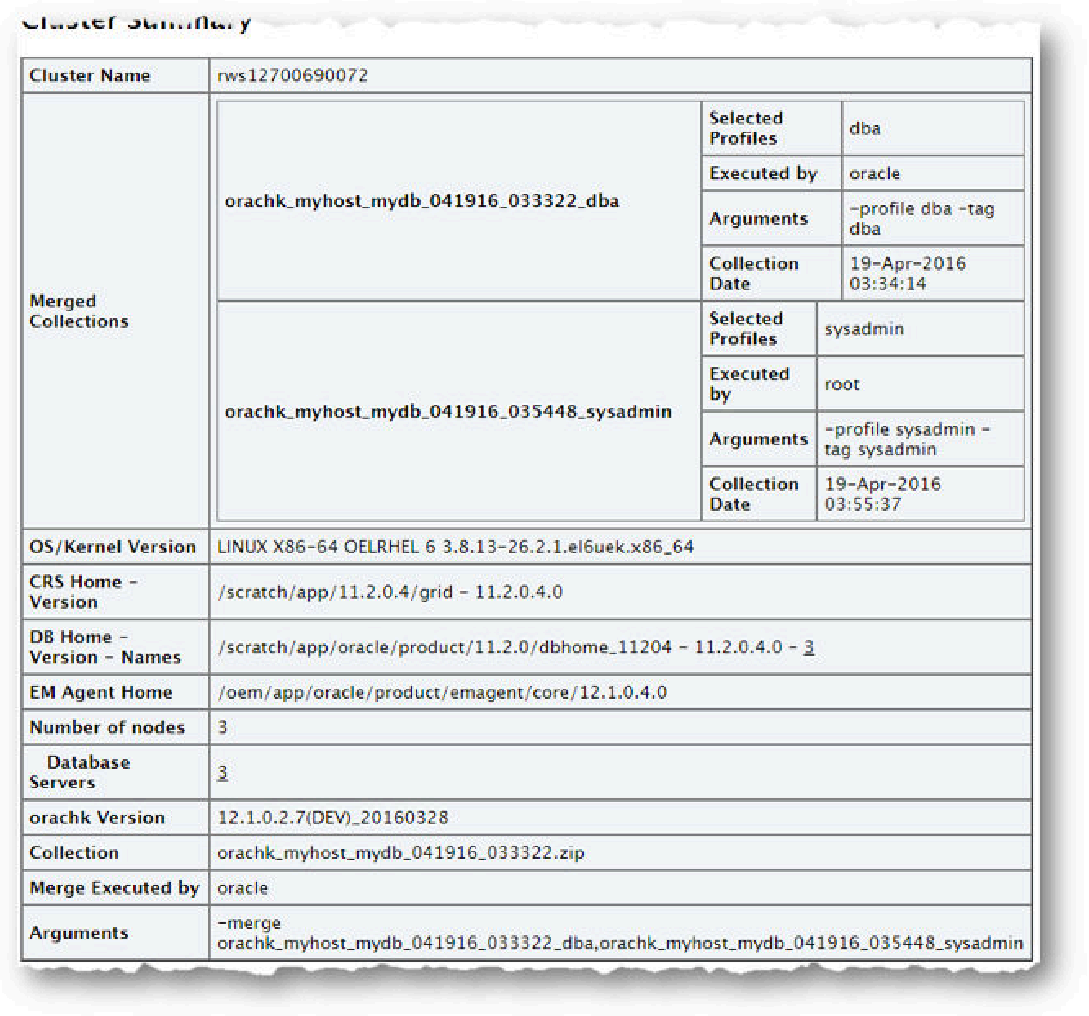
Merging reports is useful in role-separated environments where different users are run different subsets of checks and then you want to view everything as a whole.

To merge reports use the `-merge` option, followed by a comma-delimited list of directories or zip files:

```
orachk -merge
orachk_myhost_mydb_041916_033322_dba,orachk_myhost_mydb_041916_035448_sysadmi
n


exachk -merge
exachk_myhost_mydb_041916_033322_dba,exachk_myhost_mydb_041916_035448_sysadmi
n
```

The resulting merged HTML report summary will show the collections it was merged from.

Figure 3-26 Merged Report Summary

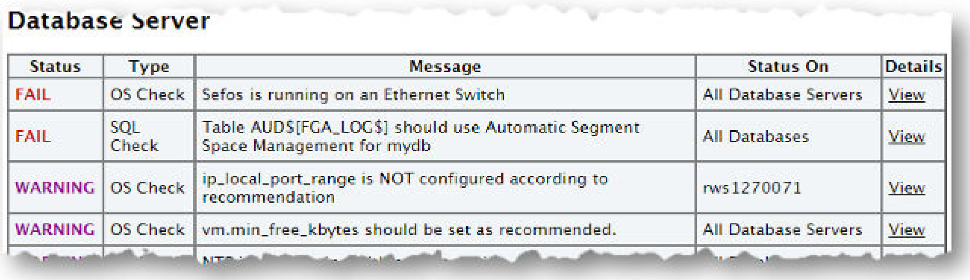


Cluster Summary

Cluster Name	rws12700690072		
Merged Collections	orachk_myhost_mydb_041916_033322_dba	Selected Profiles	dba
		Executed by	oracle
		Arguments	-profile dba -tag dba
		Collection Date	19-Apr-2016 03:34:14
	orachk_myhost_mydb_041916_035448_sysadmin	Selected Profiles	sysadmin
		Executed by	root
		Arguments	-profile sysadmin -tag sysadmin
		Collection Date	19-Apr-2016 03:55:37
OS/Kernel Version	LINUX X86-64 OELRHEL 6 3.8.13-26.2.1.el6uek.x86_64		
CRS Home - Version	/scratch/app/11.2.0.4/grid - 11.2.0.4.0		
DB Home - Version - Names	/scratch/app/oracle/product/11.2.0/dbhome_11204 - 11.2.0.4.0 - 3		
EM Agent Home	/oem/app/oracle/product/emagent/core/12.1.0.4.0		
Number of nodes	3		
Database Servers	3		
orachk Version	12.1.0.2.7(DEV)_20160328		
Collection	orachk_myhost_mydb_041916_033322.zip		
Merge Executed by	oracle		
Arguments	-merge orachk_myhost_mydb_041916_033322_dba,orachk_myhost_mydb_041916_035448_sysadmin		

The merged findings appear together.

Figure 3-27   Merged Report Findings



Database Server

Status	Type	Message	Status On	Details
FAIL	OS Check	Sefos is running on an Ethernet Switch	All Database Servers	View
FAIL	SQL Check	Table AUD$[FGA_LOG$] should use Automatic Segment Space Management for mydb	All Databases	View
WARNING	OS Check	ip_local_port_range is NOT configured according to recommendation	rws1270071	View
WARNING	OS Check	vm.min_free_kbytes should be set as recommended.	All Database Servers	View

> **Note:**
>
> For Oracle Exachk, use the `-force` option to force merge collections from `dom0` and `domu`, or `global` and `local` zones.

3.1.5.8 Maintaining Temporary Files and Directories

Oracle Orachk and Oracle Exachk create a number of temporary files and directories while running compliance checks.

Oracle Orachk and Oracle Exachk create an output directory that contains various files for you to examine. The total size of the output directory and .zip file is under 5 MB. However, the size depends on the number of Oracle stack components evaluated.

If you are running compliance checks in automated daemon mode, then set the `collection_retention` duration to purge old collections.

If you are running compliance checks on-demand or in silent mode, then it is your responsibility to implement processes and procedures to purge result output.

- Reducing the Accumulated Data Files
  Use the Oracle ORAchk and Oracle EXAchk options discussed in this section to reduce accumulated data files.

Related Topics

- Running Compliance Checks Automatically
  Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.
- Running Compliance Checks On-Demand
  Usually, compliance checks run at scheduled intervals. However, Oracle recommends that you run compliance checks on-demand when needed.
- Running Compliance Checks in Silent Mode
  Run compliance checks automatically by scheduling them with the Automated Daemon Mode operation.

- Temporary Files and Directories
  While running compliance checks, Oracle Orachk and Oracle Exachk create temporary directories and files for the purposes of data collection and assessment, and then delete them upon completion of compliance check runs.
- Output Files and Directories
  Oracle Orachk and Oracle Exachk create an output directory that contains various files for you to examine.

3.1.5.8.1 Reducing the Accumulated Data Files

Use the Oracle ORAchk and Oracle EXAchk options discussed in this section to reduce accumulated data files.

There are three options available:

- Using the `RAT_PURGE_SIZE` environment variable without the daemon
- Using the daemon option `COLLECTION_RETENTION`
- Manual reduction

> **Note:**
>
> Uploading to an Oracle Health Check Collections Manager repository or the `tfa_web` does not perform any accumulated data file reduction.

- Using the RAT_PURGE_SIZE Environment Variable Without the Daemon
- Using the Daemon Option COLLECTION_RETENTION
- Manually Reducing the Accumulated Data Files

3.1.5.8.1.1 Using the RAT_PURGE_SIZE Environment Variable Without the Daemon

Syntax

```
export RAT_PURGE_SIZE=size_in_MB
```

For example:

```
export RAT_PURGE_SIZE=2048
```

When this environment variable is set, the files in the working directory from which Oracle ORAchk or Oracle EXAchk was launched are reduced after the current Oracle ORAchk or Oracle EXAchk run completes based on two conditions:

- The total size of the working directory from which Oracle ORAchk or Oracle EXAchk run was launched exceeds the configured threshhold.
- There are files in the working directory that are more than 24 hours old from the time of the current Oracle ORAchk or Oracle EXAchk run.

Oracle ORAchk or Oracle EXAchk removes the *date-and-timestamp* subdirectories and the corresponding `*.zip` files that meet the above conditions.

For example without the `*.zip` files for brevity:

```
du -hs .
1.6G    .


[root@randomclient02 autopurge]# ls -l | egrep ^d | egrep exachk_
drwxr-x--- 9 root root   282624 Mar 26 09:46
exachk_randomclient02_PDB1_032619_090342
drwxr-x--- 9 root root   278528 Mar 26 10:33
exachk_randomclient02_PDB1_032619_095101
drwxr-x--- 9 root root   270336 Mar 26 11:16
exachk_randomclient02_PDB1_032619_103421
.
.
.
drwxr-x--- 9 root root   282624 Mar 26 15:03
exachk_randomclient02_PDB1_032619_141952
drwxr-x--- 9 root root   294912 Mar 26 15:48
exachk_randomclient02_PDB1_032619_150534
drwxr-x--- 9 root root   286720 Mar 27 08:00
exachk_randomclient02_PDB1_032719_071614


export RAT_PURGE_SIZE=1024
exachk
```

After the run completes:

```
[root@randomclient02 autopurge]# du -hs .
1.5G    .
[root@randomclient02 autopurge]# ls -l | egrep ^d | egrep exachk_
drwxr-x--- 9 root root   270336 Mar 26 11:16
exachk_randomclient02_PDB1_032619_103421
drwxr-x--- 9 root root   290816 Mar 26 11:59
exachk_randomclient02_PDB1_032619_111713
.
.
.
drwxr-x--- 9 root root   294912 Mar 26 15:48
exachk_randomclient02_PDB1_032619_150534
drwxr-x--- 9 root root   286720 Mar 27 08:00
exachk_randomclient02_PDB1_032719_071614
drwxr-x--- 9 root root   282624 Mar 27 10:36
exachk_randomclient02_PDB1_032719_094859
```

Two runs were purged, but the size did not reduce to 1 GB:

```
drwxr-x--- 9 root root   282624 Mar 26 09:46
exachk_randomclient02_PDB1_032619_090342
drwxr-x--- 9 root root   278528 Mar 26 10:33
exachk_randomclient02_PDB1_032619_095101
```

Note:

The reduction process did not reduce the total directory size to 1 GB in this example because there were not enough files in the working directory that were at least 24 hours earlier than the current Oracle ORAchk or Oracle EXAchk execution. If there are enough earlier files available, then the reduction comes close to the target size, depending upon the exact file sizes of the file set eligible for reduction.

3.1.5.8.1.2 Using the Daemon Option COLLECTION_RETENTION

This daemon option operates only upon the dates of the files eligible for reduction. Once set, any files older then the chosen target date are removed at the end of Oracle ORAchk or Oracle EXAchk run by the daemon.

Note:

Specify the `COLLECTION_RETENTION` in days.

For example, set the daemon to run the `-profile` switch every hour, retain files for 1 day.

```
exachk -id fname -set "AUTORUN_SCHEDULE=* * *;\
NOTIFICATION_EMAIL=fname.lname@somewhere.com;\
COLLECTION_RETENTION=1;\
AUTORUN_FLAGS=-profile switch"


exachk -id fname -get all

------------------------------------------------------------
ID: exachk.testuser
------------------------------------------------------------
AUTORUN_FLAGS  =  -profile switch
NOTIFICATION_EMAIL  =  fname.lname@somewhere.com
COLLECTION_RETENTION  =  1
AUTORUN_SCHEDULE  =  * * * *
------------------------------------------------------------
```

After letting the daemon run for more than a day, it can be seen the fileset has stabilized around one day's worth of hourly runs.

```
[root@randomclient02 retention]# ls -ltr | egrep ^d | egrep exachk_
drwxr-x--- 8 root root     20480 Mar 27 15:03
exachk_randomclient02_032719_150039
.
.
.
drwxr-x--- 8 root root     20480 Mar 28 04:03
exachk_randomclient02_032819_040026
drwxr-x--- 8 root root     20480 Mar 28 15:03
```

```
exachk_randomclient02_032819_150022
drwxr-x--- 8 root root     20480 Mar 28 16:03
exachk_randomclient02_032819_160022
```

> **Note:**
>
> The actual file reduction varies a bit depending upon the exact timestamps of the file set eligible for reduction and the timestamp of the current Oracle ORAchk or Oracle EXAchk run that is being executed by the daemon.

3.1.5.8.1.3 Manually Reducing the Accumulated Data Files

Run the following steps independently of any Oracle ORAchk or Orace EXAchk execution.

1. Remove the orginal `exachk.zip` file after it has been unzipped, about 250 MB.
2. Remove any debug logs that may exist after they have been uploaded to an SR or a Bug.

   ```
   -bash-4.1# du -hc *debug*
   18M     exachk_debug_120418_195653.log
   19M     exachk_debug_120418_201543.log
   24M     exachk_debug_120418_202357.log
   24M     exachk_debug_120418_205003.log
   22M     exachk_debug_120418_211816.log
   105M    total
   ```

3. Remove the date timestamp directories and zip file pairs generated by Oracle EXAchk runs after they have served their usefulness.

   For example:

   ```
   drwxr-x---  9 root root 4.0K Dec  4 20:39
   exachk_randomadm01_120418_202357
   -r--r-----  1 root root 7.0M Dec  4 20:39
   exachk_randomadm01_120418_202357.zip
   drwxr-x---  9 root root 4.0K Dec  4 20:04
   exachk_randomclient01_120418_195653
   -r--r-----  1 root root 6.4M Dec  4 20:04
   exachk_randomclient01_120418_195653.zip
   drwxr-x---  9 root root 4.0K Dec  4 20:23
   exachk_randomclient01_120418_201543
   -r--r-----  1 root root 6.4M Dec  4 20:23
   exachk_randomclient01_120418_201543.zip
   drwxr-x---  8 root root 4.0K Nov 29 20:29
   exachk_randomclient01_PDB1_112918_202702
   -r--r-----  1 root root  47K Nov 29 20:28
   exachk_randomclient01_PDB1_112918_202702.zip
   drwxr-x---  9 root root 4.0K Dec  4 22:48
   exachk_randomclient01_sing11g_120418_224719
   ```

```
-r--r-----  1 root root 113K Dec  4 22:48
exachk_randomclient01_sing11g_120418_224719.zip
```

4. Remove any `*_error.log` after it has been uploaded to an SR or a bug.

   ```
   -rw-r--r--  1 root root 4.4K Nov 27 22:51 exachk112718_223504_error.log
   ```

5. if you have manually created backups, then remove the backups when they have served their purpose.

   For example:

   ```
   /opt/oracle.SupportTools/exachk/back_up_exachk_111618_184655/build
   ```

3.1.5.9 Consuming Multiple Results in Other Tools

Optionally integrate compliance check results into various other tools.

For more information, see *Integrating Compliance Check Results with Other Tools*.

Related Topics

- Integrating Compliance Check Results with Other Tools
  Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager and other third-party tools.

3.1.6 Running Subsets of Checks

Run a subset of compliance checks where necessary.

These subsets can be a logical grouping determined by Oracle Autonomous Health Framework based on what the check is about.

You can also determine the subsets at an individual check level where you want to exclude or run only specific checks.

- Upgrade Readiness Mode (Oracle Clusterware and Oracle Database Upgrade Checks)
  You can use Upgrade Readiness Mode to obtain an Upgrade Readiness Assessment.
- Running Checks on Subsets of the Oracle Stack
  Run checks on subsets of Oracle stack such as, database, cell, switch, and so on.
- Using Profiles with Oracle Autonomous Health Framework
  Profiles are logical groupings of related checks. These related checks are grouped by a particular role, a task, or a technology.
- Excluding Individual Checks
  Excluding checks is recommended in situations where you have reviewed all check output and determined a particular check is not relevant for some particular business reason.
- Running Individual Checks
  There are times when you may want to run only specific checks.
- Finding Which Checks Require Privileged Users
  Use the **Privileged User** filter in the Health Check Catalogs to find health checks that must be run by privileged users, such as `root`.

- Option to Run Only the Failed Checks
  Option that enables Oracle Orachk and Oracle Exachk to run only the failed checks.

Related Topics

- Running Compliance Checks Automatically
  Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.
- Running Compliance Checks On-Demand
  Usually, compliance checks run at scheduled intervals. However, Oracle recommends that you run compliance checks on-demand when needed.

3.1.6.1 Upgrade Readiness Mode (Oracle Clusterware and Oracle Database Upgrade Checks)

You can use Upgrade Readiness Mode to obtain an Upgrade Readiness Assessment.

Upgrade Readiness Mode helps you plan the upgrade process for Oracle Cluster and Oracle RAC Database by automating many of the manual pre-checks and post-checks listed in the upgrade documentation.

There are two Upgrade Readiness modes:

- **Pre-upgrade check:** Run this check during the planning phase of the upgrade process. Running this check helps you ensure that you have enough time to correct potential issues before the upgrade.
- **Post-upgrade check:** Run this check after the upgrade to help you ensure the health of Oracle Grid Infrastructure and Oracle Database upgrades.

The Upgrade Readiness report provides the following information:

- The target Clusterware and database versions. The report can only provide information for releases later than 11.2.0.3.
- In pre-upgrade mode, the tool automatically detects all databases that are registered with Oracle Clusterware. It displays a list of these databases on which you can perform pre-upgrade checks.
- In post-upgrade mode, the tool detects all databases registered with Oracle Clusterware. It displays a list of databases on which you can perform post-upgrade checks. If you select any release 11.2.0.3 or earlier releases, then the tool does not perform post-upgrade checks on these databases.
- In both the modes, the tool checks the Oracle Clusterware stack and the operating system.

After the tool completes running, you are referred to the report. The report contains the upgrade readiness report and links where you can obtain additional information.

- Oracle Clusterware and Oracle Database Pre-Upgrade Checks
  During your pre-upgrade planning phase, run Oracle Autonomous Health Framework in pre-upgrade mode as the Oracle Database owner or as `root`.
- Oracle Clusterware and Oracle Database Post-Upgrade Checks
  After performing the upgrade, you can run in post-upgrade mode as the Oracle Database software owner or `root` to see further recommendations.

3.1.6.1.1 Oracle Clusterware and Oracle Database Pre-Upgrade Checks

During your pre-upgrade planning phase, run Oracle Autonomous Health Framework in pre-upgrade mode as the Oracle Database owner or as `root`.

To start pre-upgrade checking, use the `-preupgrade` option:

```
$ orachk -preupgrade
```

```
$ exachk -preupgrade
```

The tool prompts you to specify the version that you are planning to upgrade to, and then runs all of the applicable checks for that specific version.

Output is similar to a standard HTML report output. However, the report shows checks that are relevant to upgrading Oracle Clusterware and Oracle Database to the version that you have specified.

3.1.6.1.2 Oracle Clusterware and Oracle Database Post-Upgrade Checks

After performing the upgrade, you can run in post-upgrade mode as the Oracle Database software owner or `root` to see further recommendations.

To start post-upgrade checks, use the `-postupgrade` option:

```
$ orachk -postupgrade
```

```
$ exachk -postupgrade
```

Output is similar to a standard but shows only the checks that are relevant after upgrading the Clusterware and database.

Related Topics

- HTML Report Output

3.1.6.2 Running Checks on Subsets of the Oracle Stack

Run checks on subsets of Oracle stack such as, database, cell, switch, and so on.

- Running Database Checks
  During Oracle Autonomous Health Framework system checks, all Oracle Database logins are performed by using local connections.
- Running Cell Checks
  Limit the scope of compliance checks to a subset of storage servers by using the `-cell` *`cell`* option.
- Running Switch Checks
  Limit the scope of compliance checks to a subset of switches by using the `-ibswitches` *`switch`* option.

- Running Checks on Other Elements of the Oracle Stack
  The compliance checks are available for large parts of the Oracle software and hardware stack. The compliance check coverage is expanding with each new release.
- Oracle Autonomous Health Framework Support for Oracle Grid Infrastructure with no Oracle Database
  Oracle Autonomous Health Framework supports Oracle Grid Infrastructure stand-alone checks where no database is installed.

3.1.6.2.1 Running Database Checks

During Oracle Autonomous Health Framework system checks, all Oracle Database logins are performed by using local connections.

The user running the tool must have operating system authenticated system privileges in the databases where you are running the tool.

Oracle software is installed by using an Oracle software installation owner, which is commonly referred to in Oracle documentation as the Oracle user. Your system can contain multiple Oracle Database homes all owned by the same Oracle user, for example, `oracle`. Your system can also contain multiple database homes owned by different Oracle users, for example, `oracle1`, `oracle2`, `oracle3`. If you have multiple Oracle Database homes configured, and these homes are owned by different Oracle users, then you must either run the tool as `root` user, or you must log in as the Oracle user for each Oracle database that you want to check. Use that Oracle user to run the tool on the Oracle Database instance on which the user is the software installation owner.

By default, Oracle Autonomous Health Framework presents a list of running databases that are registered with Oracle Grid Infrastructure. You can run the tools on one database, run the tools on all databases, or run the tool with a comma-delimited list of numbers that designate the databases listed. When you check multiple nodes running on the cluster, you do not need to stage the tool on the other nodes in the cluster to check the database instances running on those nodes.

1. To prevent prompting for which database to run against and check all databases, use the `-dball` option.

   ```
   $ orachk -dball
   ```

   ```
   $ exachk -dball
   ```

2. To prevent prompting and skip all database checks, use the `-dbnone` option.

   ```
   $ orachk -dbnone
   ```

   ```
   $ exachk -dbnone
   ```

3. To run checks against a subset of databases, use the `-dbnames` *`database_name`* option.

You can check multiple database instances by listing them in a comma-delimited list.

```
$ orachk -dbnames db1,db2,db3
```

```
$ exachk -dbnames db1,db2,db3
```

By default, Oracle Autonomous Health Framework runs checks on all database nodes in the cluster.

4. To run checks against a subset of PDBs, use the `-pdbnames` *`pdb_name`* option.

   You can check multiple PDBs by listing them in a comma-delimited list.

   ```
   $ orachk -pdbnames pdb1,pdb2,pdb3
   ```

   ```
   $ exachk -pdbnames pdb1,pdb2,pdb3
   ```

   By default, Oracle Autonomous Health Framework runs checks on all PDBs in the cluster.

5. To run checks against a subset of cluster nodes, use the `-clusternodes` *`node`* option.

   You can check multiple cluster nodes by listing them in a comma-delimited list.

   ```
   $ orachk -clusternodes node1,node2,node3
   ```

   ```
   $ exachk -clusternodes node1,node2,node3
   ```

6. To run checks against the local node, use the `-localonly` option.

   ```
   $ orachk -localonly
   ```

   ```
   $ exachk -localonly
   ```

3.1.6.2.2 Running Cell Checks

Limit the scope of compliance checks to a subset of storage servers by using the `-cell` *`cell`* option.

1. To limit the scope to one cell, use the `-cell` option.

   ```
   orachk -cell
   ```

   ```
   exachk -cell
   ```

2. To limit the check to a set of cells, use a comma-delimited list of cells.

   ```
   $ orachk -cell cell1,cell2,cell3
   ```

   ```
   $ exachk -cell cell1,cell2,cell3
   ```

3.1.6.2.3 Running Switch Checks

Limit the scope of compliance checks to a subset of switches by using the `-ibswitches` *switch* option.

1. To limit the scope to one switch, use the `-ibswitches` option.

   ```
   $ orachk -ibswitches
   ```

   ```
   $ exachk -ibswitches
   ```

2. To limit the check to a set of switches, use a comma-delimited list of switches.

   ```
   $ orachk -ibswitches switch1,switch2
   ```

   ```
   $ exachk -ibswitches switch1,switch2
   ```

3.1.6.2.4 Running Checks on Other Elements of the Oracle Stack

The compliance checks are available for large parts of the Oracle software and hardware stack. The compliance check coverage is expanding with each new release.

The compliance checks are organized into logical groupings, which are called *profiles*. You can run subsets of checks for different areas of the Oracle stack by the applicable profile.

Refer to the Using Profiles section for a list of available profiles.

3.1.6.2.5 Oracle Autonomous Health Framework Support for Oracle Grid Infrastructure with no Oracle Database

Oracle Autonomous Health Framework supports Oracle Grid Infrastructure stand-alone checks where no database is installed.

To run Oracle Grid Infrastructure checks in an environment where Oracle Database is not installed, use the option:

```
-nordbms
```

For example:

```
$ orachk -nordbms
```

```
$ exachk -nordbms
```

3.1.6.3 Using Profiles with Oracle Autonomous Health Framework

Profiles are logical groupings of related checks. These related checks are grouped by a particular role, a task, or a technology.

The following table describes the profiles that you can use:

Table 3-5 List of Available Profiles for Oracle Autonomous Health Framework Checks

Profile	Description
`asm`	Oracle Automatic Storage Management checks.
`exatier1`	Exadata only checks with a critical alert level. These represent the top tier of problems with the most severe likely impact. You must fix the problems marked as critical as soon as possible.
`patches`	Oracle patch checks.
`bi_middleware`	Oracle Business Intelligence checks.
`clusterware`	Oracle Clusterware checks.
`compute_node`	Compute Node checks (Oracle Exalogic only).
`control_VM`	Checks only for Oracle Virtual Machine Control VM (`ec1-vm`, `ovmm`, `db`, `pc1`, `pc2`). No cross-node checks.
`corroborate`	Oracle Exadata checks, which you must review to determine pass or fail.
`dba`	Database Administrator (DBA) Checks.
`ebs`	Oracle E-Business Suite checks.
`el_extensive`	Extensive EL checks.
`el_lite`	Exalogic-Lite Checks(Oracle Exalogic Only).
`el_rackcompare`	Data Collection for Exalogic Rack Comparison Tool (Oracle Exalogic Only).
`emagent`	Oracle Enterprise Manager Cloud Control agent checks.
`emoms`	Oracle Enterprise Manager Cloud Control management server.
`em`	Oracle Enterprise Manager Cloud Control checks.
`goldengate`	Oracle GoldenGate checks.
`hardware`	Hardware-specific checks for Oracle Engineered systems.
`maa`	Maximum Availability Architecture Checks.
`nimbula`	Nimbula checks for Oracle Exalogic.
`oam`	Oracle Access Manager checks.
`obiee`	OBIEE Checks (Oracle Exalytics Only)

Table 3-5 (Cont.) List of Available Profiles for Oracle Autonomous Health Framework Checks

Profile	Description
`oim`	Oracle Identity Manager checks.
`oud`	Oracle Unified Directory server checks.
`ovn`	Oracle Virtual Networking.
`peoplesoft`	Peoplesoft best practices.
`platinum`	Platinum certification checks.
`preinstall`	Preinstallation checks.
`prepatch`	Checks to complete before patching.
`security`	Security checks.
`siebel`	Siebel Checks.
`solaris_cluster`	Oracle Solaris Cluster Checks.
`storage`	Oracle Storage Server Checks.
`switch`	InfiniBand switch checks.
`sysadmin`	System administrator checks.
`timesten`	Oracle TimesTen checks (Oracle Exalytics Only).
`user_defined_checks`	Run user-defined checks from `user_defined_checks.xml`.
`virtual_infra`	Oracle VM Server (OVS), Control VM, network time protocol (NTP), and stale virtual network interface cards (VNICs) check (Oracle Exalogic Only).
`zfs`	Oracle ZFS Storage Appliances checks (Oracle Exalogic Only).

You can run the command with an inclusion list, so that it runs only the checks in particular profiles. Run the command with the option `-profile` *`profile_name`*. You can run multiple profiles by running the command with a comma-delimited inclusion list. The inclusion list contains only the profiles that you want to run.

```
$ orachk -profile dba,clusterware
```

```
$ exachk -profile dba,clusterware
```

The output of inclusion list profile checks is similar to the standard HTML Report Output format. However, profile inclusion check reports show only output of checks that are in the specific profiles that you specify in the check.

Excluding profiles

You can also run the command with exclusion list. Run the command with the option `-excludeprofile profile_name`. When you run the command with an exclusion list, all profile checks are performed except for the checks in the profile that you list. You can list multiple profiles to exclude by running the command with a comma-delimited exclusion list.

```
$ orachk -excludeprofile dba,clusterware,ebs
```

```
$ exachk -excludeprofile dba,clusterware,ebs
```

The output of exclusion list profile checks is similar to the standard HTML Report Output format. However, profile exclusion check reports show only the checks that are not in the profiles that you specify to exclude in the check.

Including profiles

Use `-includeprofile` to specify a comma-delimited list of profiles to add profile specific checks to the existing checks list.

- `ahfctl compliance -includeprofile` *`profile1`*`,` *`profile2`*`...`
- `orachk -includeprofile` *`profile1`*`,` *`profile2`*`...`
- `exachk -includeprofile` *`profile1`*`,` *`profile2`*`...`

> **Note:**
>
> You cannot:
>
> - use `-includeprofile` and `-profile` options together
> - use `-includeprofile` and `-excludeprofile` options together

Use the `-profile` option to specify a comma-delimited list of profiles to run only the checks in the specified profiles.

Use the `-excludeprofile` option to specify a comma-delimited list of profiles to exclude from the compliance check run.

Related Topics

- HTML Report Output

3.1.6.4 Excluding Individual Checks

Excluding checks is recommended in situations where you have reviewed all check output and determined a particular check is not relevant for some particular business reason.

This allows the compliance check HTML report to be streamlined to show only the problems you need to fix.

You can exclude checks in two different ways. Both the methods require you to find the check IDs.

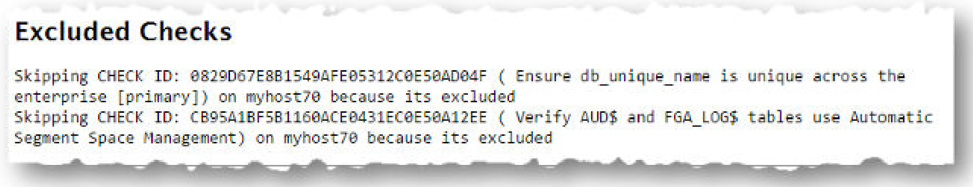
The first method is to use the `-excludecheck` *`check_id`* option. To exclude multiple check IDs, use the comma-delimited list of check IDs:

```
$ orachk -excludecheck
0829D67E8B1549AFE05312C0E50AD04F,CB95A1BF5B1160ACE0431EC0E50A12EE
```

```
$ exachk -excludecheck
0829D67E8B1549AFE05312C0E50AD04F,CB95A1BF5B1160ACE0431EC0E50A12EE
```

All excluded files are shown in the **Excluded Checks** section of the report.

Figure 3-28   Excluding Checks - Method I



Excluded Checks

```
Skipping CHECK ID: 0829D67E8B1549AFE05312C0E50AD04F ( Ensure db_unique_name is unique across the
enterprise [primary]) on myhost70 because its excluded
Skipping CHECK ID: CB95A1BF5B1160ACE0431EC0E50A12EE ( Verify AUD$ and FGA_LOG$ tables use Automatic
Segment Space Management) on myhost70 because its excluded
```

The second method of excluding individual checks is as follows:

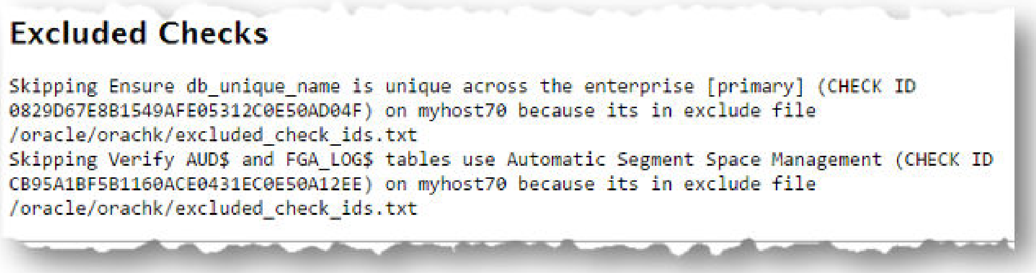
1. You must create a file called `excluded_check_ids.txt` and put all the check IDs that you want to exclude in the file one check per line.
2. You must place the file in the following directory depending on your `exachk` version:
   - For version 23.5 and down: `$AHF_HOME/exachk/`.
     Run the `exachk -showahfhome` commaned to get `AHF_HOME`.
   - For version 23.6 and up: `$EXACHK_DATA_DIR/`.
     Run the `exachk -showdatadir` command to get `EXACHK_DATA_DIR`.

   This will affect `exachk` being run manually or being called from another utility.

The `excluded_check_ids.txt` file remains in this directory. Each time the tool is run, all applicable compliance checks are run except those specified in the file.

All excluded files are shown in the **Excluded Checks** section of the report.

Figure 3-29   Excluded Checks



Excluded Checks

```
Skipping Ensure db_unique_name is unique across the enterprise [primary] (CHECK ID
0829D67E8B1549AFE05312C0E50AD04F) on myhost70 because its in exclude file
/oracle/orachk/excluded_check_ids.txt
Skipping Verify AUD$ and FGA_LOG$ tables use Automatic Segment Space Management (CHECK ID
CB95A1BF5B1160ACE0431EC0E50A12EE) on myhost70 because its in exclude file
/oracle/orachk/excluded_check_ids.txt
```

3.1.6.5 Running Individual Checks

There are times when you may want to run only specific checks.

Running individual check can particularly be useful in situations such as:

- Quickly verify if a particular issue has been fixed
- Troubleshoot performance or run specific checks
- Develop and test user-defined checks

Find the check ids before you run individual checks.

1. To run only specific checks use the `-check` *`check_id`* option.
2. To run multiple check ids, use the comma-delimited list of check ids:

```
$ orachk -check
0829D67E8B1549AFE05312C0E50AD04F,CB95A1BF5B1160ACE0431EC0E50A12EE


$ exachk -check
0829D67E8B1549AFE05312C0E50AD04F,CB95A1BF5B1160ACE0431EC0E50A12EE
```

Related Topics

- How to Find a Check ID
  Each compliance check has a unique 32 character ID.

3.1.6.6 Finding Which Checks Require Privileged Users

Use the **Privileged User** filter in the Health Check Catalogs to find health checks that must be run by privileged users, such as `root`.

Enable Javascript before you view the Health Check Catalogs.

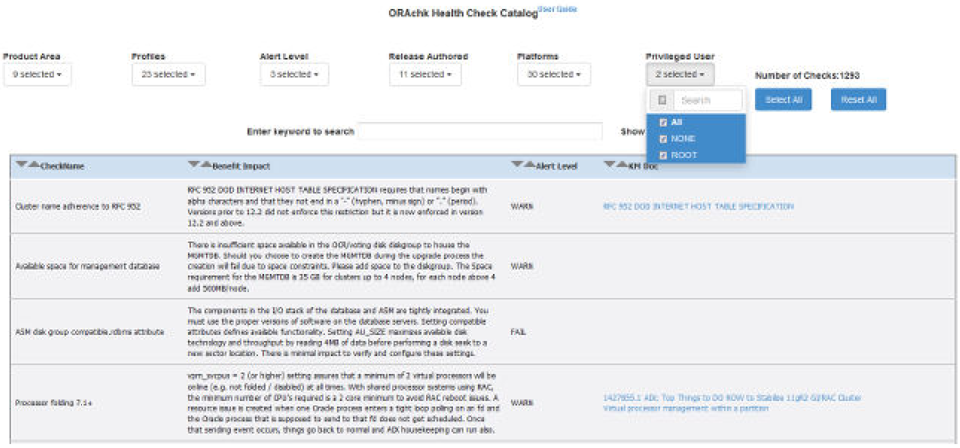
To filter health checks by privileged users:

1. Go to My Oracle Support note 2550798.1.
2. Click the **Health Check Catalog** tab.

3. Click **Open Oracle Orachk Health Check Catalog** to open or download the `ORAchk_Health_Check_Catalog.html` file.

4. Click the **Privileged User** drop-down list and then clear or select the check boxes appropriately.

Figure 3-30 Oracle Orachk - Privileged User



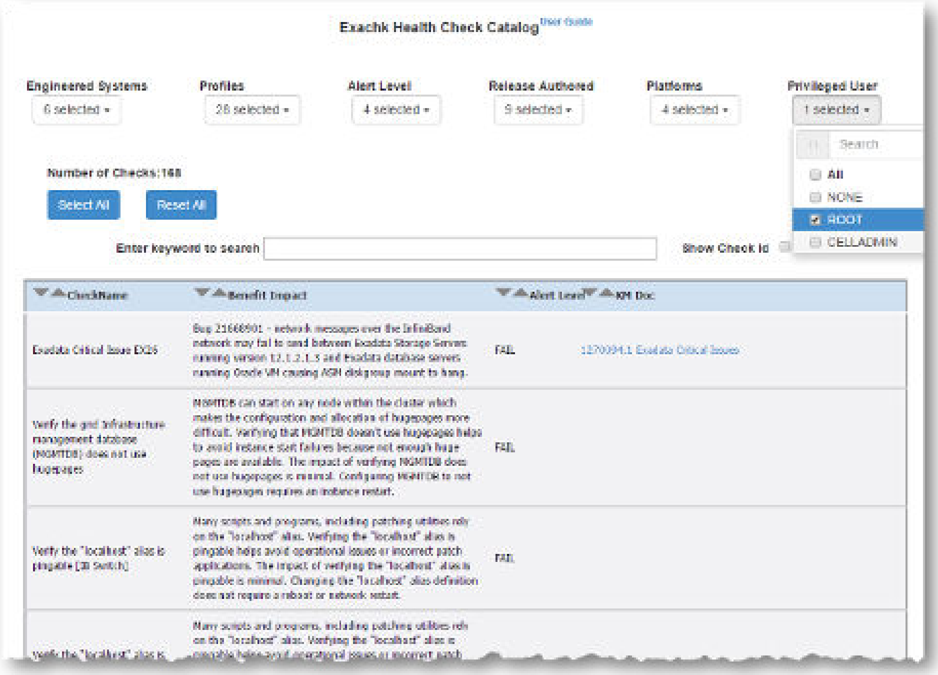
ORAchk Health Check Catalog User Guide

Product Area: 9 selected
Profiles: 23 selected
Alert Level: 3 selected
Release Authored: 11 selected
Platforms: 30 selected
Privileged User: 2 selected
☑ All
☑ NONE
☑ ROOT

Number of Checks:1293

CheckName	Benefit Impact	Alert Level	KM Doc
Cluster name adherence to RFC 952	RFC 952 DOD INTERNET HOST TABLE SPECIFICATION requires that names begin with alpha characters and that they not end in a "-" (hyphen, minus sign) or "." (period). Versions prior to 12.2 did not enforce this restriction but it is now enforced in version 12.2 and above.	WARN	RFC 952 DOD INTERNET HOST TABLE SPECIFICATION
Available space for management database	There is insufficient space available in the OCR/voting disk diskgroup to house the MGMTDB. Should you choose to create the MGMTDB during the upgrade process the creation will fail due to space constraints. Please add space to the diskgroup. The Space requirement for the MGMTDB is 35 GB for clusters up to 4 nodes, for each node above 4 add 500MB/node.	WARN	
ASM disk group compatible.rdbms attribute	The components in the I/O stack of the database and ASM are tightly integrated. You must use the proper versions of software on the database servers. Setting compatible attributes defines available functionality. Setting AU_SIZE maximizes available disk technology and throughput by reading 4MB of data before performing a disk seek to a new sector location. There is minimal impact to verify and configure these settings.	FAIL	
Processor folding 7.1+	vpm_xvcpus = 2 (or higher) setting assures that a minimum of 2 virtual processors will be online (e.g. not folded / disabled) at all times. With shared processor systems using RAC, the minimum number of CPU's required is a 2 core minimum to avoid RAC reboot issues. A resource issue is created when one Oracle process enters a tight loop polling on an fd and the Oracle process that is supposed to send to that fd does not get scheduled. Once that sending event occurs, things go back to normal and AIX housekeeping can run also.	WARN	1427855.1 AIX: Top Things to DO NOW to Stabilize 11gR2 GI/RAC Cluster Virtual processor management within a partition

Figure 3-31 Oracle Exachk - Privileged User



Exachk Health Check Catalog User Guide

Engineered Systems: 6 selected
Profiles: 28 selected
Alert Level: 4 selected
Release Authored: 9 selected
Platforms: 4 selected
Privileged User: 1 selected
☐ All
☐ NONE
☑ ROOT
☐ CELLADMIN

Number of Checks:168

CheckName	Benefit Impact	Alert Level	KM Doc
Exadata Critical Issue EX26	Bug 21668901 - network messages over the InfiniBand network may fail to send between Exadata Storage Servers running version 12.1.2.1.3 and Exadata database servers running Oracle VM causing ASM diskgroup mount to hang.	FAIL	1270094.1 Exadata Critical Issues
Verify the grid infrastructure management database (MGMTDB) does not use hugepages	MGMTDB can start on any node within the cluster which makes the configuration and allocation of hugepages more difficult. Verifying that MGMTDB doesn't use hugepages helps to avoid instance start failures because not enough huge pages are available. The impact of verifying MGMTDB does not use hugepages is minimal. Configuring MGMTDB to not use hugepages requires an instance restart.	FAIL	
Verify the "localhost" alias is pingable [IB Switch]	Many scripts and programs, including patching utilities rely on the "localhost" alias. Verifying the "localhost" alias is pingable helps avoid operational issues or incorrect patch applications. The impact of verifying the "localhost" alias is pingable is minimal. Changing the "localhost" alias definition does not require a reboot or network restart.	FAIL	
Verify the "localhost" alias is	Many scripts and programs, including patching utilities rely on the "localhost" alias. Verifying the "localhost" alias is pingable helps avoid operational issues or incorrect patch		

Related Topics

- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=2550798.1

3.1.6.7 Option to Run Only the Failed Checks

Option that enables Oracle Orachk and Oracle Exachk to run only the failed checks.

To run only the checks that failed previously:

- Generate a compliance check report
- Fix the issues identified
- Generate another compliance check report verifying only the issues that failed before

Use the failed checks option by passing in the HTML report, zip, or directory.

```
-failedchecks previous_result
```

3.1.7 Understanding Oracle Exachk specifics for Oracle Exadata and Zero Data Loss Recovery Appliance

Understand the features and learn to perform tasks specific to Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance.

- Installation Requirements for Running Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance
  Understand the requirements for installing Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance, either on your local database or on a remote device that is connected to a database.
- Using Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance
  Usage of Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance depends on other considerations such as virtualization, parallel run, and so on.
- Troubleshooting Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance
  Follow these steps to troubleshoot and fix Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance issues.

3.1.7.1 Installation Requirements for Running Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance

Understand the requirements for installing Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance, either on your local database or on a remote device that is connected to a database.

> **Note:**
>
> For more information about installing and upgrading Oracle Autonomous Health Framework, see *Installing and Upgrading Oracle Autonomous Health Framework*.

Related Topics

- Installing Oracle Autonomous Health Framework
  Learn to install Oracle Autonomous Health Framework on Linux, Unix, and Microsoft Windows operating systems.

Related Topics

- Understanding and Managing Reports and Output
  Oracle Orachk and Oracle Exachk generate a detailed HTML report with findings and recommendations.
- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=1070954.1

3.1.7.2 Using Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance

Usage of Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance depends on other considerations such as virtualization, parallel run, and so on.

- Database Default Access on the Client Interface
  If you use the client interface as the default access for your database, then use the `-clusternodes` command-line option to instruct Oracle EXAchk to communicate over the management interface.
- Virtualization Considerations
  Oracle EXAchk supports virtualization on Oracle Exadata and Zero Data Loss Recovery Appliance.
- Running Serial Data Collection
  By default, Oracle EXAchk runs parallel data collection for the storage servers, InfiniBand switches, and Oracle Databases.
- Using the root User ID in Asymmetric and Role Separated Environments
  Run Oracle EXAchk as `root` to simplify the work required in asymmetric or role separated environments.
- Environment Variables for Specifying a Different User Than root
  Review the list of environment variables for specifying a different user than `root`.
- Oracle EXAchk InfiniBand Switch Processing
  This topic explains how Oracle EXAchk InfiniBand switch processing is done when Oracle Exalogic and Oracle Exadata engineered systems reside on the same InfiniBand fabric.

3.1.7.2.1 Database Default Access on the Client Interface

If you use the client interface as the default access for your database, then use the `–clusternodes` command-line option to instruct Oracle EXAchk to communicate over the management interface.

For example, if a cluster is configured as follows, then the command must include:

```
-clusternodes dbadm01,dbadm02,dbadm03,dbadm04
```

> **Note:**
>
> When using the `-clusternodes` option, start Oracle EXAchk on the first database in the list.

Table 3-6 Example Cluster Configuration

Interface	Database Host names
Management	`dbadm01`, `dbadm02`, `dbadm03`, `dbadm04`
Client	`dbclnt01`, `dbclnt02`, `dbclnt03`, `dbclnt04`

3.1.7.2.2 Virtualization Considerations

Oracle EXAchk supports virtualization on Oracle Exadata and Zero Data Loss Recovery Appliance.

To run hardware and operating system level checks for database, storage servers, InfiniBand fabric, and InfiniBand switches:

- Install Oracle EXAchk into the management domain also referred to as `DOM0`
- Run Oracle EXAchk as `root`

When you run Oracle EXAchk from `DOM0`, Oracle EXAchk:

- Discovers all compute nodes, storage servers, and InfiniBand switches in the entire InfiniBand fabric
- Runs on all those components

To run Oracle EXAchk on a subset of nodes when Oracle EXAchk is run in the management domain, use the command-line options:

- `-clusternodes` to designate databases
- `-cells` to designate storage servers
- `-ibswitches` to designate InfiniBand switches

For example, for a full rack where only the first quarter rack is configured for virtualization, but all components are on the same InfiniBand fabric, run the following command as `root` on the `dom0` database node, *randomadm01*:

```
exachk -clusternodes randomadm01,randomadm02 \
       -cells randomceladm01,randomceladm02,randomceladm03 \
       -ibswitches randomsw-ibs0,randomsw-iba0,randomsw-ibb0
```

Run Oracle EXAchk separately for each cluster in a user domain also referred to as `DOMU`s in addition to running it in the management domain `dom0`. Within the `DOMU`, there is no need to use the above parameters because Oracle EXAchk will automatically discover the nodes in the cluster.

For example, consider 2 clusters and 4 user domains in each cluster. Although there are a total of 8 user domains, Oracle EXAchk runs only twice. Once on the first node of the first cluster running in the first user domain and once on the first node of second cluster running in the second user domain. The user domain runs do not include hardware or operating system level checks on the database, storage servers, or InfiniBand switches.

> **Note:**
>
> Run Oracle EXAchk as `root` in the management domain and the user domains.

3.1.7.2.3 Running Serial Data Collection

By default, Oracle EXAchk runs parallel data collection for the storage servers, InfiniBand switches, and Oracle Databases.

You can also configure Oracle EXAchk to run serial data collection.

To run serial data collection for the storage server, database, and InfiniBand switches, set the following environment variables:

- `RAT_COMPUTE_RUNMODE`
- `RAT_CELL_RUNMODE`
- `RAT_IBSWITCH_RUNMODE`

1. To collect database server data in serial:

   ```
   export RAT_COMPUTE_RUNMODE=serial
   ```

2. To collect storage server data in serial:

   ```
   export RAT_CELL_RUNMODE=serial
   ```

3. To collect InfiniBand switch data in serial:

   ```
   export RAT_IBSWITCH_RUNMODE=serial
   ```

Related Topics

- Slow Performance, Skipped Checks, and Timeouts
  Follow these procedures to fix slow performance and other issues.

3.1.7.2.4 Using the root User ID in Asymmetric and Role Separated Environments

Run Oracle EXAchk as `root` to simplify the work required in asymmetric or role separated environments.

If database homes are not symmetric, then install Oracle EXAchk on multiple databases in the cluster, such that there is one installation for each Oracle Database home located on a subset of databases.

For this example, assume the following configuration in the same cluster:

Table 3-7 Using root User ID in Asymmetric and Role Separated Environments

Owner User ID	Oracle Database Home	Installed on	Databases
user1	/path1/dbhome_1	db01, db02, db03, db04	dbm-a
user2	/path2/dbhome_2	db05, db06, db07, db08	dbm-b,dbm-c
grid	/path3/grid	db01, db02, db03, db04, db05, db06, db07, db08	+ASM

Further, there is role separation between user1 and user2 and Grid, such that none can access the database structure of the others. You can also enforce company policy to isolate the system administrators from the database administrators.

Do the following:

1. As root, install Oracle EXAchk in the /tmp/exachk/121026 directory on db01 .
2. As root, install Oracle EXAchk the /tmp/exachk/121026 directory on db05.
3. As root , on db01:

   ```
   cd /tmp/exachk/121026
   exachk -clusternodes db01,db02,db03,db04
   ```

   Choose dbm-a from the database selection list to collect the database checks for dbm-a.
4. As root on db05:

   ```
   cd /tmp/exachk/121026
   exachk -excludeprofiles storage,switch -clusternodes db05,db06,db07,db08
   ```

   Choose dbm-b and dbm-c from the Oracle Database selection list to collect the database checks for dbm-b and dbm-c.
5. If desired, use the -merge command-line option to merge the reports.

3.1.7.2.5 Environment Variables for Specifying a Different User Than root

Review the list of environment variables for specifying a different user than root.

- RAT_CELL_SSH_USER

  By default, Oracle EXAchk runs as root to run checks on an Oracle Exadata Storage Server.

  If security policies do not permit connection to a storage server as root over SSH, then you can specify a different user by setting this environment variable:

  ```
  export RAT_CELL_SSH_USER=celladmin
  ```

> **Note:**
>
> If you specify `RAT_CELL_SSH_USER`, then a subset of checks is run, based upon the privileges of the alternate user you specify.

- `RAT_IBSWITCH_USER`

  By default, Oracle EXAchk runs as `root` to run checks on the InfiniBand switches, when you run Oracle EXAchk on an Oracle Database as `root`. By default, when Oracle EXAchk is run as a user other than `root` on a database, the `nm2user` is used to run checks on the InfiniBand switches.

  If security policies do not permit connection to an InfiniBand switch as either the `root` or `nm2user` user over SSH, then specify a different user by setting this environment variable:

  ```
  export RAT_IBSWITCH_USER=ilom-admin
  ```

> **Note:**
>
> If you specify `RAT_IBSWITCH_USER` , then a subset of checks is run, based upon the privileges of the alternate user you specify.

3.1.7.2.6 Oracle EXAchk InfiniBand Switch Processing

This topic explains how Oracle EXAchk InfiniBand switch processing is done when Oracle Exalogic and Oracle Exadata engineered systems reside on the same InfiniBand fabric.

When an Oracle Exalogic and Oracle Exadata engineered system reside on the same InfiniBand fabric:

1. Running Oracle EXAchk on an Oracle Exadata database server excludes the Exalogic gateway switches.
2. Running Oracle EXAchk on an Oracle Exalogic compute node excludes the Exadata switches.

3.1.7.3 Troubleshooting Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance

Follow these steps to troubleshoot and fix Oracle Exachk on Oracle Exadata and Zero Data Loss Recovery Appliance issues.

Error RC-003 - No Audit Checks Were Found

Description: While identifying the environment characteristics, Oracle Exachk

- Constructs environment variables
- Compares with the Oracle Exachk rules database to determine what checks to run

If one of the environment variables does not match a known profile in the rules database, then Oracle Exachk displays an error `error RC-003 - no audit checks were found...` and exits.

Cause: The most common case occurs when an older version of Oracle Exachk is used in an Oracle Exadata Database machine environment with recently released components. This may occur because of a delay between the release of a new component or version and when Oracle Exachk incorporates support for it.

For example, when Oracle Exachk earlier than 2.1.3_20111212 were run on an Oracle Exadata Database machine where Oracle Database release 11.2.0.3.0 was deployed, Oracle Exachk exited with the following message:

```
Error RC-003 - No audit checks were found for LINUXX8664OELRHEL5_112030-.
Please refer to the section for this error code in
"Appendix A - Troubleshooting Scenarios" of the "Exachk User Guide".
```

In this example, `_112030` indicates that Oracle Database release 11.2.0.3.0 was installed on the system. Since the version of Oracle Exachk used did not support 11.2.0.3.0, Oracle Exachk could not find a known match in the Oracle Exachk rules database.

How Long Should It Take to Run Oracle Exachk?

The time it takes to run the tool varies based on the number of nodes in a cluster, CPU load, network latency, and so on. Normally the entire process takes only a few minutes per node, that is, less than 5 minutes per node. If it takes substantially more time than 5 minutes, then investigate the problem.

With the introduction of parallelized database collection in 2.2.5, the elapsed time for systems with many databases is reduced. Experience in the field is that, it normally takes about 10 minutes for a quarter rack X2-2 system with one database. On an internal X3-2 half rack with 20 storage servers, 9 InfiniBand switches, and 44 databases, the elapsed time was 44 minutes.

Related Topics

- Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options
  Review the list of Compliance Framework (Oracle Orachk and Oracle Exachk) command-line options.
- https://support.oracle.com/rs?type=doc&id=1070954.1

3.1.8 Integrating Compliance Check Results with Other Tools

Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager and other third-party tools.

- Integrating Compliance Check Results with Oracle Enterprise Manager
  Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager.
- Integrating Compliance Check Results with Third-Party Tool
  Integrate Oracle Orachk and Oracle Exachk compliance check results into various third-party log monitoring and analytics tools, such as Elasticsearch and Kibana.
- Integrating Compliance Check Results with Custom Application
  Oracle Orachk and Oracle Exachk upload collection results from multiple instances into a single database for easier consumption of check results across your enterprise.

3.1.8.1 Integrating Compliance Check Results with Oracle Enterprise Manager

Integrate Oracle Orachk and Oracle Exachk compliance check results into Oracle Enterprise Manager.

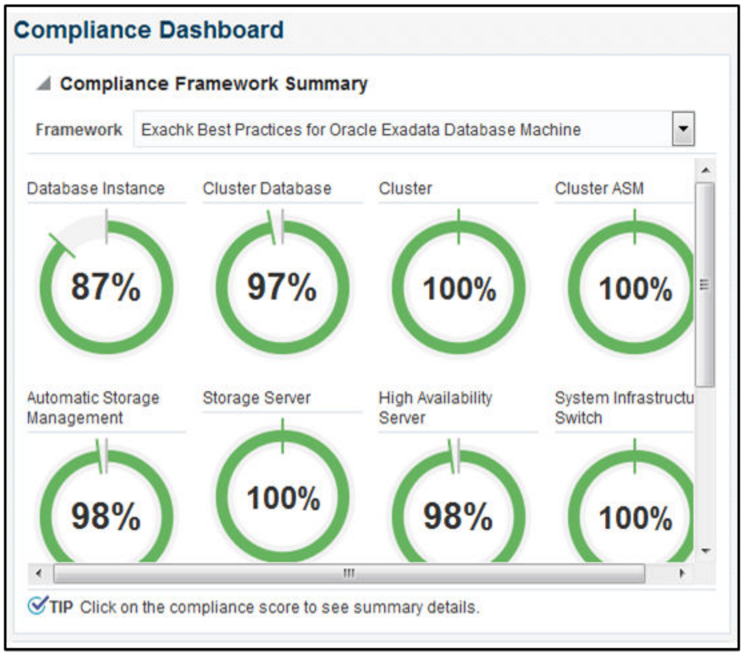
Oracle Enterprise Manager Cloud Control releases 13.1 and 13.2 support integration with Oracle Orachk and Oracle Exachk through the Oracle Enterprise Manager ORAchk Healthchecks Plug-in. The Oracle Engineered System Healthchecks plug-in supported integration with Oracle Orachk and Oracle Exachk for Oracle Enterprise Manager Cloud Control 12*c* release 12.1.0.5 and earlier releases.

With Oracle Enterprise Manager Cloud Control 13.1, Oracle Orachk and Oracle Exachk check results are integrated into the compliance framework. Integrating check results into the compliance framework enables you to display Compliance Framework Dashboards and browse checks by compliance standards.

For more information about AHF Oracle Exachk Compliance Standards for Exadata Engineered Systems managed by Enterprise Manager utilizing Autonomous Health Framework (AHF), see *AHF Exachk Compliance Standards*.

- Integrate check results into Oracle Enterprise Manager compliance framework.
- View compliance check results in native Oracle Enterprise Manager compliance dashboards.

Figure 3-32   Compliance Dashboard



Compliance Dashboard

Compliance Framework Summary

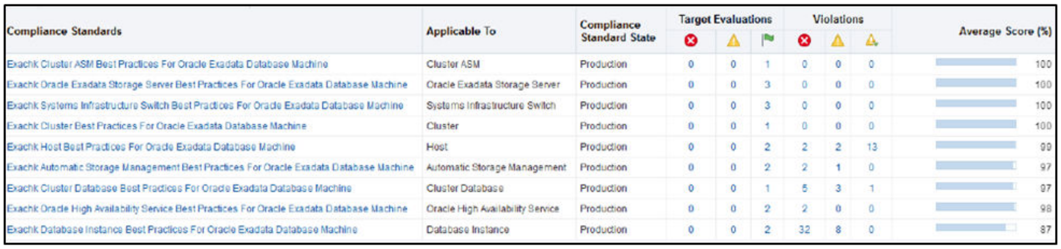
Framework: Exachk Best Practices for Oracle Exadata Database Machine

Database Instance	Cluster Database	Cluster	Cluster ASM
87%	97%	100%	100%
Automatic Storage Management	**Storage Server**	**High Availability Server**	**System Infrastructu Switch**
98%	100%	98%	100%

TIP Click on the compliance score to see summary details.

- Related checks are grouped into compliance standards where you can view targets checked, violations, and average score.

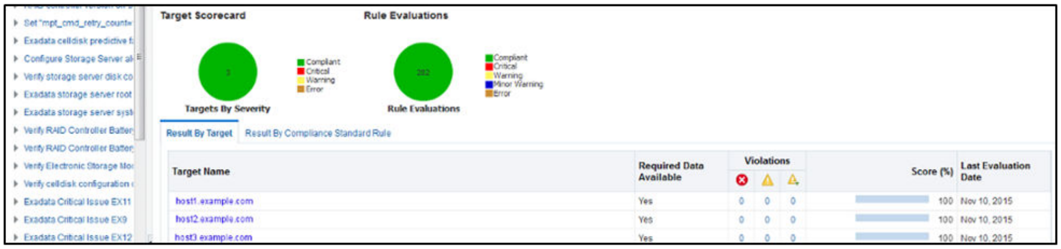
Figure 3-33 Compliance Standards



Compliance Standards	Applicable To	Compliance Standard State	Target Evaluations			Violations			Average Score (%)
			⊗	⚠	⚑	⊗	⚠	⚠	
Exachk Cluster ASM Best Practices For Oracle Exadata Database Machine	Cluster ASM	Production	0	0	1	0	0	0	100
Exachk Oracle Exadata Storage Server Best Practices For Oracle Exadata Database Machine	Oracle Exadata Storage Server	Production	0	0	3	0	0	0	100
Exachk Systems Infrastructure Switch Best Practices For Oracle Exadata Database Machine	Systems Infrastructure Switch	Production	0	0	3	0	0	0	100
Exachk Cluster Best Practices For Oracle Exadata Database Machine	Cluster	Production	0	0	1	0	0	0	100
Exachk Host Best Practices For Oracle Exadata Database Machine	Host	Production	0	0	2	2	2	13	99
Exachk Automatic Storage Management Best Practices For Oracle Exadata Database Machine	Automatic Storage Management	Production	0	0	2	2	1	0	97
Exachk Cluster Database Best Practices For Oracle Exadata Database Machine	Cluster Database	Production	0	0	1	5	3	1	97
Exachk Oracle High Availability Service Best Practices For Oracle Exadata Database Machine	Oracle High Availability Service	Production	0	0	2	2	0	0	98
Exachk Database Instance Best Practices For Oracle Exadata Database Machine	Database Instance	Production	0	0	2	32	8	0	87

- From within a compliance standard, drill-down to see individual check results and break the results by targets.

Figure 3-34 Compliance Standards Drill-Down


Set "mpt_cmd_retry_counte
Exadata celldisk predictive f
Configure Storage Server al
Verify storage server disk co
Exadata storage server root
Exadata storage server syst
Verify RAID Controller Batter
Verify RAID Controller Batter
Verify Electronic Storage Mo
Verify celldisk configuration
Exadata Critical Issue EX11
Exadata Critical Issue EX9
Exadata Critical Issue EX12
Target Scorecard
3
Compliant
Critical
Warning
Error
Targets By Severity
Rule Evaluations
282
Compliant
Critical
Warning
Minor Warning
Error
Rule Evaluations
Result By Target
Result By Compliance Standard Rule

Target Name	Required Data Available	Violations			Score (%)	Last Evaluation Date
		⊗	⚠	⚠		
host1.example.com	Yes	0	0	0	100	Nov 10, 2015
host2.example.com	Yes	0	0	0	100	Nov 10, 2015
host3.example.com	Yes	0	0	0	100	Nov 10, 2015

> **Note:**
>
> Although Oracle Orachk and Oracle Exachk do not require additional licenses, you require applicable Oracle Enterprise Manager licenses.

Related Topics

- AHF Exachk Compliance Standards
- Oracle Enterprise Manager Orachk Healthchecks Plug-in User's Guide
- Oracle Enterprise Manager Licensing Information User Manual

3.1.8.2 Integrating Compliance Check Results with Third-Party Tool

Integrate Oracle Orachk and Oracle Exachk compliance check results into various third-party log monitoring and analytics tools, such as Elasticsearch and Kibana.

JSON provides many tags to allow dashboard filtering based on facts such as:

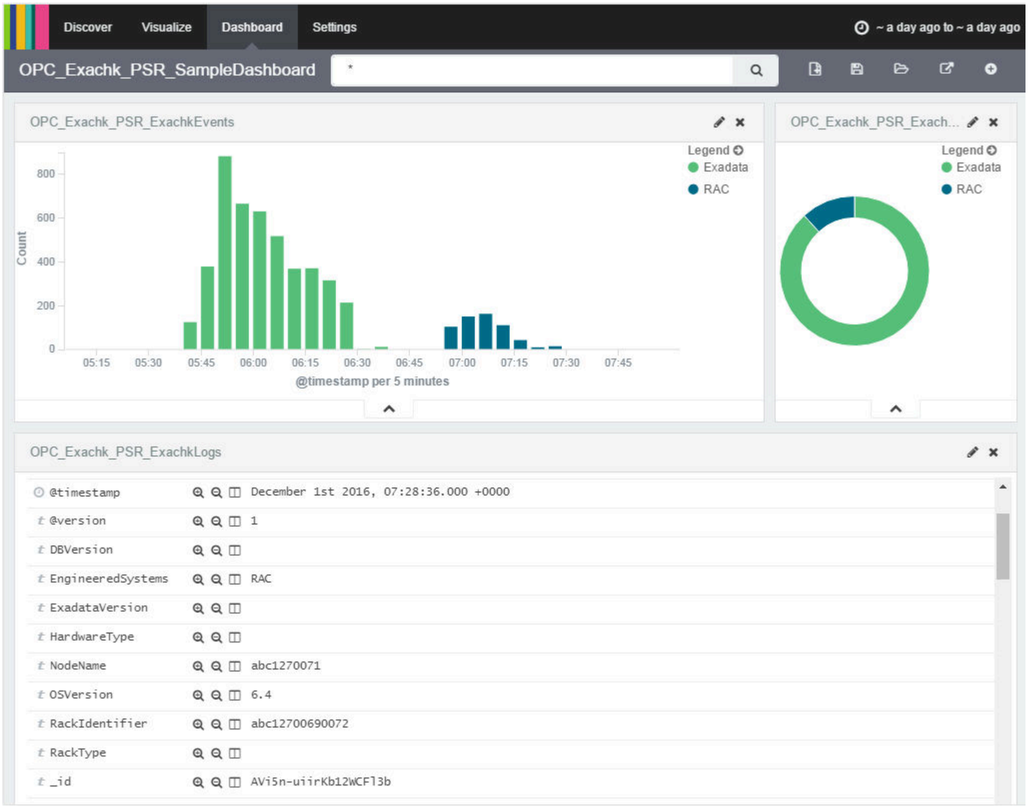
- Engineered System type
- Engineered System version
- Hardware type
- Node name
- Operating system version
- Rack identifier
- Rack type

- Database version

Use the Kibana dashboard to view compliance check across the data center.

Filter the results based on any combination of exposed system attributes.

Figure 3-35 Third-Party Tool Integration



@timestamp	December 1st 2016, 07:28:36.000 +0000
@version	1
DBVersion	
EngineeredSystems	RAC
ExadataVersion	
HardwareType	
NodeName	abc1270071
OSVersion	6.4
RackIdentifier	abc12700690072
RackType	
_id	AVi5n-uiirKb12WCFl3b

Oracle Orachk and Oracle Exachk create JSON output results in the output upload directory.

For example:

```
Report_Output_Dir/upload/mymachine_orachk_results.json
Report_Output_Dir/upload/mymachine_orachk_exceptions.json


Report_Output_Dir/upload/mymachine_exachk_results.json
Report_Output_Dir/upload/mymachine_exachk_exceptions.json
```

1. Run the `-syslog` option to write JSON results to the `syslog` daemon.
   For example:

   ```
   orachk -syslog
   ```

   ```
   exachk -syslog
   ```

2. Verify the `syslog` configuration by running the following commands:
   Oracle Orachk and Oracle Exachk use the message levels:

   - `CRIT`
   - `ERR`
   - `WARN`
   - `INFO`

   ```
   $  logger -p user.crit crit_message
   $  logger -p user.err err_message
   $  logger -p user.warn warn_message
   $  logger -p user.info info_message
   ```

3. Verify in your configured message location that each test message is written.
   For example: `/var/adm/messages`

Related Topics

- https://docs.oracle.com/cd/E19424-01/820-4809/log_syslog/index.html
- Elasticsearch: RESTful, Distributed Search & Analytics | Elastic
- Kibana: Explore, Visualize, Discover Data | Elastic

3.1.8.3 Integrating Compliance Check Results with Custom Application

Oracle Orachk and Oracle Exachk upload collection results from multiple instances into a single database for easier consumption of check results across your enterprise.

Use Oracle Health Check Collections Manager or your own custom application to consume the compliance check results.

1. Upload the collection results into the following tables at the end of a collection:

Table 3-8 Uploading Collection Results into a Database

Table	What Get's Uploaded
`rca13_docs`	Full zipped collection results.
`auditcheck_result`	Compliance check results.
`auditcheck_patch_result`	Patch check results.

   If you install Oracle Health Check Collections Manager, then these tables are created by the install script.

2. If the tables are not created, then use the following DDL statements:

   - **DDL for the RCA13_DOCS table**

   ```
   CREATE TABLE RCA13_DOCS (
       DOC_ID          NUMBER DEFAULT
   to_number(sys_guid(),'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX') NOT NULL
   ENABLE,
       COLLECTION_ID   VARCHAR2(40 BYTE),
       FILENAME        VARCHAR2(1000 BYTE) NOT NULL ENABLE,
   ```

```
    FILE_MIMETYPE   VARCHAR2(512 BYTE),
    FILE_CHARSET    VARCHAR2(512 BYTE),
    FILE_BLOB       BLOB NOT NULL ENABLE,
    FILE_COMMENTS   VARCHAR2(4000 BYTE),
    TAGS            VARCHAR2(4000 BYTE),
    ATTR1           VARCHAR2(200 BYTE),
    UPLOADED_BY     VARCHAR2(200 BYTE) DEFAULT USER,
    UPLOADED_ON     TIMESTAMP (6) DEFAULT systimestamp,
    SR_BUG_NUM      VARCHAR2(20 BYTE),
    CONSTRAINT RCA13_DOCS_PK PRIMARY KEY (DOC_ID),
    CONSTRAINT RCA13_DOCS_UK1 UNIQUE (FILENAME)
  );
```

- **DDL for the auditcheck_result table**

```
CREATE TABLE auditcheck_result (
     COLLECTION_DATE          TIMESTAMP NOT NULL ENABLE,
     CHECK_NAME               VARCHAR2(256),
     PARAM_NAME               VARCHAR2(256),
     STATUS                   VARCHAR2(256),
     STATUS_MESSAGE           VARCHAR2(256),
     ACTUAL_VALUE             VARCHAR2(256),
     RECOMMENDED_VALUE        VARCHAR2(256),
     COMPARISON_OPERATOR      VARCHAR2(256),
     HOSTNAME                 VARCHAR2(256),
     INSTANCE_NAME            VARCHAR2(256),
     CHECK_TYPE               VARCHAR2(256),
     DB_PLATFORM              VARCHAR2(256),
     OS_DISTRO                VARCHAR2(256),
     OS_KERNEL                VARCHAR2(256),
     OS_VERSION               NUMBER,
     DB_VERSION               VARCHAR2(256),
     CLUSTER_NAME             VARCHAR2(256),
     DB_NAME                  VARCHAR2(256),
     ERROR_TEXT               VARCHAR2(256),
     CHECK_ID                 VARCHAR2(40),
     NEEDS_RUNNING            VARCHAR2(100),
     MODULES                  VARCHAR2(4000),
     DATABASE_ROLE            VARCHAR2(100),
     CLUSTERWARE_VERSION      VARCHAR2(100),
     GLOBAL_NAME              VARCHAR2(256),
     UPLOAD_COLLECTION_NAME   VARCHAR2(256) NOT NULL ENABLE,
     AUDITCHECK_RESULT_ID     VARCHAR2(256) DEFAULT sys_guid()
NOT NULL ENABLE,
     COLLECTION_ID            VARCHAR2(40),
     TARGET_TYPE              VARCHAR2(128),
     TARGET_VALUE             VARCHAR2(256),
     CONSTRAINT "AUDITCHECK_RESULT_PK" PRIMARY KEY
("AUDITCHECK_RESULT_ID")
);
```

- **DDL for the auditcheck_patch_result table**

```
CREATE TABLE  auditcheck_patch_result (
       COLLECTION_DATE         TIMESTAMP(6) NOT NULL,
                HOSTNAME                 VARCHAR2(256),
                ORACLE_HOME_TYPE         VARCHAR2(256),
                ORACLE_HOME_PATH         VARCHAR2(256),
                ORACLE_HOME_VERSION      VARCHAR2(256),
                PATCH_NUMBER             NUMBER,
                CLUSTER_NAME             VARCHAR2(256),
                DESCRIPTION              VARCHAR2(256),
                PATCH_TYPE               VARCHAR2(128),
                APPLIED                  NUMBER,
                UPLOAD_COLLECTION_NAME   VARCHAR2(256),
                RECOMMENDED              NUMBER
        );
```

- Viewing and Reattempting Failed Uploads
  Use these procedures to view and reattempt to upload the failed uploads.

3.1.8.3.1 Viewing and Reattempting Failed Uploads

Use these procedures to view and reattempt to upload the failed uploads.

Values are stored in *collection_dir*/outfiles/check_env.out to record if the previous database upload was successful or not.

For example, this shows database upload has been setup, but the last upload was unsuccessful:

```
DATABASE_UPLOAD_SETUP=1
DATABASE_UPLOAD_STATUS=0
```

Oracle Autonomous Health Framework -checkfaileduploads

To see failed collections, use the -checkfaileduploads option:

```
orachk -checkfaileduploads
```

```
exachk -checkfaileduploads
```

```
$ orachk -checkfaileduploads
List of failed upload collections
/home/oracle/orachk_myserver_042016_232011.zip
/home/oracle/orachk_myserver_042016_231732.zip
/home/oracle/orachk_myserver_042016_230811.zip
/home/oracle/orachk_myserver_042016_222227.zip
/home/oracle/orachk_myserver_042016_222043.zip
```

Oracle Autonomous Health Framework -uploadfailed

To reattempt collection upload you can use the `-uploadfailed` option, specifying either all to upload all or a comma-delimited list of collections:

```
orachk -uploadfailed all|list of failed collections
```

```
exachk -uploadfailed all|list of failed collections
```

```
orachk -uploadfailed "/home/oracle/orachk_myserver_042016_232011.zip, /
home/oracle/orachk_myserver_042016_231732.zip"
```

> **Note:**
>
> You cannot upload previously uploaded collections because of the SQL unique constraint.

3.1.9 Using Oracle Orachk to Confirm System Readiness for Implementing Application Continuity

Application Continuity Checking for Application Continuity enables you to deploy Application Continuity easily and transparently.

> **Note:**
>
> Starting with Oracle Database 19.10, Application Continuity Protection Check has replaced `orachk acchk`. For more information, see *Ensuring Application Continuity* in the *Oracle® Real Application Clusters Administration and Deployment Guide*.

Related Topics

- Ensuring Application Continuity

3.1.10 Running Oracle ZFS Storage Appliance Compliance Checks

Learn to run the compliance checks for Oracle ZFS Storage Appliances.

To run Oracle Autonomous Health Framework on one Oracle ZFS appliance, use the `–zfssa` option.

To run Oracle Autonomous Health Framework on multiple Oracle ZFS appliances, specify a comma-delimited list of Oracle ZFS Storage Appliances:

```
orachk -zfssa node1,node2
```

3.1.11 Using Oracle Exachk on Oracle Big Data Appliance

Understand the features and learn to perform tasks specific to Oracle Exachk on Oracle Big Data Appliance.

- Scope and Supported Platforms for Running Oracle Exachk on Oracle Big Data Appliance
  Oracle Exachk for Oracle Big Data Appliance supports all Oracle Big Data Appliance versions later than 2.0.1.
- Running Compliance Checks on Oracle Big Data Using Oracle Exachk
  Run the `exachk compliance -h` command to view the list of options supported for Oracle Big Data Appliance.
- Reviewing Oracle Big Data Compliance Checks Output
  Identify the checks that you must act immediately to remediate, or investigate further to assess the checks that can cause performance or stability issues.
- Troubleshooting Oracle Exachk on Oracle BigData Appliance
  In addition to the base troubleshooting, the following are also applicable to Oracle Exachk on Oracle BigData.

3.1.11.1 Scope and Supported Platforms for Running Oracle Exachk on Oracle Big Data Appliance

Oracle Exachk for Oracle Big Data Appliance supports all Oracle Big Data Appliance versions later than 2.0.1.

Oracle Exachk for Oracle Big Data Appliance audits important configuration settings within an Oracle Big Data Appliance. Oracle Exachk examines the following components:

- CPU
- Hardware, firmware, and BIOS
- Operating System kernel parameters, system packages
- Ethernet network, InfiniBand switches
- RAM, hard disks
- Software Installed

Goals for Oracle Big Data Appliance Health Checks

1. Provide a mechanism to check the complete health of an Oracle Big Data Appliance on a proactive and reactive basis.
2. Provide a “recommendation engine” for best practices and tips to fix Oracle Big Data Appliance known issues.

Recommended Validation Frequency

Oracle recommends validating Oracle Big Data Appliance immediately after initial deployment, before and after any change, and at least once a quarter as part of planned maintenance operations. The runtime duration of Oracle Autonomous Health Framework depends on the number of nodes to check, CPU load, network latency, and so on.

> **Note:**
>
> Plan to run Oracle Exachk when there is less load on the Oracle Big Data Appliance. This helps you avoid runtime timeouts during health checks.

3.1.11.2 Running Compliance Checks on Oracle Big Data Using Oracle Exachk

Run the `exachk compliance -h` command to view the list of options supported for Oracle Big Data Appliance.

> **Note:**
>
> Run Oracle Exachk as `root` from *node1* of the Oracle Big Data Appliance cluster.
>
> Most of the data collection options require password for each InfiniBand switch. This is required only if there is no SSH user equivalency from running compute node to switch.

1. To view the command options, run the following command as `root` or non-root user:

   ```
   exachk -h
   ```

> **Note:**
>
> If you run any other profiles that are not not supported, then Oracle Exachk returns an error as follows:
>
> ```
> <profile_name> is not supported component. EXAchk will run generic
> checks for components identified from environment
> ```

For example, to perform all checks including the best practice checks and recommendations, run:

```
# exachk -a
```

> **Note:**
>
> If you do not specify any options, then Oracle Exachk runs with the `-a` by default.

3.1.11.3 Reviewing Oracle Big Data Compliance Checks Output

Identify the checks that you must act immediately to remediate, or investigate further to assess the checks that can cause performance or stability issues.

The following message statuses are specific to Oracle Exachk on Oracle Big Data:

Oracle Exachk on Oracle Big Data Message Definitions

Table 3-9 Oracle Exachk on Oracle Big Data Message Definitions

Message Status	Description or Possible Impact	Action to be Taken
FAIL	Shows checks that did not pass due to issues.	Address the issue immediately.
WARNING	Shows checks that can cause performance or stability issues if not addressed.	Investigate the issue further.
INFO	Indicates information about the system.	Read the information displayed in these checks and follow the instructions provided, if any.

Related Topics

- How to Remove Checks from an Existing HTML Report
  Hide individual findings from the report using **Remove findings** .
- HTML Report Output
- Comparing Two Reports
  Oracle Autonomous Health Framework automatically compare the two most recent HTML reports and generate a third diff report, when run in automated daemon mode.

3.1.11.4 Troubleshooting Oracle Exachk on Oracle BigData Appliance

In addition to the base troubleshooting, the following are also applicable to Oracle Exachk on Oracle BigData.

If you face any problems running Oracle Exachk, then create a service request through My Oracle Support.

Refer to My Oracle Support note 1643715.1 for the latest known issues specific to Oracle Exachk on Oracle BigData Appliance:

- Timeouts Checking Switches

Related Topics

- https://support.oracle.com/rs?type=doc&id=1643715.1

3.1.11.4.1 Timeouts Checking Switches

If there is a slow SSH on a given switch, then Oracle EXAchk throws an error:

```
Starting to run root privileged commands in background on INFINIBAND SWITCH
<cluster>sw-ib1.

Timed out
Unable to create temp directory on <cluster>sw-ib1

Skipping root privileged commands on INFINIBAND SWITCH <cluster> sw-ib1 is
available but SSH is blocked.
```

To resolve, increase the SSH timeout using Oracle EXAchk environment variable.

1. Reset the environment variable `RAT_PASSWORDCHECK_TIMEOUT`:

   ```
   # set RAT_PASSWORDCHECK_TIMEOUT=40
   ```

2. Rerun Oracle EXAchk.

   ```
   # exachk -a
   ```

3.1.12 Easily Manage Cell, Switches, Databases and exacli Passwords

Learn to manage passwords for cells, switches, databases, and `exacli` using the following commands:

> **Note:**
>
> The `tfactl setpassword`, `tfactl checkpassword`, and `tfactl unsetpassword` commands have been deprecated in 21.1. Oracle recommends using `ahfctl setpassword`, `ahfctl checkpassword`, and `ahfctl unsetpassword` instead.

- `tfactl setpassword`
- `tfactl checkpassword`
- `tfactl unsetpassword`

Syntax

Each command is used in this format:

```
tfactl setpassword [-nodes nodes] [-dbs databases] [-user user] [-
exacli]
```

Where:

- `-nodes`: provides a list of multiple nodes
- `-dbs`: provides a list of database names
- `-user`: provides the name of a user
- `-exacli`: to set `exacli` user of a cell

Related Topics

- ahfctl checkpassword
  Use the `ahfctl checkpassword` command to check cell, switches, databases and `exacli` passwords.
- ahfctl setpassword
  Use the `ahfctl setpassword` command to set cell, switches, databases and `exacli` passwords.
- ahfctl unsetpassword
  Use the `ahfctl unsetpassword` command to unset cell, switches, databases and `exacli` passwords.

3.1.13 Using the exadcli Utility to Collect Cell Metric Data for Guest VMs (domUs)

`exadcli` enables you to run an ExaCLI command on multiple remote nodes. Remote nodes are referenced by their host name or IP address.

Prerequisites

- Before using `exadcli`, you must use ExaCLI to accept the identity certificate of cell or database nodes. This needs to be done only once per cell (unless the cell is upgraded or a new certificate is uploaded to the remote database or cell node).
  You must accept the certificate on every cell or database node and save the cookies. The `cookie-jar` file is valid for 24 hours.

  For more information, see *Using exadcli for the First Time*.
- Java version 1.8 or later
  You can determine the version of Java by running the `java -version` command. In addition, the `JAVA_HOME` environment variable must be set to point to the installation directory of the proper version of Java.

How to run exachk to collect cell metric data

> **Note:**
>
> You can collect cell metrics only from cloud systems.

Run,

```
exachk -profile  workload-capacity
```

The output is stored in the `capacity_exadcli.out` file.

```
ls -ltra
/opt/oracle.ahf/data/.../exachk_**autostart_client_capacity***/.CELLDIR/
capacity_exadcli.out
```

Related Topics

- Using exadcli for the First Time

3.1.14 Query AHF Message Codes to Understand More About the Context and Next Steps

You can now query Oracle Orachk and Oracle Exachk check details using a four digit code representing the check.

To use this:

1. Find the four digit code for a check in the JSON result file.
2. Run: `$AHF_HOME/bin/oerr` AHF code
   For example: `$AHF_HOME/bin/oerr` *`AHF 4040`*

3.2 Oracle Health Check Collections Manager for Oracle Application Express 20.2+

Oracle Health Check Collections Manager is a companion application to Oracle Autonomous Health Framework that gives you an enterprise-wide view of your compliance check collection data.

To install or upgrade APEX, see Oracle APEX Documentation.

- Scope and Supported Platforms
  Review the scope and platforms supported for Oracle Health Check Collections Manager.
- Prerequisites
  Review the list of Oracle Health Check Collections Manager prerequisites.
- Installation
  Follow the installation procedures sequentially to install Oracle Health Check Collections Manager.
- Upgrading Oracle Health Check Collections Manager Application
  Oracle Autonomous Health Framework automatically upgrades new versions of the Oracle Health Check Collections Manager.
- Getting Started
  Familiarize yourself with the Oracle Health Check Collections Manager Application.
- Oracle Health Check Collections Manager Application Features
  Familiarize yourself with the features of Oracle Health Check Collections Manager Application.
- Viewing and Reattempting Failed Uploads
  Configure Oracle Autonomous Health Framework to display and reattempt to upload the failed uploads.
- Oracle Health Check Collections Manager Application Uninstallation
  Anytime you can decommission Oracle Health Check Collections Manager Application setup. Follow these steps sequentially to uninstall the application leaving no residual files.

- Troubleshooting Oracle Health Check Collections Manager
  This topic describes how to troubleshoot Oracle Health Check Collections Manager.
- Integrating Collection Manager with Oracle Internet Directory (LDAP) for Authentication
  After installing APEX, you can integrate AHF Collection Manager with Oracle Internet Directory (LDAP) for authentication. The steps are provided below.

Related Topics

- Documentation and reference material for Oracle APEX

3.2.1 Scope and Supported Platforms

Review the scope and platforms supported for Oracle Health Check Collections Manager.

It is difficult to run compliance checks and maintain collection data when you have several systems to manage. Oracle Health Check Collections Manager provides you an enterprise-wide view of your compliance check collection data.

Oracle Health Check Collections Manager:

- Provides a dashboard to track your collection data in one easy-to-use interface
- Displays collection data based on Business Units and time
- Serves as an enterprise-wide repository of all collections
- Uploads collection automatically

Use Oracle Application Express 20.2 or later with Oracle Database 11g Release 2, Oracle Database 12c Release 1, Oracle Database 12c Release 1, Oracle Database 12c Release 2, Oracle Database 18c, and Oracle Database 19c. Express Edition (XE) is supported only through the Oracle Technology Network (OTN) discussion forums and not through Oracle Support Services.

3.2.2 Prerequisites

Review the list of Oracle Health Check Collections Manager prerequisites.

- Oracle Database 11g Release 2 or later.
- Oracle Application Express 20.2 or later.

3.2.3 Installation

Follow the installation procedures sequentially to install Oracle Health Check Collections Manager.

> **Note:**
>
> Upgrade Oracle Health Check Collections Manager directly from Oracle Autonomous Health Framework.

- Configuring Oracle Application Express and Creating a Workspace
  Configure Oracle Application Express and create a workspace.

- Install Oracle Health Check Collections Manager Application
  To install Oracle Health Check Collections Manager, follow these procedures.
- Log in to Oracle Health Check Collections Manager Application
  To log in to Oracle Health Check Collections Manager, follow these procedures.
- Apply a Theme
  To apply a theme, follow these procedures.

Related Topics

- Running Oracle Health Check Collections Manager Commands
  Use the `-cmupgrade` command to upgrade Oracle Health Check Collections Manager.

3.2.3.1 Configuring Oracle Application Express and Creating a Workspace

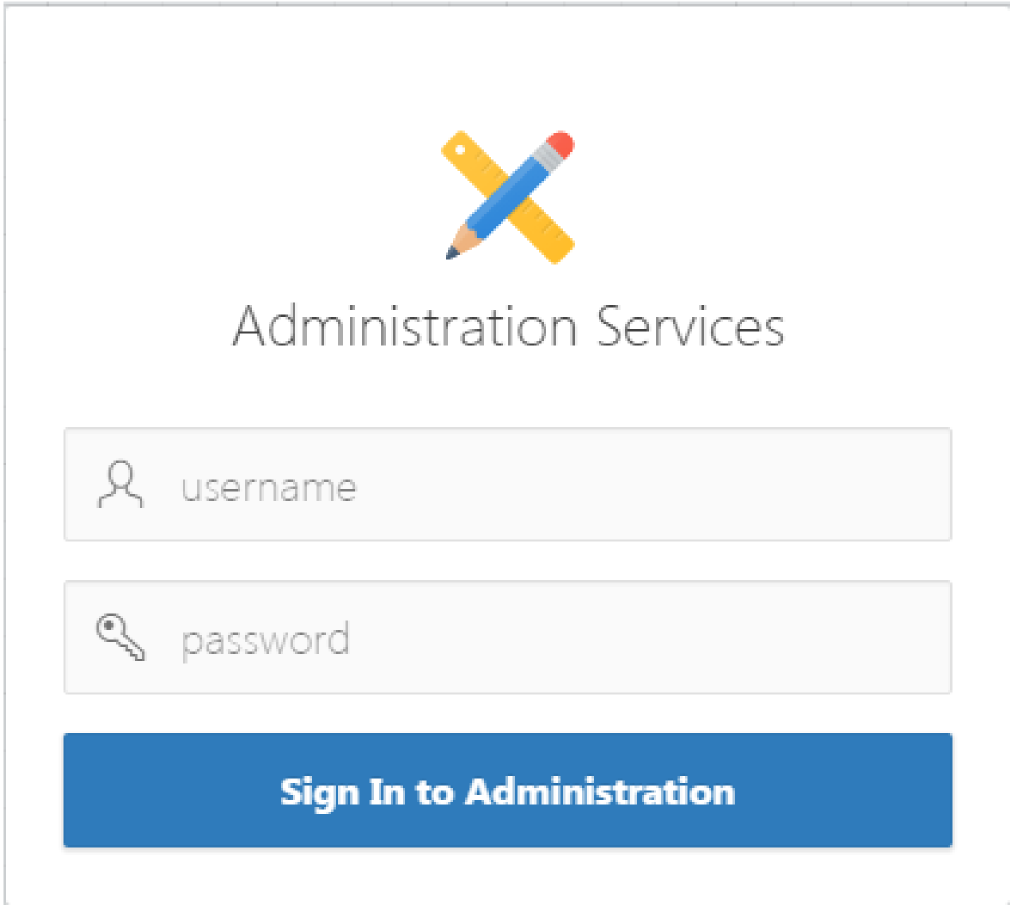
Configure Oracle Application Express and create a workspace.

1. Download the latest version of Oracle Application Express.
2. To install and configure Oracle Application Express, refer to the Application Express Installation Guide:
3. Create a workspace.
   a. Log in to Oracle Application Express administration services.

> **Note:**
>
> The URLs used for accessing the Oracle Health Check Collections Manager application depend on how Oracle Application Express was deployed initially.
>
> - If you have configured Oracle Application Express using the Oracle HTTP Server with `mod_plsql`, then specify the URL as follows:
>
>   ```
>   http://host:port/pls/apex/apex_admin
>   ```
>
> - If you have configured Oracle Application Express the Oracle XML DB HTTP listener with the embedded PL/SQL gateway, then specify the URL as follows:
>
>   ```
>   http://host:port/apex/apex_admin
>   ```
>
>   For example:
>
>   ```
>   http://dbserver.domain.com:8080/apex/apex_admin
>   ```

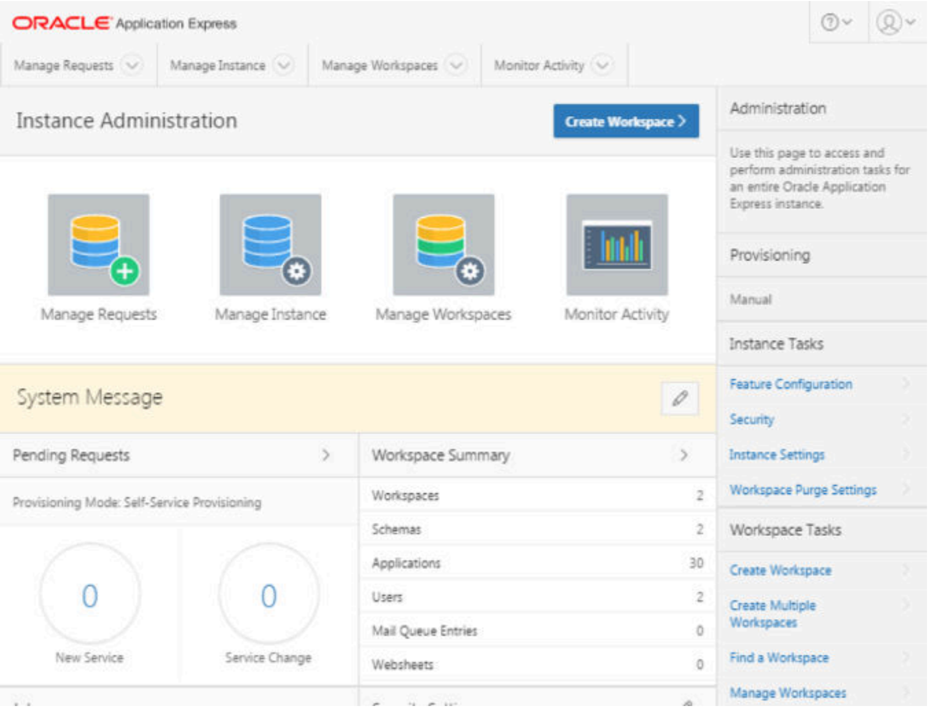
- The default schema user for Oracle Application Express administration services in the Oracle database is `ADMIN`.
- The password is the one you gave at the time of configuring the Oracle Application Express component in the Oracle database.

Figure 3-36   Administration Services Login



b. In the Oracle Application Express Admin home page, click **Manage Workspaces**.

Figure 3-37 Manage Workspace



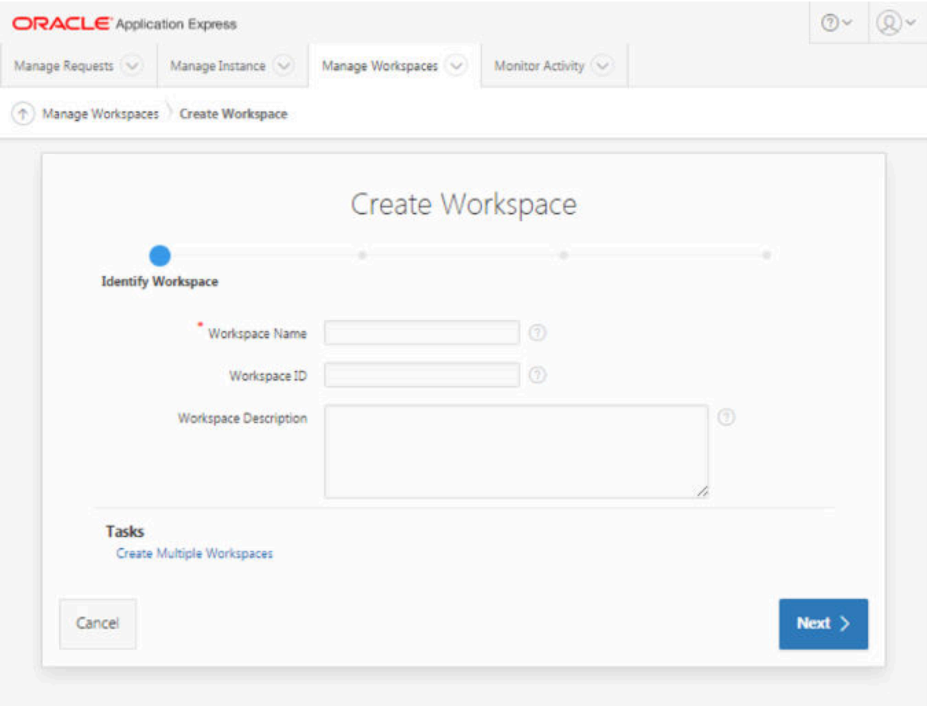
Use this page to access and perform administration tasks for an entire Oracle Application Express instance.

Workspaces	2
Schemas	2
Applications	30
Users	2
Mail Queue Entries	0
Websheets	0

c. Under **Workspace Actions**, click **Create Workspace**.

The Create Workspace Wizard appears.

Figure 3-38 Identify Workspace

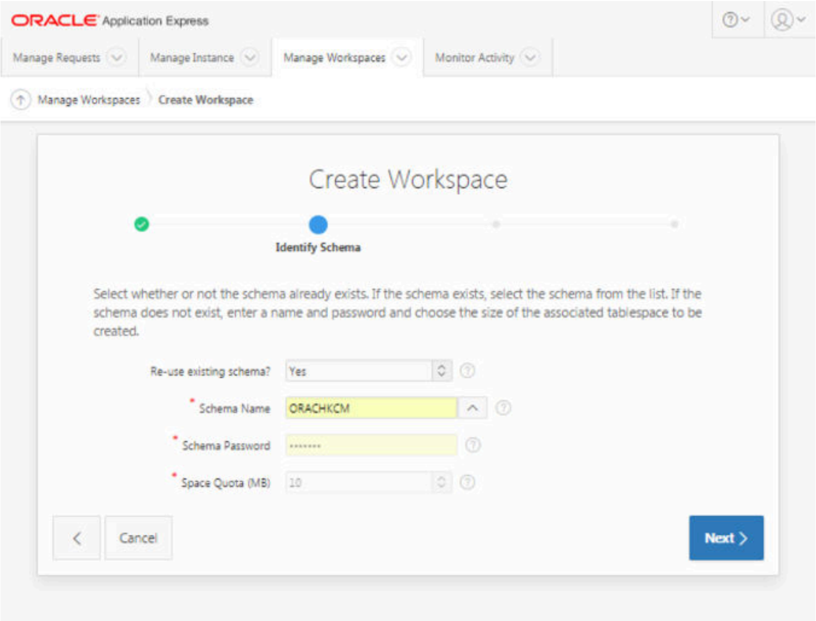


- **Identify Workspace:**
  1. **Workspace Name**: Enter a unique workspace name, for example, `ORAchk_CM_WS`.
  2. **Workspace ID**: Leave Workspace ID blank to have the new Workspace ID automatically generated.
     Workspace ID must be a positive integer greater than 100000.
  3. **Workspace Description**: Enter workspace description.
  4. Click **Next**.

> **Note:**
>
> Associate a workspace with a database schema.

- **Identify Schema:**
  1. Specify whether you are reusing an existing schema or creating a new one. This depends on whether you already have Oracle Orachk and Oracle Exachk configured to upload data to a schema in the database. If you do, then specify the existing schema. If not, then the name of the schema you create must be the one you intend to use for uploading the Oracle Orachk data once configured.
  2. If you choose an existing schema in the database, then it should not be an Oracle Application Express administration schema (admin).
     – If you are using an existing schema:
       1. For **Re-use existing schema**, select **YES**.
       2. Select a schema from the list.
       3. Click **Next**.

Figure 3-39 Identify Schema - Reuse Schema



Select whether or not the schema already exists. If the schema exists, select the schema from the list. If the schema does not exist, enter a name and password and choose the size of the associated tablespace to be created.

Re-use existing schema? Yes

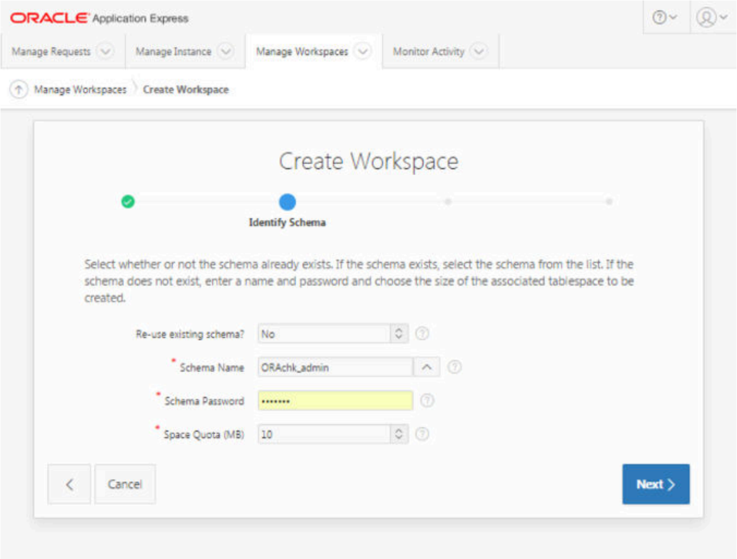
* Schema Name ORACHKCM

* Schema Password ••••••••

* Space Quota (MB) 10

- If you are creating a new schema:
  1. For **Re-use existing schema**, select **NO**.
  2. Enter the schema name and password, for example, ORAchk_admin, and so on.
  3. Specify the space quota.
  4. Click **Next**.

Figure 3-40 Identify Schema - New Schema



Create Workspace

Select whether or not the schema already exists. If the schema exists, select the schema from the list. If the schema does not exist, enter a name and password and choose the size of the associated tablespace to be created.

Re-use existing schema? No

* Schema Name ORAchk_admin

* Schema Password •••••••

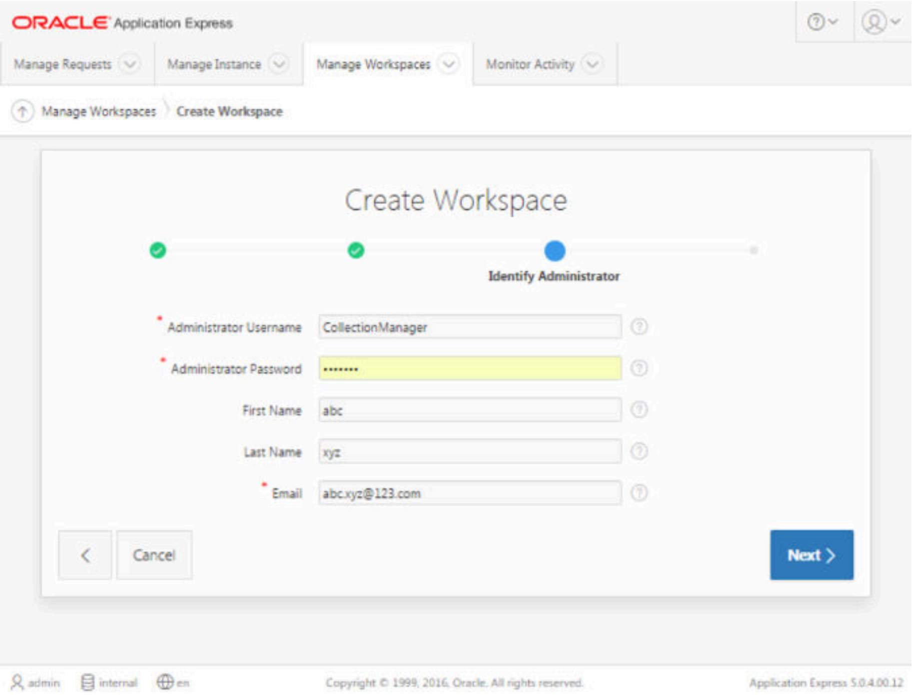
* Space Quota (MB) 10

Note:

Minimum Space Quota should not be less than 100 MB to prevent application import failures.

- **Identify Administrator:**
  1. Enter administrator user name and password.
  2. Enter Personal details.
  3. Click **Next**.

Figure 3-41   Identify Administrator



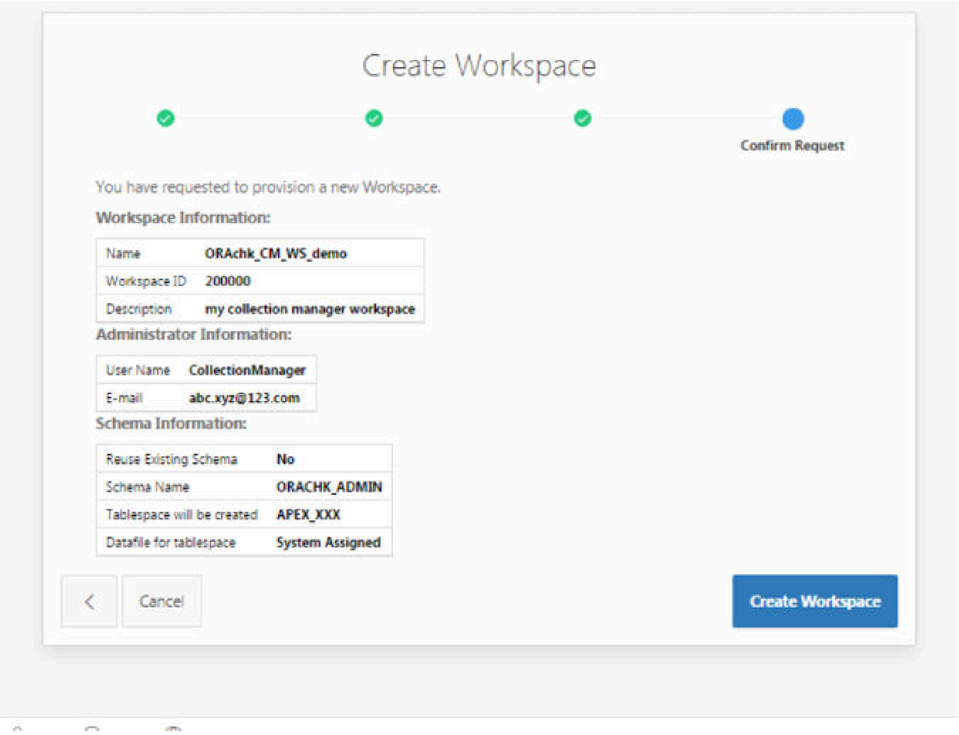
Create Workspace

Identify Administrator

* Administrator Username	CollectionManager
* Administrator Password	•••••••
First Name	abc
Last Name	xyz
* Email	abc.xyz@123.com

- Confirm your selections and then click **Create Workspace**.

Figure 3-42   Create Workspace - Confirm Request



Create Workspace

Confirm Request

You have requested to provision a new Workspace.

Workspace Information:

Name	ORAchk_CM_WS_demo
Workspace ID	200000
Description	my collection manager workspace

Administrator Information:

User Name	CollectionManager
E-mail	abc.xyz@123.com

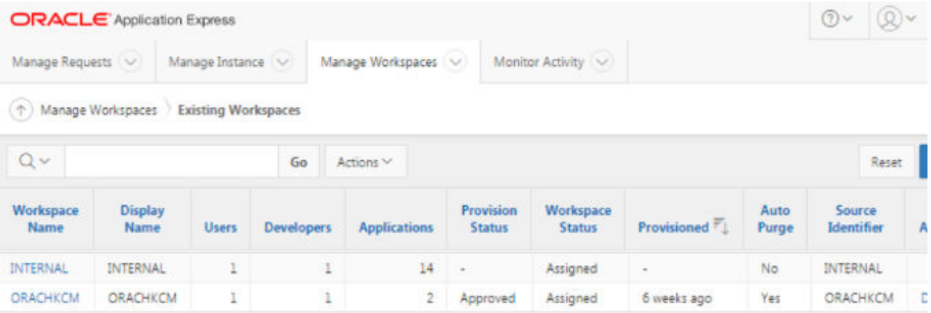
Schema Information:

Reuse Existing Schema	No
Schema Name	ORACHK_ADMIN
Tablespace will be created	APEX_XXX
Datafile for tablespace	System Assigned

Your workspace is created.

4. Click **Manage Workspaces**.
   - Under **Workspace Reports**, click **Existing Workspaces**.

     Figure 3-43 Manage Workspaces - Existing Workspaces

Workspace Name	Display Name	Users	Developers	Applications	Provision Status	Workspace Status	Provisioned	Auto Purge	Source Identifier	A
INTERNAL	INTERNAL	1	1	14	-	Assigned	-	No	INTERNAL	
ORACHKCM	ORACHKCM	1	1	2	Approved	Assigned	6 weeks ago	Yes	ORACHKCM	D

   - To edit Workspace information, click the workspace name, edit any necessary details, and then click **Apply Changes**.
   - Log out from Oracle Application Express Administration services.

- Log in to the Workspace
  Log in to Oracle Application Express admin user workspace using these procedures.
- Oracle Application Express User Accounts
  Oracle Application Express provides three types of users, namely, workspace administrators, developers, and end users.

Related Topics

- http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html
- https://docs.oracle.com/cd/E59726_01/install.50/e39144/toc.htm

3.2.3.1.1 Log in to the Workspace

Log in to Oracle Application Express admin user workspace using these procedures.

1. Log in to Oracle Application Express Admin User Workspace.

Note:

The URLs used for accessing the Oracle Health Check Collections Manager application depend on how Oracle Application Express was deployed initially.

- If you have configured Oracle Application Express the Oracle HTTP Server with `mod_plsql`, then specify the URL as follows:

  ```
  http://host:port/pls/apex/apex_admin
  ```

- If you have configured Oracle Application Express using the Oracle XML DB HTTP listener with the embedded PL/SQL gateway, then specify the URL as follows:

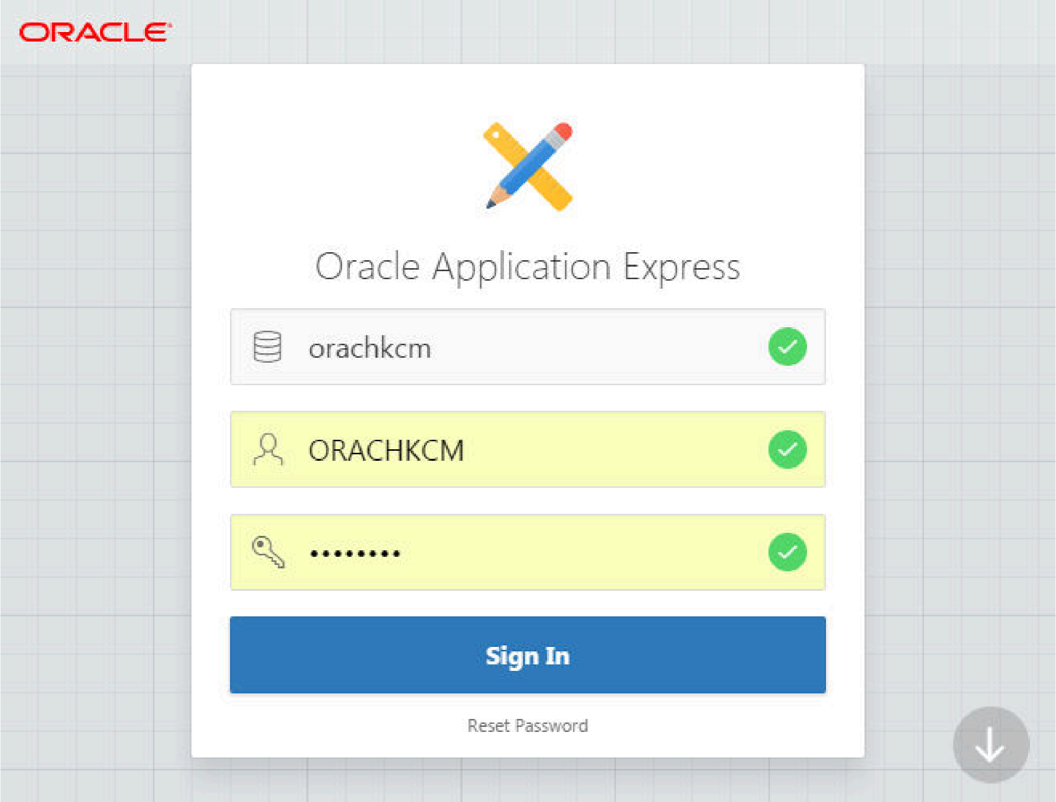
  ```
  http://host:port/apex/apex_admin
  ```

  For example:

  ```
  http://dbserver.domain.com:8080/apex/apex_admin
  ```

2. To log in, enter the workspace name, workspace user name, and password details.

Figure 3-44 Log in to the Workspace



Oracle Application Express

orachkcm

ORACHKCM

••••••••

3. For the first time login, Application Express prompts you to change the password.

4. Log in again using the new password.

3.2.3.1.2 Oracle Application Express User Accounts

Oracle Application Express provides three types of users, namely, workspace administrators, developers, and end users.

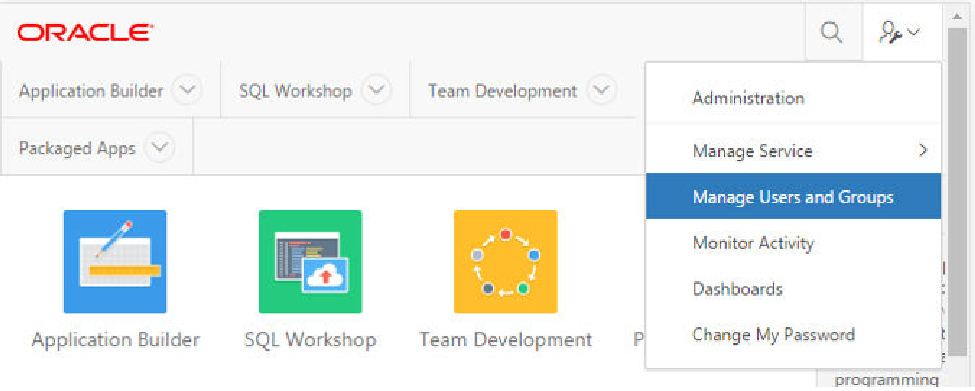
Table 3-10 Oracle Application Express Types of Users

Type of User	Description
Workspace administrators	Workspace administrators can also create and edit user accounts, manage groups, and manage development services.
Developers	Developers can create and modify applications and database objects.
End users	End users are non-administrative who have no development privileges and can only access applications that do not use an external authentication scheme. For the Oracle Health Check Collections Manager Application, almost all the users fall into this category. A special role within the Oracle Health Check Collections Manager Application, DBA Managers, and the DBAs manage all application users.

To grant access to the Oracle Health Check Collections Manager Application for non-administrative users, log in to the Workspace as an administrator.

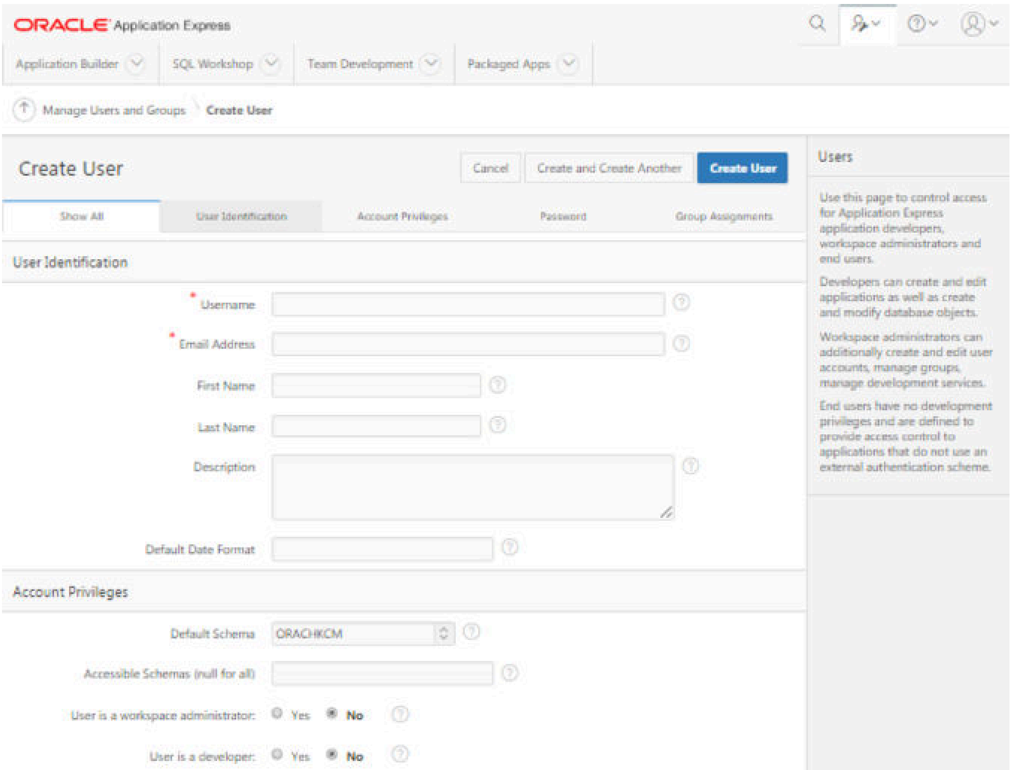
1. Log in to Oracle Application Express admin user workspace.
2. Click the **Administration** tab.
3. Click **Manage Users and Groups**.

Figure 3-45 Manage Users and Groups



4. Click **Create User**.
   - These users are application admin users, DBA Managers, and DBAs who can authenticate to the application and manage their collections.
5. Fill in the user details.
   - Follow a consistent naming convention and specify unique user names. A reasonable naming convention would be `firstname.lastname`.

Figure 3-46 Application Express User Accounts



Create User

User Identification

* Username	
* Email Address	
First Name	
Last Name	
Description	
Default Date Format	

Account Privileges

Default Schema	ORACHKCM
Accessible Schemas (null for all)	
User is a workspace administrator:	○ Yes ● No
User is a developer:	○ Yes ● No

Users

Use this page to control access for Application Express application developers, workspace administrators and end users.

Developers can create and edit applications as well as create and modify database objects.

Workspace administrators can additionally create and edit user accounts, manage groups, manage development services.

End users have no development privileges and are defined to provide access control to applications that do not use an external authentication scheme.

- For non-administrators, use the default, **No** for **User is a developer** and **User is a Workspace Administrator** options.

6. Assign a temporary password for each user and communicate that password to them. Application Express prompts them to change this password the first time they log in.
7. Click **Create User**.

3.2.3.2 Install Oracle Health Check Collections Manager Application

To install Oracle Health Check Collections Manager, follow these procedures.

1. Verify if the workspace admin schema owner and the owner of the schema used for import of the Oracle Health Check Collections Manager Application have grants to:

   - `Create Job`
   - Execute on the database packages `DBMS_RLS` and `UTL_SMTP` owned by the `SYS` user.

   The Oracle Health Check Collections Manager Application is distributed as an SQL script. Stage the script on the workstation that is used to install the application.

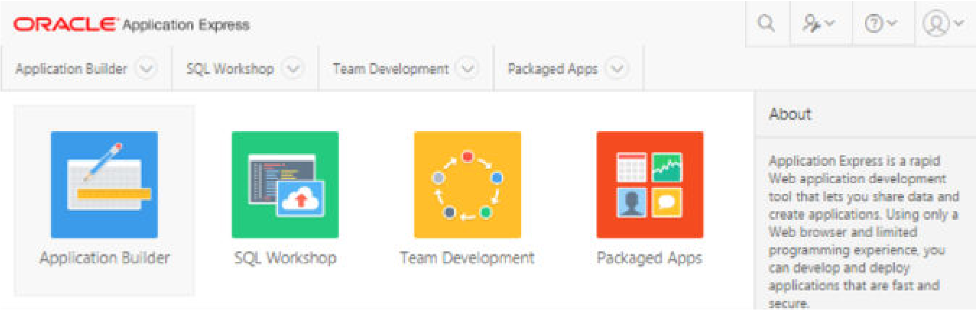
   Execute privilege on the database package `UTL_SMTP` is required only if you use Oracle Health Check Collections Manager Email Notification System Feature. Oracle Health Check Collections Manager uses `UTL_SMTP` package on one of the objects `RAC13_EMAIL`. Failing to grant `EXECUTE ON UTL_SMTP` privilege to workspace owner ends up in compilation error. You can see this information in the **Installation Summary**. Ignore this information, if you are not using the Oracle Health Check Collections Manager Email Notification System feature.

2. Verify if you have required privileges by running the SQL query as follows:

```
select GRANTEE,TABLE_NAME,PRIVILEGE  from USER_TAB_PRIVS;
GRANTEE       TABLE_NAME     PRIVILEGE
CM_USER      DBMS_RLS         EXECUTE
CM_USER      UTL_SMTP         EXECUTE

select USERNAME,PRIVILEGE from USER_SYS_PRIVS;
USERNAME     PRIVILEGE
CM_USER      CREATE JOB
```

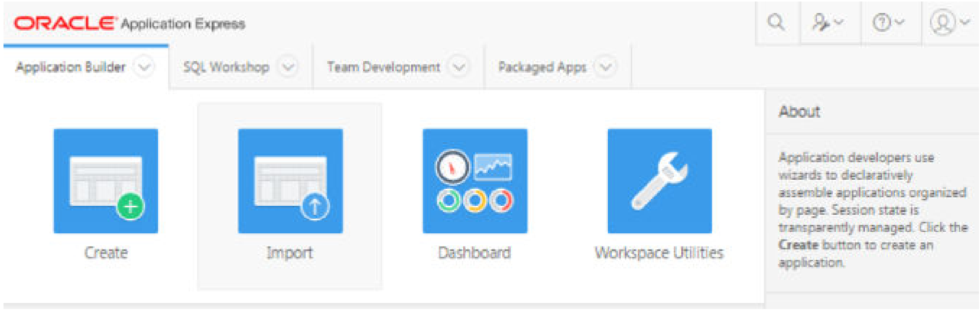
3. Log in to the Oracle Application Express workspace administration services.
4. Click **Application Builder** on the **Home** page.

Figure 3-47   Home Page



Application Express is a rapid Web application development tool that lets you share data and create applications. Using only a Web browser and limited programming experience, you can develop and deploy applications that are fast and secure.

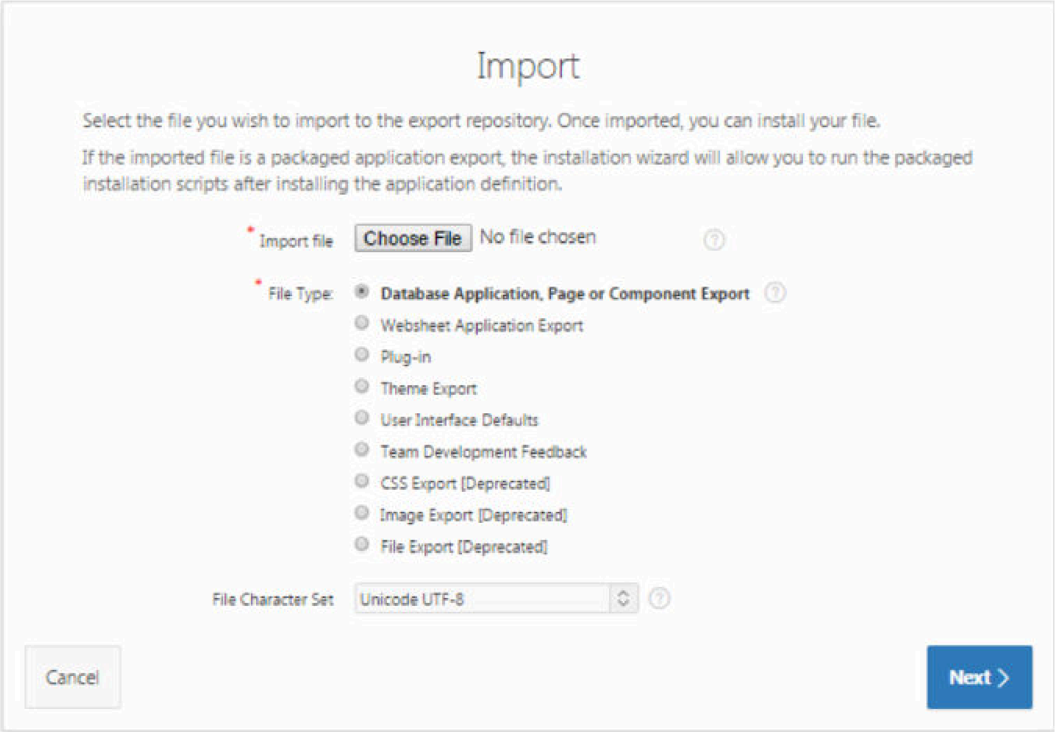
Figure 3-48   Application Builder



Application developers use wizards to declaratively assemble applications organized by page. Session state is transparently managed. Click the **Create** button to create an application.

5. Click **Import** .
6. Click **Choose import file**, select the SQL script appropriate for the Oracle Application Express version you are using:
   - `Apex5_CollectionManager_App.sql` when using Oracle Application Express 5.x
7. **File type**: select the default option **Database Application**, or **Component Export**.
8. **File Character Set**: select the default option **Unicode UTF-8**.
9. Click **Next**.

Figure 3-49 Specify File



Import

Select the file you wish to import to the export repository. Once imported, you can install your file.

If the imported file is a packaged application export, the installation wizard will allow you to run the packaged installation scripts after installing the application definition.

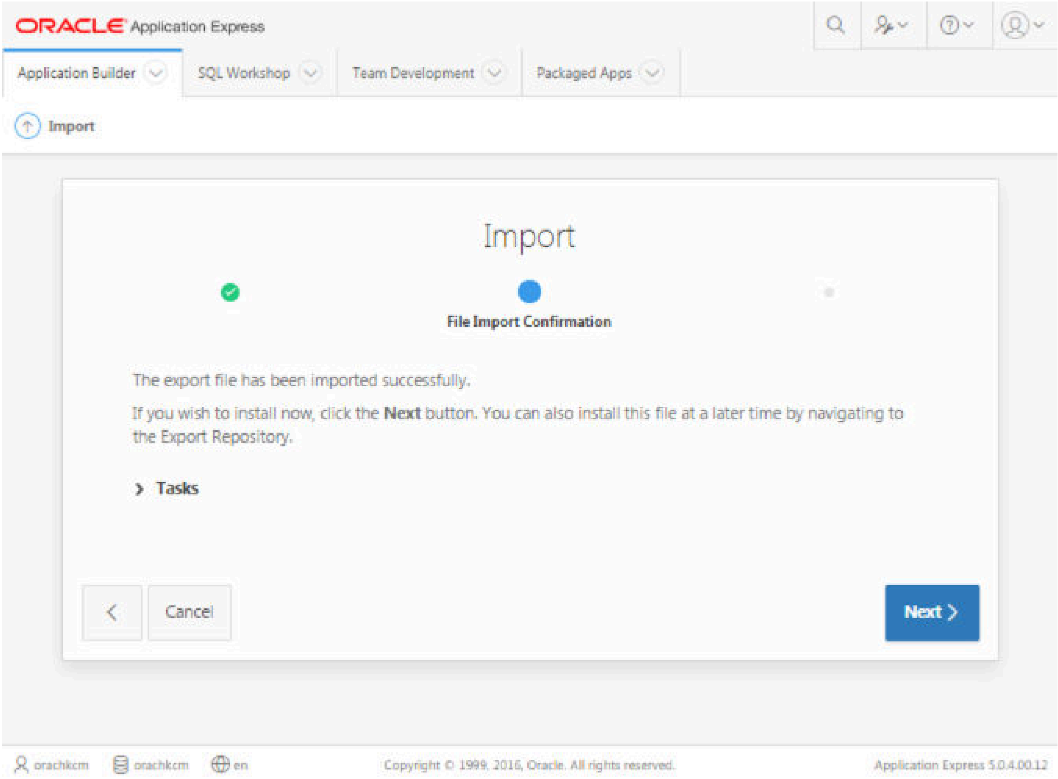
* Import file: Choose File No file chosen

* File Type:
- ● Database Application, Page or Component Export
- ○ Websheet Application Export
- ○ Plug-in
- ○ Theme Export
- ○ User Interface Defaults
- ○ Team Development Feedback
- ○ CSS Export [Deprecated]
- ○ Image Export [Deprecated]
- ○ File Export [Deprecated]

File Character Set: Unicode UTF-8

10. Click **Install Application**.

Figure 3-50 File Import Confirmation



ORACLE Application Express
Application Builder
SQL Workshop
Team Development
Packaged Apps
Import

Import

File Import Confirmation

The export file has been imported successfully.

If you wish to install now, click the **Next** button. You can also install this file at a later time by navigating to the Export Repository.

› Tasks

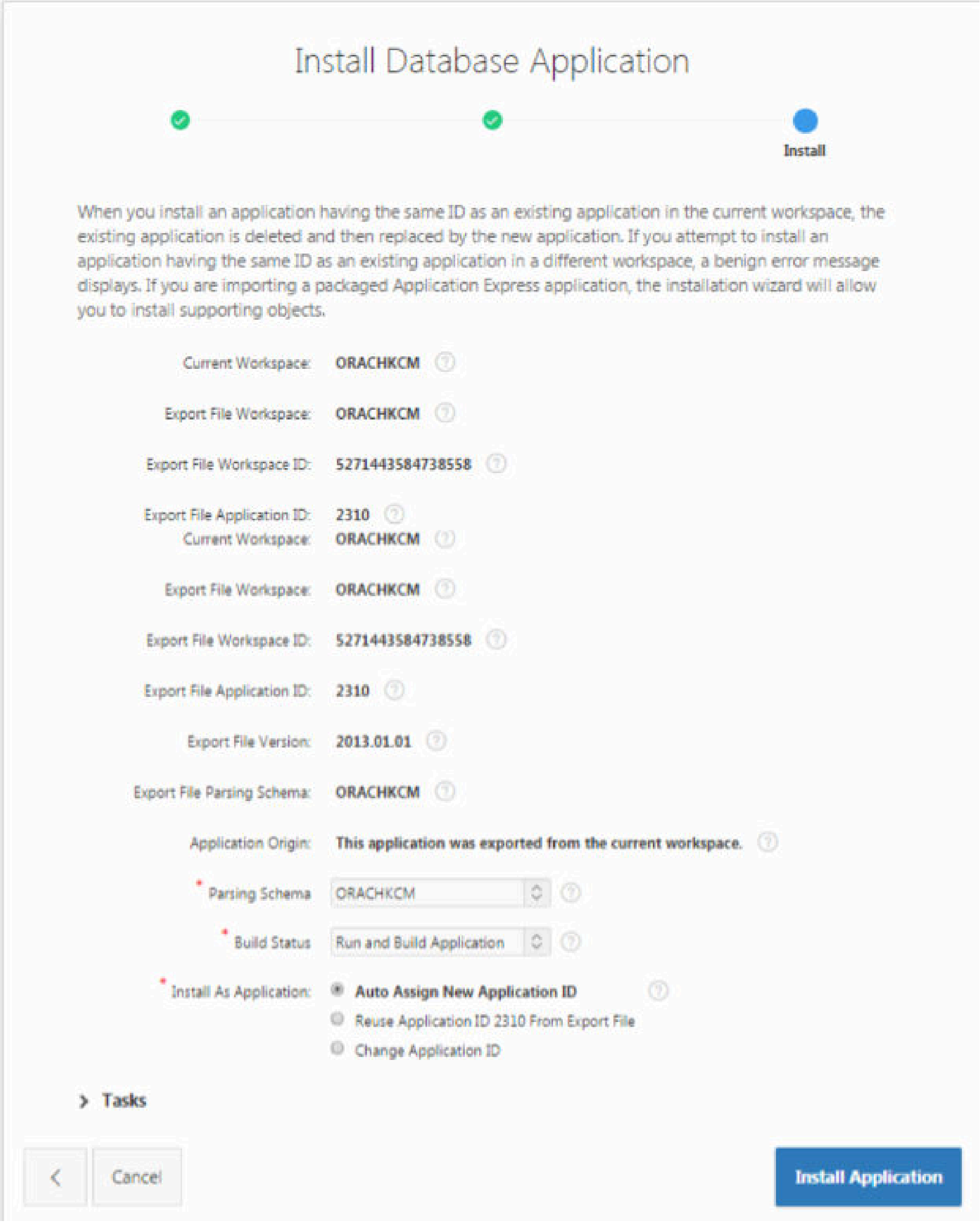
‹
Cancel
Next ›
orachkcm
orachkcm
en
Copyright © 1999, 2016, Oracle. All rights reserved.
Application Express 5.0.4.00.12

11. Click **Next**.

> **Note:**
>
> Ensure that the execute privilege on `DBMS_RLS` and `UTL_SMTP` packages and `create job` sys privilege are granted to parsing schema owner before starting the import of the application. This prevents database support object creation failures that prevent the proper installation of the application.

- For Parsing Schema, select the schema specified for the workspace.
- **Build Status**: select default option **Run and Build Application**.
- Install As Application.
- Select any one option based on your requirement or if possible use the same application id as it is easy to upgrade the application in future. However, the application Id must be unique. Ensure that the application ID is not used by any other application, or any workspace administrators within Oracle Application Express Administration server.

Figure 3-51 Install Application



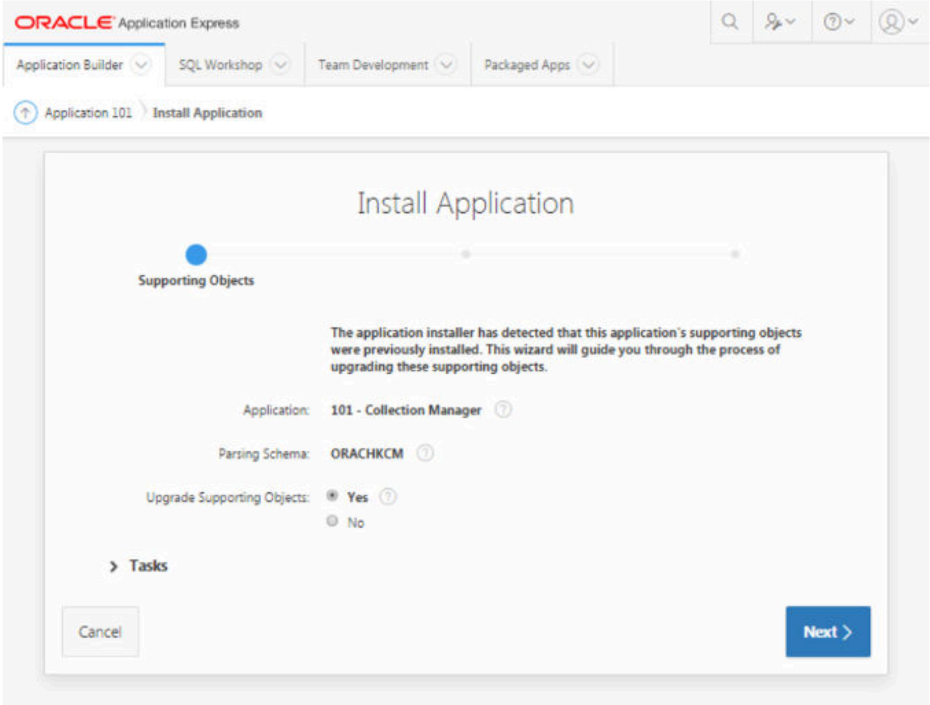
Install Database Application

When you install an application having the same ID as an existing application in the current workspace, the existing application is deleted and then replaced by the new application. If you attempt to install an application having the same ID as an existing application in a different workspace, a benign error message displays. If you are importing a packaged Application Express application, the installation wizard will allow you to install supporting objects.

Current Workspace:	ORACHKCM
Export File Workspace:	ORACHKCM
Export File Workspace ID:	5271443584738558
Export File Application ID:	2310
Current Workspace:	ORACHKCM
Export File Workspace:	ORACHKCM
Export File Workspace ID:	5271443584738558
Export File Application ID:	2310
Export File Version:	2013.01.01
Export File Parsing Schema:	ORACHKCM
Application Origin:	This application was exported from the current workspace.
* Parsing Schema	ORACHKCM
* Build Status	Run and Build Application
* Install As Application:	● Auto Assign New Application ID ○ Reuse Application ID 2310 From Export File ○ Change Application ID

12. Click **Install Application**.
    - Installing Application takes some time, please wait.
    - Verify the application name and parsing schema, free space allocated for the application. Ensure that install Supporting Objects, is always**Yes**.

Figure 3-52 Supporting Objects



The application installer has detected that this application's supporting objects were previously installed. This wizard will guide you through the process of upgrading these supporting objects.

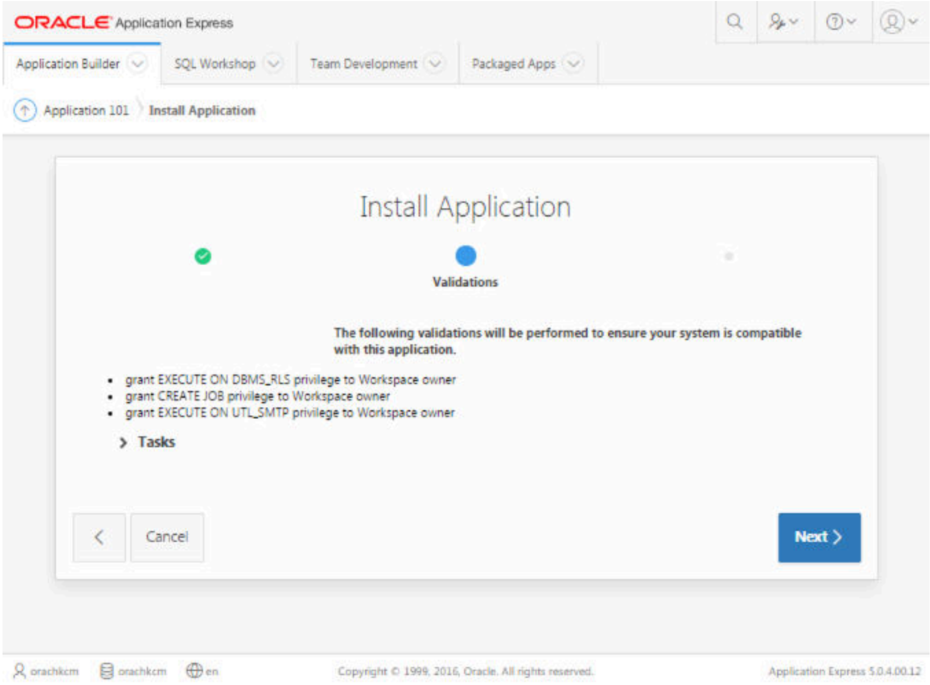
Application: 101 - Collection Manager

Parsing Schema: ORACHKCM

Upgrade Supporting Objects: ● Yes ○ No

- Grant the required privileges to the workspace owner.

Figure 3-53 Validations

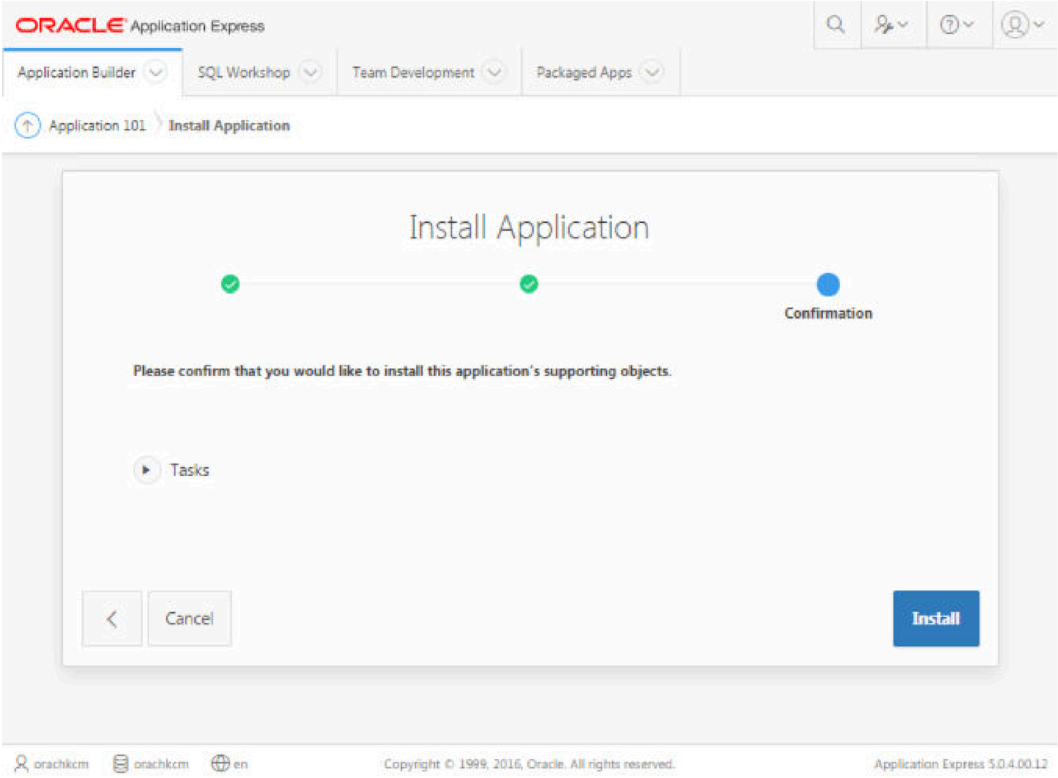


The following validations will be performed to ensure your system is compatible with this application.

- grant EXECUTE ON DBMS_RLS privilege to Workspace owner
- grant CREATE JOB privilege to Workspace owner
- grant EXECUTE ON UTL_SMTP privilege to Workspace owner

13. Click **Next**.

Figure 3-54 Install Applications Supporting Objects

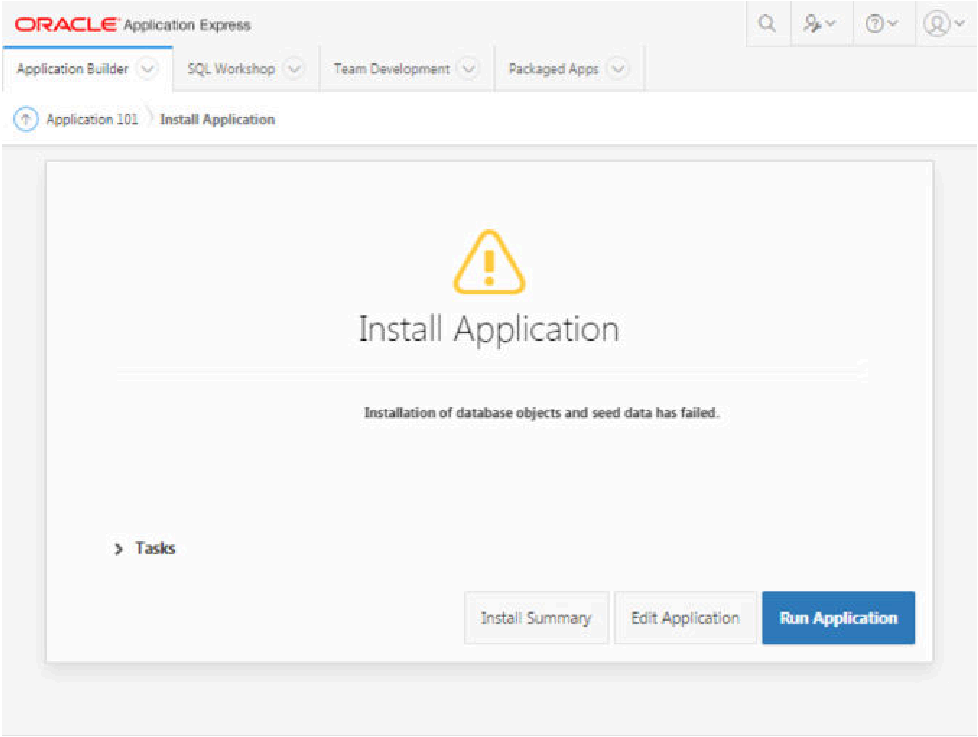


Please confirm that you would like to install this application's supporting objects.

Tasks
Cancel
Install
orachkcm
orachkcm
en
Copyright © 1999, 2016, Oracle. All rights reserved.
Application Express 5.0.4.00.12

14. Click **Install**.

Figure 3-55 Application Installed Successfully



Installation of database objects and seed data has failed.

15. Review the **Installation summary** for any errors or installation of database objects and seed data has failures.
16. Capture the application ID generated for the application from the dialog upon successful installation of the application.

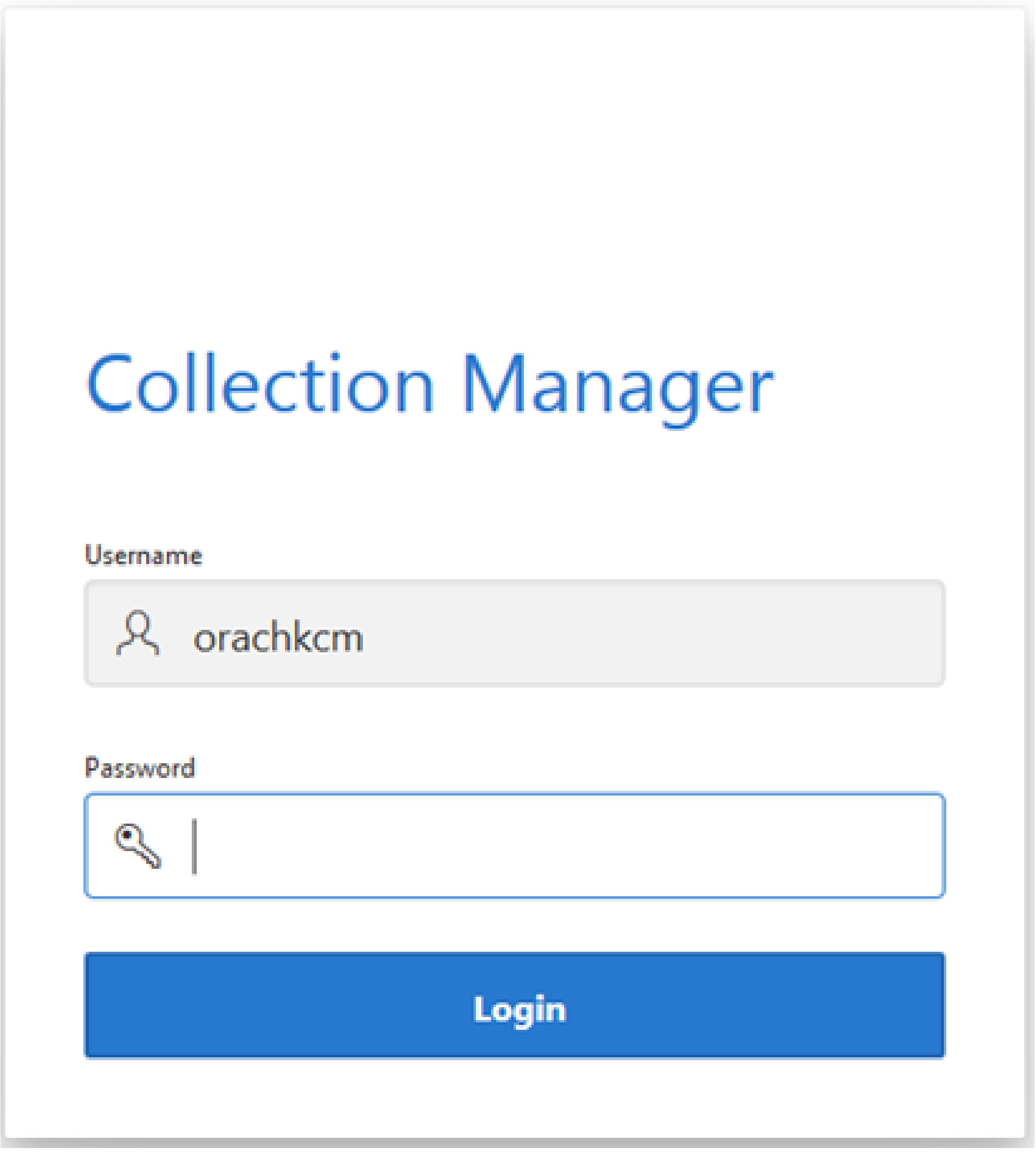
    The application ID is used in the URLs for accessing the application. Distribute the correct URL to the eventual users of the application.
17. Click **Run Application**.

3.2.3.3 Log in to Oracle Health Check Collections Manager Application

To log in to Oracle Health Check Collections Manager, follow these procedures.

1. Enter user name and password details to log in to the Oracle Health Check Collections Manager Application, click **Login**.

Figure 3-56 Log in to Oracle Health Check Collections Manager Application



Collection Manager

Username

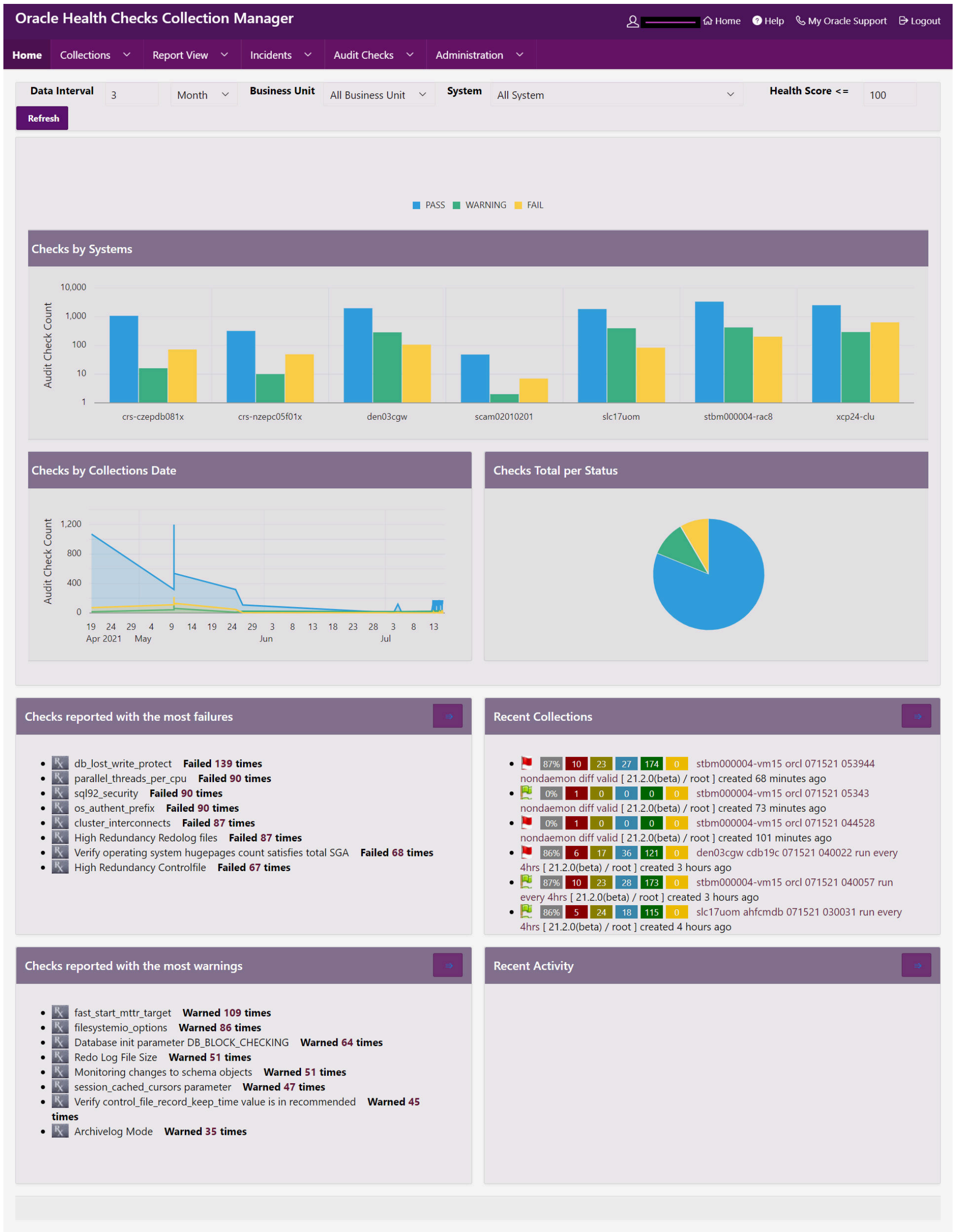
orachkcm

Password

After successful login, you are all set to use Oracle Health Check Collections Manager Application and its features.

By default, the Oracle Health Check Collections Manager Application is deployed with some default sample data for acclimating new users to the application. Oracle Health Check Collections Manager displays the sample data In the **Home** page. Sample data is hidden automatically once your own data starts streaming into the application as you establish the automation and upload functionality of the tool. If you are already using the upload functionality and have your audit check results data in the database tables, and that data replaces the sample data.

Figure 3-57 Oracle Health Check Collections Manager Default View



Data Interval 3 Month

Business Unit All Business Unit

System All System

Health Score <= 100

Checks reported with the most failures

- db_lost_write_protect **Failed 139 times**
- parallel_threads_per_cpu **Failed 90 times**
- sql92_security **Failed 90 times**
- os_authent_prefix **Failed 90 times**
- cluster_interconnects **Failed 87 times**
- High Redundancy Redolog files **Failed 87 times**
- Verify operating system hugepages count satisfies total SGA **Failed 68 times**
- High Redundancy Controlfile **Failed 67 times**

Recent Collections

- 🚩 87% 10 23 27 174 0 stbm000004-vm15 orcl 071521 053944 nondaemon diff valid [21.2.0(beta) / root] created 68 minutes ago
- 🏁 0% 1 0 0 0 0 stbm000004-vm15 orcl 071521 05343 nondaemon diff valid [21.2.0(beta) / root] created 73 minutes ago
- 🚩 0% 1 0 0 0 0 stbm000004-vm15 orcl 071521 044528 nondaemon diff valid [21.2.0(beta) / root] created 101 minutes ago
- 🚩 86% 6 17 36 121 0 den03cgw cdb19c 071521 040022 run every 4hrs [21.2.0(beta) / root] created 3 hours ago
- 🏁 87% 10 23 28 173 0 stbm000004-vm15 orcl 071521 040057 run every 4hrs [21.2.0(beta) / root] created 3 hours ago
- 🏁 86% 5 24 18 115 0 slc17uom ahfcmdb 071521 030031 run every 4hrs [21.2.0(beta) / root] created 4 hours ago

Checks reported with the most warnings

- fast_start_mttr_target **Warned 109 times**
- filesystemio_options **Warned 86 times**
- Database init parameter DB_BLOCK_CHECKING **Warned 64 times**
- Redo Log File Size **Warned 51 times**
- Monitoring changes to schema objects **Warned 51 times**
- session_cached_cursors parameter **Warned 47 times**
- Verify control_file_record_keep_time value is in recommended **Warned 45 times**
- Archivelog Mode **Warned 35 times**

Recent Activity

The **Home** page contains Oracle Jet Charts for **Checks by Systems**, **Checks by Collection Date**, and so on.

Apply filters for all charts by hovering over the check statuses: **PASS**, **WARNING**, or **FAIL** and selecting or de-selecting them. This will still honor the global filters such as **Data Interval**, **Business Unit**, **System**, and **Health Score**.

Click any chart series to display specific type of checks in detail for that system.

2. Log in to Oracle Health Check Collections Manager Application as End user:

- The end user is not an administrator. The end users have only limited access to the application. Non-administrator users cannot do any administrative access unless administrator or developer privileges are granted.
- The **End User** accounts must exist in the workspace where the application is installed.
- To log in to the application, end user needs an application URL and login credentials.

  Provide the end users with one of the following URLs (they are interchangeable) and the temporary password that was assigned for them.

  ```
  http://hostname:port/apex/f?p=ApplicationID
  ```

  ```
  http://hostname:port/pls/apex/f?p=ApplicationID
  ```

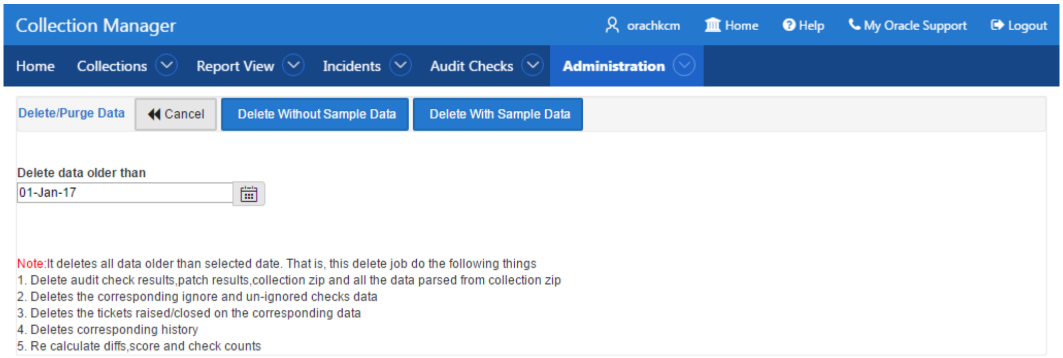
  For example:

  ```
  http://dbserver.domain.com:8080/apex/f?p=103
  ```

3. Delete the sample data using one of two methods:

   Administration > **Delete Old Data**: Select a date and then click **Delete With Sample Data**.

Figure 3-58   Oracle Health Check Collections Manager - Delete Old Data

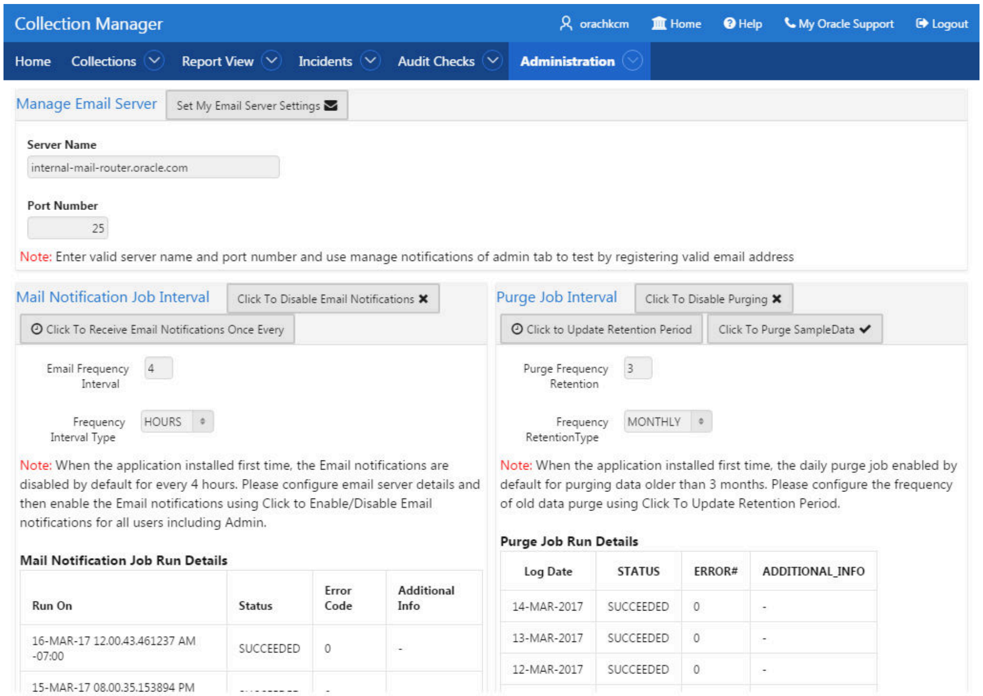


Delete data older than
01-Jan-17

Note:It deletes all data older than selected date. That is, this delete job do the following things
1. Delete audit check results,patch results,collection zip and all the data parsed from collection zip
2. Deletes the corresponding ignore and un-ignored checks data
3. Deletes the tickets raised/closed on the corresponding data
4. Deletes corresponding history
5. Re calculate diffs,score and check counts

Configure Email > **Configure Mail Server/Notification/Purge Job**: click **Click To Purge SampleData**.

Figure 3-59 Oracle Health Check Collections Manager - Purge Sample Data


Collection Manager
orachkcm
Home
Help
My Oracle Support
Logout
Home
Collections
Report View
Incidents
Audit Checks
Administration
Manage Email Server
Set My Email Server Settings
Mail Notification Job Interval
Click To Disable Email Notifications ✖
Click To Receive Email Notifications Once Every
Purge Job Interval
Click To Disable Purging ✖
Click to Update Retention Period
Click To Purge SampleData ✔

Server Name
internal-mail-router.oracle.com

Port Number
25

Note: Enter valid server name and port number and use manage notifications of admin tab to test by registering valid email address

Email Frequency Interval: 4

Frequency Interval Type: HOURS

Note: When the application installed first time, the Email notifications are disabled by default for every 4 hours. Please configure email server details and then enable the Email notifications using Click to Enable/Disable Email notifications for all users including Admin.

Mail Notification Job Run Details

Run On	Status	Error Code	Additional Info
16-MAR-17 12.00.43.461237 AM -07:00	SUCCEEDED	0	-
15-MAR-17 08.00.35.153894 PM			

Purge Frequency Retention: 3

Frequency RetentionType: MONTHLY

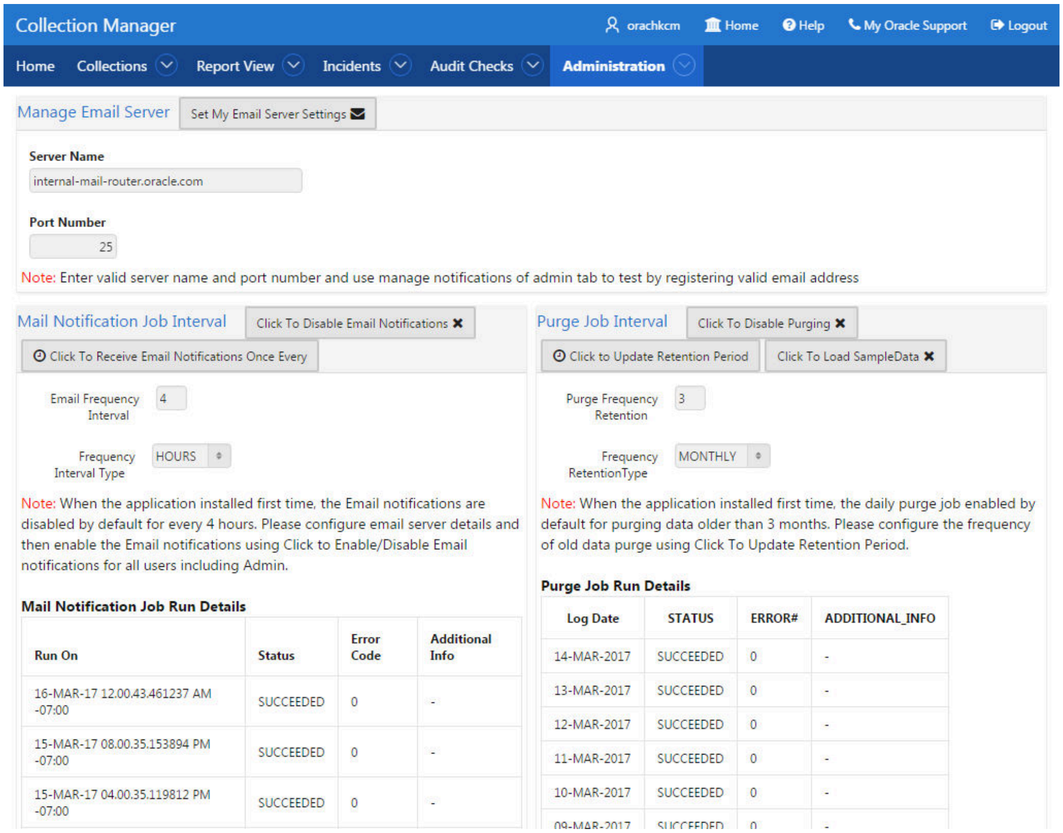
Note: When the application installed first time, the daily purge job enabled by default for purging data older than 3 months. Please configure the frequency of old data purge using Click To Update Retention Period.

Purge Job Run Details

Log Date	STATUS	ERROR#	ADDITIONAL_INFO
14-MAR-2017	SUCCEEDED	0	-
13-MAR-2017	SUCCEEDED	0	-
12-MAR-2017	SUCCEEDED	0	-

4. To load sample data again, **Configure Email** > **Configure Mail Server/ Notification/Purge Job** and then click **Click to Load SampleData**.

Figure 3-60   Oracle Health Check Collection Manager - Load Sample Data



Server Name: internal-mail-router.oracle.com

Port Number: 25

Note: Enter valid server name and port number and use manage notifications of admin tab to test by registering valid email address

Email Frequency Interval: 4

Frequency Interval Type: HOURS

Note: When the application installed first time, the Email notifications are disabled by default for every 4 hours. Please configure email server details and then enable the Email notifications using Click to Enable/Disable Email notifications for all users including Admin.

Mail Notification Job Run Details

Run On	Status	Error Code	Additional Info
16-MAR-17 12.00.43.461237 AM -07:00	SUCCEEDED	0	-
15-MAR-17 08.00.35.153894 PM -07:00	SUCCEEDED	0	-
15-MAR-17 04.00.35.119812 PM -07:00	SUCCEEDED	0	-

Purge Frequency Retention: 3

Frequency RetentionType: MONTHLY

Note: When the application installed first time, the daily purge job enabled by default for purging data older than 3 months. Please configure the frequency of old data purge using Click To Update Retention Period.

Purge Job Run Details

Log Date	STATUS	ERROR#	ADDITIONAL_INFO
14-MAR-2017	SUCCEEDED	0	-
13-MAR-2017	SUCCEEDED	0	-
12-MAR-2017	SUCCEEDED	0	-
11-MAR-2017	SUCCEEDED	0	-
10-MAR-2017	SUCCEEDED	0	-
09-MAR-2017	SUCCEEDED	0	-

3.2.3.4 Apply a Theme

To apply a theme, follow these procedures.

1. Enter user name and password details to log in to the Oracle Health Check Collections Manager Application, click **Login**.
2. Click the **Administration** drop-down list and then select **Application Theme Style**.
3. Select a theme from the **Desktop Theme Style** list, and then click **Appy Changes**.

   You can select any of the following Desktop Theme Styles:

   - **Aubergine**
   - **Choco-Mint**
   - **Redwood-Light**
   - **Vita**
   - **Vita-Slate**

3.2.4 Upgrading Oracle Health Check Collections Manager Application

Oracle Autonomous Health Framework automatically upgrades new versions of the Oracle Health Check Collections Manager.

Upgrade Oracle Health Check Collections Manager application from Oracle Autonomous Health Framework. Oracle Health Check Collections Manager application is upgraded to the latest version of whichever application your database can support.

- Upgrade Oracle Health Check Collections Manager by running the following commands.

  ```
  orachk -cmupgrade
  ```

  or

  ```
  exachk -cmupgrade
  ```

  If the Oracle Health Check Collections Manager schema changes in the future and Oracle Autonomous Health Framework requires an Oracle Health Check Collections Manager upgrade, then the tool automatically prompts you to upgrade.

  Oracle Health Check Collections Manager goes offline during upgrade and not it is available to receive new collections. If any collections fail to upload during upgrade, then you can upload again by viewing and reattempting failed uploads.

  > **Note:**
  >
  > Running the command exits with the following messages, if an incompatible APEX version is found.
  >
  > ```
  > Found APEX version {current version}.
  > The newer version of Collection Manager requires APEX 20.2 or
  > higher. Exiting.
  >
  > Collection Manager Fresh install has to be imported from apex
  > framework.
  > ```

3.2.5 Getting Started

Familiarize yourself with the Oracle Health Check Collections Manager Application.

- Incident Ticket System Lookup Lists and Seed Data
  Oracle Health Check Collections Manager Application provides a basic Incident Ticket system.
- Access Control System
  Limit and control access based on functional roles.
- Oracle Health Check Collections Manager Application Administration
  To restrict authorized users alone to access the application, grant sufficient privileges to different roles.

- Selectively Capturing Users During Login
  By default, Oracle Health Check Collections Manager captures details of the users logging in using LDAP authentication, and assigns them DBA role.
- Configuring Email Notification System
  The Oracle Health Check Collections Manager Application provides an email notification system that users can subscribe to.
- Bulk Mapping Systems to Business Units
  If you have many systems, then you can quickly map those systems to business units in Oracle Health Check Collections Manager using an XML bulk upload.
- Purging Old Collections
  By default, Oracle Health Check Collections Manager runs a purge job daily, removing data older than three months.

3.2.5.1 Incident Ticket System Lookup Lists and Seed Data

Oracle Health Check Collections Manager Application provides a basic Incident Ticket system.

Oracle Health Check Collections Manager Application is deployed with seed data for the lookup lists used for data entry for incident tickets:

- Products
- Category
- Customer Contacts
- Notifications
- Status Codes
- Incident Severity
- Incident Urgency

The seed data is values that are commonly used. Add or change the seed data provided with the application. However, you must have administrator privileges to manage seed data through the **Administration** tab.

To access the **Administration** tab, click the gear icon at the upper-right corner.

3.2.5.2 Access Control System

Limit and control access based on functional roles.

By default, the Access Control system is disabled. If Access Control is disabled, then all authenticated users are granted administrator privileges and can access all application features. To assign one or more roles to the end users, manage access controls through the **Administration** tab. You can enable the following three functional roles available in the Oracle Health Check Collections Manager.

- **Admin:** Admin role user can also be a Workspace Administrator for the application and it depends on your functional roles requirements.
- **DBA Manager:** The DBA Manager can edit user roles, or assign systems to other users in the DBA Manager BU. The scope of a DBA Manager is an entire BU, or multiple BUs.
- **DBA:** DBA has read-only access.Manage systems within one or more BUs, if the DBA Managers of those BUs assign them. Manage any incidents assigned to them.

- **Read Only:** The user who is assigned with Read Only role will have only access to monitor irrespective of BU admin roles.

  > **Note:**
  >
  > The **Read Only** role will take precedence and it will limit access to the **Administration** tab and what activities can be done on **Upload Collections**.

> **Note:**
>
> Irrespective of whether Access Control is enabled or disabled, a user still has to authenticate successfully into the application.

Assign role to the users after configuring the Access Control system.

3.2.5.3 Oracle Health Check Collections Manager Application Administration

To restrict authorized users alone to access the application, grant sufficient privileges to different roles.

Admin

Any end user who is granted an admin role by the workspace administrator has administrator privileges within the Collection Manager application.

Log in to Oracle Health Check Collections Manager Application using a URL as follows:

```
http://hostname:port/apex/f?p=ApplicationID
http://hostname:port/pls/apex/f?p=ApplicationID
```

For example:

```
http://dbserver.domain.com:8080/apex/f?p=103
```

As an admin user, you must see the **Administration** menu at the upper-right corner.

- Following are the admin user privileges:
  - Add or revoke admin privileges
  - Define Business Units (BU)
  - Assign DBA Manager role to users
  - Assign DBA Managers to one or more BUs
  - Assign systems to BUs (a system can belong to one BU)
  - Assign DBAs to DBA Managers
  - Assign systems to DBAs
  - Ignore any check on a collection, BU, or system

  - Create and assign incidents to any user
  - Manage all incidents
- Only Admin role can edit any section under the **Administration** menu.
- The administrators must configure data based on their requirements under the administration menu to prepare for the wider usage of the application. This is a one-time activity, however, change the configuration over time to suit your needs.

  Examples of the configuration data that you need set up are:

  - Products
  - Customers (internal designations for workgroups)
  - Categories
  - Notifications
  - Status codes
  - Manage Email Server and Job details
  - Manage Notifications
  - Incident Severity
  - Urgency
  - Manage User Roles and Assign systems to users
  - Business Units (BUs)
  - Assign systems to BUs

DBA Manager

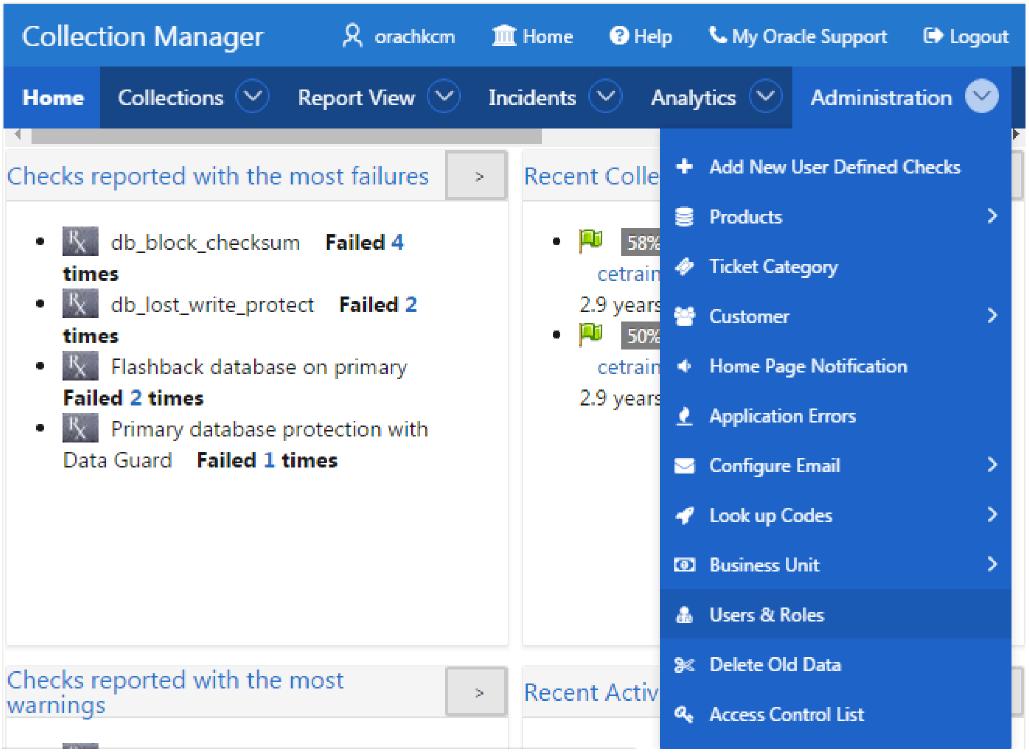
Any user who is granted the DBA Manager role.

Log in to Oracle Health Check Collections Manager Application using a URL as follows:

```
http://hostname:port/apex/f?p=ApplicationID
http://hostname:port/pls/apex/f?p=ApplicationID
```

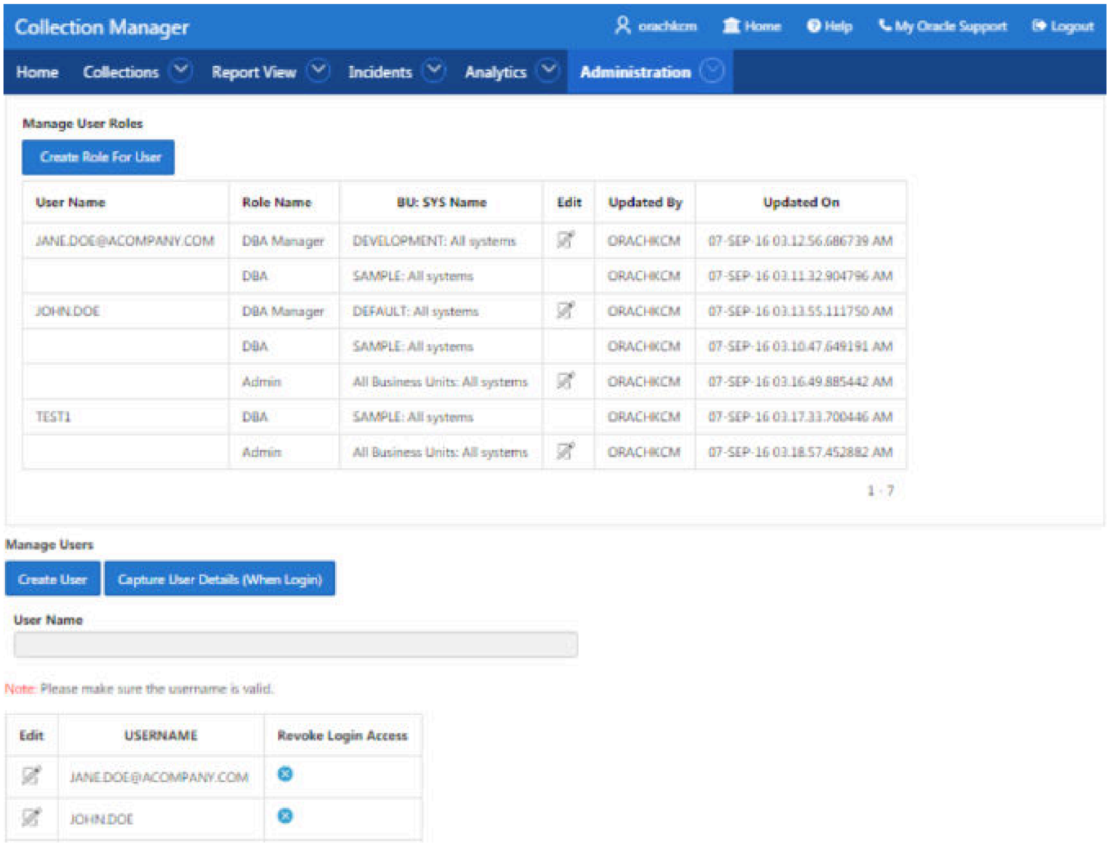
The DBA Managers see an Administration menu at the upper-right corner of the application.

Figure 3-61   Oracle Health Check Collections Manager - DBA Manager Administration



Click **Users and Roles**.

Figure 3-62 Oracle Health Check Collections Manager - DBA Manager - Manage User Roles



User Name	Role Name	BU: SYS Name	Edit	Updated By	Updated On
JANE.DOE@ACOMPANY.COM	DBA Manager	DEVELOPMENT: All systems	✎	ORACHKCM	07-SEP-16 03.12.56.686739 AM
	DBA	SAMPLE: All systems		ORACHKCM	07-SEP-16 03.11.32.904796 AM
JOHN.DOE	DBA Manager	DEFAULT: All systems	✎	ORACHKCM	07-SEP-16 03.13.55.111750 AM
	DBA	SAMPLE: All systems		ORACHKCM	07-SEP-16 03.10.47.649191 AM
	Admin	All Business Units: All systems	✎	ORACHKCM	07-SEP-16 03.16.49.885442 AM
TEST1	DBA	SAMPLE: All systems		ORACHKCM	07-SEP-16 03.17.33.700446 AM
	Admin	All Business Units: All systems	✎	ORACHKCM	07-SEP-16 03.18.57.452882 AM

Note: Please make sure the username is valid.

Edit	USERNAME	Revoke Login Access
✎	JANE.DOE@ACOMPANY.COM	⊗
✎	JOHN.DOE	⊗

The DBA Manager can edit user roles, or assign systems to other users in the DBA Manager BU. The scope of a DBA Manager is an entire BU, or multiple BUs.

Following are the DBA manager privileges:

- Assign DBAs to BUs the manager manages
- Assign DBAs to one or more systems
- Ignore any check on a collection, BU, or system
- Create incidents for any system
- Assign incidents to DBAs that manage the systems in their BUs
- Manage any incidents for systems within their assigned BUs

DBA

Any user who is granted the DBA role.

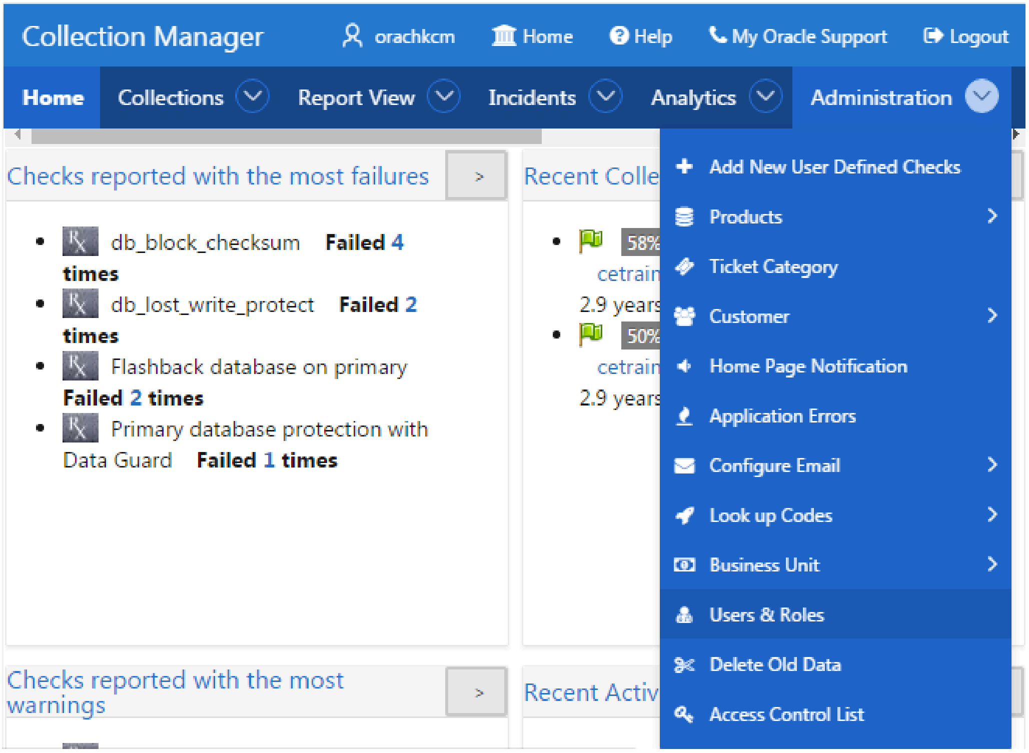
Log in to Oracle Health Check Collections Manager Application using a URL as follows:

```
http://hostname:port/apex/f?p=ApplicationID
http://hostname:port/pls/apex/f?p=ApplicationID
```

The DBA must see the Administration menu at the upper-right corner of the application.

Any end user who is granted administrator role by the workspace administrator has administrator privileges within the Oracle Health Check Collections Manager application.

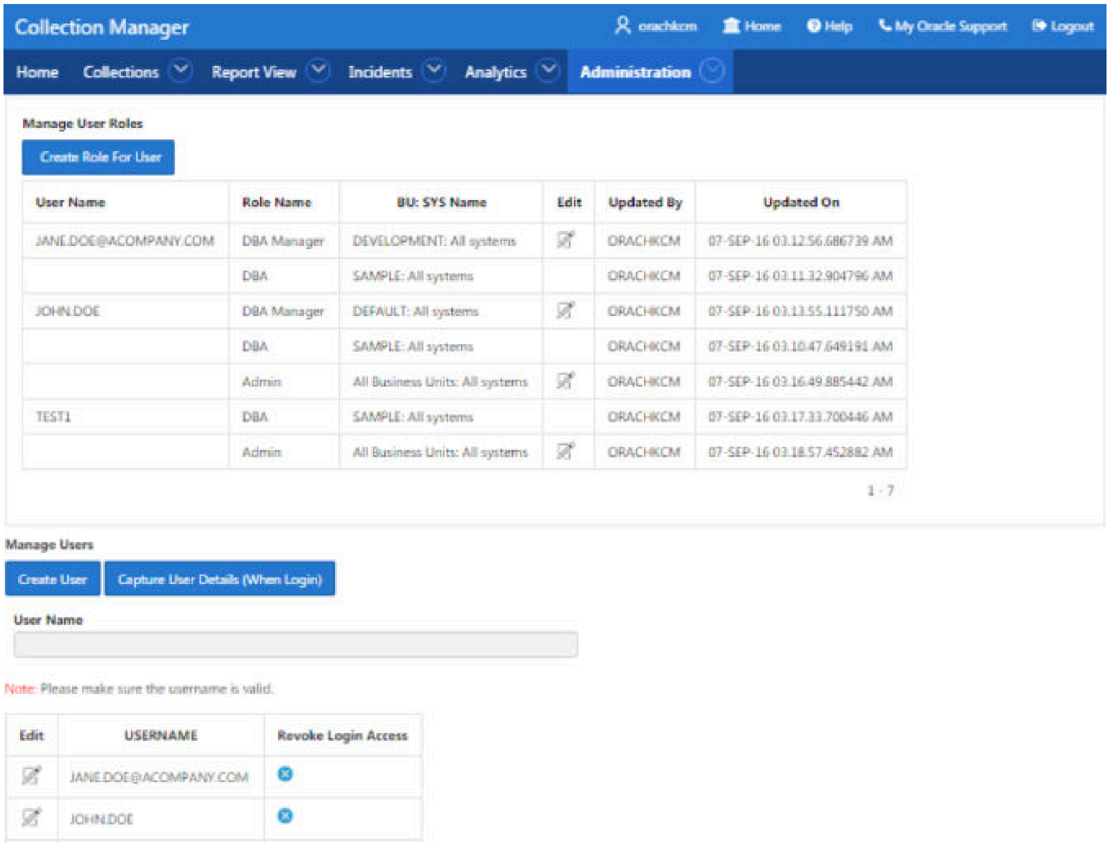
Figure 3-63   Oracle Health Check Collections Manager - DBA Manager Administration



Click **Users and Roles**.

DBA has read-only access.

Figure 3-64   Oracle Health Check Collections Manager - DBA Manager - Manage User Roles



Manage User Roles

User Name	Role Name	BU: SYS Name	Edit	Updated By	Updated On
JANE.DOE@ACOMPANY.COM	DBA Manager	DEVELOPMENT: All systems	✎	ORACHKCM	07-SEP-16 03.12.56.686739 AM
	DBA	SAMPLE: All systems		ORACHKCM	07-SEP-16 03.11.32.904796 AM
JOHN.DOE	DBA Manager	DEFAULT: All systems	✎	ORACHKCM	07-SEP-16 03.13.55.111750 AM
	DBA	SAMPLE: All systems		ORACHKCM	07-SEP-16 03.10.47.649191 AM
	Admin	All Business Units: All systems	✎	ORACHKCM	07-SEP-16 03.16.49.885442 AM
TEST1	DBA	SAMPLE: All systems		ORACHKCM	07-SEP-16 03.17.33.700446 AM
	Admin	All Business Units: All systems	✎	ORACHKCM	07-SEP-16 03.18.57.452882 AM

1 - 7

Manage Users

User Name

Note: Please make sure the username is valid.

Edit	USERNAME	Revoke Login Access
✎	JANE.DOE@ACOMPANY.COM	⊗
✎	JOHN.DOE	⊗

Following are the DBA privileges:

- Cannot manage Access Control List
- Manage systems within one or more BUs, if the DBA Managers of those BUs assign them
- Ignore any check on a collection or system they manage
- Manage any incidents assigned to them

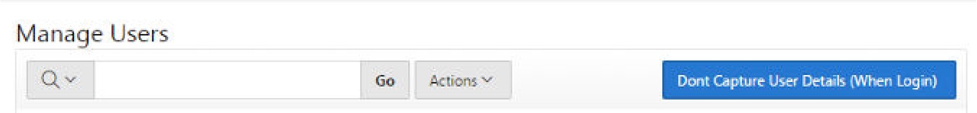
3.2.5.4 Selectively Capturing Users During Login

By default, Oracle Health Check Collections Manager captures details of the users logging in using LDAP authentication, and assigns them DBA role.

However, you can disable automatic capture and re-enable anytime later. If you disable, then you must manually create users and assign them roles.

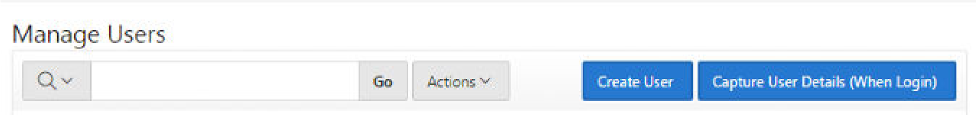
1. Click **Administration**, and then select **Users and Roles**.
2. To disable automatic capture of users details, click **Don’t Capture User Details (When Login)**.

Figure 3-65 Don’t Capture User Details (When Login)



3. To re-enable automatic capture of user details, click **Capture User Details (When Login)**.

Figure 3-66 Capture User Details (When Login)



3.2.5.5 Configuring Email Notification System

The Oracle Health Check Collections Manager Application provides an email notification system that users can subscribe to.

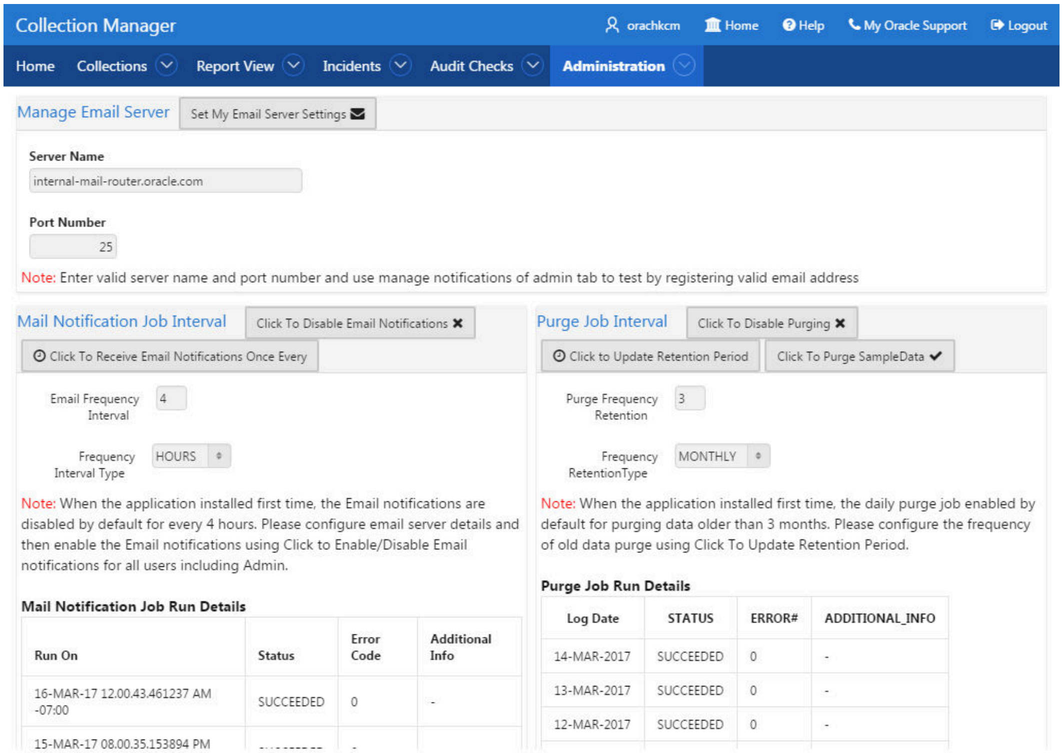
The setup involves:

- Configuring the email server, port, and the frequency of email notifications.
- Registering the email address

> **Note:**
>
> Only the administrators have the privilege to manage **Email Notification Server and Job details**.

1. Log in to Oracle Health Check Collections Manager, and then click **Administration** > **Configure Email** > **Configure Email Server/Notification/Purge** tab.

Figure 3-67 Oracle Health Check Collections Manager - Configure Email Server


Collection Manager
orachkcm
Home
Help
My Oracle Support
Logout
Home
Collections
Report View
Incidents
Audit Checks
Administration
Manage Email Server
Set My Email Server Settings
Mail Notification Job Interval
Click To Disable Email Notifications
Click To Receive Email Notifications Once Every
Purge Job Interval
Click To Disable Purging
Click to Update Retention Period
Click To Purge SampleData

Server Name
internal-mail-router.oracle.com

Port Number
25

Note: Enter valid server name and port number and use manage notifications of admin tab to test by registering valid email address

Email Frequency Interval: 4

Frequency Interval Type: HOURS

Note: When the application installed first time, the Email notifications are disabled by default for every 4 hours. Please configure email server details and then enable the Email notifications using Click to Enable/Disable Email notifications for all users including Admin.

Mail Notification Job Run Details

Run On	Status	Error Code	Additional Info
16-MAR-17 12.00.43.461237 AM -07:00	SUCCEEDED	0	-
15-MAR-17 08.00.35.153894 PM			

Purge Frequency Retention: 3

Frequency RetentionType: MONTHLY

Note: When the application installed first time, the daily purge job enabled by default for purging data older than 3 months. Please configure the frequency of old data purge using Click To Update Retention Period.

Purge Job Run Details

Log Date	STATUS	ERROR#	ADDITIONAL_INFO
14-MAR-2017	SUCCEEDED	0	-
13-MAR-2017	SUCCEEDED	0	-
12-MAR-2017	SUCCEEDED	0	-

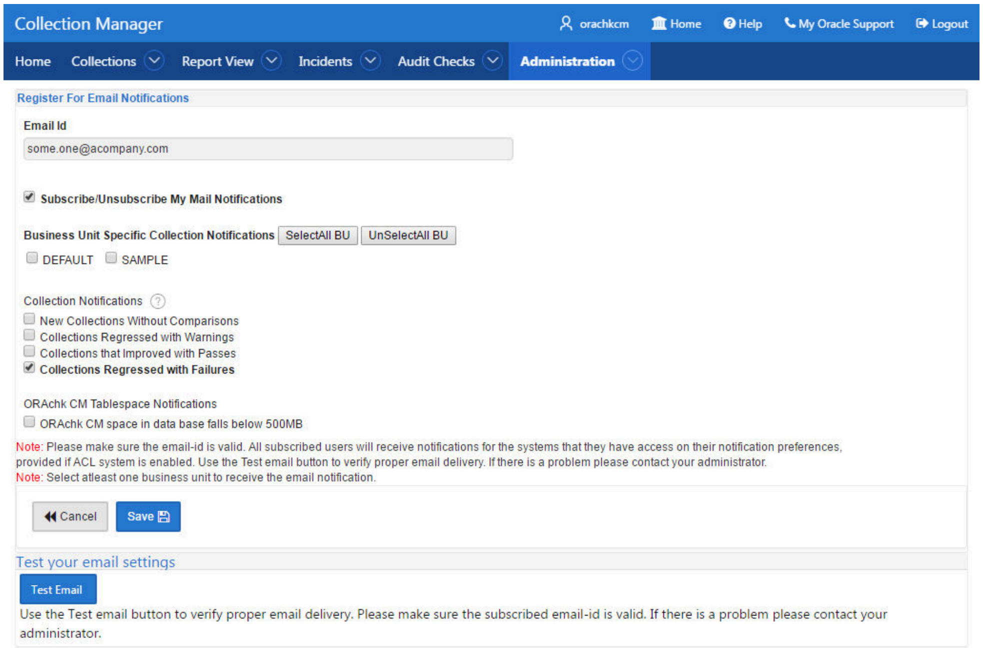
a. Specify a valid **Email Server Name**, **Port Number**, and then click **Set My Email Server Settings**.

b. Set **Email Notification Frequency** as per your needs.

   See the **Notification Job Run Details** on the same page.

2. Click **Administration** > **Configure Email** > **Email Notification Preferences**.

Figure 3-68 Oracle Health Check Collections Manager - Email Notification Preferences



Register For Email Notifications

Email Id

some.one@acompany.com

☑ Subscribe/Unsubscribe My Mail Notifications

Business Unit Specific Collection Notifications

□ DEFAULT □ SAMPLE

Collection Notifications

□ New Collections Without Comparisons
□ Collections Regressed with Warnings
□ Collections that Improved with Passes
☑ Collections Regressed with Failures

ORAchk CM Tablespace Notifications

□ ORAchk CM space in data base falls below 500MB

Note: Please make sure the email-id is valid. All subscribed users will receive notifications for the systems that they have access on their notification preferences, provided if ACL system is enabled. Use the Test email button to verify proper email delivery. If there is a problem please contact your administrator.
Note: Select atleast one business unit to receive the email notification.

Test your email settings

Use the Test email button to verify proper email delivery. Please make sure the subscribed email-id is valid. If there is a problem please contact your administrator.

a. If you are accessing for the first time, then enter your email address.

   Subsequent access to **Manage Notifications** page shows your email address automatically.

b. By default, **Subscribe/Unsubscribe My Mail Notifications** is checked. Leave as is.

c. Under **Business Unit Specific Collection Notifications**, choose the business unit that you want notifications for.

d. Under **Collection Notifications**, choose the type of collections for which you want to receive notifications.

e. Select to receive notification when the available space in `ORAchk CM` tablespace falls below 100 MB.

f. Validate the notification delivery by clicking **Test** under **Test your email settings**.

   If the configuration is correct, you must receive an email. If you do not receive an email, check with your admin.

   Following is the sample notification:

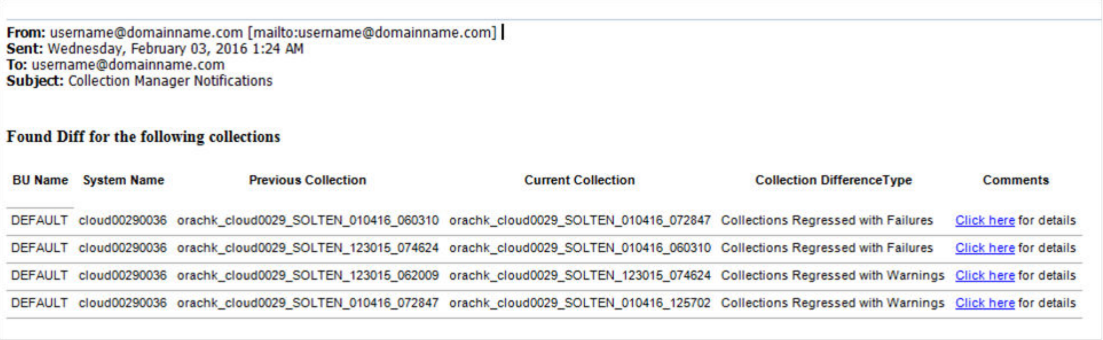
```
From: username@domainname.com
Sent: Thursday, January 28, 2016 12:21 PM
To: username@domainname.com
Subject: Test Mail From Collection Manager

Testing Collection Manager Email Notification System
```

g. Click **Submit**.

> **Note:**
>
> Manage Notifications section under the Administration menu is available for all users irrespective of the role.
>
> If the ACL system is enabled, then the registered users receive notifications for the systems that they have access to. If the ACL system is not configured, then all registered users receive all notifications.

Depending on the selections, you made under **Collection Notifications** section, you receive an email with `Subject: Collection Manager Notifications` containing application URL with results.

Figure 3-69   Oracle Health Check Collections Manager - Sample Email Notification



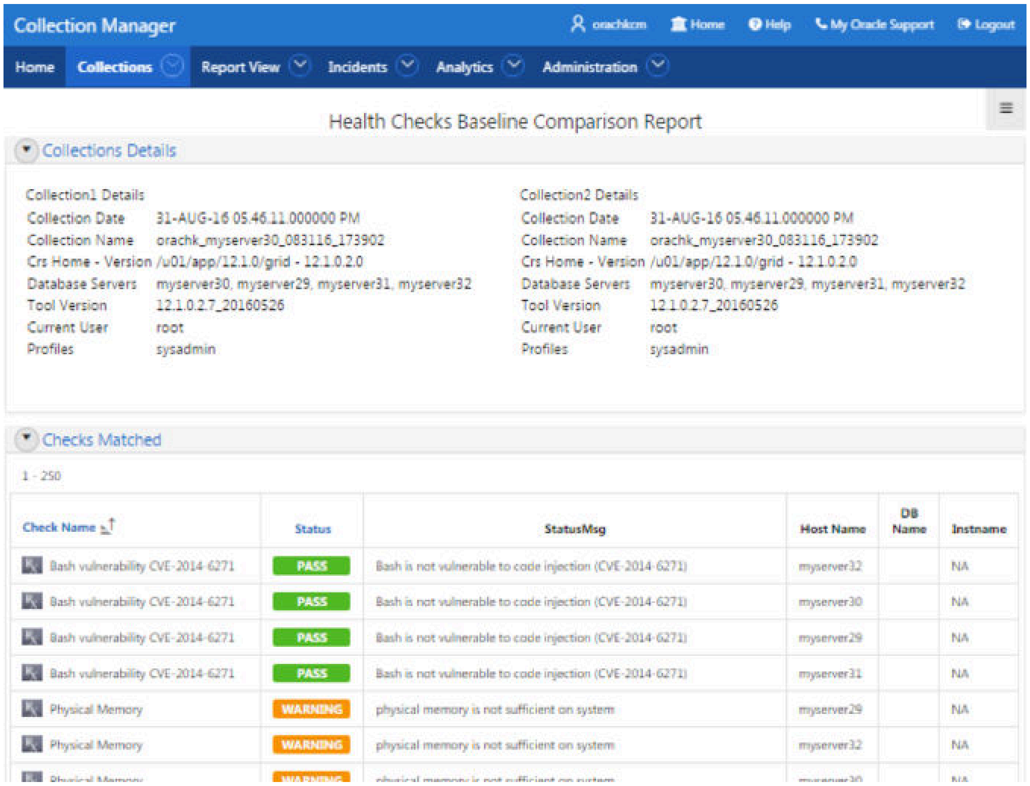
From: username@domainname.com [mailto:username@domainname.com]
Sent: Wednesday, February 03, 2016 1:24 AM
To: username@domainname.com
Subject: Collection Manager Notifications

Found Diff for the following collections

BU Name	System Name	Previous Collection	Current Collection	Collection DifferenceType	Comments
DEFAULT	cloud00290036	orachk_cloud0029_SOLTEN_010416_060310	orachk_cloud0029_SOLTEN_010416_072847	Collections Regressed with Failures	Click here for details
DEFAULT	cloud00290036	orachk_cloud0029_SOLTEN_123015_074624	orachk_cloud0029_SOLTEN_010416_060310	Collections Regressed with Failures	Click here for details
DEFAULT	cloud00290036	orachk_cloud0029_SOLTEN_123015_062009	orachk_cloud0029_SOLTEN_123015_074624	Collections Regressed with Warnings	Click here for details
DEFAULT	cloud00290036	orachk_cloud0029_SOLTEN_010416_072847	orachk_cloud0029_SOLTEN_010416_125702	Collections Regressed with Warnings	Click here for details

Under **Comments** column, click the **Click here** links for details. Click the respective URLs, authenticate, and then view respective comparison report.

Figure 3-70   Oracle Health Check Collections Manager - Sample Diff Report



Health Checks Baseline Comparison Report

Collections Details

Collection1 Details		Collection2 Details	
Collection Date	31-AUG-16 05.46.11.000000 PM	Collection Date	31-AUG-16 05.46.11.000000 PM
Collection Name	orachk_myserver30_083116_173902	Collection Name	orachk_myserver30_083116_173902
Crs Home - Version	/u01/app/12.1.0/grid - 12.1.0.2.0	Crs Home - Version	/u01/app/12.1.0/grid - 12.1.0.2.0
Database Servers	myserver30, myserver29, myserver31, myserver32	Database Servers	myserver30, myserver29, myserver31, myserver32
Tool Version	12.1.0.2.7_20160526	Tool Version	12.1.0.2.7_20160526
Current User	root	Current User	root
Profiles	sysadmin	Profiles	sysadmin

Checks Matched

1 - 250

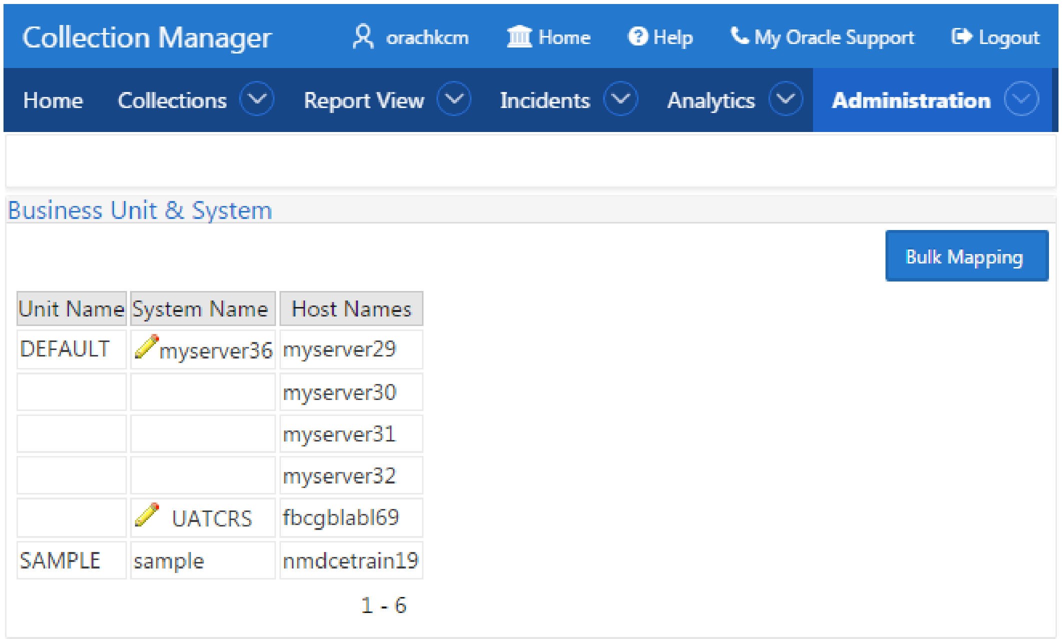
Check Name	Status	StatusMsg	Host Name	DB Name	Instname
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver32		NA
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver30		NA
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver29		NA
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver31		NA
Physical Memory	WARNING	physical memory is not sufficient on system	myserver29		NA
Physical Memory	WARNING	physical memory is not sufficient on system	myserver32		NA
Physical Memory	WARNING	physical memory is not sufficient on system	myserver30		NA

3.2.5.6 Bulk Mapping Systems to Business Units

If you have many systems, then you can quickly map those systems to business units in Oracle Health Check Collections Manager using an XML bulk upload.

1. Click **Administration** > **Business Unit** > **Assign System to BU**.
2. Click **Bulk Mapping**.

Figure 3-71   Bulk Mapping



Unit Name	System Name	Host Names
DEFAULT	myserver36	myserver29
		myserver30
		myserver31
		myserver32
	UATCRS	fbcgblabl69
SAMPLE	sample	nmdcetrain19

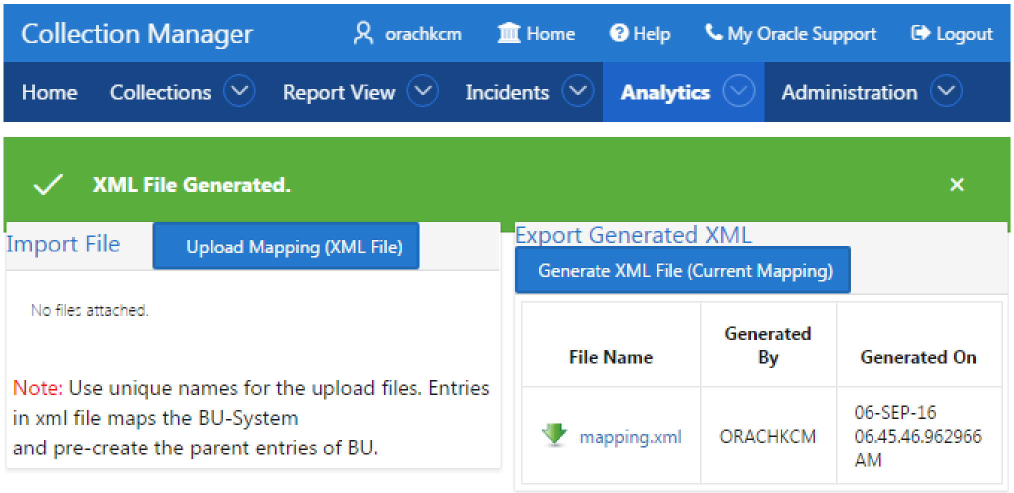
1 - 6

3. Upload a mapping XML.

   a. Click **Generate XML File (Current Mapping)**.

   b. Download the resulting XML file that contains your current system to business unit mappings.

Figure 3-72   Upload a mapping XML



✓ XML File Generated.

No files attached.

Note: Use unique names for the upload files. Entries in xml file maps the BU-System and pre-create the parent entries of BU.

File Name	Generated By	Generated On
mapping.xml	ORACHKCM	06-SEP-16 06.45.46.962966 AM

   c. Amend the XML to show mappings that you want.

d. Upload new Mapping XML through **Upload Mapping (XML File)**.

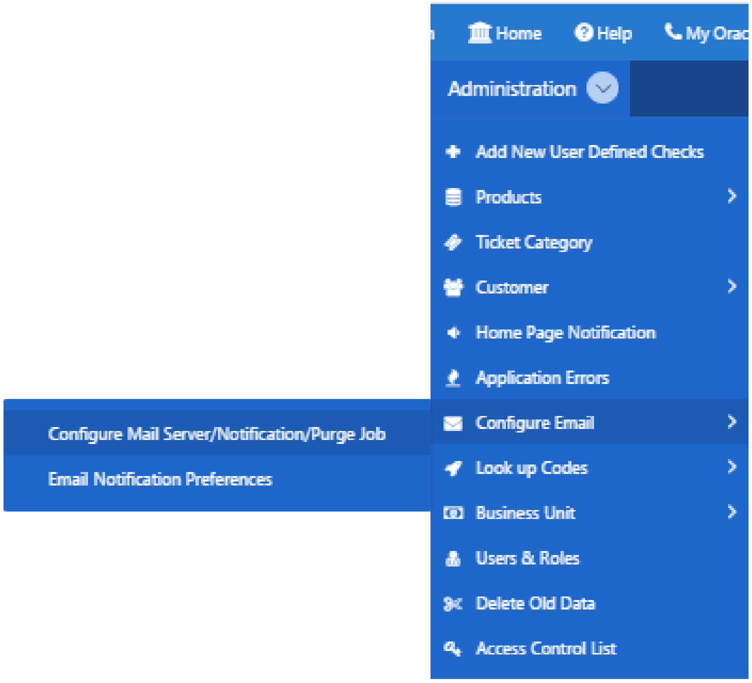
3.2.5.7 Purging Old Collections

By default, Oracle Health Check Collections Manager runs a purge job daily, removing data older than three months.

To adjust or disable the collection purging frequency:

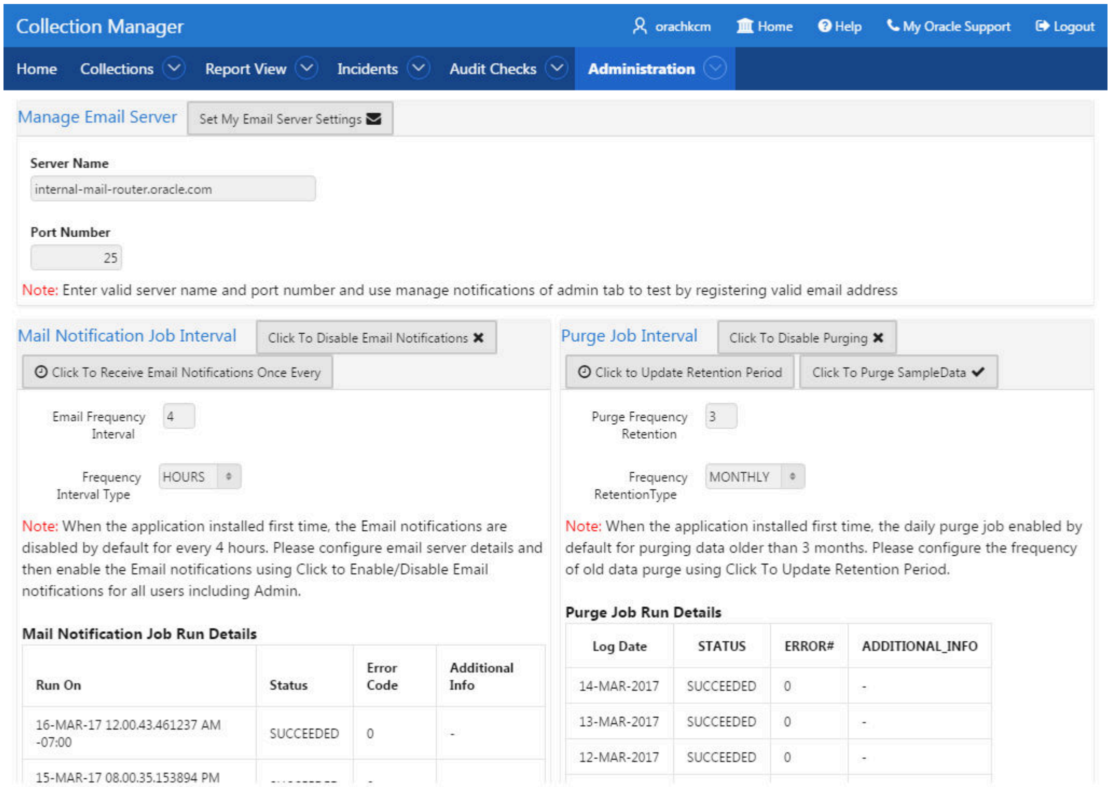
1. Click **Administration** > **Configure Email** > **Configure Mail Server/Notification/ Purge Job**.

Figure 3-73 Manage Email Server and Job Details



2. Select an appropriate option:
   - Change the frequency of purges by setting different values in **Purge Frequency** , and then click **Click To Purge Every**.
   - To disable purging, click **Click To Disable Purging**.
   - To re-enable purging, click **Click To Enable Purging**.

Figure 3-74   Oracle Health Check Collections Manager - Configure Purging



Manage Email Server   Set My Email Server Settings

Server Name
internal-mail-router.oracle.com

Port Number
25

Note: Enter valid server name and port number and use manage notifications of admin tab to test by registering valid email address

Mail Notification Job Interval   Click To Disable Email Notifications ✖
Click To Receive Email Notifications Once Every

Email Frequency Interval: 4

Frequency Interval Type: HOURS

Note: When the application installed first time, the Email notifications are disabled by default for every 4 hours. Please configure email server details and then enable the Email notifications using Click to Enable/Disable Email notifications for all users including Admin.

Mail Notification Job Run Details

Run On	Status	Error Code	Additional Info
16-MAR-17 12.00.43.461237 AM -07:00	SUCCEEDED	0	-
15-MAR-17 08.00.35.153894 PM			

Purge Job Interval   Click To Disable Purging ✖
Click to Update Retention Period   Click To Purge SampleData ✔

Purge Frequency Retention: 3

Frequency RetentionType: MONTHLY

Note: When the application installed first time, the daily purge job enabled by default for purging data older than 3 months. Please configure the frequency of old data purge using Click To Update Retention Period.

Purge Job Run Details

Log Date	STATUS	ERROR#	ADDITIONAL_INFO
14-MAR-2017	SUCCEEDED	0	-
13-MAR-2017	SUCCEEDED	0	-
12-MAR-2017	SUCCEEDED	0	-

3.2.6 Oracle Health Check Collections Manager Application Features

Familiarize yourself with the features of Oracle Health Check Collections Manager Application.

- Global Select Lists
  Oracle Health Check Collections Manager Application provides an option to display data based on the select lists like Business Units, Systems, and Data for last periods of time.
- Home Tab
  Displays systems and their statuses, and recent activities of all users who has permission to access the application.
- Collections Tab
  Displays incidence information for each collection, and collection score for failed, warning, and failed checks.
- Collections > Browse Sub Tab
  Enables you to list individual checks based on filters set.
- Collections > Compare Sub Tab
  Compare tab enables you to compare audit check results and patch results.
- Report View Tab
  Provides a graphical representation of database checks, instance checks, home path checks, and system health checks.

- Upload Collections Sub Tab
  Provides an interface to manually upload a collection into Oracle Health Check Collections Manager Application and provides a list of uploaded collections and file details.
- Tracking Support Incidents
  The **Incidents** tab gives you a complete system for tracking support incidents.
- Authoring User-Defined Checks
  User-defined checks are checks written, tested, verified, and maintained by you that are specific to your environment.

3.2.6.1 Global Select Lists

Oracle Health Check Collections Manager Application provides an option to display data based on the select lists like Business Units, Systems, and Data for last periods of time.

All these select lists are global within the application and options available on starting of each tab.

- Business Unit
- System
- Data interval

3.2.6.2 Home Tab

Displays systems and their statuses, and recent activities of all users who has permission to access the application.

- Displays systems and their statuses in graphs with color coded green, orange, and red based on check results (passed, warning, and failed).
- The **Home** tab provides an option to display the data based on select lists like Business Units and Data for last periods of time. There is also an option to filter the most failed/warned checks and recent collections based on system name.
- The **Most Failed Checks** region displays information for the most frequently failed checks for all collections for the time period, Business Unit, or System selected, and displays the check name, fail count. There is a similar region for most warned checks.
- The **Recent Collections** region displays brief information about recently uploaded collections based on time frame, Overall score with Fail, Warning, and Pass counts and a Status flag. Recent collections are automatically compared to the last collection from the same system, whenever it occurred, if there is one.

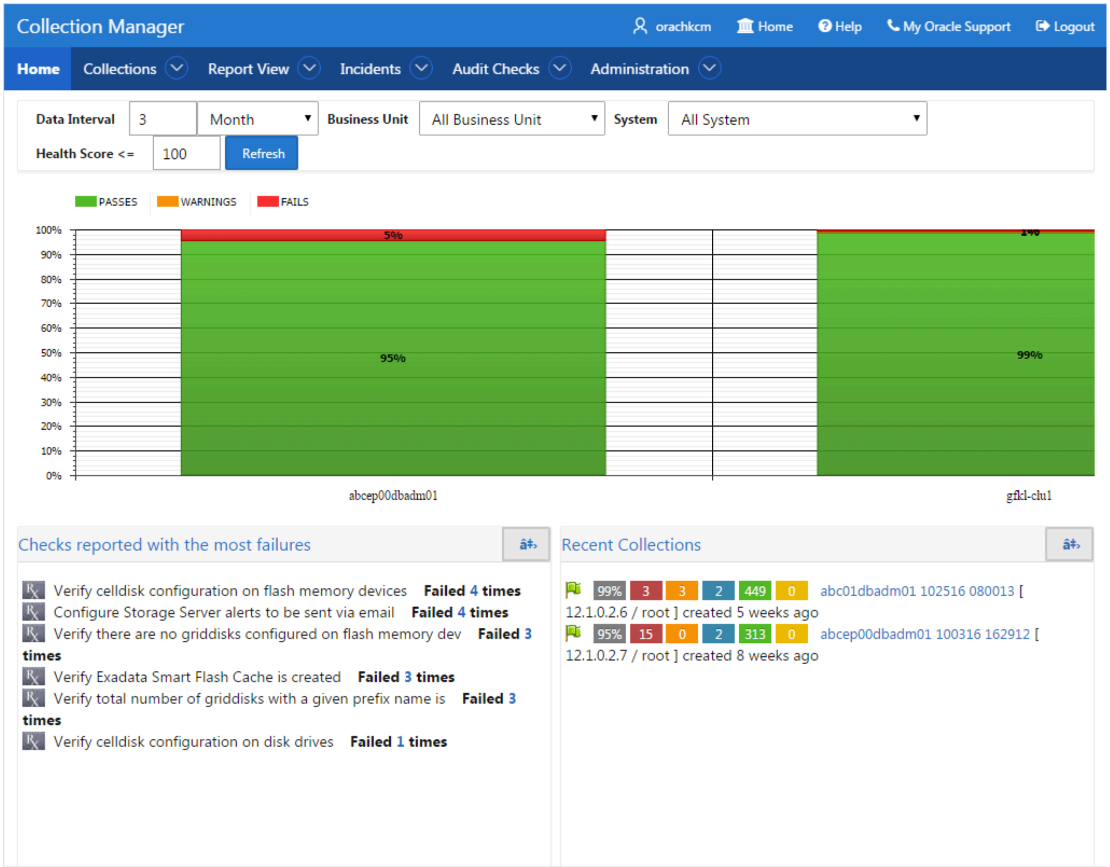
  Status Flags are color-coded green, orange, or red based on the comparison between the recent collection and the last collection, if any.

  - GREEN: There is no difference at all between the two collections or one or more findings from the last collection improved from WARNING or FAIL to PASS or there was no earlier collection to compare with.
  - ORANGE: There were one or more regressions between the last collection and the most recent on a given system. In other words some findings transitioned in a negative way, for example, PASS to WARNING.

  - RED: There were one or more regressions between the last collection and the most recent on a given system. In other words some findings transitioned in a negative way, for example, PASS to FAIL.

- Recent Activity in **User Range** shows recent activities by all users across all collections specific to the access role granted the user.
  - DBA role users can see everything that happens in the systems assigned to them.
  - DBA Manager role users can see everything within their Business Unit and the systems assigned to them.
  - Admin role user can see everything when there is a collection data uploaded in to the application.

Figure 3-75 Home Tab



Data Interval 3 Month
Business Unit All Business Unit
System All System
Health Score <= 100

Checks reported with the most failures

Verify celldisk configuration on flash memory devices **Failed 4 times**
Configure Storage Server alerts to be sent via email **Failed 4 times**
Verify there are no griddisks configured on flash memory dev **Failed 3 times**
Verify Exadata Smart Flash Cache is created **Failed 3 times**
Verify total number of griddisks with a given prefix name is **Failed 3 times**
Verify celldisk configuration on disk drives **Failed 1 times**

Recent Collections

99% 3 3 2 449 0 abc01dbadm01 102516 080013 [12.1.0.2.6 / root] created 5 weeks ago
95% 15 0 2 313 0 abcep00dbadm01 100316 162912 [12.1.0.2.7 / root] created 8 weeks ago

3.2.6.3 Collections Tab

Displays incidence information for each collection, and collection score for failed, warning, and failed checks.

- Displays all collections and allows you to filter the list of collections based on Business units and System. You can also filter based on Status flag. The list is also inherently filtered to those collections the user has access to, based on their assigned role.

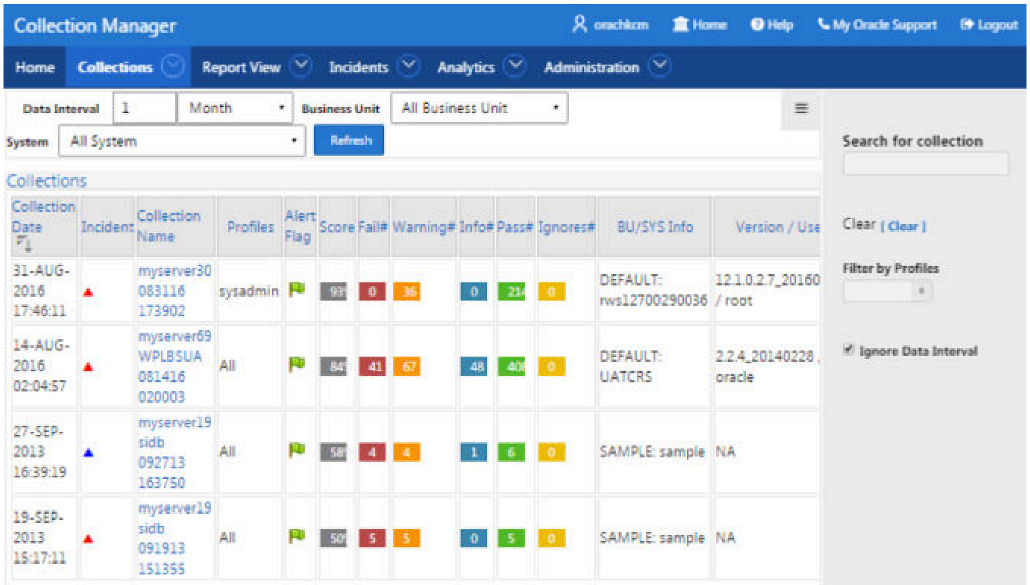
- Displays incident information for each collection indicated by Delta (Δ) color coded red, blue, and green based on ticket status. Click the delta symbol to raise a new ticket or alter the ticket for an entire collection.
  - **RED (No Incident ticket exists)**: Click to create a new incident ticket for the collection or individual checks.
  - **BLUE (An open Incident ticket exists)**: Click to open the incident ticket for editing.
  - **GREEN (A closed Incident ticket exists)**: Click opens the closed incident ticket for viewing.
- Collection Score is calculated based on failed, warning, and passed checks.

  If a user raised a ticket for the collection, resolved the issues and the ticket is closed signifying the issues have all been resolved, then Oracle Health Check Collections Manager changes the collection score to 100%.

  If a user raised a ticket for an individual check and if it is closed signifying that the finding has been resolved, then Oracle Health Check Collections Manager changes the status of the check as PASS and recalculates the collection score.

  Collection Score is derived using following formula.
  - Every check has 10 points.
  - Failure deducts 10 points.
  - Warning deducts 5 points.
  - Info deducts 3 points.
- A **More Info** link next to a collection indicates that the collection was manually uploaded into the application.
- Click the linked collection name in the list to load the collection in the **Browse** tab.

Figure 3-76   Collections Tab



Data Interval 1 Month
Business Unit All Business Unit
System All System
☑ Ignore Data Interval

Collection Date	Incident	Collection Name	Profiles	Alert Flag	Score	Fail#	Warning#	Info#	Pass#	Ignores#	BU/SYS Info	Version / Use
31-AUG-2016 17:46:11	▲	myserver30 083116 173902	sysadmin	⚑	93	0	36	0	21	0	DEFAULT: rws12700290036	12.1.0.2.7_20160 / root
14-AUG-2016 02:04:57	▲	myserver69 WPLBSUA 081416 020003	All	⚑	84	41	67	48	40	0	DEFAULT: UATCRS	2.2.4_20140228 / oracle
27-SEP-2013 16:39:19	▲	myserver19 sidb 092713 163750	All	⚑	58	4	4	1	6	0	SAMPLE: sample	NA
19-SEP-2013 15:17:11	▲	myserver19 sidb 091913 151355	All	⚑	50	5	5	0	5	0	SAMPLE: sample	NA

3.2.6.4 Collections > Browse Sub Tab

Enables you to list individual checks based on filters set.

- Set filters once the list of checks is created.
- Create and alter incident tickets for individual audit check findings similar to as described in the **Collections** tab.
- Select checks to ignore and to undo previously ignored checks. Select the check box beside the audit check and click **Ignore Selected**. Oracle Health Check Collections Manager marks them as **FAIL-IGNORED**, indicating that the check had failed but is ignored.

  Oracle Health Check Collections Manager ignores the checks for the entire level based on the level selected for ignoring.

  To ignore selected failed checks, you must choose the ignore type from the following list:

  - Ignore from collection
  - Ignore from system
  - Ignore from a business unit
  - Ignore from all business units

  > **Note:**
  >
  > The domain for ignoring checks is within the role assigned to the user.

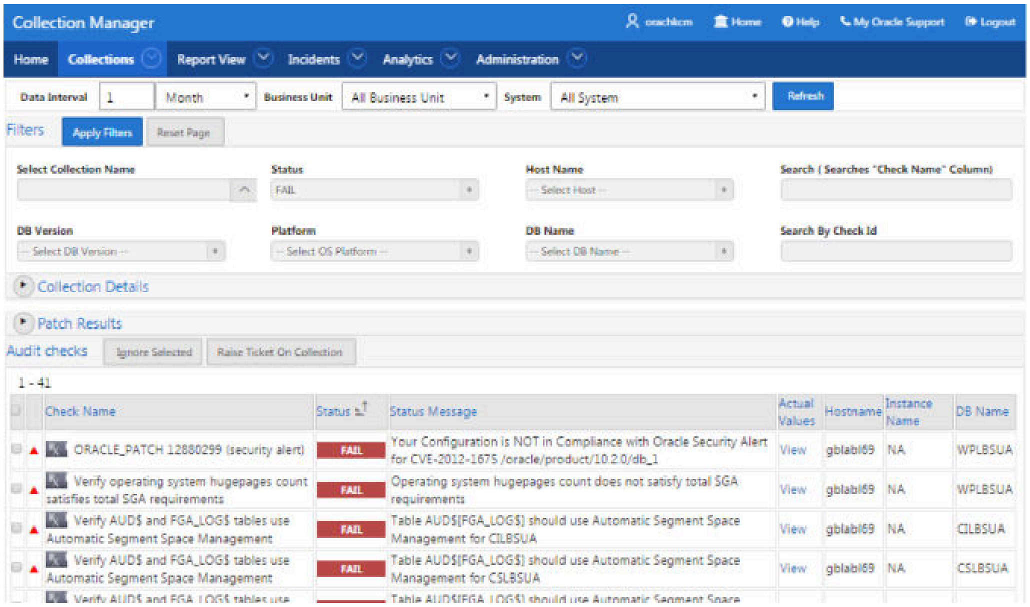
  All ignored checks are listed under the **Ignored Checks** tab. If needed, undo ignore.

  To undo the selected Ignored checks, consider the type from the following list:

  - Undo ignore from collection
  - Undo ignore from system
  - Undo ignore from business unit
  - Undo ignore from all business units

  > **Note:**
  >
  > The domain for undoing ignored checks is within the role assigned to the user.

Figure 3-77 Browse Sub Tab



Data Interval 1 Month
Business Unit All Business Unit
System All System

Select Collection Name
Status FAIL
Host Name -- Select Host --
Search (Searches "Check Name" Column)
DB Version -- Select DB Version --
Platform -- Select OS Platform --
DB Name -- Select DB Name --
Search By Check Id

1 - 41

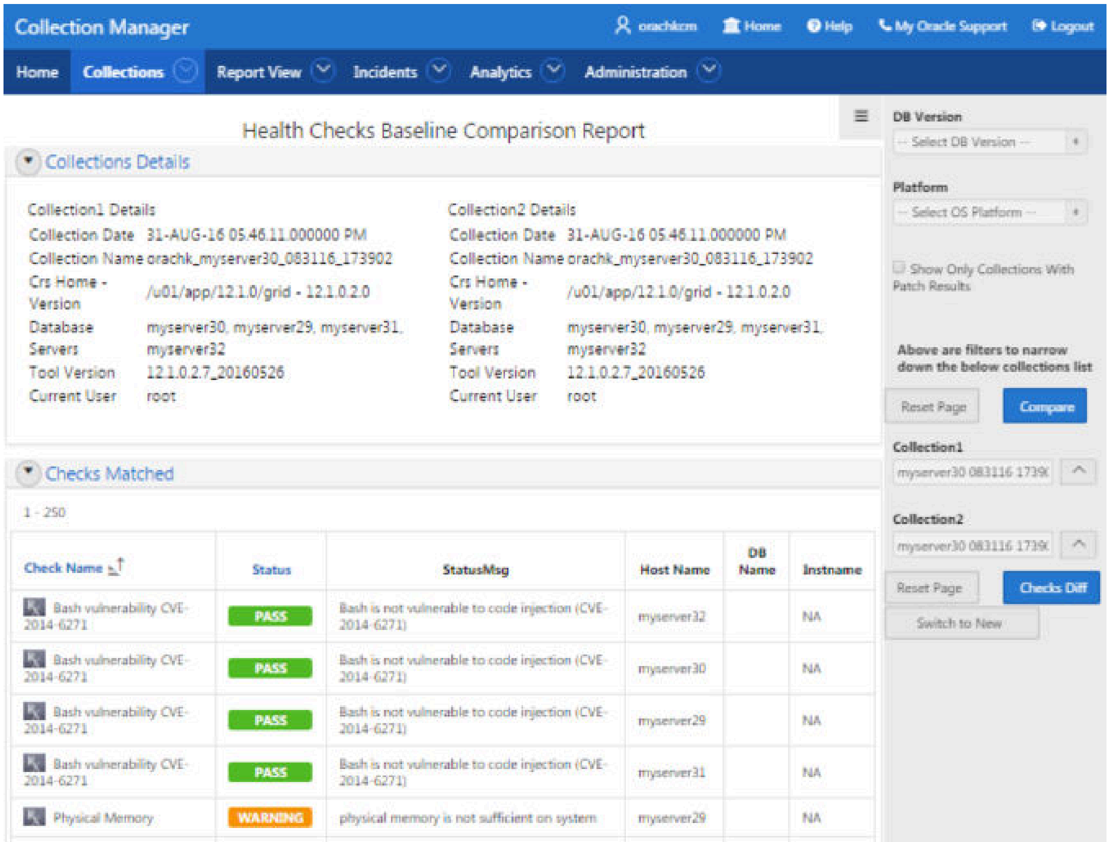
□		Check Name	Status	Status Message	Actual Values	Hostname	Instance Name	DB Name
□	▲	ORACLE_PATCH 12880299 (security alert)	FAIL	Your Configuration is NOT in Compliance with Oracle Security Alert for CVE-2012-1675 /oracle/product/10.2.0/db_1	View	gblabl69	NA	WPLBSUA
□	▲	Verify operating system hugepages count satisfies total SGA requirements	FAIL	Operating system hugepages count does not satisfy total SGA requirements	View	gblabl69	NA	WPLBSUA
□	▲	Verify AUD$ and FGA_LOG$ tables use Automatic Segment Space Management	FAIL	Table AUD$[FGA_LOG$] should use Automatic Segment Space Management for CILBSUA	View	gblabl69	NA	CILBSUA
□	▲	Verify AUD$ and FGA_LOG$ tables use Automatic Segment Space Management	FAIL	Table AUD$[FGA_LOG$] should use Automatic Segment Space Management for CSLBSUA	View	gblabl69	NA	CSLBSUA
		Verify AUD$ and FGA_LOG$ tables use		Table AUD$[FGA_LOG$] should use Automatic Segment Space				

3.2.6.5 Collections > Compare Sub Tab

Compare tab enables you to compare audit check results and patch results.

- **Compare Audit check Results**
  - Compare the audit check findings from two different collections based on Business Unit, System, DB Version and Platform. The collections available for comparison are limited to filters set.
  - Compare collections from the same or different systems.
- **Compare Patch Results**
  - Compare installed Oracle patches from two different collections. The comparison displays the difference between the two collections based on patch results.

Figure 3-78   Compare Sub Tab - Audit Checks Diff



Health Checks Baseline Comparison Report

Collections Details

Collection1 Details		Collection2 Details	
Collection Date	31-AUG-16 05.46.11.000000 PM	Collection Date	31-AUG-16 05.46.11.000000 PM
Collection Name	orachk_myserver30_083116_173902	Collection Name	orachk_myserver30_083116_173902
Crs Home - Version	/u01/app/12.1.0/grid - 12.1.0.2.0	Crs Home - Version	/u01/app/12.1.0/grid - 12.1.0.2.0
Database Servers	myserver30, myserver29, myserver31, myserver32	Database Servers	myserver30, myserver29, myserver31, myserver32
Tool Version	12.1.0.2.7_20160526	Tool Version	12.1.0.2.7_20160526
Current User	root	Current User	root

Checks Matched

1 - 250

Check Name	Status	StatusMsg	Host Name	DB Name	Instname
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver32		NA
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver30		NA
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver29		NA
Bash vulnerability CVE-2014-6271	PASS	Bash is not vulnerable to code injection (CVE-2014-6271)	myserver31		NA
Physical Memory	WARNING	physical memory is not sufficient on system	myserver29		NA

DB Version: -- Select DB Version --

Platform: -- Select OS Platform --

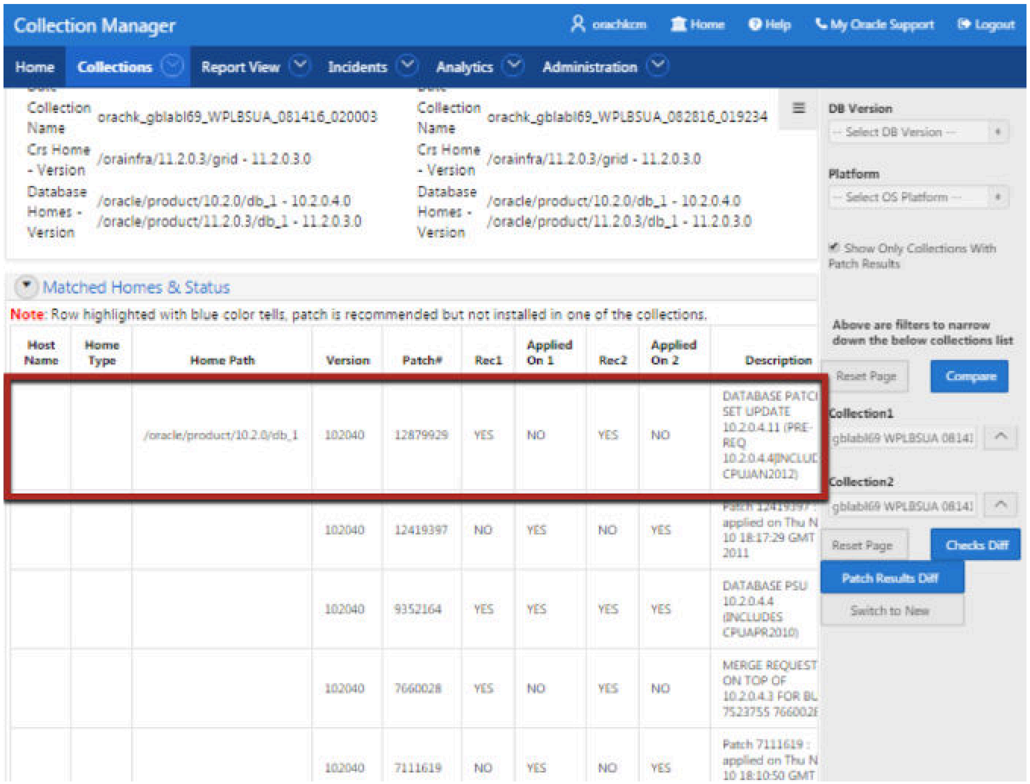
☐ Show Only Collections With Patch Results

Above are filters to narrow down the below collections list

Collection1: myserver30 083116 1739(

Collection2: myserver30 083116 1739(

Figure 3-79   Compare Sub Tab - Patch Results Diff



Collection Name: orachk_gblabl69_WPLBSUA_081416_020003
Crs Home - Version: /orainfra/11.2.0.3/grid - 11.2.0.3.0
Database Homes - Version: /oracle/product/10.2.0/db_1 - 10.2.0.4.0
/oracle/product/11.2.0.3/db_1 - 11.2.0.3.0

Collection Name: orachk_gblabl69_WPLBSUA_082816_019234
Crs Home - Version: /orainfra/11.2.0.3/grid - 11.2.0.3.0
Database Homes - Version: /oracle/product/10.2.0/db_1 - 10.2.0.4.0
/oracle/product/11.2.0.3/db_1 - 11.2.0.3.0

DB Version: -- Select DB Version --
Platform: -- Select OS Platform --
☑ Show Only Collections With Patch Results

Above are filters to narrow down the below collections list

Collection1: gblabl69 WPLBSUA 08141
Collection2: gblabl69 WPLBSUA 08141

Matched Homes & Status

Note: Row highlighted with blue color tells, patch is recommended but not installed in one of the collections.

Host Name	Home Type	Home Path	Version	Patch#	Rec1	Applied On 1	Rec2	Applied On 2	Description
		/oracle/product/10.2.0/db_1	102040	12879929	YES	NO	YES	NO	DATABASE PATCH SET UPDATE 10.2.0.4.11 (PRE-REQ 10.2.0.4.4)(INCLUD CPUJAN2012)
			102040	12419397	NO	YES	NO	YES	Patch 12419397 : applied on Thu N 10 18:17:29 GMT 2011
			102040	9352164	YES	YES	YES	YES	DATABASE PSU 10.2.0.4.4 (INCLUDES CPUAPR2010)
			102040	7660028	YES	NO	YES	NO	MERGE REQUEST ON TOP OF 10.2.0.4.3 FOR BL 7523755 766002
			102040	7111619	NO	YES	NO	YES	Patch 7111619 : applied on Thu N 10 18:10:50 GMT

Note:

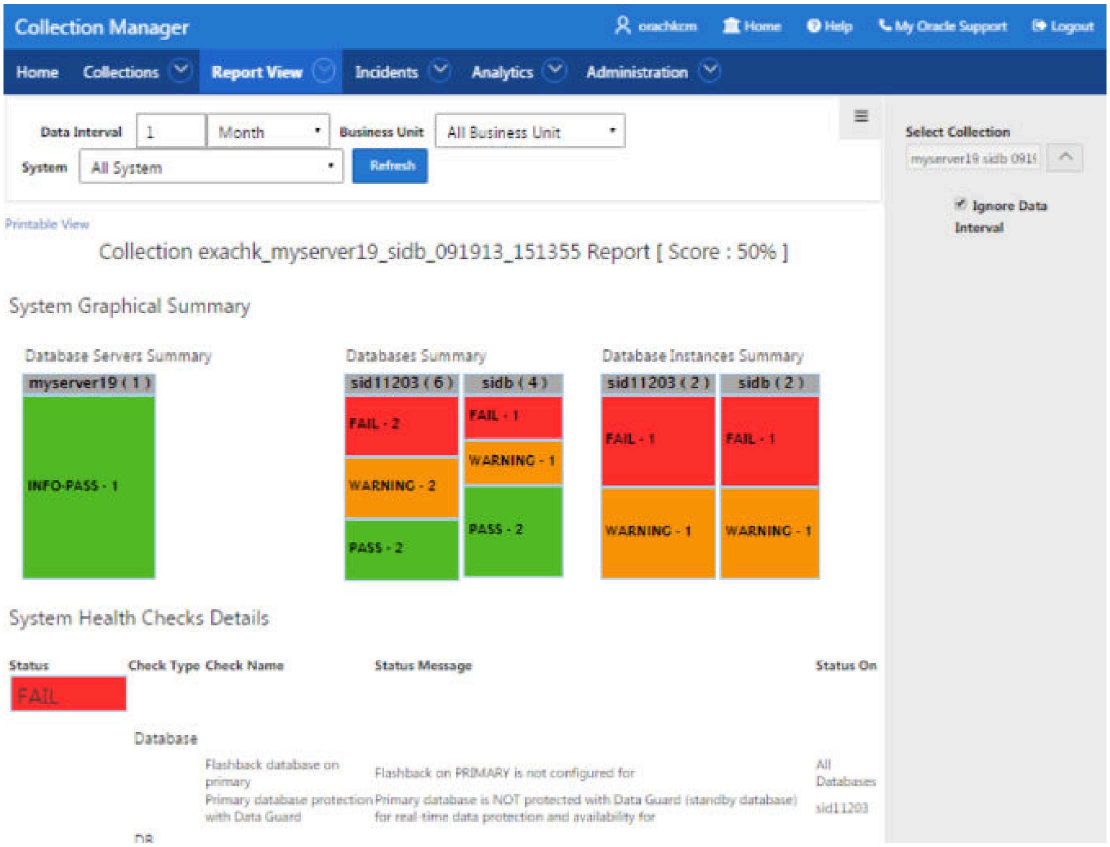
Row highlighted indicates that a patch is recommended, but it is not installed in either of the collections.

3.2.6.6 Report View Tab

Provides a graphical representation of database checks, instance checks, home path checks, and system health checks.

- Provides a printable view option to print the graphical summary of system collection
- Displays separate graphical summary view for database checks, instance checks, and home path checks breakup based on check type and check status in collection
- Displays system health check details based on status and check type in collection

Figure 3-80 Report View Tab - Summary



Data Interval 1 Month
Business Unit All Business Unit
System All System

Select Collection myserver19 sidb 091

☑ Ignore Data Interval

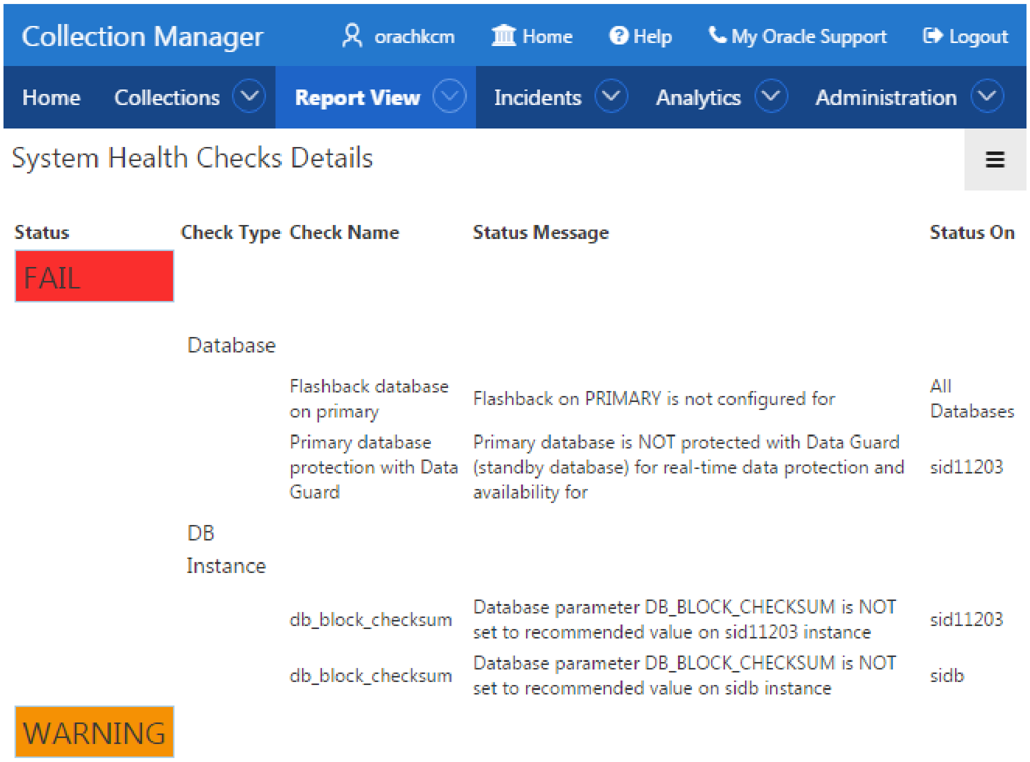
Collection exachk_myserver19_sidb_091913_151355 Report [Score : 50%]

System Graphical Summary

System Health Checks Details

Status	Check Type	Check Name	Status Message	Status On
FAIL				
	Database			
		Flashback database on primary	Flashback on PRIMARY is not configured for	All Databases
		Primary database protection with Data Guard	Primary database is NOT protected with Data Guard (standby database) for real-time data protection and availability for	sid11203
	DB			

Figure 3-81 Report View Tab - Details



System Health Checks Details

Status	Check Type	Check Name	Status Message	Status On
FAIL				
	Database			
		Flashback database on primary	Flashback on PRIMARY is not configured for	All Databases
		Primary database protection with Data Guard	Primary database is NOT protected with Data Guard (standby database) for real-time data protection and availability for	sid11203
	DB Instance			
		db_block_checksum	Database parameter DB_BLOCK_CHECKSUM is NOT set to recommended value on sid11203 instance	sid11203
		db_block_checksum	Database parameter DB_BLOCK_CHECKSUM is NOT set to recommended value on sidb instance	sidb
WARNING				

3.2.6.7 Upload Collections Sub Tab

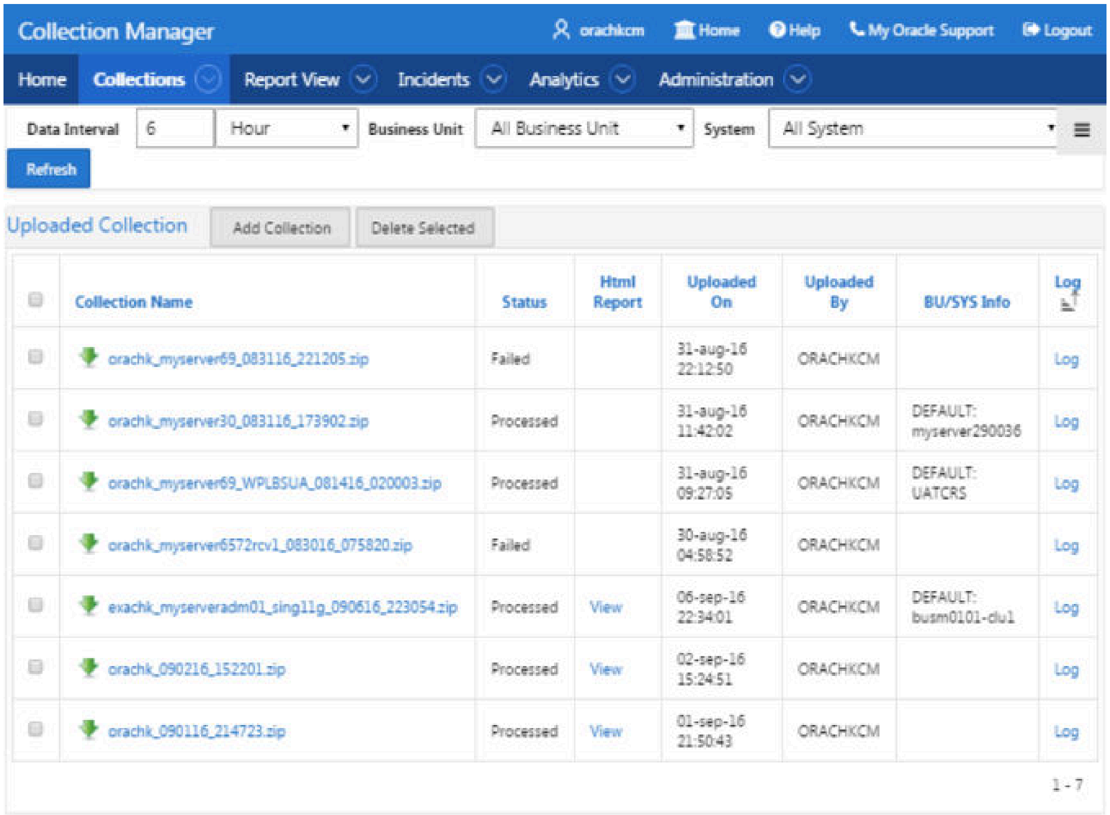
Provides an interface to manually upload a collection into Oracle Health Check Collections Manager Application and provides a list of uploaded collections and file details.

These manually uploaded collections are unzipped and their data imported into the framework as if they had been uploaded at runtime when the tool was run. Therefore, even if the tool is not configured for automatic upload into the Oracle Health Check Collections Manager Application, you can always upload collections manually.

Note:

Using a combination of tables and environment variables, you can automate the process of uploading collections into the database hosting the Oracle Health Check Collections Manager Application at runtime.

Figure 3-82   Upload Collections Sub Tab



□	Collection Name	Status	Html Report	Uploaded On	Uploaded By	BU/SYS Info	Log
□	orachk_myserver69_083116_221205.zip	Failed		31-aug-16 22:12:50	ORACHKCM		Log
□	orachk_myserver30_083116_173902.zip	Processed		31-aug-16 11:42:02	ORACHKCM	DEFAULT: myserver290036	Log
□	orachk_myserver69_WPLBSUA_081416_020003.zip	Processed		31-aug-16 09:27:05	ORACHKCM	DEFAULT: UATCRS	Log
□	orachk_myserver6572rcv1_083016_075820.zip	Failed		30-aug-16 04:58:52	ORACHKCM		Log
□	exachk_myserveradm01_sing11g_090616_223054.zip	Processed	View	06-sep-16 22:34:01	ORACHKCM	DEFAULT: busm0101-clu1	Log
□	orachk_090216_152201.zip	Processed	View	02-sep-16 15:24:51	ORACHKCM		Log
□	orachk_090116_214723.zip	Processed	View	01-sep-16 21:50:43	ORACHKCM		Log

1 - 7

3.2.6.8 Tracking Support Incidents

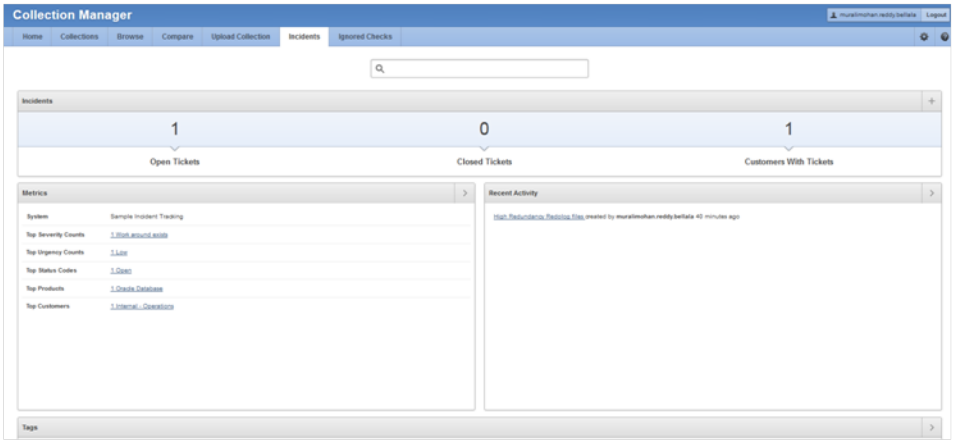
The **Incidents** tab gives you a complete system for tracking support incidents.

- Specify contact details of each customer, products and categories, and then set up values to limit status codes, severity, and urgency attributes for an incident
- Raise a new ticket by clicking the Delta (Δ) symbol. Oracle Health Check Collections Manager displays the delta symbol only in the **Collections** and **Browse** tabs
- The **Browse** tab enables you to create a new ticket on individual checks
- The **Collections** tab enables you to create a single ticket for entire the collection
- Delta (Δ) symbol is color coded red, blue, and green based on the ticket status
  - **RED (No Incident ticket exists)**: Initiates the process to create a new incident ticket for the collection or individual checks
  - **BLUE (An open Incident ticket exists)**: Opens the incident ticket for editing
  - **GREEN (A closed Incident ticket exists)**: Opens the closed incident ticket for viewing
- Track the progress of the ticket in an update area of the ticket, or add attachments and links to the incident
- Use tags to classify incidents and use the resulting tag cloud in your reports

- Incident access and management happen only within your access control range

> **Note:**
>
> Incident Tracking feature is a basic stand-alone system and it is not designed for integration with other commercial enterprise-level trouble ticketing systems.

Figure 3-83 Incidents Tab



1	0	1
Open Tickets	Closed Tickets	Customers With Tickets

System	Sample Incident Tracking
Top Severity Counts	1 Work around exists
Top Urgency Counts	1 Low
Top Status Codes	1 Open
Top Products	1 Oracle Database
Top Customers	1 Internal - Operations

High Redundancy Redolog files created by **muralimohan.reddy.bellala** 40 minutes ago

Incident Tracking Features

- Search options
- Track and analyze incident tickets
- Flexible and updateable incident status
- Robust reporting
- Link, Note, and File Attachments
- Flexible Access Control (reader, contributor, administrator model)
- Incidents Tab
  Create or edit incident tickets for individual checks or for an entire collection.

3.2.6.8.1 Incidents Tab

Create or edit incident tickets for individual checks or for an entire collection.

The statuses of each ticket is represented by icons with different colors. You can act upon by clicking those icons.

- Creating Incident Tickets
  Follow these procedures to create incident tickets.
- Editing Incident Tickets
  Follow these procedures to edit incident tickets.

3.2.6.8.1.1 Creating Incident Tickets

Follow these procedures to create incident tickets.

1. Click the **Delta (Δ)** symbol colored RED.
2. Add your ticket details.
3. Click **Next.**
4. Select the **Product** and **Product Version**.
5. Click **Next**.
6. Select the `Urgency` of the ticket.
7. Select the **Severity** of the ticket.
8. Select the **Status** of the ticket.
9. Select the **Category** of the ticket.
10. Enter a summary and description of the incident.
11. Click **Create Ticket**.

3.2.6.8.1.2 Editing Incident Tickets

Follow these procedures to edit incident tickets.

1. Click the **Incident** tab.
2. Click **Open Tickets**.
3. Click the ticket.
4. Click **Edit Ticket**.
5. Alter required details, click **Apply Changes**.

> **Note:**
>
> Click the delta symbol colored GREEN in the **Collections** or **Browse** tabs to edit incident tickets.

3.2.6.9 Authoring User-Defined Checks

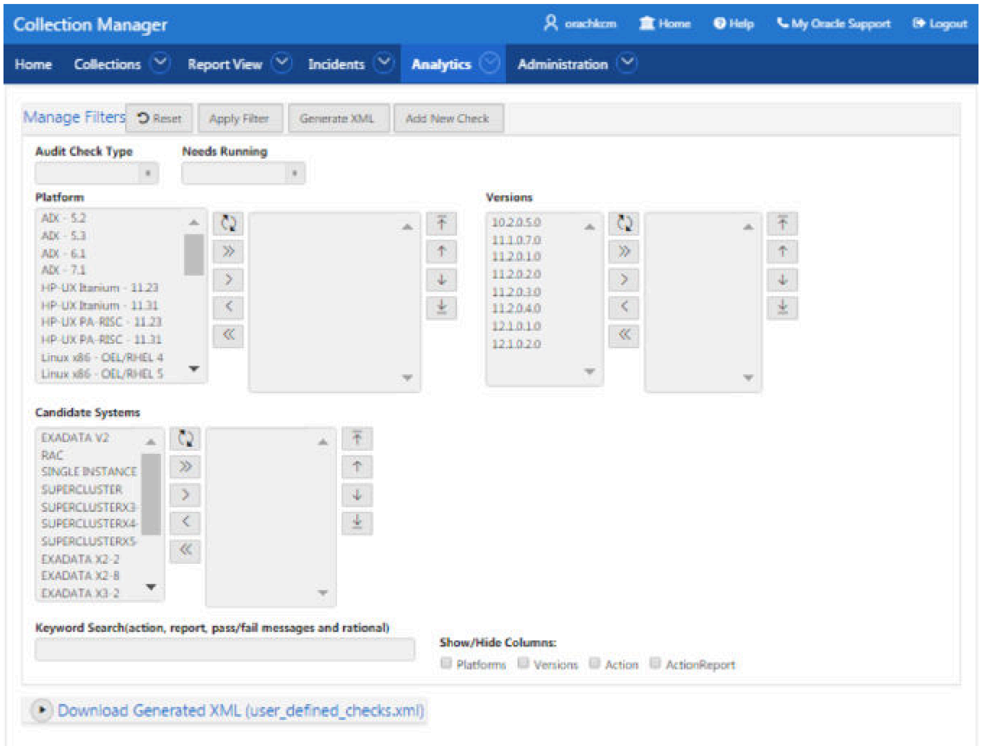
User-defined checks are checks written, tested, verified, and maintained by you that are specific to your environment.

Oracle supports the framework for creating and running user-defined checks, but not the logic of the checks. It is your responsibility to test, verify, author, maintain, and support these checks. The checks are run at runtime by the Oracle Orachk and Oracle Exachk script. Oracle Orachk and Oracle Exachk display the results of the user-defined checks in the **User Defined Checks** section of the HTML report.

The user-defined checks are stored in the Oracle Health Check Collections Manager schema and output to an XML file, which is co-located with the Oracle Orachk script. When Oracle Orachk 12.1.0.2.5 and later run on your system, the tool checks for the presence of this XML file. If found, then Oracle Orachk runs the checks contained therein, and includes the results in the standard HTML report.

1. Click **Analytics** > **User Defined Checks** (or alternatively, **Administration** > **Add New User Defined Checks** to skip to step 3).

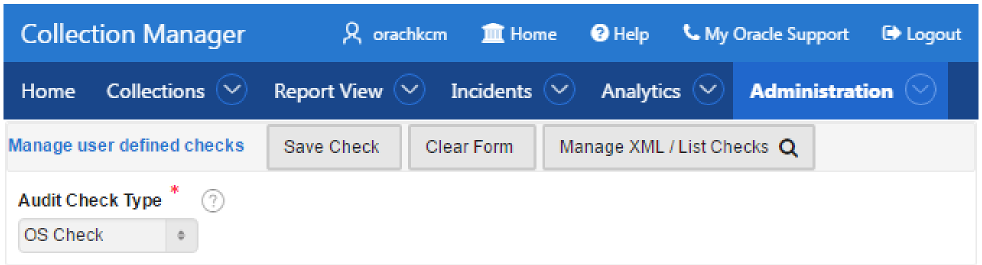
Figure 3-84   User Defined Checks



2. Select **Add New Check**.
3. Select **OS Check** or **SQL Check** as **Audit Check Type**.

   This choice decides how your check logic is coded. Operation System checks use a system command to determine the check status. SQL checks run an SQL statement to determine the check status.

Figure 3-85   User Defined Checks Tab - Audit Check Type



Audit Check Type *

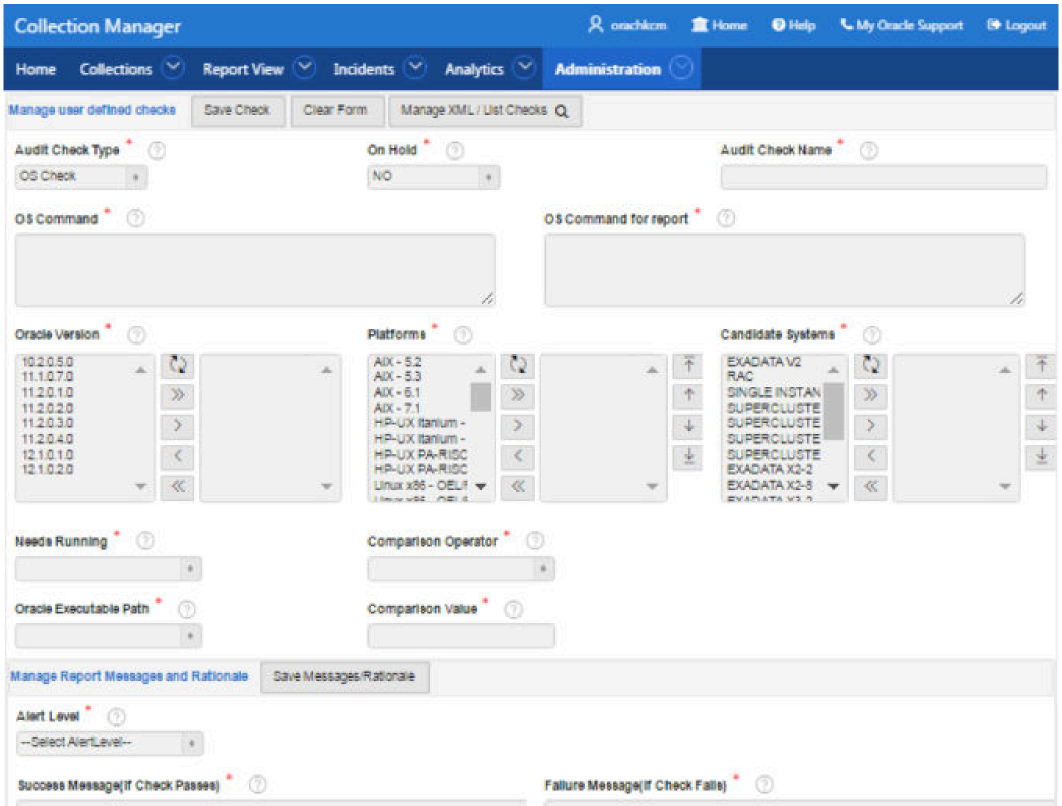
OS Check

Once you have selected an Audit Check Type, Oracle Health Check Collections Manager updates the applicable fields.

Any time during authoring, click the question mark next to a field to see help documentation specific to that field.

OS and SQL commands are supported. Running user defined checks as `root` is NOT supported.

Figure 3-86 User Defined Checks Tab - Audit Check Type - OS Check



Audit Check Type * : OS Check

On Hold * : NO

Audit Check Name *

OS Command *

OS Command for report *

Needs Running *

Comparison Operator *

Oracle Executable Path *

Comparison Value *

Alert Level * : --Select AlertLevel--

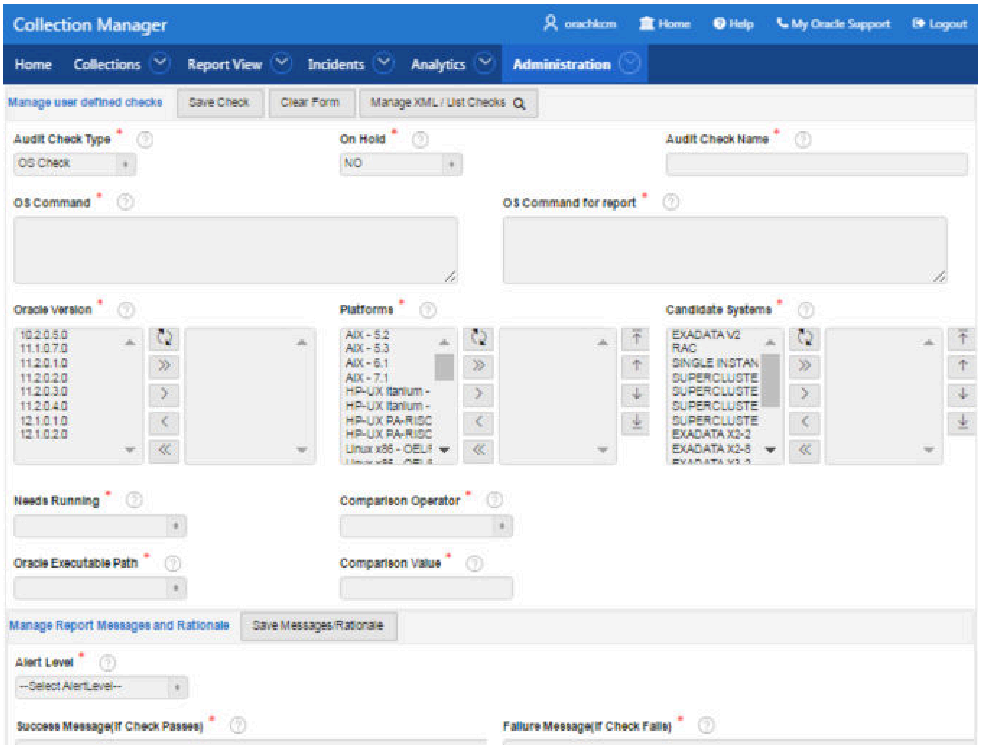
Success Message(If Check Passes) *

Failure Message(If Check Fails) *

Once a check is created, it is listed in the **Available Audit Checks** section.

You can create checks and each can be filtered using the filters on this page.

Figure 3-87   User Defined Checks Tab - Available Audit Checks



Audit Check Type: OS Check

On Hold: NO

Audit Check Name:

OS Command:

OS Command for report:

Oracle Version: 10.2.0.5.0, 11.1.0.7.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, 11.2.0.4.0, 12.1.0.1.0, 12.1.0.2.0

Platforms: AIX - 5.2, AIX - 5.3, AIX - 6.1, AIX - 7.1, HP-UX Itanium -, HP-UX Itanium -, HP-UX PA-RISC, HP-UX PA-RISC, Linux x86 - OEL!

Candidate Systems: EXADATA V2, RAC, SINGLE INSTAN, SUPERCLUSTE, SUPERCLUSTE, SUPERCLUSTE, SUPERCLUSTE, EXADATA X2-2, EXADATA X2-8

Needs Running:

Comparison Operator:

Oracle Executable Path:

Comparison Value:

Alert Level: --Select AlertLevel--

Success Message(If Check Passes):

Failure Message(If Check Fails):

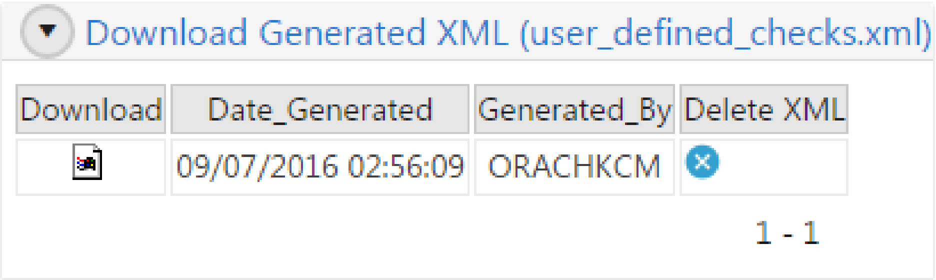
4. Click the **Generate XML**.

   On the right, find a link to download the generated `user_defined_checks.xml` file.

   All the checks that have been authored and have not been placed on hold are included in the XML file when generated. Placing checks on hold is equivalent to a logical delete. If a problem is discovered with a check or the logic has not been perfected, it can be placed on hold to keep it from being included in the XML file until it is production ready. The hold can be removed to include it in the XML file next time it is generated.

   Download the `user_defined_checks.xml` file and save it into the same directory as Oracle Orachk and Oracle Exachk tools. Oracle Orachk and Oracle Exachk run the user-defined checks the next time they run.

Figure 3-88   User Defined Checks Tab - Download User Defined Checks



Download Generated XML (user_defined_checks.xml)

Download	Date_Generated	Generated_By	Delete XML
	09/07/2016 02:56:09	ORACHKCM	✕

1 - 1

Alternatively, to run only the user-defined checks use the profile `user_defined_checks`. When this option is used, then the user-defined checks are the only checks run. The **User Defined Checks** section is the only one with results displayed in the report.

```
orachk -profile user_defined_checks
```

```
exachk -profile user_defined_checks
```

To omit the user-defined checks at runtime, use the `–excludeprofile`option.

```
orachk -excludeprofile user_defined_checks
```

```
exachk -excludeprofile user_defined_checks
```

3.2.7 Viewing and Reattempting Failed Uploads

Configure Oracle Autonomous Health Framework to display and reattempt to upload the failed uploads.

The tools store the values in the *`collection_dir`*`/outfiles/check_env.out` file to record if the previous database upload was successful or not.

The following example shows that database upload has been set up, but the last upload was unsuccessful:

```
DATABASE_UPLOAD_SETUP=1
DATABASE_UPLOAD_STATUS=0
```

To view and reattempt failed uploads:

1. To view failed collections, use the `-checkfaileduploads` option.

   ```
   orachk -checkfaileduploads
   ```

   ```
   exachk -checkfaileduploads
   ```

   For example:

   ```
   $ orachk -checkfaileduploads
   List of failed upload collections
   /home/oracle/orachk_myserver_042016_232011.zip
   /home/oracle/orachk_myserver_042016_231732.zip
   /home/oracle/orachk_myserver_042016_230811.zip
   /home/oracle/orachk_myserver_042016_222227.zip
   /home/oracle/orachk_myserver_042016_222043.zip
   ```

2. To reattempt collection upload, use the `-uploadfailed` option

Specify either all to upload all collections or a comma-delimited list of collections:

```
orachk -uploadfailed all|list of failed collections
```

```
exachk -uploadfailed all|list of failed collections
```

For example:

```
orachk -uploadfailed "/home/oracle/
orachk_myserver_042016_232011.zip, /home/oracle/
orachk_myserver_042016_231732.zip"
```

> **Note:**
>
> You cannot upload collections uploaded earlier because of the SQL unique constraint.

3.2.8 Oracle Health Check Collections Manager Application Uninstallation

Anytime you can decommission Oracle Health Check Collections Manager Application setup. Follow these steps sequentially to uninstall the application leaving no residual files.

- Deleting Oracle Health Check Collections Manager Application
  You need administrative privileges to uninstall Oracle Health Check Collections Manager Application.
- Deleting Workspace Admin
  You need administrative privileges to delete a workspace. There may exist one or more workspaces so be cautious while deleting workspaces.

3.2.8.1 Deleting Oracle Health Check Collections Manager Application

You need administrative privileges to uninstall Oracle Health Check Collections Manager Application.

After successful uninstallation, application definition and the supporting objects are deleted from the hosting database.

1. Log in to Oracle Health Check Collections Manager Application.

   ```
   http://hostname:port/apex
   http://hostname:port/pls/apex/
   ```

   For example:

   ```
   http://dbserver.domain.com:8080/apex/
   ```

2. Specify the **Workspace Name**, **Workspace Username**, and **Password**, and then click **Login**.
3. Click **Application Builder**.
4. Select **Collection Manager Application**, then click **Edit**.
5. Click **Edit Application Page**.
6. Click **Delete**.
7. Choose **Deinstallation Options**.
   - Select the **Remove Application Definition** & **Deinstall Supporting Objects** Deinstallation Options.
   - Click **Deinstall**.

3.2.8.2 Deleting Workspace Admin

You need administrative privileges to delete a workspace. There may exist one or more workspaces so be cautious while deleting workspaces.

1. Log in to Oracle Application Express.
2. Click **Manage Workspaces**.
3. Under **Workspace Reports**, click **Existing Workspaces**, and check the **Workspace** name.
4. Under **Action**, click **Delete**.
5. Select the check box to confirm that you want to proceed with the removal and then click **Next**.
6. Click **Remove Workspace**.

The install process displays the `Workspace has been successfully removed` message.

Related Topics

- http://docs.oracle.com/cd/E59726_01/install.50/e39144/db_pluggable.htm#HTMIG29436

3.2.9 Troubleshooting Oracle Health Check Collections Manager

This topic describes how to troubleshoot Oracle Health Check Collections Manager.

1. If you see any error like, `error at line 13: PLS-00201: identifier 'UTL_SMTP' must be declared` in the **Installation Summary**, then grant execute on `UTL_SMTP` privilege to the parsing schema or workspace owner.
2. If there is a requirement to download files from within the Oracle Health Check Collections Manager, then two more steps are required. These steps are NOT required to upload files into Oracle Health Check Collections Manager.
3. Before installing the Oracle Health Check Collections Manager, run the DDL mentioned below to re-create the Application Express built-in function `WWV_FLOW_EPG_INCLUDE_MOD_LOCAL` in the `APEX_XXXXX` or `FLOW_XXXXXX` schema whichever

is appropriate to your environment. After re-creating the function, ensure that it is in VALID state.

```
CREATE OR replace FUNCTION Wwv_flow_epg_include_mod_local(
procedure_name IN VARCHAR2)
RETURN BOOLEAN
IS
BEGIN
    RETURN TRUE; ----- It should be always “RETURN TRUE”
    IF Upper(procedure_name) IN ( '' ) THEN
        RETURN TRUE;
    ELSE
        RETURN FALSE;
    END IF;
END Wwv_flow_epg_include_mod_local;
```

Once the Oracle Health Check Collections Manager is installed, run RCA13_GET_DOC to enable file downloads:

```
SQL> grant execute on RCA13_GET_DOC to public;
```

4. Ensure that Oracle Application Express is installed successfully. If you have revoked any default system privileges from default Application Express users, then grant them again.
5. Ensure that all the Oracle Application Express related users are not locked and expired.

```
alter user ANONYMOUS account unlock;
alter user XDB account unlock;
alter user APEX_PUBLIC_USER account unlock;
alter user FLOWS_FILES account unlock;
```

6. If you see any issues in setting up email notifications, then verify your ACL permissions and privileges to the application schema on the SMTP mail server.

   For example, to create ACL system and grant privileges to Application schema, do as follows:

```
BEGIN
    DBMS_NETWORK_ACL_ADMIN.CREATE_ACL(acl => 'apex1.xml',
        description => 'APEX ACL',
        principal => 'ORACHK CM USERNAME',
        is_grant => true,
        privilege => 'connect');
    DBMS_NETWORK_ACL_ADMIN.ADD_PRIVILEGE(acl => 'apex1.xml',
        principal => 'ORACHK CM USERNAME',
        is_grant => true,
        privilege => 'resolve');
    DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL(acl => 'apex1.xml',
        host =>
'mailservername.com',lower_port=>10,upper_port=>1000);
END;
```

```
/
COMMIT;
```

7. If you see that any uploaded collection processing is not started or collection status is **NEW** for long time, then verify the database scheduler job `RCA13_PROCESS_DATA` status and ensure that the job is enabled and running fine.

   ```
   select * from user_scheduler_jobs where job_name like 'RCA13_%';
   select * from user_scheduler_running_jobs where job_name like 'RCA13_%'


   select * from user_scheduler_job_run_details where job_name like 'RCA13_%'
   order by log_date desc;
   ```

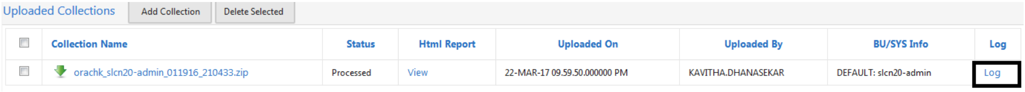
   `RCA13_COL_%` job is used for processing each collection by having unique job.

   This logger helps you in debugging the non-processing collections with reference like

   ```
   select * from rca13_log order by ins_date desc;
   ```

   You can view the logs by clicking **Upload Collections** > **Log**.

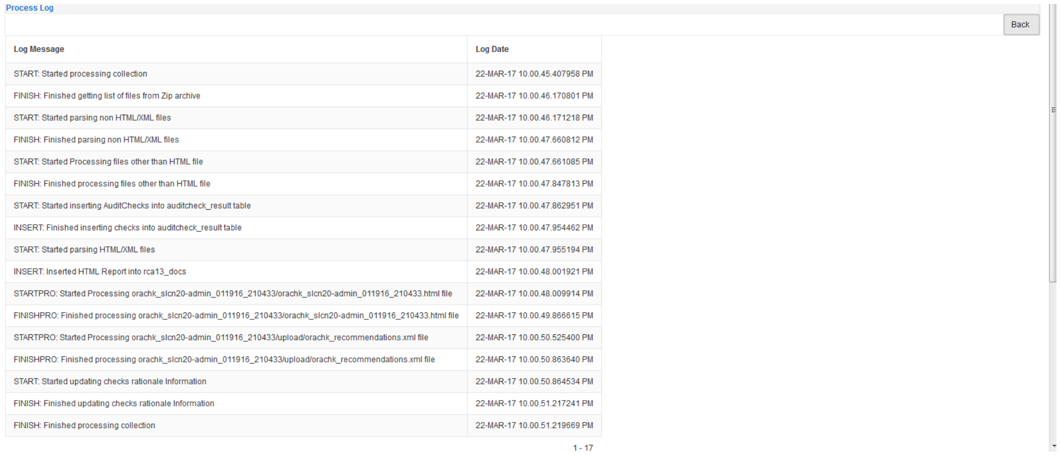
   Figure 3-89 Upload Collections - Log

   Uploaded Collections | Add Collection | Delete Selected

□	Collection Name	Status	Html Report	Uploaded On	Uploaded By	BU/SYS Info	Log
□	orachk_slcn20-admin_011916_210433.zip	Processed	View	22-MAR-17 09.59.50.000000 PM	KAVITHA.DHANASEKAR	DEFAULT: slcn20-admin	Log

   Figure 3-90 Upload Collections - Viewing Logs

   Process Log

   Back

Log Message	Log Date
START: Started processing collection	22-MAR-17 10.00.45.407958 PM
FINISH: Finished getting list of files from Zip archive	22-MAR-17 10.00.46.170801 PM
START: Started parsing non HTML/XML files	22-MAR-17 10.00.46.171218 PM
FINISH: Finished parsing non HTML/XML files	22-MAR-17 10.00.47.660812 PM
START: Started Processing files other than HTML file	22-MAR-17 10.00.47.661085 PM
FINISH: Finished processing files other than HTML file	22-MAR-17 10.00.47.847813 PM
START: Started inserting AuditChecks into auditcheck_result table	22-MAR-17 10.00.47.862951 PM
INSERT: Finished inserting checks into auditcheck_result table	22-MAR-17 10.00.47.954462 PM
START: Started parsing HTML/XML files	22-MAR-17 10.00.47.955194 PM
INSERT: Inserted HTML Report into rca13_docs	22-MAR-17 10.00.48.001921 PM
STARTPRO: Started Processing orachk_slcn20-admin_011916_210433/orachk_slcn20-admin_011916_210433.html file	22-MAR-17 10.00.48.009914 PM
FINISHPRO: Finished processing orachk_slcn20-admin_011916_210433/orachk_slcn20-admin_011916_210433.html file	22-MAR-17 10.00.49.866615 PM
STARTPRO: Started Processing orachk_slcn20-admin_011916_210433/upload/orachk_recommendations.xml file	22-MAR-17 10.00.50.525400 PM
FINISHPRO: Finished processing orachk_slcn20-admin_011916_210433/upload/orachk_recommendations.xml file	22-MAR-17 10.00.50.863640 PM
START: Started updating checks rationale Information	22-MAR-17 10.00.50.864534 PM
FINISH: Finished updating checks rationale Information	22-MAR-17 10.00.51.217241 PM
FINISH: Finished processing collection	22-MAR-17 10.00.51.219669 PM

   1 - 17

8. If you see that collection process is failed due to lack of space in Oracle Application Express tablespace and application schema tablespace, then increase the tablespace sizes as much as needed.

3.2.10 Integrating Collection Manager with Oracle Internet Directory (LDAP) for Authentication

After installing APEX, you can integrate AHF Collection Manager with Oracle Internet Directory (LDAP) for authentication. The steps are provided below.

> **Note:**
>
> These screenshots are from an APEX 18.x release.

1. Ensure that LDAP authentication is working fine.

   ```
   -bash-4.2$ which ldapbind
   /scratch/testuser/Middleware/Oracle_Home/bin/ldapbind
   ```

   For non-SSL:

   ```
   -bash-4.2$ ldapbind -h host.example.com -p 3060 -D 'cn=orcladmin' -
   w ********
   bind successful
   ```

   For SSL:

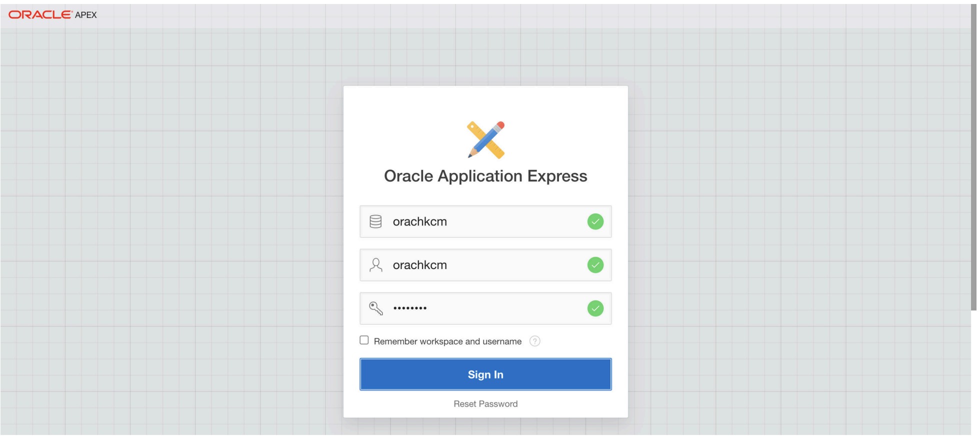
   ```
   -bash-4.2$ ldapbind -h host.example.com -p 3131 -U 1 -D
   'cn=orcladmin' -w ********
   bind successful
   ```

2. Log in to APEX as the collection manager workspace ADMIN.

   For example:

   ```
   Workspace: orachkcm, User: orachkcm, Password: ********
   ```

Figure 3-91 Oracle Application Express Login



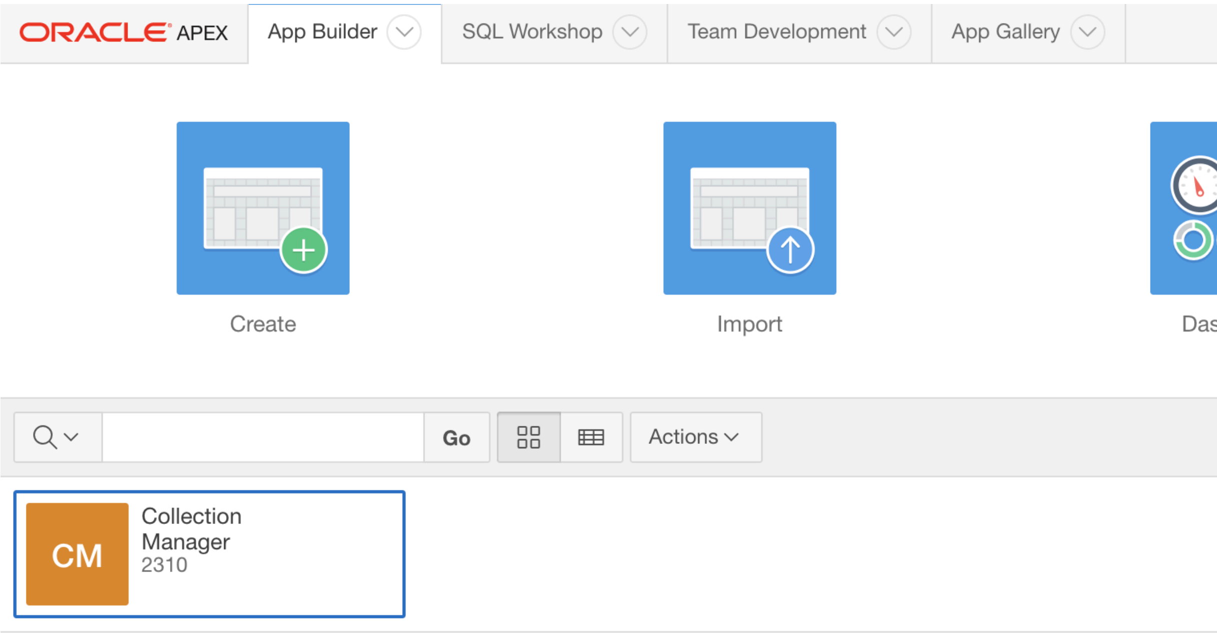
orachkcm

orachkcm

••••••••

3. Click **App Builder** menu and then the **Collection Manager** App.

Figure 3-92 App Builder



4. Click **Shared Components** and then **Security: Authentication Schemes**.

Figure 3-93 Shared Components

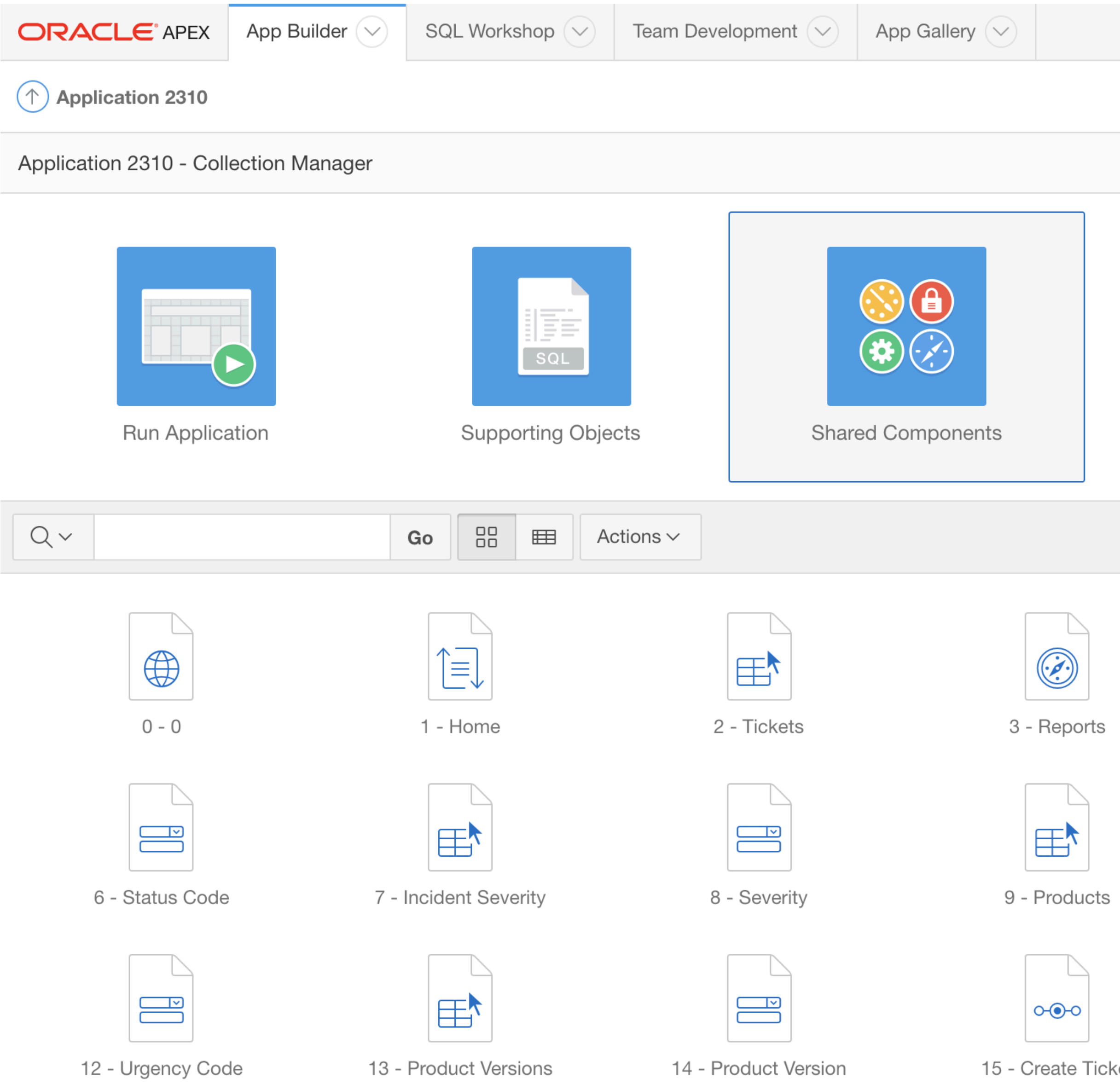
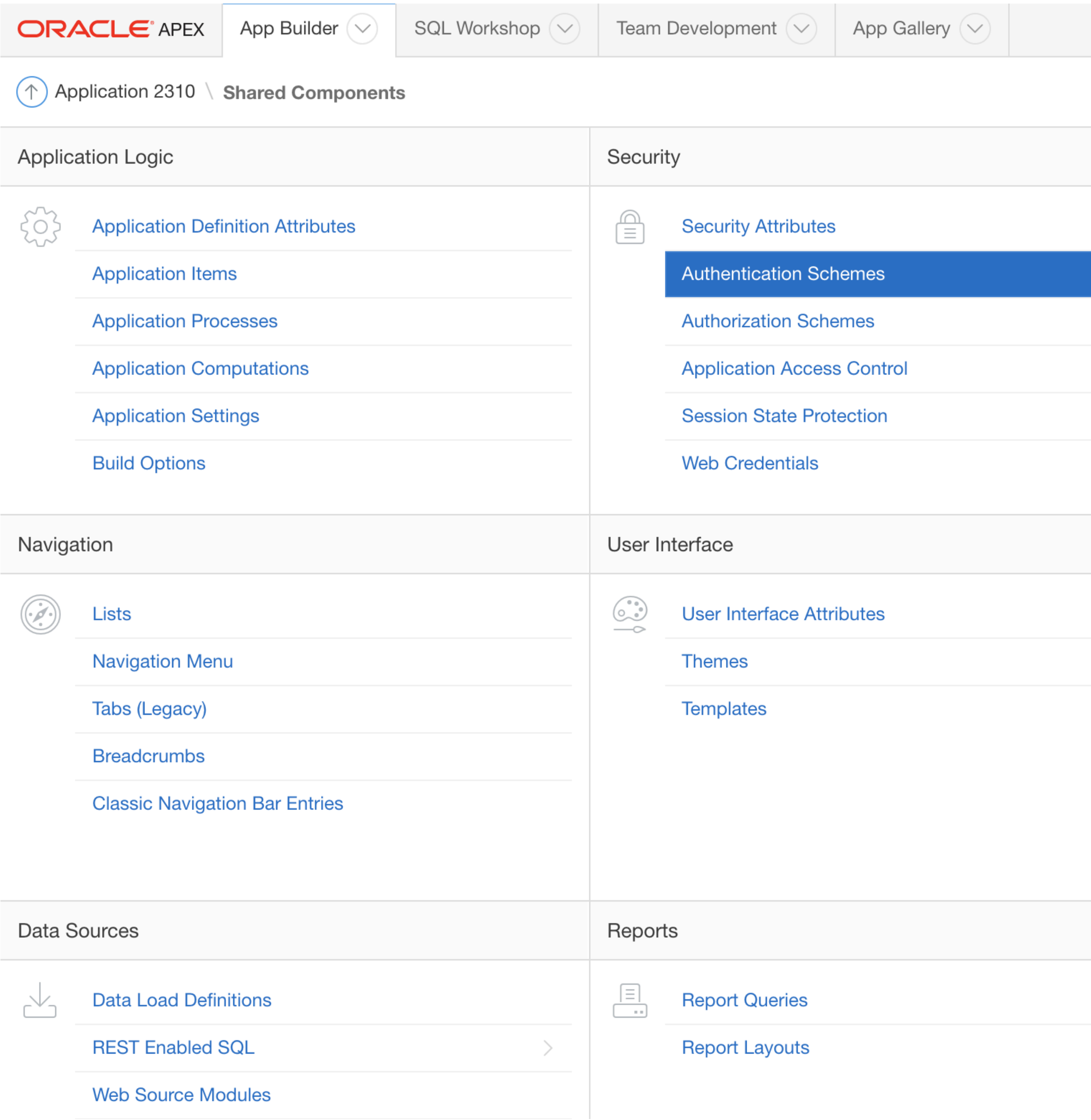
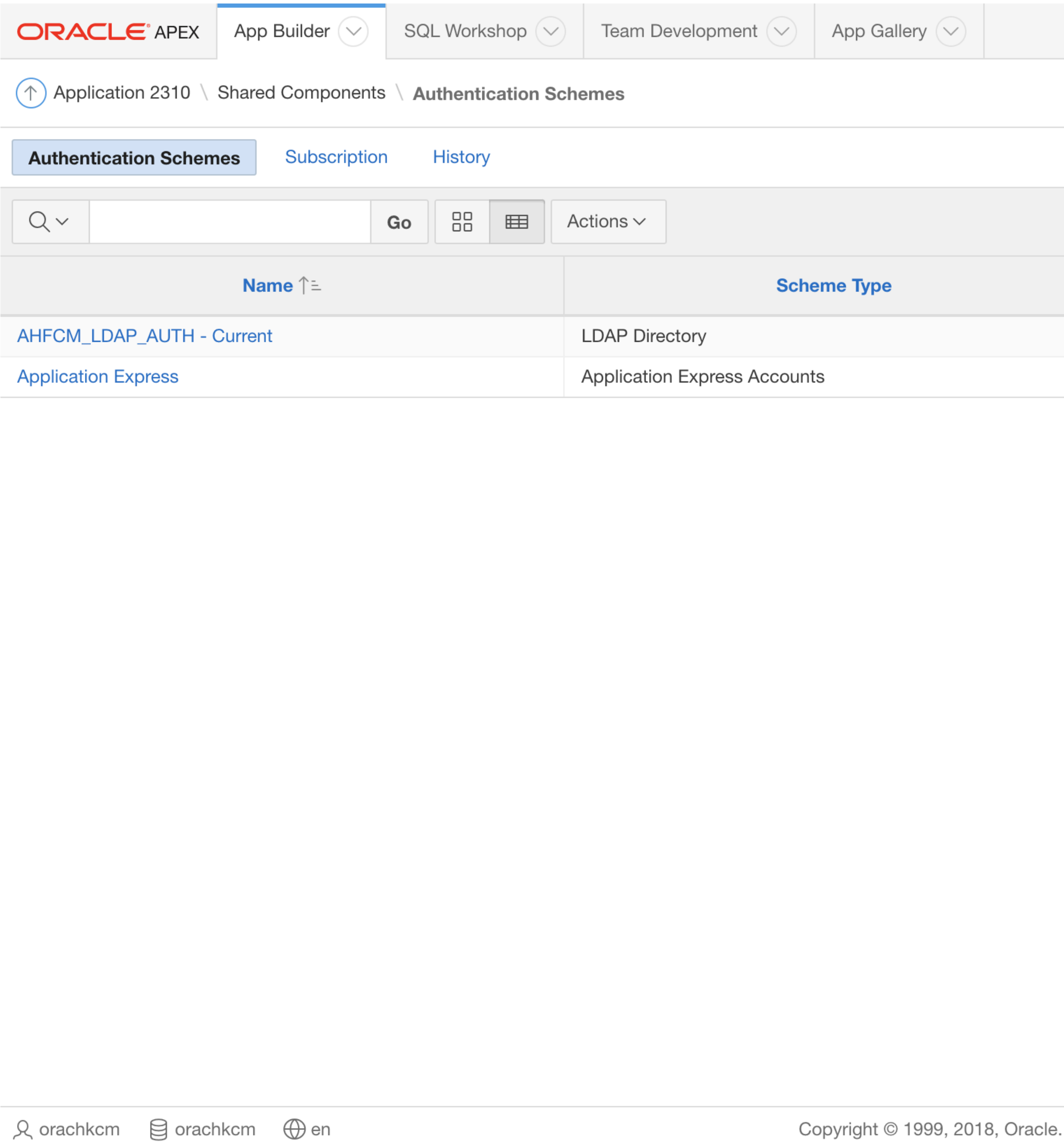


Figure 3-94 Security Authentication Schemes



5. On the Authentication Schemes page, click **Create**.

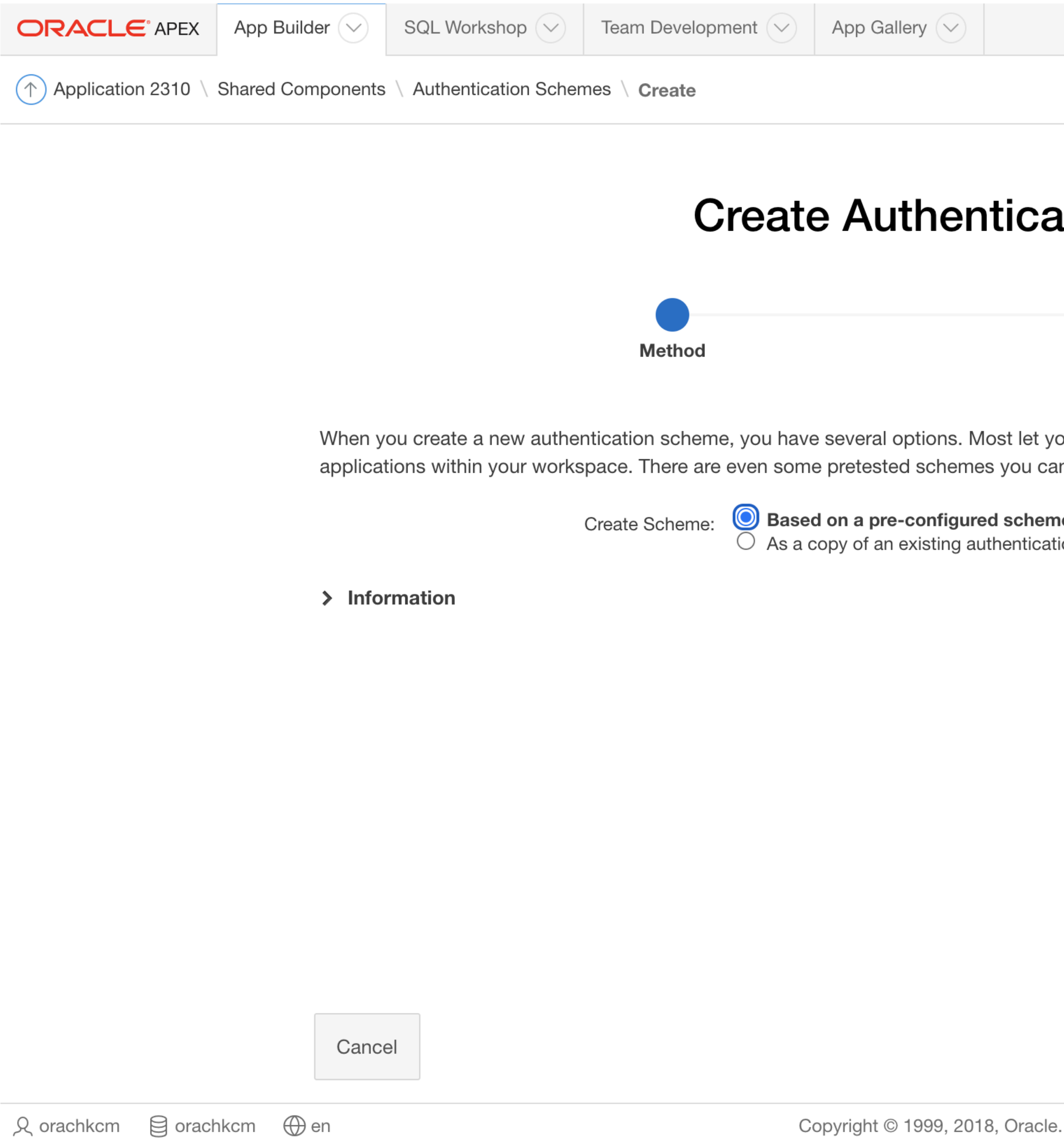
Figure 3-95   Create Authentication Schemes



Name	Scheme Type
AHFCM_LDAP_AUTH - Current	LDAP Directory
Application Express	Application Express Accounts

6. On the Create Authentication Scheme page, select **Based on a pre-configured scheme from the gallery** and then click **Next**.

Figure 3-96   Create Authentication Schemes



ORACLE APEX
App Builder
SQL Workshop
Team Development
App Gallery
Application 2310 \ Shared Components \ Authentication Schemes \ Create

Create Authentica

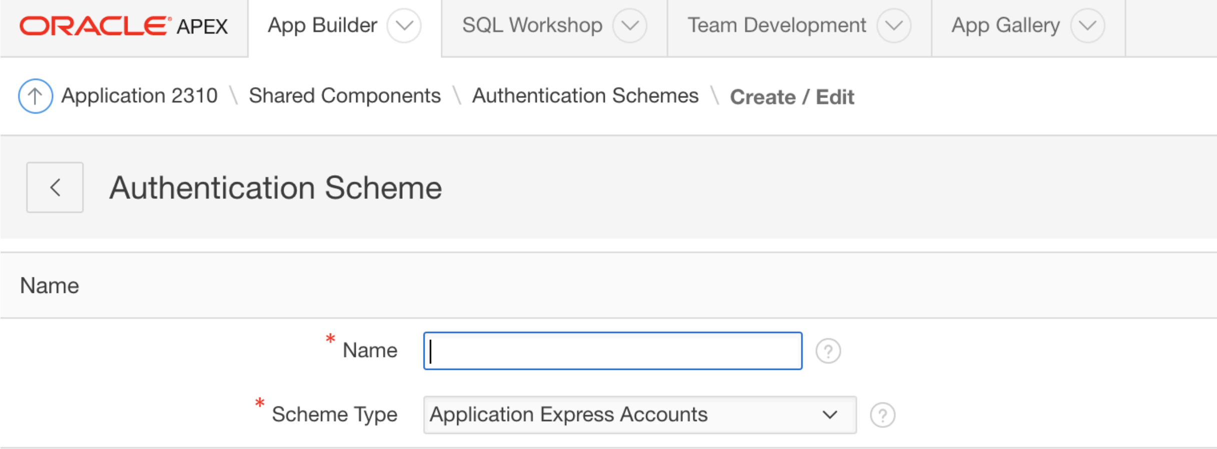
When you create a new authentication scheme, you have several options. Most let yo
applications within your workspace. There are even some pretested schemes you car

Create Scheme: ● **Based on a pre-configured scheme**
○ As a copy of an existing authenticatio

Copyright © 1999, 2018, Oracle.

Create / Edit Authentication Scheme page is displayed.

Figure 3-97 Create/Edit Authentication Scheme


ORACLE APEX
App Builder
SQL Workshop
Team Development
App Gallery
Application 2310 \ Shared Components \ Authentication Schemes \ Create / Edit
Authentication Scheme
Name
* Name
* Scheme Type
Application Express Accounts

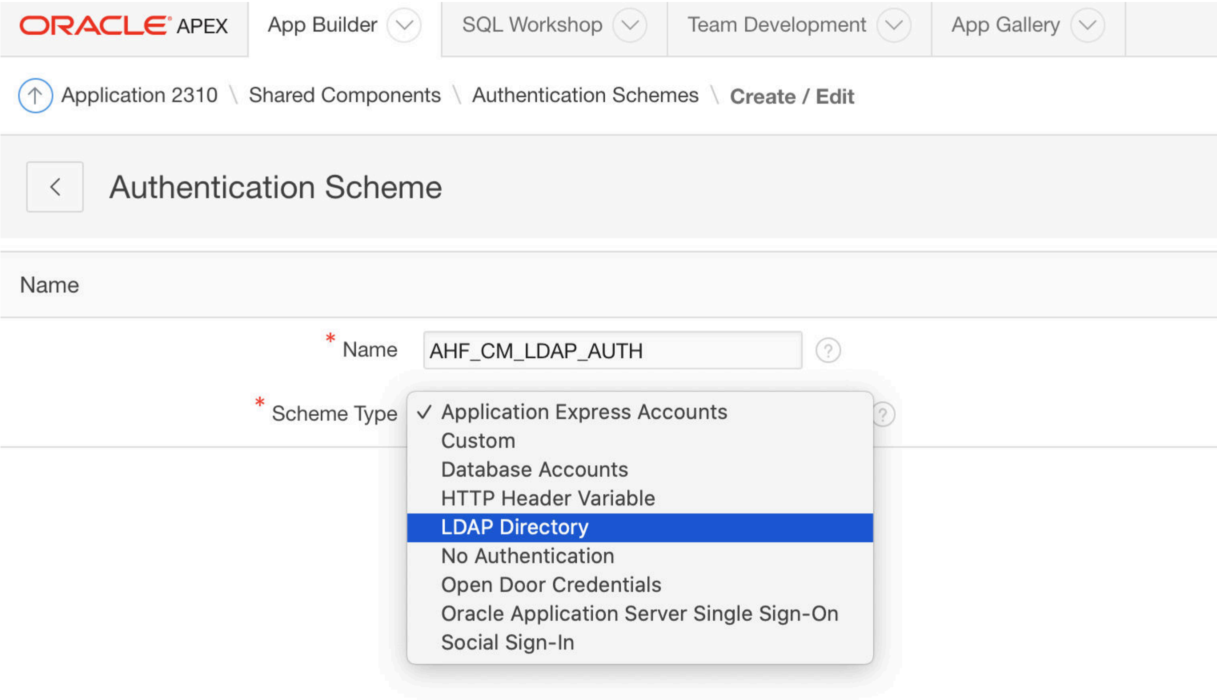
7. On the Create/Edit Authentication Scheme page, enter **Name** and **Scheme Type**.

   For example:

   Name: `AHF_CM_OID_AUTH`

   Scheme Type: Select `LDAP Directory`

Figure 3-98   Create/Edit Authentication Scheme



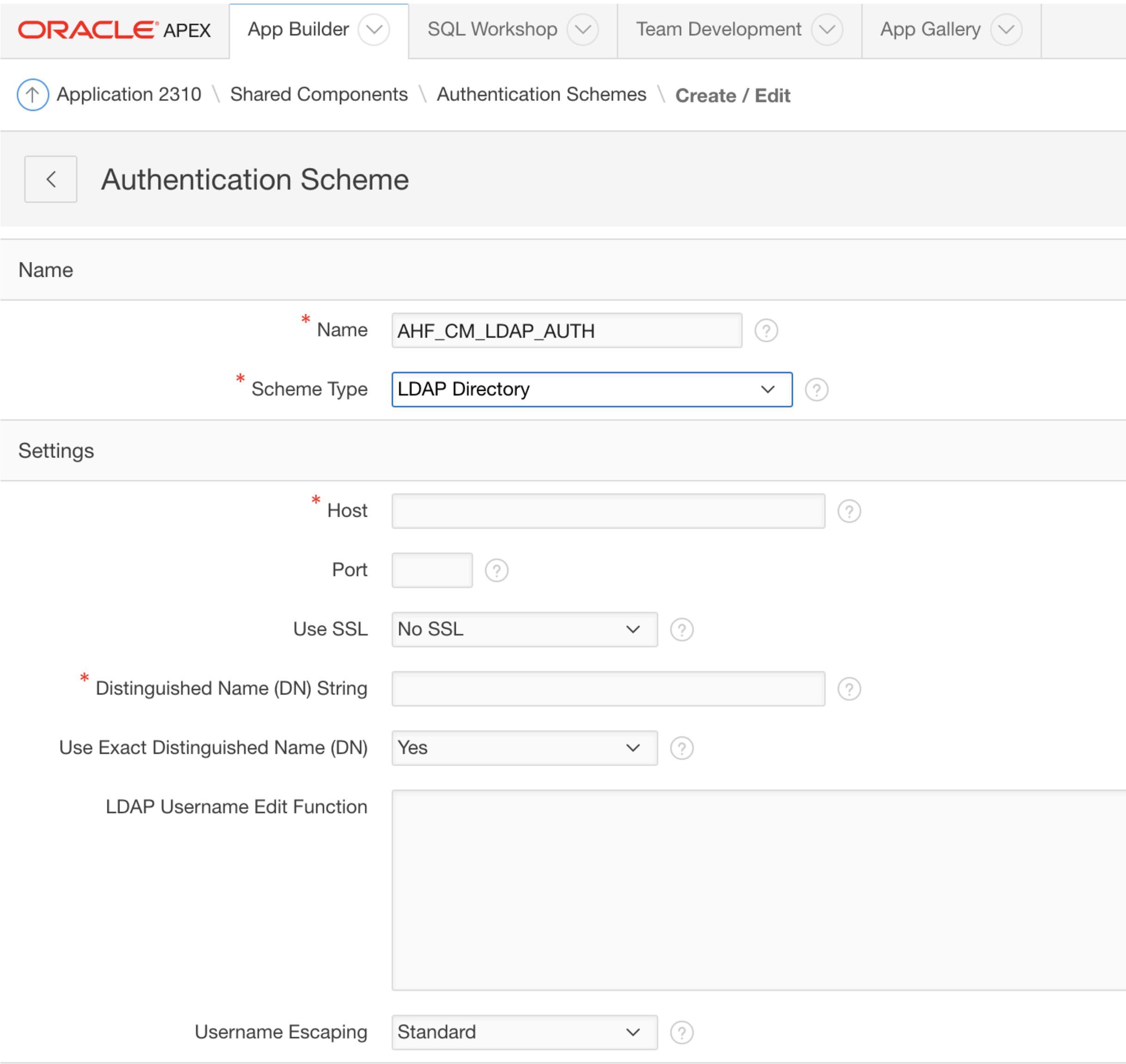
* Name: AHF_CM_LDAP_AUTH

* Scheme Type: LDAP Directory

The Create/Edit Authentication Scheme page expands.

8. Enter additional LDAP settings.

Figure 3-99 Additional LDAP Settings



Name

* Name	AHF_CM_LDAP_AUTH
* Scheme Type	LDAP Directory

Settings

* Host	
Port	
Use SSL	No SSL
* Distinguished Name (DN) String	
Use Exact Distinguished Name (DN)	Yes
LDAP Username Edit Function	
Username Escaping	Standard

Enter the details that match your Oracle Internet Directory (LDAP) environment.

For example:

Host: `host.example.com`

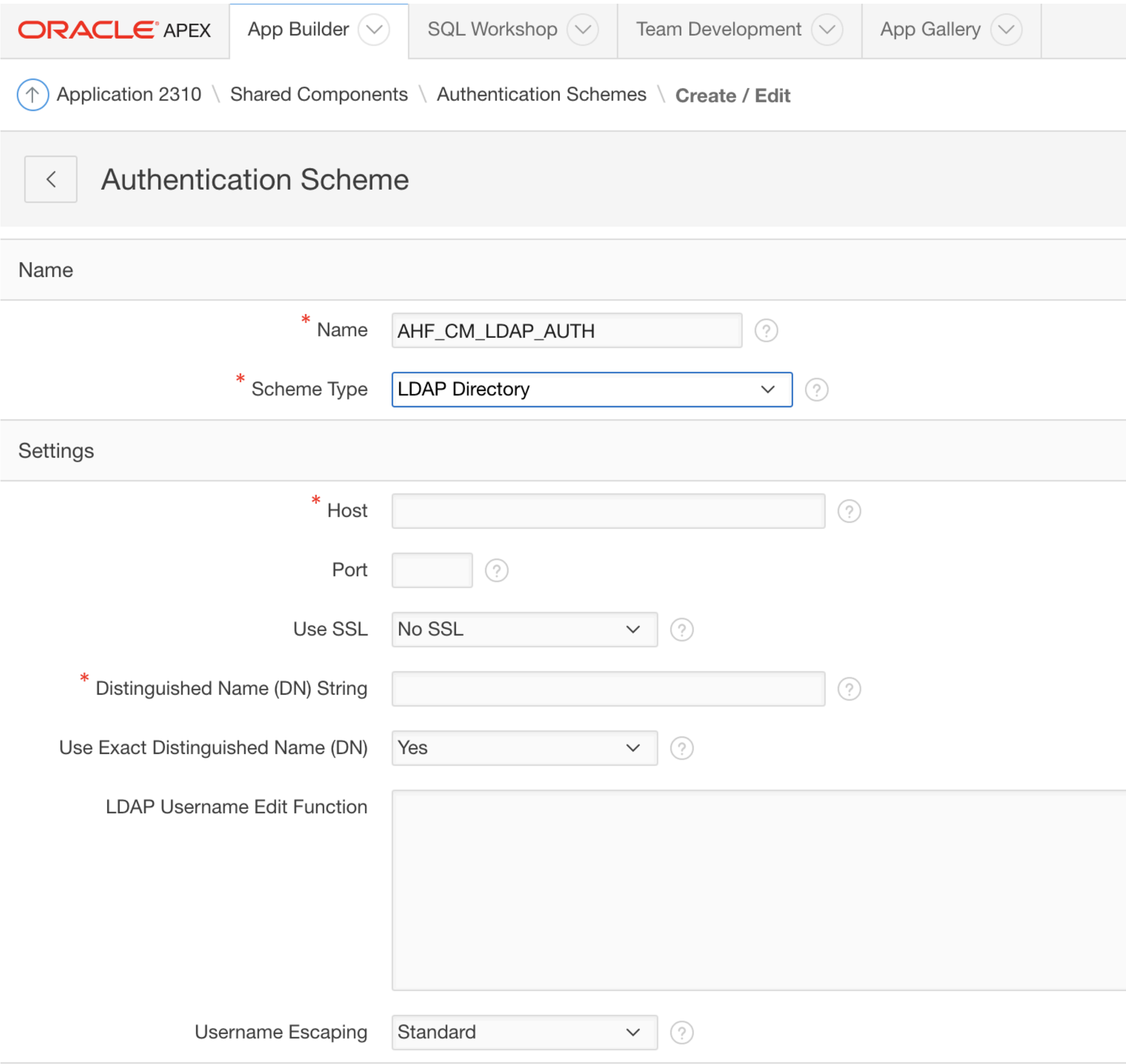
Port: 3131

Use SSL: SSL

Distinguished Name (DN) String: `cn=%LDAP_USER%`

Use Exact Distinguished Name: Yes

Figure 3-100   Additional LDAP Settings



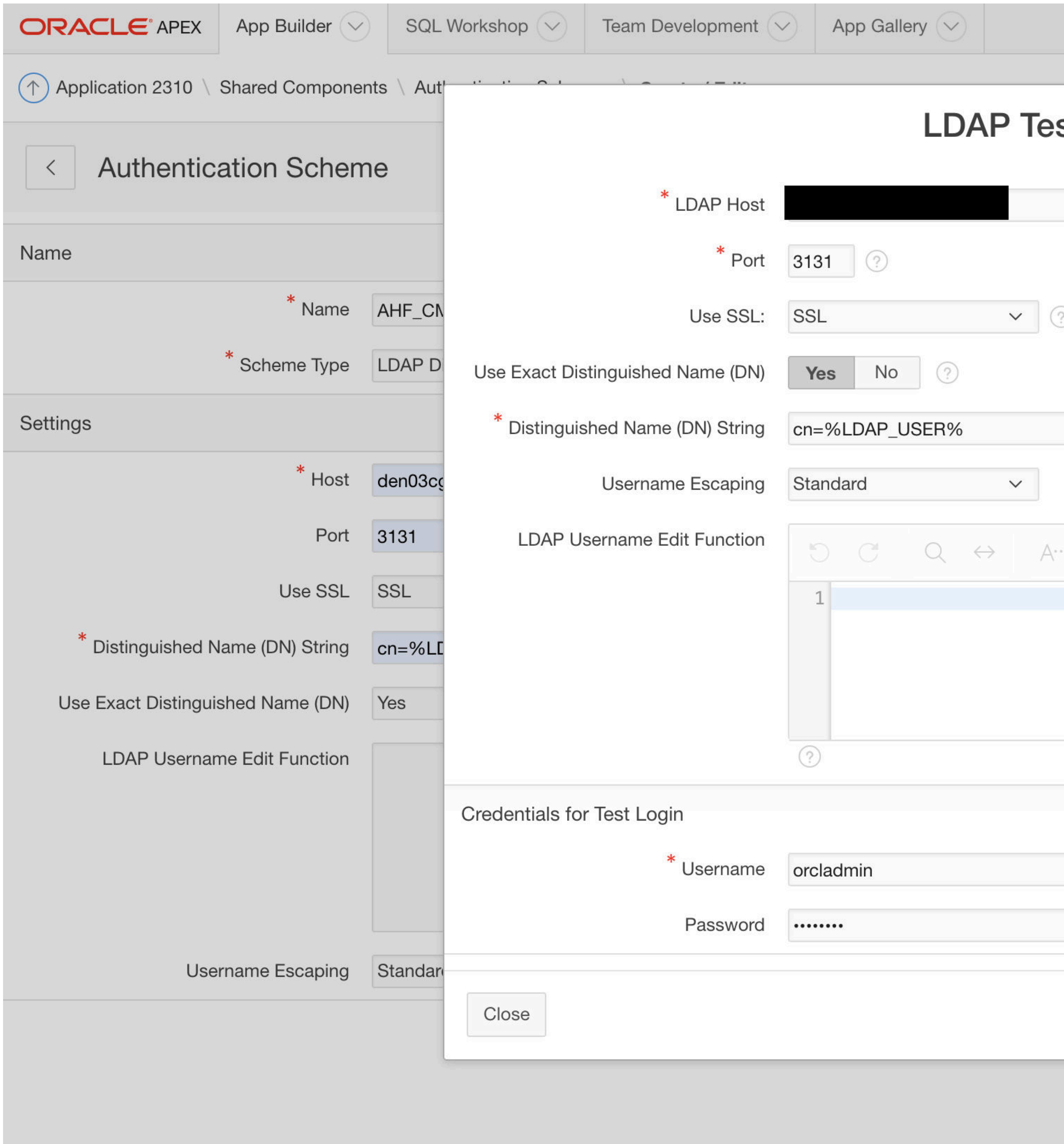
* Name	AHF_CM_LDAP_AUTH
* Scheme Type	LDAP Directory
* Host	
Port	
Use SSL	No SSL
* Distinguished Name (DN) String	
Use Exact Distinguished Name (DN)	Yes
LDAP Username Edit Function	
Username Escaping	Standard

9. Click **Test LDAP Login**.

   This will populate most of the data you entered previously.

10. Under **Credentials for Test Login**, enter the LDAP username and password that you would like to test.

Figure 3-101 LDAP Test



* Name: AHF_CM
* Scheme Type: LDAP D
* Host: den03cg
Port: 3131
Use SSL: SSL
* Distinguished Name (DN) String: cn=%LD
Use Exact Distinguished Name (DN): Yes
LDAP Username Edit Function
Username Escaping: Standar

LDAP Tes

* LDAP Host: [redacted]
* Port: 3131
Use SSL: SSL
Use Exact Distinguished Name (DN): Yes No
* Distinguished Name (DN) String: cn=%LDAP_USER%
Username Escaping: Standard
LDAP Username Edit Function

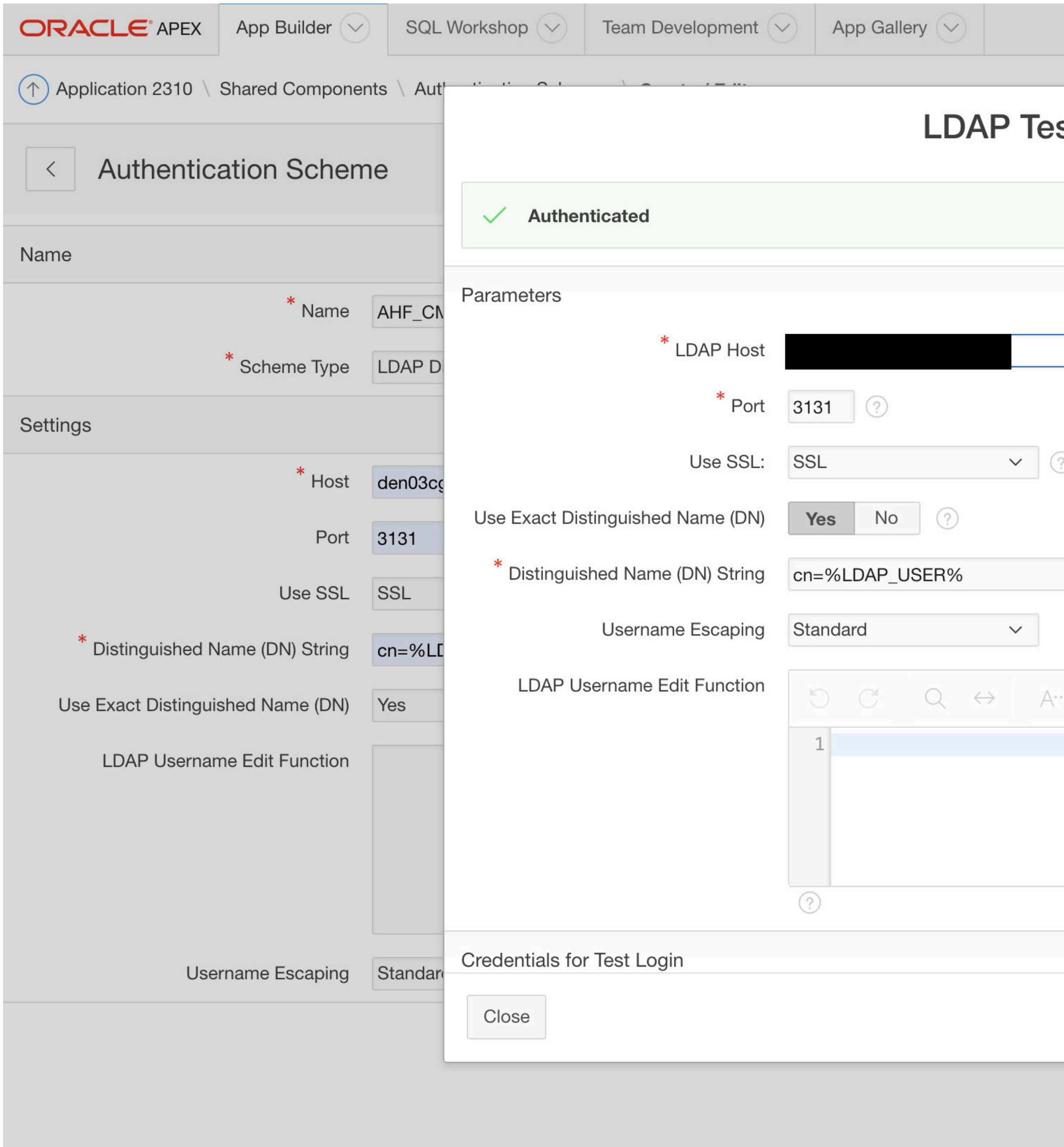
Credentials for Test Login

* Username: orcladmin
Password: ••••••••

11. Click **Test Login**.

    If the details we provided are correct and the OID (LDAP) is configured correctly. then you will notice and "Authenticated" Message:

Figure 3-102 LDAP Test



Authentication Scheme

Name

* Name: AHF_CM

* Scheme Type: LDAP D

Settings

* Host: den03cg

Port: 3131

Use SSL: SSL

* Distinguished Name (DN) String: cn=%LD

Use Exact Distinguished Name (DN): Yes

LDAP Username Edit Function

Username Escaping: Standar

LDAP Tes

✓ Authenticated

Parameters

* LDAP Host: [redacted]

* Port: 3131

Use SSL: SSL

Use Exact Distinguished Name (DN): Yes No

* Distinguished Name (DN) String: cn=%LDAP_USER%

Username Escaping: Standard

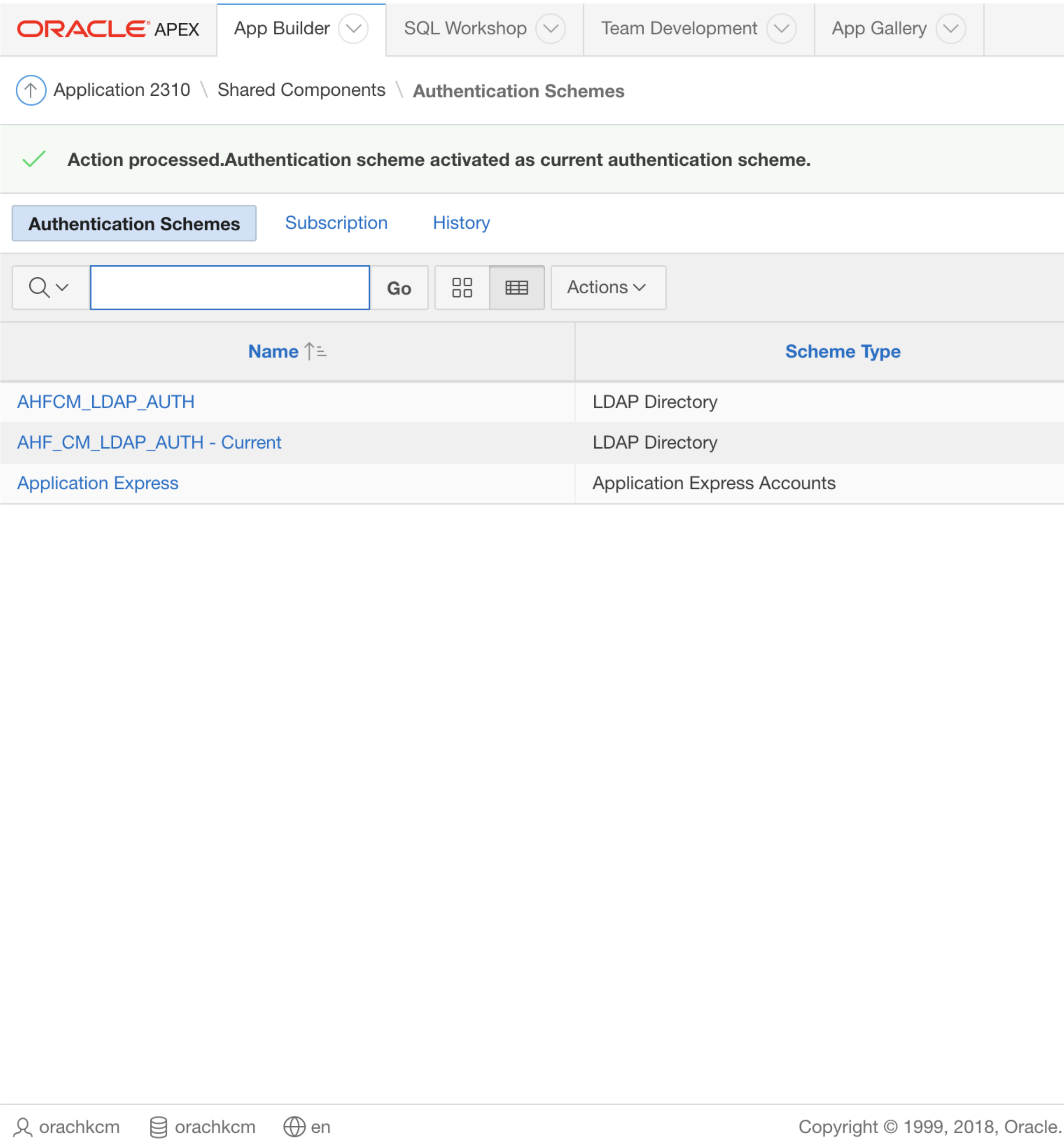
LDAP Username Edit Function

Credentials for Test Login

> **Note:**
>
> If the authentication fails, validate the LDAP details using `ldapbind` command from an OID client home and then click **Apply Changes** and click **Create Authentication Scheme**.

At this time, you should see the following screen.

Figure 3-103 Authentication Scheme Activated



ORACLE APEX
App Builder
SQL Workshop
Team Development
App Gallery
Application 2310 \ Shared Components \ Authentication Schemes

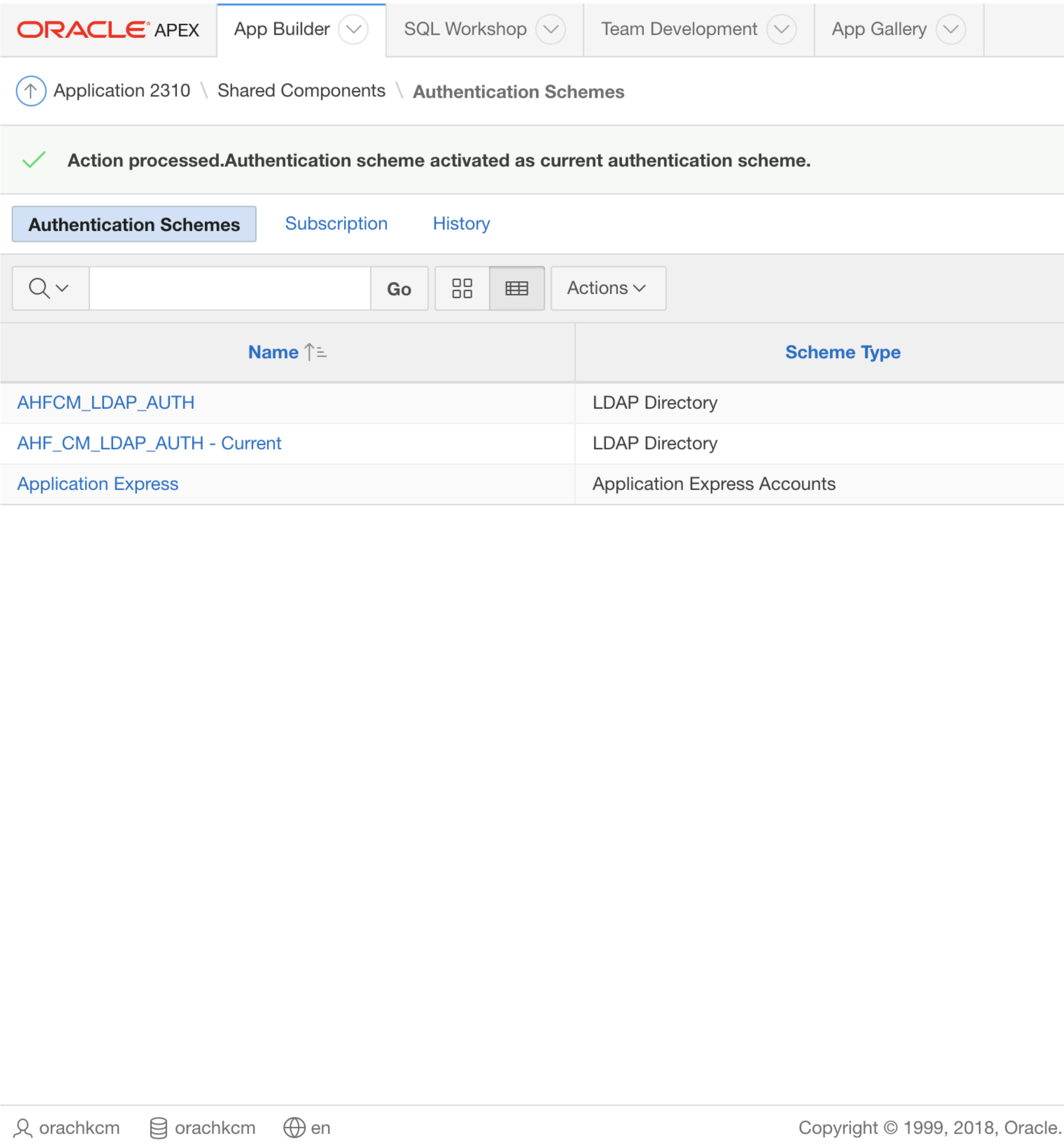
✓ Action processed.Authentication scheme activated as current authentication scheme.

Name	Scheme Type
AHFCM_LDAP_AUTH	LDAP Directory
AHF_CM_LDAP_AUTH - Current	LDAP Directory
Application Express	Application Express Accounts

Note that the most recent LDAP Directory scheme will be shown as **Current**.

12. Now, sign out as the ADMIN for `ORACHKCM` workspace.

Figure 3-104   Workspace Sign Out


ORACLE APEX
App Builder
SQL Workshop
Team Development
App Gallery
Application 2310 \ Shared Components \ Authentication Schemes

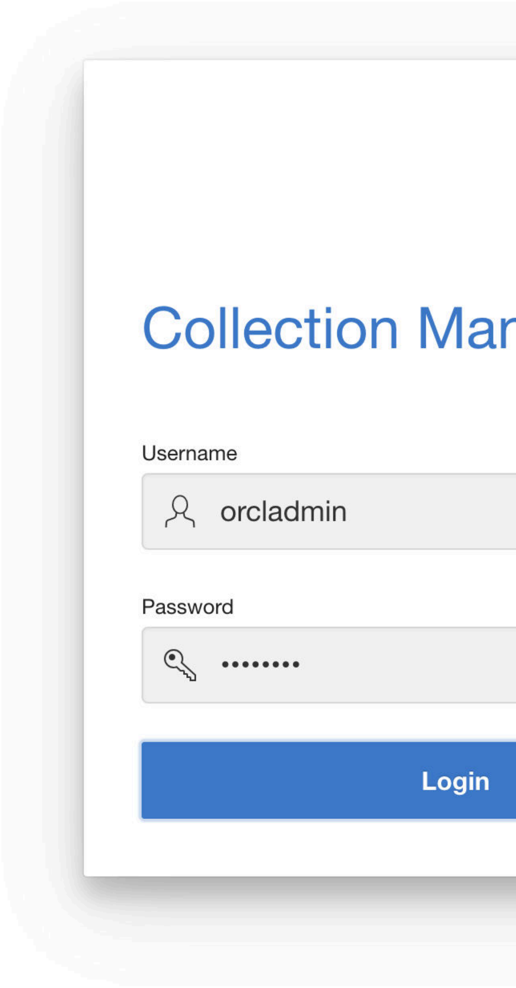
✓ Action processed.Authentication scheme activated as current authentication scheme.

Name	Scheme Type
AHFCM_LDAP_AUTH	LDAP Directory
AHF_CM_LDAP_AUTH - Current	LDAP Directory
Application Express	Application Express Accounts

13. Log in to Collection Manager Application directly using the LDAP user.

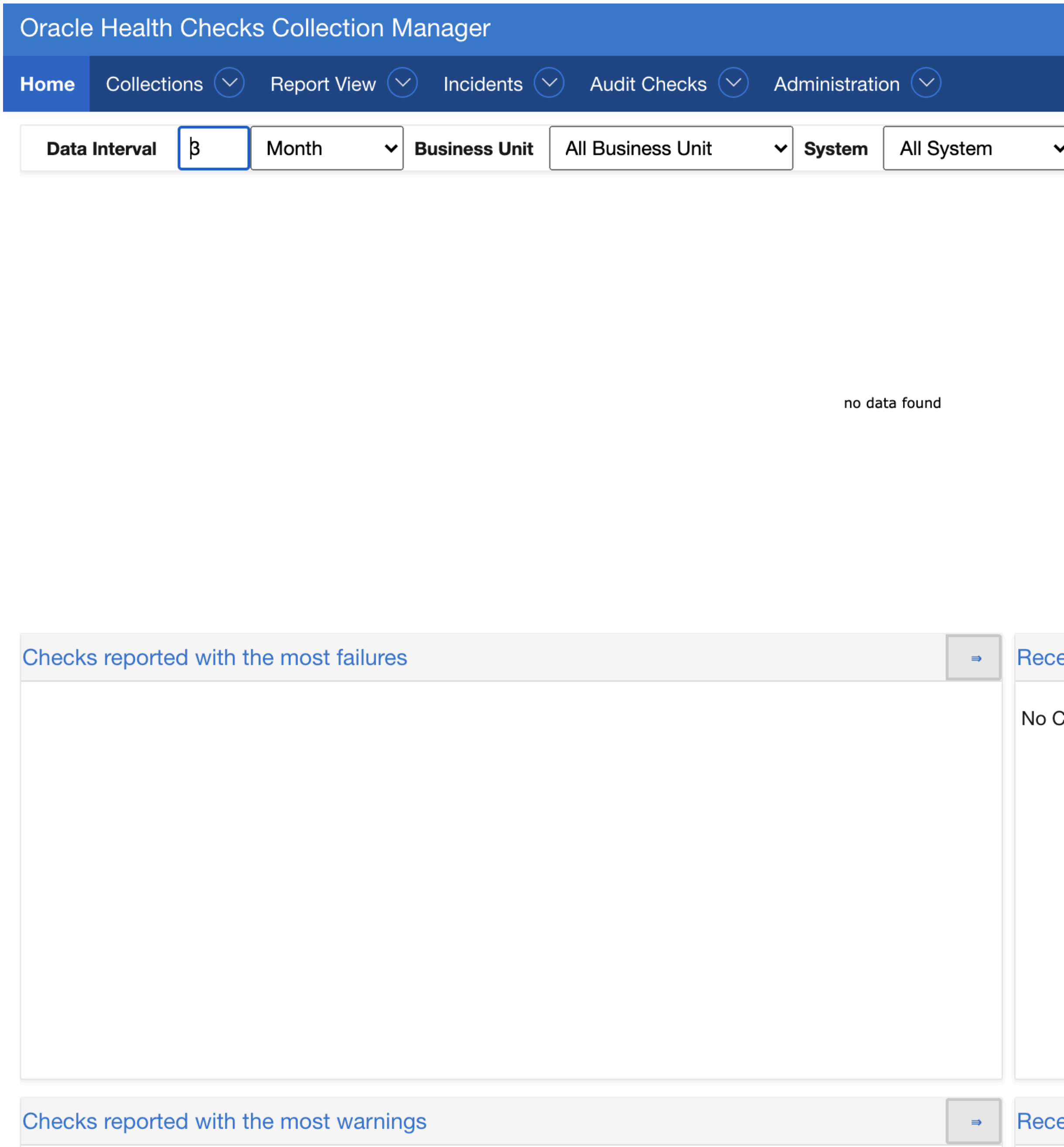
    For example: `orcladmin/********`

Figure 3-105   Log in to Collection Manager



A successful login will authenticate and bring you into the collection manager application.

Figure 3-106 Logging successfully in to Collection Manager



Data Interval 3 Month Business Unit All Business Unit System All System

no data found

Checks reported with the most failures

Rece

No C

Checks reported with the most warnings

Rece

4 Collect Diagnostic Data

- Managing and Configuring Oracle Trace File Analyzer
  This section helps you manage Oracle Trace File Analyzer daemon, diagnostic collections, and the collection repository.
- Using Automatic Diagnostic Collections
  Oracle Trace File Analyzer monitors your logs for significant problems, such as internal errors like `ORA-00600`, or node evictions.
- Using On-Demand Diagnostic Collections
  Run Oracle Trace File Analyzer on demand using `tfactl` command-line tool.
- Proactively Detecting and Diagnosing Performance Issues for Oracle RAC
  Oracle Cluster Health Advisor provides system and database administrators with early warning of pending performance issues, and root causes and corrective actions for Oracle RAC databases and cluster nodes. Use Oracle Cluster Health Advisor to increase availability and performance management.
- Collecting Operating System Resources Metrics
  CHM is a high-performance, lightweight daemon that collects, analyzes, aggregates, and stores a large set of operating system metrics to help you diagnose and troubleshoot system issues.
- Monitoring System Metrics for Cluster Nodes
  This chapter explains the methods to monitor Oracle Clusterware.
- Managing Oracle Database and Oracle Grid Infrastructure Logs
  This section enables you to manage Oracle Database and Oracle Grid Infrastructure diagnostic data and disk usage snapshots.

4.1 Managing and Configuring Oracle Trace File Analyzer

This section helps you manage Oracle Trace File Analyzer daemon, diagnostic collections, and the collection repository.

- Querying Oracle Trace File Analyzer Status and Configuration
  Use the `print` command to query the status or configuration.
- Managing the Oracle Trace File Analyzer Daemon
  Oracle Trace File Analyzer runs from `init` on UNIX systems or `init/upstart/systemd` on Linux, or Microsoft Windows uses a Windows Service so that Oracle Trace File Analyzer starts automatically whenever a node starts.
- Managing the Repository
  Oracle Trace File Analyzer stores all diagnostic collections in the repository.
- Managing Collections
  Manage directories configured in Oracle Trace File Analyzer and diagnostic collections.
- Configuring the Host
  You must have `root` or `sudo` access to `tfactl` to add hosts to Oracle Trace File Analyzer configuration.

- Configuring the Ports
  The Oracle Trace File Analyzer daemons in a cluster communicate securely over ports 5000 to 5005.
- Configuring SSL and SSL Certificates
  View and restrict SSL/TLS protocols. Configure Oracle Trace File Analyzer to use self-signed or CA-signed certificates.
- Configuring Email Notification Details
  Configure Oracle Trace File Analyzer to send an email to the registered email address after an automatic collection completes.
- Managing the Index
  Oracle Trace File Analyzer uses multiple indexes to store diagnostic data.

4.1.1 Querying Oracle Trace File Analyzer Status and Configuration

Use the `print` command to query the status or configuration.

Table 4-1 Configuration Listing and Descriptions

Configuration Listing	Default Value	Description
Automatic diagnostic collection	ON	Triggers a collection if a significant problem occurs. Possible values: • ON • OFF
Trimming of files during diagnostic collection	ON	Trims the log files to only entries within the time range of the collection. Possible values: • ON • OFF
Repository maximum size in MB	Smaller of either 10GB or 50% of free space in the file system.	The largest size the repository can be.
Trace Level	INFO	Increases the level of verbosity. Possible values: • FATAL • ERROR • WARNING • INFO • DEBUG • TRACE A value of INFO results in the least amount of trace. A value of TRACE results in the most amount of trace. Oracle recommends changing the trace level value only at the request of Oracle Support.

Table 4-1 (Cont.) Configuration Listing and Descriptions

Configuration Listing	Default Value	Description
Automatic Purging	ON	Purges collections when: Free space in the repository falls below 1 GB. Or Before closing the repository. Purging removes collections from largest size through to smallest. Purging continues until the repository has enough space to open.
Minimum Age of Collections to Purge (Hours)	12	The least number of hours to keep a collection, after which it is eligible for purging.
Minimum Space free to enable Alert Log Scan (MB)	500	Suspends log scanning if free space in the `tfa_home` falls below this value.

Related Topics

- tfactl print
  Use the `tfactl print` command to print information from the Berkeley DB (BDB).

4.1.2 Managing the Oracle Trace File Analyzer Daemon

Oracle Trace File Analyzer runs from `init` on UNIX systems or `init/upstart/systemd` on Linux, or Microsoft Windows uses a Windows Service so that Oracle Trace File Analyzer starts automatically whenever a node starts.

To manage Oracle Trace File Analyzer daemon:

The `init` control file `/etc/init.d/init.tfa` is platform dependant.

1. To start or stop Oracle Trace File Analyzer manually:
   - `tfactl start`: Starts the Oracle Trace File Analyzer daemon
   - `tfactl stop`: Stops the Oracle Trace File Analyzer daemon

   If the Oracle Trace File Analyzer daemon fails, then the operating system restarts the daemon automatically.
2. To enable or disable automatic restarting of the Oracle Trace File Analyzer daemon:
   - `tfactl disable`: Disables automatic restarting of the Oracle Trace File Analyzer daemon.
   - `tfactl enable`: Enables automatic restarting of the Oracle Trace File Analyzer daemon.

4.1.3 Managing the Repository

Oracle Trace File Analyzer stores all diagnostic collections in the repository.

The repository size is the maximum space Oracle Trace File Analyzer is able to use on disk to store collections.

- Purging the Repository Automatically
- Purging the Repository Manually

4.1.3.1 Purging the Repository Automatically

Oracle Trace File Analyzer closes the repository, if:

- Free space in `TFA_HOME` is less than 100 MB, also stops indexing
- Free space in `ORACLE_BASE` is less than 100 MB, also stops indexing
- Free space in the repository is less than 1 GB
- Current size of the repository is greater than the repository max size (`reposizeMB`)

The Oracle Trace File Analyzer daemon monitors and automatically purges the repository when the free space falls below 1 GB or before closing the repository. Purging removes collections from largest size through to smallest until the repository has enough space to open.

Oracle Trace File Analyzer automatically purges only the collections that are older than `minagetopurge`. By default, `minagetopurge` is 12 hours.

To purge the repository automatically

1. To change the minimum age to purge:

   ```
   set minagetopurge=number of hours
   ```

   For example:

   ```
   tfactl set minagetopurge=48
   ```

   Purging the repository automatically is enabled by default.
2. To disable or enable automatic purging:

   ```
   set autopurge=ON|OFF
   ```

   For example:

   ```
   tfactl set autopurge=ON
   ```

3. To change the location of the repository:

   ```
   set repositorydir=dir
   ```

   For example:

> **Note:**
>
> You must name your new directory as `repository`.

```
tfactl set repositorydir=/opt/repository
```

4. To change the size of the repository:

   ```
   set reposizeMB
   ```

   For example:

   ```
   tfactl set reposizeMB=20480
   ```

Related Topics

- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.

4.1.3.2 Purging the Repository Manually

To purge the repository manually:

1. To view the status of the Oracle Trace File Analyzer repository:

   ```
   tfactl print repository
   ```

2. To view statistics about collections:

   ```
   tfactl print collections
   ```

3. To manually purge collections that are older than a specific time:

   ```
   tfactl purge -older number[h|d] [-force]
   ```

Related Topics

- tfactl purge
  Use the `tfactl purge` command to delete collections and log files from AHF components from the local node.
- tfactl print
  Use the `tfactl print` command to print information from the Berkeley DB (BDB).

4.1.4 Managing Collections

Manage directories configured in Oracle Trace File Analyzer and diagnostic collections.

- Including Directories
  Add directories to the Oracle Trace File Analyzer configuration to include the directories in diagnostic collections.
- Managing the Size of Collections
  Use the Oracle Trace File Analyzer configuration options `trimfiles`, `maxcorefilesize`, `maxcorecollectionsize`, and `diagcollect -cores` to include core files.
- Temporarily Restrict Automatic Diagnostic Collections for Specific Events
  Use the `tfactl blackout` command to suppress automatic diagnostic collections.

4.1.4.1 Including Directories

Add directories to the Oracle Trace File Analyzer configuration to include the directories in diagnostic collections.

Oracle Trace File Analyzer then stores diagnostic collection metadata about the:

- Directory
- Subdirectories
- Files in the directory and all sub directories

All Oracle Trace File Analyzer users can add directories they have read access to.

To manage directories:

1. To view the current directories configured in Oracle Trace File Analyzer

   ```
   tfactl print directories [ -node all | local | n1,n2,... ]
   [ -comp component_name1,component_name2,.. ]
   [ -policy  exclusions | noexclusions ]
   [ -permission public | private ]
   ```

2. To add directories:

   ```
   tfactl directory add dir
   [ -public ]
   [ -exclusions | -noexclusions | -collectall ]
   [ -node all | n1,n2,... ]
   ```

3. To remove a directory from being collected:

   ```
   tfactl directory remove dir [ -node all | n1,n2,... ]
   ```

Related Topics

- tfactl directory
  Use the `tfactl directory` command to add a directory to, or remove a directory from the list of directories to analyze their trace or log files.
- tfactl print
  Use the `tfactl print` command to print information from the Berkeley DB (BDB).

4.1.4.2 Managing the Size of Collections

Use the Oracle Trace File Analyzer configuration options `trimfiles`, `maxcorefilesize`, `maxcorecollectionsize`, and `diagcollect -cores` to include core files.

To manage the size of collections:

1. To trim files during diagnostic collection:

   ```
   tfactl set trimfiles=ON|OFF
   ```

   - When set to ON (default), Oracle Trace File Analyzer trims files to include data around the time of the event
   - When set to OFF, any file that was written to at the time of the event is collected in its entirety

2. To set the maximum size of core file to *n* MB (default 50 MB):

   ```
   tfactl set maxcorefilesize=n
   ```

   Oracle Trace File Analyzer skips core files that are greater than `maxcorefilesize`.

3. To set the maximum collection size of core files to *n* MB (default 500 MB):

   ```
   tfactl set maxcorecollectionsize=n
   ```

   Oracle Trace File Analyzer skips collecting core files after `maxcorecollectionsize` is reached.

4. To collect core files with diagnostic collections:

   ```
   tfactl diagcollect -cores
   ```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.
- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.

4.1.4.3 Temporarily Restrict Automatic Diagnostic Collections for Specific Events

Use the `tfactl blackout` command to suppress automatic diagnostic collections.

If you set blackout for a target, then Oracle Trace File Analyzer stops automatic diagnostic collections if it finds events in the alert logs for that target while scanning.

You can also restrict automatic diagnostic collection at a granular level, for example, only for `ORA-00600` or even only `ORA-00600` with specific arguments.

```
tfactl blackout add -targettype database -target mydb -event "ORA-00600"
```

Event "ORA-00600" is blacked out until Wed Feb 20 00:20:34 PST 2019 on targettype : database, target : mydb

You can also blackout a resource that does not exist yet. For example, if you want to create a database and you do not want to care about the status until the provisioning is completed, then do as follows:

1. Blackout the database you are about to create
2. Create the database
3. Remove the blackout

Related Topics

- tfactl blackout
  Use the `tfactl blackout` command to suppress diagnostic collections at a more granular level. By default, blackout will be in effect for 24 hours.

4.1.5 Configuring the Host

You must have `root` or `sudo` access to `tfactl` to add hosts to Oracle Trace File Analyzer configuration.

To add, remove, and replace SSL certificates:

1. To view the list of current hosts in the Oracle Trace File Analyzer configuration:

   ```
   tfactl print hosts
   ```

2. To add a host to the Oracle Trace File Analyzer configuration for the first time:
   a. If necessary, install and start Oracle Trace File Analyzer on the new host.
   b. From the existing host, synchronize authentication certificates for all hosts by running:

      ```
      tfactl syncnodes
      ```

      If needed, then Oracle Trace File Analyzer displays the current node list it is aware of and prompts you to update this node list.
   c. Select **Y**, and then enter the name of the new host.

      Oracle Trace File Analyzer contacts Oracle Trace File Analyzer on the new host to synchronize certificates and add each other to their respective hosts lists.
3. To remove a host:

   ```
   tfactl host remove host
   ```

4. To add a host and the certificates that are already synchronized:

   ```
   tfactl host add host
   ```

   Oracle Trace File Analyzer generates self-signed SSL certificates during installation. Replace those certificates with one of the following:

- Personal self-signed certificate
- CA-signed certificate

4.1.6 Configuring the Ports

The Oracle Trace File Analyzer daemons in a cluster communicate securely over ports 5000 to 5005.

If the port range is not available on your system, then replace it with the ports available on your system.

To change the ports:

1. To set the primary port use the `tfactl set port` command:

   ```
   tfactl set port=port_1
   ```

   Or, specify a comma-delimited list of sequentially numbered ports to use. You can specify a maximum of five ports.

   ```
   tfactl set port=port_1,port_2,port_3,port_4,port_5
   ```

2. Restart Oracle Trace File Analyzer on all nodes:

   ```
   tfactl restart
   ```

4.1.7 Configuring SSL and SSL Certificates

View and restrict SSL/TLS protocols. Configure Oracle Trace File Analyzer to use self-signed or CA-signed certificates.

- Configuring SSL/TLS Protocols
  The Oracle Trace File Analyzer daemons in a cluster communicate securely using the SSL/TLS protocols.
- Configuring Self-Signed Certificates
  Use `Java keytool` to replace self-signed SSL certificates with personal self-signed certificates.
- Configuring CA-Signed Certificates
  Use `Java keytool` and `openssl` to replace self-signed SSL certificates with the Certificate Authority (CA) signed certificates.
- Configuring SSL Cipher Suite
  The cipher suite is a set of cryptographic algorithms used by the TLS/SSL protocols to create keys and encrypt data.

4.1.7.1 Configuring SSL/TLS Protocols

The Oracle Trace File Analyzer daemons in a cluster communicate securely using the SSL/TLS protocols.

The SSL protocols available for use by Oracle Trace File Analyzer are:

- `TLSv1.2`

- `TLCv1.1`
- `TLSv1`

Oracle Trace File Analyzer always restricts use of older the protocols `SSLv3` and `SSLv2Hello`.

To view and restrict protocols:

1. To view the available and restricted protocols:

   ```
   tfactl print protocols
   ```

   For example:

   ```
   $ tfactl print protocols
   .---------------------------------------.
   |                 node1                 |
   +---------------------------------------+
   | Protocols                             |
   +---------------------------------------+
   | Available : [TLSv1, TLSv1.2, TLSv1.1] |
   | Restricted : [SSLv3, SSLv2Hello]      |
   '---------------------------------------'
   ```

2. To restrict the use of certain protocols:

   ```
   tfactl restrictprotocol [-force] protocol
   ```

   For example:

   ```
   tfactl restrictprotocol TLSv1
   ```

4.1.7.2 Configuring Self-Signed Certificates

Use `Java keytool` to replace self-signed SSL certificates with personal self-signed certificates.

> **Note:**
>
> The key size of default self-signed certificates shipped by TFA is 2048 bits.

To configure Oracle Trace File Analyzer to use self-signed certificates:

1. Create a private key and keystore file containing the self-signed certificate for the server:

   ```
   keytool -genkey -alias server_full -keyalg RSA -keysize 2048 -
   validity 18263 -keystore myserver.jks
   ```

2. Create a private key and keystore file containing the private key and self signed-certificate for the client:

   ```
   keytool -genkey -alias client_full -keyalg RSA -keysize 2048 -validity
   18263 -keystore myclient.jks
   ```

3. Export the server public key certificate from the server keystore:

   ```
   keytool -export -alias server_full -file myserver_pub.crt -keystore
   myserver.jks -storepass password
   ```

4. Export the client public key certificate from the client keystore:

   ```
   keytool -export -alias client_full -file myclient_pub.crt -keystore
   myclient.jks -storepass password
   ```

5. Import the server public key certificate into the client keystore:

   ```
   keytool -import -alias server_pub -file myserver_pub.crt -keystore
   myclient.jks -storepass password
   ```

6. Import the client public key certificate into the server keystore:

   ```
   keytool -import -alias client_pub -file myclient_pub.crt  -keystore
   myserver.jks -storepass password
   ```

7. Restrict the permissions on the keystores to `root read-only`.

   ```
   chmod 400 myclient.jks myserver.jks
   ```

8. Configure Oracle Trace File Analyzer to use the new certificates:

   ```
   tfactl set sslconfig
   ```

   ```
   tfactl set sslconfig
   Please Enter server certificate path : /u01/oracle.ahf/data/host/tfa/myserver.jks
   Please Enter Password for server keystore keypass :
   Please Confirm Password for server keystore keypass :
   Please Enter Password for server keystore storepass :
   Please Confirm Password for server keystore storepass :
   Please Enter client certificate path? : /u01/oracle.ahf/data/host/tfa/myclient.jks
   Please Enter Password for client keystore keypass :
   Please Confirm Password for client keystore keypass :
   Please Enter Password for client keystore storepass :
   Please Confirm Password for client keystore storepass :
   SSL certificate details successfully set
   The certificates are restricted to root read only
   ```

9. Restart the Oracle Trace File Analyzer process to start using new certificates:

   ```
   tfactl restart
   ```

4.1.7.3 Configuring CA-Signed Certificates

Use `Java keytool` and `openssl` to replace self-signed SSL certificates with the Certificate Authority (CA) signed certificates.

To configure Oracle Trace File Analyzer to use CA-signed certificates:

1. Create a private key for the server request:

   ```
   openssl genrsa -aes256 -out myserver.key 2048
   ```

2. Create a private key for the client request:

   ```
   openssl genrsa -aes256 -out myclient.key 2048
   ```

3. Create a Certificate Signing Request (CSR) for the server:

   ```
   openssl req -key myserver.key -new -sha256 -out myserver.csr
   ```

4. Create a Certificate Signing Request (CSR) for the client:

   ```
   openssl req -key myclient.key -new -sha256 -out myclient.csr
   ```

5. Send the resulting CSR for the client and the server to the relevant signing authority.

   The signing authority sends back the signed certificates:

   - *`myserver`*`.cert`
   - *`myclient`*`.cert`
   - CA root certificate
   - Intermediate certificate

6. Convert the certificates to JKS format for the server and the client:

   ```
   openssl pkcs12 -export -out serverCert.pkcs12 -in myserver.cert -
   inkey myserver.key


   keytool -v -importkeystore -srckeystore serverCert.pkcs12 -
   srcstoretype PKCS12 -destkeystore myserver.jks -deststoretype JKS


   openssl pkcs12 -export -out clientCert.pkcs12 -in myclient.cert -
   inkey myclient.key


   keytool -v -importkeystore -srckeystore clientCert.pkcs12 -
   srcstoretype PKCS12 -destkeystore myclient.jks -deststoretype JKS
   ```

7. Import the server public key into to the client `jks` file:

   ```
   keytool -import -v -alias server-ca -file myserver.cert -keystore
   myclient.jks
   ```

8. Import the client public key to the server `jks` file:

   ```
   keytool -import -v -alias client-ca -file myclient.cert -keystore
   myserver.jks
   ```

9. Import CA root certificate from the signing authority into the Oracle Trace File Analyzer server certificate:

   ```
   keytool -importcert -trustcacerts -alias root -file caroot.cert -keystore
   myserver.jks
   ```

10. Import Intermediate certificate into the Oracle Trace File Analyzer server certificate:

    ```
    keytool -importcert -trustcacerts -alias inter -file intermediate.cert -
    keystore myserver.jks
    ```

11. Import Intermediate certificate into the Oracle Trace File Analyzer client certificate:

    ```
    keytool -importcert -trustcacerts -alias inter -file intermediate.cert -
    keystore myclient.jks
    ```

12. Validate aliases.

    List contents of server keystore:

    ```
    keytool -list -keystore myserver.jks -storepass <password>
    ```

    Output should contain the following aliases:

    ```
    1, client-ca, root, inter
    ```

    List contents of client keystore:

    ```
    keytool -list -keystore myclient.jks -storepass <password>
    ```

    Output should contain the following aliases:

    ```
    1, server-ca, inter
    ```

> **Note:**
>
> - If alias 1 (`PrivateKeyEntry`) is missing in `myserver.jks`, then run below command to update alias.
>   Change alias name for `PrivateKeyEntry` in `myserver.jks`:
>
>   ```
>   keytool -changealias -alias "<alias of PrivateKeyEntry>"
>   -destalias "1" -keystore myserver.jks -storepass
>   <password>
>   ```
>
> - If alias 1 (`PrivateKeyEntry`) is missing in `myclient.jks`, then run below command to update alias.
>   Change alias name for `PrivateKeyEntry` in `myclient.jks`:
>
>   ```
>   keytool -changealias -alias "<alias of PrivateKeyEntry>"
>   -destalias "1" -keystore myclient.jks -storepass
>   <password>
>   ```

13. Restrict the permissions on the keystores to `root read-only`:

    ```
    chmod 400 myclient.jks myserver.jks
    ```

14. Configure Oracle Trace File Analyzer to use the new certificates:

    ```
    tfactl set sslconfig
    ```

    ```
    tfactl set sslconfig
    Please Enter server certificate path : /u01/oracle.ahf/data/host/tfa/
    myserver.jks
    Please Enter Password for server keystore keypass :
    Please Confirm Password for server keystore keypass :
    Please Enter Password for server keystore storepass :
    Please Confirm Password for server keystore storepass :
    Please Enter client certificate path? : /u01/oracle.ahf/data/host/tfa/
    myclient.jks
    Please Enter Password for client keystore keypass :
    Please Confirm Password for client keystore keypass :
    Please Enter Password for client keystore storepass :
    Please Confirm Password for client keystore storepass :
    SSL certificate details successfully set
    The certificates are restricted to root read only
    ```

15. Restart the Oracle Trace File Analyzer process to start using the new certificates.

    ```
    tfactl stop
    tfactl start
    ```

4.1.7.4 Configuring SSL Cipher Suite

The cipher suite is a set of cryptographic algorithms used by the TLS/SSL protocols to create keys and encrypt data.

Oracle Trace File Analyzer supports any of the cipher suites used by JRE 1.8.

The default cipher suite used is `TLS_RSA_WITH_AES_128_CBC_SHA256`.

- You can change the cipher suite with the command:

  ```
  tfactl set ciphersuite=cipher_suite
  ```

  For example:

  ```
  tfactl set ciphersuite=TLS_RSA_WITH_AES_128_GCM_SHA256
  ```

  For a list of JRE cipher suites, see:
  https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider

4.1.8 Configuring Email Notification Details

Configure Oracle Trace File Analyzer to send an email to the registered email address after an automatic collection completes.

To send emails, configure the system on which Oracle Trace Analyzer is running. You must configure notification with a user email address to enable it to work.

To configure email notification details:

1. To set the notification email to use for a specific `ORACLE_HOME`, include the operating system owner in the command:

   ```
   tfactl set notificationAddress=os_user:email
   ```

   For example:

   ```
   tfactl set notificationAddress=oracle:some.body@example.com
   ```

2. To set the notification email to use for any `ORACLE_HOME`:

   ```
   tfactl set notificationAddress=email
   ```

   For example:

   ```
   tfactl set notificationAddress=another.body@example.com
   ```

3. Configure the SMTP server using `tfactl set smtp`.

   Set the SMTP parameters when prompted.

Table 4-2 tfactl diagnosetfa Command Parameters

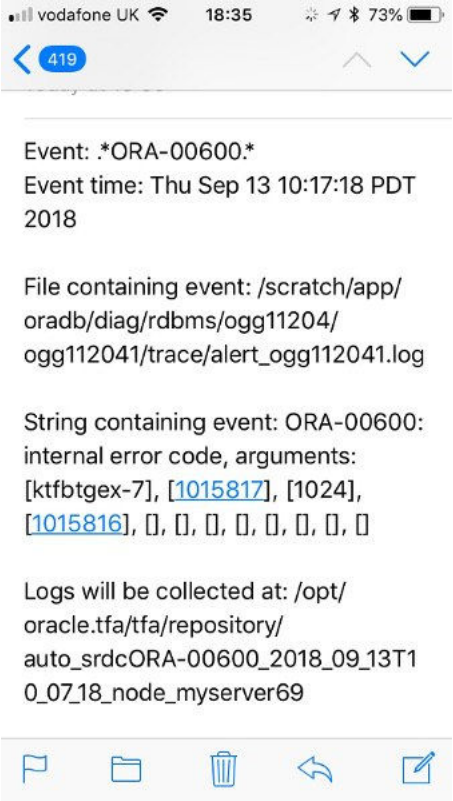
Parameter	Description
`smtp.host`	Specify the SMTP server host name.
`smtp.port`	Specify the SMTP server port.
`smtp.user`	Specify the SMTP user.
`smtp.password`	Specify password for the SMTP user.
`smtp.auth`	Set the Authentication flag to true or false.
`smtp.ssl`	Set the SSL flag to true or false.
`smtp.from`	Specify the from mail ID.
`smtp.to`	Specify the comma-delimited list of recipient mail IDs.
`smtp.cc`	Specify the comma-delimited list of CC mail IDs.
`smtp.bcc`	Specify the comma-delimited list of BCC mail IDs.
`smtp.debug`	Set the Debug flag to true or false.

> **Note:**
>
> You can view current SMTP configuration details using `tfactl print smtp`.

4. Verify SMTP configuration by sending a test email using `tfactl sendmail` *`email_address`*.

   When Oracle Trace File Analyzer detects a significant error has occurred it will send an email notification as follows:

Figure 4-1 Email Notification



Event: .*ORA-00600.*
Event time: Thu Sep 13 10:17:18 PDT 2018

File containing event: /scratch/app/oradb/diag/rdbms/ogg11204/ogg112041/trace/alert_ogg112041.log

String containing event: ORA-00600: internal error code, arguments: [ktfbtgex-7], [1015817], [1024], [1015816], [], [], [], [], [], [], [], []

Logs will be collected at: /opt/oracle.tfa/tfa/repository/auto_srdcORA-00600_2018_09_13T10_07_18_node_myserver69

5. Do the following after receiving the notification email:
   a. To find the root cause, inspect the referenced collection details.
   b. If you can fix the issue, then resolve the underlying cause of the problem.
   c. If you do not know the root cause of the problem, then log an SR with Oracle Support, and upload the collection details.

4.1.9 Managing the Index

Oracle Trace File Analyzer uses multiple indexes to store diagnostic data.

The DBA tools and diagnostic collections can use either an index (default), or the shipped Berkeley DB (BDB).

Using the index results in lower CPU usage and faster average execution times for diagnostic collections and the running of DBA tools such as `ls`, `grep`, `tail`, `vi`, and so on. However, using the index requires more ongoing resource consumption than the Berkeley DB (BDB).

If you do not use the DBA tools and are prepared to wait longer for collections to complete, you can disabled this indexing by running:

```
tfactl set indexInventory=false
```

ISA telemetry data is stored in a Lucene index. Occasionally this index can get corrupted. If corruption is detected then by default the index will be dropped and recreated. This can result in the loss of some ISA telemetry data.

If you do not want to risk losing any ISA data you can change this behavior to restore, so the index is backed up and redo data is maintained.

1. (Default) To drop and recreate, use:

   ```
   tfactl set indexRecoveryMode=recreate
   ```

2. To backup, maintain redo data and restore the index, use:

   ```
   tfactl set indexRecoveryMode=restore
   ```

4.2 Using Automatic Diagnostic Collections

Oracle Trace File Analyzer monitors your logs for significant problems, such as internal errors like `ORA-00600`, or node evictions.

- Collecting Diagnostics Automatically
  This section explains automatic diagnostic collection concepts.
- Configuring Email Notification Details
  Configure Oracle Trace File Analyzer to send an email to the registered email address after an automatic collection completes.
- Collecting Problems Detected by Oracle Cluster Health Advisor
  Configure Oracle Cluster Health Advisor to automatically collect diagnostics for abnormal events, and send email notifications.
- Sanitizing Sensitive Information in Oracle Trace File Analyzer Collections
  After collecting copies of diagnostic data, Oracle Trace File Analyzer uses Adaptive Classification and Redaction (ACR) to sanitize sensitive data in the collections.
- Flood Control for Similar Issues
  Flood control mechanism helps you save resource through fewer repeat collections for similar issues.

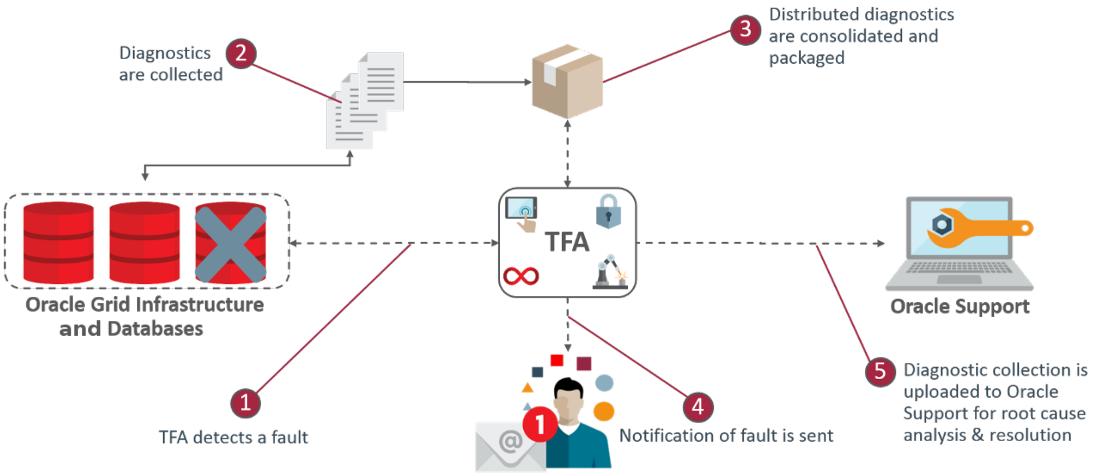
4.2.1 Collecting Diagnostics Automatically

This section explains automatic diagnostic collection concepts.

If Oracle Trace File Analyzer detects any problems, then it performs the following actions:

- Runs necessary diagnostics and collects all relevant log data at the time of a problem
- Trims log files to collect only what is necessary for diagnosis
- Collects and packages all trimmed diagnostics from all nodes in the cluster, consolidating everything on a single node
- Stores diagnostic collections in the Oracle Trace File Analyzer repository
- Sends you email notification of the problem and details of diagnostic collection that is ready for upload to Oracle Support

Figure 4-2   Automatic Diagnostic Collections


2 Diagnostics are collected
3 Distributed diagnostics are consolidated and packaged
TFA
Oracle Grid Infrastructure and Databases
Oracle Support
1 TFA detects a fault
4 Notification of fault is sent
5 Diagnostic collection is uploaded to Oracle Support for root cause analysis & resolution

Oracle Trace File Analyzer has a mechanism that prevents repeat errors from overwhelming your system with excessive, automatic collections.

Identifying an event triggers the start point for a collection and five minutes later Oracle Trace File Analyzer starts collecting diagnostic data. Starting five minutes later enables Oracle Trace File Analyzer to capture other relevant events in one operation. If events are still occurring after five minutes, then diagnostic collection continues to wait. Oracle Trace File Analyzer waits for 30 seconds with no events occurring up to an additional five minutes.

If events continue after 10 minutes, then Oracle Trace File Analyzer continues to perform diagnostic collection.

After completing the diagnostic collections, Oracle Trace File Analyzer sends email notifications that include the collection location to the designated recipients.

If your environment can make a connection to **oracle.com**, then you can use Oracle Trace File Analyzer to upload the collection to a Service Request.

```
$ tfactl set autodiagcollect=ON|OFF
```

Automatic collections are `ON` by default.

Table 4-3 Log Entries that Trigger Automatic collection

String Pattern	Log Monitored
ORA-297(01|02|03|08|09|10|40) ORA-00600 ORA-07445 ORA-04(69|([7-8][0-9]|9([0-3]|[5-8]))) ORA-32701 ORA-00494 ORA-04020 ORA-04021 ORA-01578 ORA-00700 System State dumped	Alert Log - Oracle Database Alert Log - Oracle Database/ Oracle ASM Alert Log - Oracle Database/ Oracle ASM Proxy Alert Log - Oracle Database
CRS-016(07|10|11|12)	Alert Log - Oracle Clusterware

Additionally, when Oracle Cluster Health Advisor detects a problem event, Oracle Trace File Analyzer automatically triggers the relevant diagnostic collection.

4.2.2 Configuring Email Notification Details

Configure Oracle Trace File Analyzer to send an email to the registered email address after an automatic collection completes.

To send emails, configure the system on which Oracle Trace Analyzer is running. You must configure notification with a user email address.

To configure email notification details:

1. To set the notification email for a specific `ORACLE_HOME`, include the operating system owner in the command:

   ```
   tfactl set notificationAddress=os_user:email
   ```

   For example:

   ```
   tfactl set notificationAddress=oracle:some.body@example.com
   ```

2. To set the notification email for any `ORACLE_HOME`:

   ```
   tfactl set notificationAddress=email
   ```

   For example:

   ```
   tfactl set notificationAddress=another.body@example.com
   ```

3. Configure the SMTP server using `tfactl set smtp`.

   Set the SMTP parameters when prompted.

Table 4-4 tfactl diagnosetfa Command Parameters

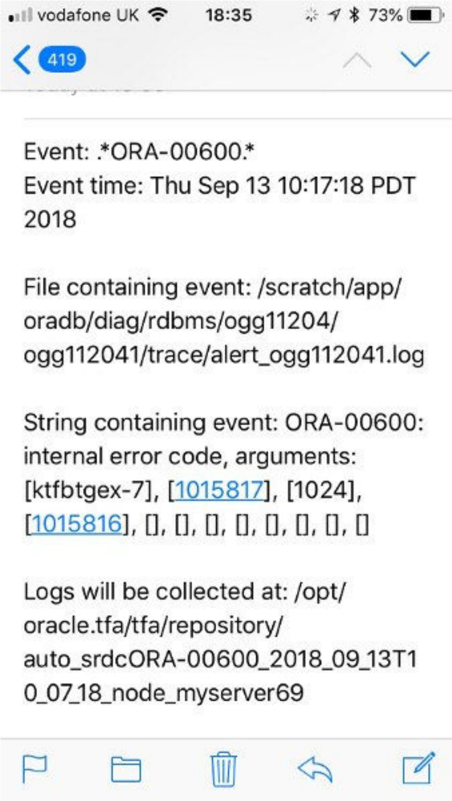
Parameter	Description
`smtp.host`	Specify the SMTP server host name.
`smtp.port`	Specify the SMTP server port.
`smtp.user`	Specify the SMTP user.
`smtp.password`	Specify password for the SMTP user.
`smtp.auth`	Set the Authentication flag to true or false.
`smtp.ssl`	Set the SSL flag to true or false.
`smtp.from`	Specify the from mail ID.
`smtp.to`	Specify the comma-delimited list of recipient mail IDs.
`smtp.cc`	Specify the comma-delimited list of CC mail IDs.
`smtp.bcc`	Specify the comma-delimited list of BCC mail IDs.
`smtp.debug`	Set the Debug flag to true or false.

> **Note:**
>
> You can view current SMTP configuration details using `tfactl print smtp`.

4. Verify SMTP configuration by sending a test email using `tfactl sendmail` *`email_address`*.

   If Oracle Trace File Analyzer detects that a significant error has occurred, then it sends an email notification as follows:

Figure 4-3 Email Notification



Event: .*ORA-00600.*
Event time: Thu Sep 13 10:17:18 PDT 2018

File containing event: /scratch/app/oradb/diag/rdbms/ogg11204/ogg112041/trace/alert_ogg112041.log

String containing event: ORA-00600: internal error code, arguments: [ktfbtgex-7], [1015817], [1024], [1015816], [], [], [], [], [], [], [], []

Logs will be collected at: /opt/oracle.tfa/tfa/repository/auto_srdcORA-00600_2018_09_13T10_07_18_node_myserver69

5. Do the following after receiving the notification email:
   a. To find the root cause, inspect the referenced collection details.
   b. If you can fix the issue, then resolve the underlying cause of the problem.
   c. If you do not know the root cause of the problem, then log an SR with Oracle Support, and upload the collection details.

4.2.3 Collecting Problems Detected by Oracle Cluster Health Advisor

Configure Oracle Cluster Health Advisor to automatically collect diagnostics for abnormal events, and send email notifications.

1. To configure Oracle Cluster Health Advisor auto collection for abnormal events:

```
tfactl set chaautocollect=ON
```

2. To enable Oracle Cluster Health Advisor notification through Oracle Trace File Analyzer:

```
tfactl set chanotification=on
```

3. To configure an email address for Oracle Cluster Health Advisor notifications to be sent to:

```
tfactl set notificationAddress=chatfa:john.doe@acompany.com
```

4.2.4 Sanitizing Sensitive Information in Oracle Trace File Analyzer Collections

After collecting copies of diagnostic data, Oracle Trace File Analyzer uses Adaptive Classification and Redaction (ACR) to sanitize sensitive data in the collections.

> **Note:**
>
> Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release.

To mask or sanitize sensitive data in collections:

```
tfactl set redact=mask|sanitize|none
```

`mask`: blocks out the sensitive data in all collections, for example, replaces *myhost1* with *******

`sanitize`: replaces the sensitive data in all collections with random characters, for example, replaces myhost1 with *orzhmv1*

`none` (default): does not mask or sanitize sensitive data in collections

You can use the `-sanitize` and `-mask` options with the `diagcollect` command to sanitize or mask sensitive data in a specific collection.

To mask sensitive data:

1. To mask sensitive data in all collections:

   ```
   tfactl set redact=mask
   ```

2. To sanitize sensitive data in all collections:

   ```
   tfactl set redact=sanitize
   ```

3. To mask or sanitize sensitive data in a specific collection:

   For example:

   ```
   tfactl diagcollect -SRDC ORA-00600 -mask
   ```

   ```
   tfactl diagcollect -SRDC ORA-00600 -sanitize
   ```

Related Topics

- Deprecated Oracle Trace File Analyzer Masking in Release 24.1
  Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release.

4.2.5 Flood Control for Similar Issues

Flood control mechanism helps you save resource through fewer repeat collections for similar issues.

You can:

- Enable or disable flood control.
- How many times to collect for an event.
- Pause flood control.

The flood control data is stored in Berkeley Database and persists across Oracle Trace File Analyzer restarts.

Example 4-1   Flood Control Examples

To check if flood control is enabled or disabled:

```
# tfactl get floodcontrol
.----------------------------------------.
|               testhost                 |
+--------------------------------+-------+
| Configuration Parameter        | Value |
+--------------------------------+-------+
| Flood Control ( floodcontrol ) | ON    |
'--------------------------------+-------'
```

To check flood control limit:

```
# tfactl get fc.limit
.------------------------------------------------.
|                   testhost                     |
+----------------------------------------+-------+
| Configuration Parameter                | Value |
+----------------------------------------+-------+
| Flood Control Limit Count ( fc.limit ) | 3     |
'----------------------------------------+-------'
```

To check flood control limit time:

```
# tfactl get fc.limittime
.--------------------------------------------------------------.
|                          testhost                            |
+------------------------------------------------------+-------+
| Configuration Parameter                              | Value |
+------------------------------------------------------+-------+
| Flood Control Limit Time (minutes) ( fc.limitTime )  | 60    |
'------------------------------------------------------+-------'
```

To check flood control pause time:

```
# tfactl get fc.pausetime
.-------------------------------------------------------------.
|                          testhost                           |
+-----------------------------------------------------+-------+
| Configuration Parameter                             | Value |
+-----------------------------------------------------+-------+
| Flood Control Pause Time (minutes) ( fc.pauseTime ) | 120   |
'-----------------------------------------------------+-------'
```

To print flood control details:

```
# tfactl floodcontrol print

.----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-.
| Event                    | Count | Start Date                    | Last 
Date                     | Limit | Limit Time | Pause Time | Coll Count | 
Skip Count |
+-------------------------+-------+------------------------------
+------------------------------+-------+------------+------------
+------------+------------+
| orcl:ORA-00600:user1    |      1 | Thu May 21 09:18:56 UTC 2020 | Thu May 21 
09:18:56 UTC 2020 |     3 |         60 |        120 |           1 | 
0 |
+-------------------------+-------+------------------------------
+------------------------------+-------+------------+------------
+------------+------------+
| orcl:ORA-00600:user2    |      1 | Thu May 21 09:18:25 UTC 2020 | Thu May 21 
09:18:25 UTC 2020 |     3 |         60 |        120 |           4 | 
2 |
'-------------------------+-------+------------------------------
+------------------------------+-------+------------+------------
+------------+------------'
```

To clear flood control:

```
# tfactl floodcontrol clear -event orcl:ORA-00600:user1
Successfully cleared Event orcl:ORA-00600:user1

# tfactl floodcontrol print
.----------------------------------------------------------------------------
-----------------------------------------.
| Event                    | Count | Start Date | Last Date | Limit | Limit 
Time | Pause Time | Coll Count | Skip Count |
+-------------------------+-------+------------+-----------+-------
+------------+------------+------------+------------+
| orcl:ORA-00600:user1    |      0 | null       | null      |     3 | 
60 |        120 |          3 |          2 |
'-------------------------+-------+------------+-----------+-------
+------------+------------+------------+------------'
```

To udate flood control details:

```
# tfactl floodcontrol update -event orcl:ORA-00600:user1 -limit 10 -
limittime 90 -pausetime 180
Successfully updated Flood Control Event

# tfactl floodcontrol print -event orcl:ORA-00600:user1
.----------------------------------------------------------------------
-----------------------------------------------------------------------
-------------.
| Event                  | Count | Start Date                   | Last
Date                    | Limit | Limit Time | Pause Time | Coll Count
| Skip Count |
+------------------------+-------+------------------------------
+------------------------------+-------+------------+------------
+------------+------------+
| orcl:ORA-00600:user1   |     1 | Thu May 21 09:18:25 UTC 2020 | Thu
May 21 09:18:25 UTC 2020 |    10 |         90 |        180 |
4 |          2 |
'------------------------+-------+------------------------------
+------------------------------+-------+------------+------------
+------------+------------'
```

Related Topics

- tfactl floodcontrol
  Use the `tfactl floodcontrol` command to limit or stop Oracle Trace File Analyzer collecting the same events in a given frame of time.

4.3 Using On-Demand Diagnostic Collections

Run Oracle Trace File Analyzer on demand using `tfactl` command-line tool.

- Collecting Diagnostics and Analyzing Logs On-Demand
  The `tfactl` command uses a combination of different Oracle Database support tools when it performs analysis.
- Viewing System and Cluster Summary
  The summary command gives you a real-time report of system and cluster status.
- Investigating Logs for Errors
  Use Oracle Trace File Analyzer to analyze all of your logs across your cluster to identify recent errors.
- Analyzing Logs Using the Oracle Database Support Tools
  The Oracle Database support tools bundle is available only when you download Oracle Trace File Analyzer from My Oracle Support note 2550798.1.
- Searching Oracle Trace File Analyzer Metadata
  You can search all metadata stored in the Oracle Trace File Analyzer index using `tfactl search -showdatatypes|-json [json_details]`.
- Oracle Trace File Analyzer Service Request Data Collections (SRDCs)
  Oracle Trace File Analyzer Service Request Data Collections (SRDCs) enable you to quickly collect the right diagnostic data.

- Diagnostic Upload
  Diagnostic upload eliminates the need for different set of commands to upload Oracle ORAchk, Oracle EXAchk, and Oracle Trace File Analyzer diagnostic collections to AHF Service, database, and Oracle Support.
- Changing Oracle Grid Infrastructure Trace Levels
  Enable trace levels to collect enough diagnostics to diagnose the cause of the problem.
- Performing Custom Collections
  Use the custom collection options to change the diagnostic collections from the default.
- Limit the Maximum Amount of Memory Used by Oracle Trace File Analyzer
  You can now limit the amount of memory used by Oracle Trace File Analyzer.
- Limit Oracle Trace File Analyzer's CPU Usage
  On Linux the CPU usage of Oracle Trace File Analyzer can be limited with the command `ahfctl setresourcelimit [-value value]`

4.3.1 Collecting Diagnostics and Analyzing Logs On-Demand

The `tfactl` command uses a combination of different Oracle Database support tools when it performs analysis.

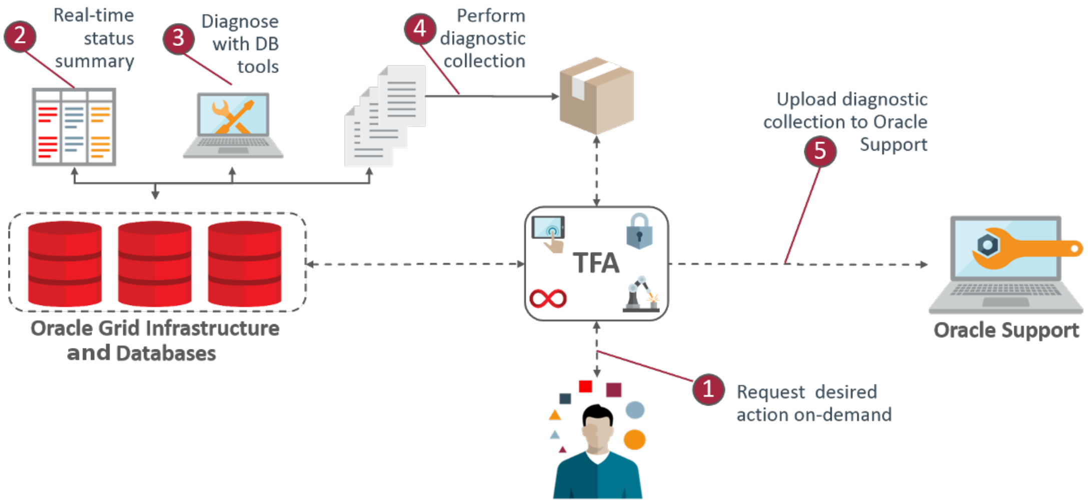
The `tfactl` command enables you to access Oracle Database support tools using common syntax. Using common syntax hides the complexity of the syntax differences between the tools.

Use the Oracle Trace File Analyzer tools to perform analysis and resolve problems. If you need more help, then use the `tfactl` command to collect diagnostics for Oracle Support.

Oracle Trace File Analyzer does the following:

- Collects all relevant log data from a time of your choosing.
- Trims log files to collect only what is necessary for diagnosis.
- Packages all diagnostics on the node where `tfactl` was run from.

Figure 4-4 On-Demand Collections


2
Real-time status summary
3
Diagnose with DB tools
4
Perform diagnostic collection
Upload diagnostic collection to Oracle Support
5
TFA
Oracle Grid Infrastructure and Databases
Oracle Support
1
Request desired action on-demand

4.3.2 Viewing System and Cluster Summary

The summary command gives you a real-time report of system and cluster status.

Syntax

```
tfactl summary [options]
```

For more help use:

```
tfactl summary -help
```

4.3.3 Investigating Logs for Errors

Use Oracle Trace File Analyzer to analyze all of your logs across your cluster to identify recent errors.

1. To find all errors in the last one day:

   ```
   $ tfactl analyze -last 1d
   ```

2. To find all errors over a specified duration:

   ```
   $ tfactl analyze -last 18h
   ```

3. To find all occurrences of a specific error on any node, for example, to report `ORA-00600` errors:

   ```
   $ tfactl analyze -search "ora-00600" -last 8h
   ```

Related Topics

- tfactl summary
  Use the `tfactl summary` command to view the summary of Oracle Trace File Analyzer deployment.
- tfactl analyze
  Use the `tfactl analyze` command to obtain analysis of your system by parsing the database, Oracle Automatic Storage Management (Oracle ASM), and Oracle Grid Infrastructure alert logs, system message logs, OSWatcher Top, and OSWatcher Slabinfo files.

4.3.4 Analyzing Logs Using the Oracle Database Support Tools

The Oracle Database support tools bundle is available only when you download Oracle Trace File Analyzer from My Oracle Support note 2550798.1.

Oracle Trace File Analyzer with Oracle Database support tools bundle includes the following tools:

Table 4-5 Tools Included in Linux and UNIX

Tool	Description
`orachk` or `exachk`	Provides health checks for the Oracle stack. Oracle Autonomous Health Framework installs either Oracle EXAchk for engineered systems or Oracle ORAchk for all non-engineered systems. For more information, see My Oracle Support notes 1070954.1 and 2550798.1.
`oswatcher (oswbb)`	Collects and archives operating system metrics. These metrics are useful for instance or node evictions and performance Issues. For more information, see My Oracle Support note 301137.1.
`procwatcher (prw)`	Automates and captures database performance diagnostics and session level hang information. For more information, see My Oracle Support note 459694.1.
`oratop`	Provides near real-time database monitoring. For more information, see My Oracle Support note 1500864.1.
`alertsummary`	Provides summary of events for one or more database or Oracle ASM alert files from all nodes.
`ls`	Lists all files that Oracle Trace File Analyzer knows about for a given file name pattern across all nodes.
`pstack`	Generates the process stack for the specified processes across all nodes.
`grep`	Searches for a given string in the alert or trace files with a specified database.
`summary`	Provides high-level summary of the configuration.
`vi`	Opens alert or trace files for viewing a given database and file name pattern in the `vi` editor.
`tail`	Runs a tail on an alert or trace files for a given database and file name pattern.
`param`	Shows all database and operating system parameters that match a specified pattern.
`dbglevel`	Sets and unsets multiple Oracle Clusterware trace levels with one command.
`history`	Shows the shell history for the `tfactl` shell.
`changes`	Reports changes in the system setup over a given time period. The report includes database parameters, operating system parameters, and the patches that are applied.
`calog`	Reports major events from the cluster event log.
`events`	Reports warnings and errors in the logs.
`managelogs`	Shows disk space usage and purges Automatic Diagnostic Repository (ADR) log and trace files.
`ps`	Finds processes.
`triage`	Summarizes `oswatcher` or `exawatcher` data.

Table 4-6 Tools Included in Microsoft Windows

Tool	Description
`calog`	Reports major events from the cluster event log.
`changes`	Reports changes in the system setup over a given time period. The report includes database parameters, operating system parameters, and patches applied.
`dir`	Lists all files Oracle Trace File Analyzer knows about for a given file name pattern across all nodes.
`events`	Reports warnings and errors seen in the logs.
`findstr`	Searches for a given string in the alert or trace files with a specified database.
`history`	Shows the shell history for the `tfactl` shell.
`managelogs`	Shows disk space usage and purges ADR log and trace files.
`notepad`	Opens alert or trace files for viewing a given database and file name pattern in the `notepad` editor.
`param`	Shows all database and operating system parameters that match a specified pattern.
`summary`	Provides high-level summary of the configuration.
`tasklist`	Finds processes.

To verify which tools you have installed:

```
$ tfactl toolstatus
```

You can run each tool using `tfactl` either in command line or shell mode. To run a tool from the command line:

```
$ tfactl run tool
```

The following example shows how to use `tfactl` in shell mode. Running the command starts `tfactl`, connects to the database *MyDB*, and then runs `oratop`:

```
$ tfactl
tfactl > database MyDB
MyDB tfactl > oratop
```

Related Topics

- https://support.oracle.com/rs?type=doc&id=2550798.1
- https://support.oracle.com/rs?type=doc&id=1070954.1
- https://support.oracle.com/rs?type=doc&id=301137.1
- https://support.oracle.com/rs?type=doc&id=1500864.1
- https://support.oracle.com/rs?type=doc&id=215187.1

4.3.5 Searching Oracle Trace File Analyzer Metadata

You can search all metadata stored in the Oracle Trace File Analyzer index using `tfactl search -showdatatypes|-json [json_details]`.

You can search for all events for a particular Oracle Database between certain dates.

For example, on Linux systems:

```
tfactl search -json
'{
  "data_type":"event",
  "content":"oracle",
  "database":"rac11g",
  "from":"01/20/2017 00:00:00",
  "to":"12/20/2018 00:00:00"
 }'
```

For example, on Linux and Windows systems:

```
tfactl search -json
"{
   \"data_type\":\"event\",
   \"content\":\"oracle\",
   \"database\":\"rac11g\",
   \"from\":\"01/20/2017 00:00:00\",
   \"to\":\"12/20/2018 00:00:00\"
}"
```

To list all index events on Linux, AIX, and Solaris systems: `tfactl search -json '{"data_type":"event"}'`

To list all index events on Windows systems: `tfactl search -json "{\"data_type\":\"event\"}"`

To list all available datatypes: `tfactl search -showdatatypes`

4.3.6 Oracle Trace File Analyzer Service Request Data Collections (SRDCs)

Oracle Trace File Analyzer Service Request Data Collections (SRDCs) enable you to quickly collect the right diagnostic data.

To perform Service Request Data Collections:

```
$ tfactl diagcollect -srdc srdc_name
```

Running the command trims and collects all important log files updated in the past *n* hours across the whole cluster. The default number of hours for log collection varies from SRDC to SRDC. You can change the `diagcollect` timeframe with the `-last n h|d` option.

Oracle Support often asks you to run a Service Request Data Collection (SRDC). The SRDC depends on the type of problem that you experienced. An SRDC is a series of many data gathering instructions aimed at diagnosing your problem. Collecting the SRDC manually can be difficult with many different steps required.

Oracle Trace File Analyzer can run SRDC collections with a single command:

```
$ tfactl diagcollect
[-srdc srdc_profile]
[-sr sr_number]
[-tag tagname]
[-z filename]
[-last nh|d | -from time -to time | -for date]
[-database database]
```

Option	Description
[-srdc *srdc_profile*]	Specify the SRDC profile.
-tag *description*	Use this parameter to create a subdirectory for the resulting collection in the Oracle Trace File Analyzer repository.
-z *file_name*	Use this parameter to specify an output file name.

Option	Description

`[-last` *`nh`*`|`*`d`*` | -from` *`time`*` -to` *`time`*` | -for` *`date`*`]`	• Specify the `-last` parameter to collect files that have relevant data for the past specific number of hours (*h*) or days (*d*). By default, using the command with this parameter also trims files that are large and shows files only from the specified interval.
	You can also use `-since`, which has the same functionality as `-last`. This option is included for backward compatibility.
	• Specify the `-from` and `-to` parameters (you must use these two parameters together) to collect files that have relevant data during a specific time interval, and trim data before this time where files are large.
	Supported time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`
	• Specify the `-for` parameter to collect files that have relevant data for the date specified. The files `tfactl` collects will have timestamps in between which the time you specify after `-for` is included. No data trimming is done for this option.
	Supported time formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`
	Note:
	If you specify both date and time, then you must enclose both the values in double quotation marks (""). If you specify only the date or the time, then you do not have to enclose the single value in quotation marks.

`-database` *`database`*	Specify the name of the database.

Note:

To upload collections to the SR as part of diag collection:

If you have already set MOS configuration using the `tfactl setupmos` command, then you can use the `-sr` option along with the diag collection command. Note that `tfactl setupmos` is supported only in versions earlier than 20.2.

If you have not set MOS configuration using the `tfactl setupmos` command, then set up MOS configuration using the new generic command, `ahfctl setupload -name mos -type https` and follow the instructions.

For example: `tfactl diagcollect -srdc` *`srdc_type`* `-sr` *`sr_number`*

To run SRDCs, use one of the Oracle privileged user accounts:

- `ORACLE_HOME` owner
- `GRID_HOME` owner

Table 4-7 One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`ahf`	Oracle Orachk and Oracle Exachk problems (to be run after running with `-debug`)	Local only	No
`avs`	Audit Vault Server related files	Cluster-wide	No
`crs`	Collect `crs` traces	Cluster-wide	No
`crsasm`	ASM CRS-related problems	Cluster-wide	No
`crsasmcell`	ASM CRS CELL-related problems	Cluster-wide	No
`dbacl`	Problems with Access Control Lists (ACLs)	Local only	No
`dbaqgen`	Problems in an Oracle Advanced Queuing environment	Local only	No
`dbaqmon`	Queue Monitor (QMON) problems	Local only	No
`dbaqnotify`	Notification problems in an Oracle Advanced Queuing environment	Local only	No
`dbaqperf`	Performance problems in an Oracle Advanced Queuing environment	Local only	No
`dbaqpurge`	Non-purged messages in an Oracle Advanced Queuing environment problems	Local only	No
`dbasm`	Oracle Database storage problems	Local only	No
`dbaudit`	Standard information for Oracle Database auditing	Local only	No
`dbaum`	AUM: Checklist of Evidence to Supply (Doc ID 1682741.1)	Local only	No
`dbaumwaitevents`	Wait Events related to Undo: Checklist of Evidence to Supply (Doc ID 1682723.1)	Local only	No
`dbawrspace`	Oracle Database Automatic Workload Repository (AWR) space problems	Local only	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`dbbeqconnection`	Bequeath Connection Issues: Checklist of Evidence to Supply (Doc ID 1928047.1)	Local only	No
`dbcorrupt`	Generic Oracle Database corruption	Local only	No
`dbdataguard`	Data Guard problems including Broker	Local only	No
`dbawrspace`	Excessive SYSAUX space is used by the Automatic Workload Repository (AWR)	Local only	No
`dbdatapatch`	Datapatch problems	Local only	No
`dbddlerrors`	DDL Errors: Checklist of Evidence to Supply (Doc ID 2383662.1)	Local only	No
`dbemon`	Event Monitor (EMON) problems	Local only	No
`dbenqdeq`	Collect standard information for Advanced Queueing problems using TFA Collector (recommended) or manual steps	Local only	No

`dbexpdp`
`dbexpdpapi`
`dbexpdpperf`
`dbexpdptts`
	Oracle Data Pump Export (`expdp`)	Local only	No

`dbfs`	Oracle Automatic Storage Management (Oracle ASM) / Database File System (DBFS) / Direct NFS / Oracle Advanced Cluster File System (Oracle ACFS) problems	Local only	No
`dbfra`	Fast Recovery Area, also known as Flash Recovery Area problems	Local only	No
`dbggclassicmode` `dbggintegratedmode`	Oracle GoldenGate	Local only	No
`dbhang`	Oracle Database hang problems	Local only	No
`dbhangperflite`	Oracle Database performance and hang problems	Local only	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
dbimpdp dbimpdpperf	Oracle Data Pump Import (impdp)	Local only	No
dbimpdpperf	Data Pump Import performance problems	Local only	No
dbinstall dbupgrade dbpreupgrade	Oracle Database install / upgrade problems	Local only	No
dbparameters	Oracle Database single instance shutdown problems	Local only	No
dbparameterfiles	Parameter Files: Checklist of Evidence to Supply (Doc ID 1914153.1)	Local only	No
dbpartition	Create or maintain partitioned table, subpartitioned table, and index problems	Local only	No
dbpartitionperf	Slow Create, Alter, or Drop commands against partitioned table or index	Local only	No
dbpatchinstall dbpatchconflict	Oracle Database patching problems	Local only	No
dbperf	Oracle Database performance problems	Cluster-wide	No
dbperf_and_hang	Oracle Database performance and hang problems on FASaaS environments	Local only	No
dbplugincompliance	Enterprise Manager compliance related issues	Local only	No
dbpreupgrade	Oracle Database preupgrade problems	Local only	No
dbprocmgmt	Generic Process Management and Related Issues: Checklist of Evidence to Supply (Doc ID 2500734.1)	Local only	No
dbrac	Oracle RAC-related data collection for Oracle Clusterware and Oracle ASM problems	Local only	No
dbracinst	Oracle RAC-related data collection for Oracle Database problems	Local only	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`dbracperf`	Oracle RAC-related performance problems	Cluster-wide	No
`dbresmgr`	Oracle Database problems related to Resource Manager	Local only	No
`dbrman` `dbrmanperf`	Recovery Manager (RMAN) problems	Local only	No
`dbscn`	System Change Number (SCN)	Local only	No
`dbshutdown` `dbstartup`	Oracle Database startup or shutdown problems	Local only	No
`dbslowddl`	Slow DDL: Checklist of Evidence to Supply	Local only	No
`dbspacewait`	Space Related Wait Events and Performance Issues : Checklist of Evidence to Supply (Doc ID 2560286.1)	Local only	No
`dbspatialexportimport`	Oracle Spatial export or import problems	Local only	No
`dbspatialinstall`	Oracle Spatial installation problems	Local only	No
`dbspatialperf`	Oracle Spatial performance problems	Local only	No
`dbspatialupgrade`	Oracle Spatial upgrade problems	Local only	No
`dbspatialusage`	Oracle Spatial usage problems	Local only	No
`dbsqlperf`	SQL performance problems	Local only	No
`dbstandalonedbca`	Oracle Database Configuration Assistant (Oracle DBCA) problems	Local only	No
`dbstoragestructuregeneric`	Storage structure related diagnosis	Local only	No
`dbtablespacegeneric`	Generic Tablespace and Segment Management: Checklist of Evidence to Supply (Doc ID 2560291.1)	Local only	No
`dbtde`	Transparent Data Encryption (TDE) problems	Local only	No
`dbtextindex`	Oracle Text problems	Local only	No
`dbtextissue`	Oracle Text installation problems - 12c.	Local only	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
dbtextupgrade dbtextinstall	Oracle Text version 12.1.0.1 and later upgrade problems	Local only	No
dbunixresources	Oracle Database resource problems	Local only	No
dbvault	Collect standard information for Database Vault	Local only	No
dbwindowsresources	Oracle Database on Microsoft Windows resources: Checklist of Evidence to Supply	Local only	No
dbwinservice	OracleService on Microsoft Windows: Checklist of Evidence to Supply (Doc ID 1918781.1)	Local only	No
dbxdb	XDB installation or invalid object problems	Local only	No
dbxdbgeneric	XDB installation and invalid object problems	Local only	No
dbxdbupgrade	XDB installation and invalid object problems in 12c and above	Local only	No
dnfs	XDB upgrade problems	Local only	No
emagentgeneric	Collect trace/log information for Enterprise Manager Management Agent generic problems	Oracle Management Service (OMS) and Agent	No
emagentpatching	Enterprise Manager failures during agent patching	Oracle Management Service (OMS) and Agent	No
emagentperf	Enterprise Manager 13c Agent performance problems	Agent	No
emagentssl	Enterprise Manager Agent SSL configuration issues	Oracle Management Service (OMS) and Agent	No
emagentstartup	Enterprise Manager 13c Agent startup problems	Agent	No
emagentunreach	Enterprise Manager 13c Agent unreachable errors or status	Agent	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`emagentupload`	Enterprise Manager 13c Agent upload errors	Agent	No
`emagtpatchdeploy`	Enterprise Manager 13c Agent patch deployment problems	Oracle Management Service (OMS) and Agent	No
`emagtupginst`	Collecting diagnostic data for Enterprise Manager 13c Agent installation, upgrade, or deployment problems	Agent	No
`emagtupgpatch`	Enterprise Manager 13c Agent upgrade, local installation, or patching problems.	Oracle Management Service (OMS) and Agent	No
`emauthldap`	Enterprise Manager authentication using LDAP provider issues	Oracle Management Service (OMS)	No
`emblackout`	Enterprise Manager blackout issues	Oracle Management Service (OMS) and Agent	No

`emcliadd`
`emclusdisc`
`emdbsys`
`emgendisc`
	Enterprise Manager target discovery or add problems	Oracle Management Service (OMS) and Agent
		Agent
		Oracle Management Service (OMS) and Agent
		Oracle Management Service (OMS) and Agent
			No

`emcomm`	Enterprise Manager communication information between Oracle Management Service (OMS) and Agent	Oracle Management Service (OMS) and Agent	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`emdbaasdeploy`	Database As A Service (DBaaS): Collect trace or log information for failures during DBaaS deployment.	Oracle Management Service (OMS) and remote DBaaS deployment server	No
`emdebugon` `emdebugoff`	Enterprise Manager debug log collection Run `emdebugon`, reproduce the problem then run `emdebugoff`, which disables debug again and collects debug logs	Oracle Management Service (OMS) or Agent	No
`emfleetpatching`	Enterprise Manager Fleet Maintenance Patching problems	Oracle Management Service (OMS) and Agent	No
`emjobs`	Enterprise Manager all job related issues	Oracle Management Service (OMS)	No
`emmetricalert`	Enterprise Manager general metrics page or threshold problems	Agent	No
`emnotif`	Enterprise Manager incident rules and notification issues	Oracle Management Service (OMS)	No
`emomsfailstart`	Enterprise Manager Oracle Management Service (OMS) startup failures	Oracle Management Service (OMS)	No
`emomscrash`	Enterprise Manager Oracle Management Service (OMS) crash problems	Oracle Management Service (OMS)	No
`emomsheap`	Enterprise Manager Java heap usage or performance problems	Oracle Management Service (OMS)	No
`emomshungcpu`	Enterprise Manager Oracle Management Service (OMS) crash, restart or performance problems	Oracle Management Service (OMS)	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`emomspatching`	Enterprise Manager failures during Oracle Management Service (OMS) patching	Oracle Management Service (OMS)	No
`emomsssl`	Enterprise Manager Oracle Management Service (OMS) SSL configuration issues	Oracle Management Service (OMS)	No
`emomsupginst`	Enterprise Manager Oracle Management Service (OMS) installation, upgrade, and patching	Local only	No
`empatchplancrt`	Enterprise Manager patch plan creation problems	Oracle Management Service (OMS) and Agent	No
`emprocdisc`	Oracle Database, Listener, or ASM target is not discovered or detected by the discovery process	Local only	No
`emtbsmetric`	Enterprise Manager tablespace usage metric problems	Local only (on Enterprise Manager Agent target)	No
`emwlsssl`	Enterprise Manager WebLogic Server (WLS) SSL configuration issues	Local only	No
`emdbrat`	Enterprise Manager RAT collection issues	Target replay/ capture database	No
`emcreds`	Enterprise Manager credential issues	Oracle Management Service (OMS) and Agent	No
`emdbpluginstatus`	Enterprise Manager DB plugin issues	Oracle Management Service (OMS) and/or Agent	No
`emdeployoms`	Enterprise Manager deploying additional Oracle Management Service (OMS) issues	Oracle Management Service (OMS)	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`emomsmigration`	Enterpriser Manager Oracle Management Service (OMS) migration/ cloning issues	Oracle Management Service (OMS)	No
`esexalogic`	Oracle Exalogic full Exalogs data collection information	Local only	No
`exadata`	Collect Oracle Exadata information	Local only	No
`exservice`	Oracle Exadata: Storage software service or offload server service problems	Local only	No
`exsmartscan`	Oracle Exadata: Smart Scan not working problems	Local only	No
`generic`	Fallthrough SRDC for Oracle Database error	Local only	No
`gg_abend`	Oracle GoldenGate covering both classic and microservices implementations	Local only	No
`ggintegratedmodenodb`	Oracle GoldenGate extract/ replicate abends problems	Local only	No
`gridinfra`	Oracle RAC-related data collection for Oracle Clusterware problems	Local only	No
`gridinfrainst`	Oracle RAC upgrade and patching problems	Local only	No
`instterm`	Collect traces for the following ORA errors: • `ORA-00469` • `ORA-00470` • `ORA-00480` • `ORA-00490` • `ORA-00491` • `ORA-00492` • `ORA-00493` • `ORA-00495` • `ORA-00496` • `ORA-00497` • `ORA-00498`	Local only	No
`internalerror`	Other internal Oracle Database errors	Local only	No
`listener_services`	Listener errors: `TNS-12516` / `TNS-12518` / `TNS-12519` / `TNS-12520`	Local only	No

Table 4-7 (Cont.) One Command Service Request Data Collections

Available SRDCs	Type of Problem	Collection Scope	Auto Collection
`naming_services`	Naming service errors: `TNS-12154` / `TNS-12528`	Local only	No

`ORA-00020`
`ORA-00060`
`ORA-00494`
`ORA-00600`
`ORA-00700`
`ORA-01031`
`ORA-01555`
`ORA-01578`
`ORA-01628`
`ORA-03137`
`ORA-04020`
`ORA-04021`
`ORA-04030`
`ORA-04023`
`ORA-04031`
`ORA-04063`
`ORA-07445`
`ORA-08102`
`ORA-08103`
`ORA-22924`
`ORA-27300`
`ORA-27301`
`ORA-27302`
`ORA-30036`
	ORA Errors	Local only	Only the following SRDCs:
			• `ORA-00600`
			• `ORA-04030`
			• `ORA-04031`
			• `ORA-04021`
			• `ORA-07445`
			• `ORA-01578`

`ORA-01000`	Open Cursors problems	Local only	No
`ORA-00018`	`ORA-00018` or sessions parameter problems	Local only	No
`ORA-12751`	`ORA-12751` collection errors	Local only	No
`ORA-25319`	Collect information for troubleshooting `ORA-25319` error in an Advanced Queuing Environment `ORA-25319` problems in an Oracle Advanced Queuing Environment	Local only	No
`ORA-00227`	Collect information for troubleshooting Control File block corruption reported by error `ORA-00227`	Local only	No
`privsroles`	Data Collection for privileges and roles	Local only	No
`xdb600`	Diagnostic data collection for XDB `ORA-00600` and `ORA-07445` internal rrror issues using TFA Collector	Local only	No
`zlgeneric`	Zero Data Loss Recovery Appliance (ZDLRA) problems	Local only	No

For more information about SRDCs, run `tfactl diagcollect -srdc -help`.

Note:

When you run the `tfactl diagcollect` command to query an `ora-*` error event, for example, `tfactl diagcollect -srdc ora-600`, AHF lists all `ora-*` error events without filtering. This is because of generic event mapping for all `ORA-*` error events in the `srdc_dbrac.xml` file.

The types of information that the SRDCs collect varies for each type, for example, the following table lists and describes what the SRDCs collect for each type.

Table 4-8 SRDC collections

Command	What gets collected
`$ tfactl diagcollect -srdc ORA-04031`	• Incident Packaging Service (IPS) package • Patch listing • Automatic Workload Repository (AWR) report • Memory information
`$ tfactl diagcollect -srdc dbperf`	• Automatic Database Diagnostic Monitor (ADDM) report • Automatic Workload Repository (AWR) for good period and problem period • Automatic Workload Repository (AWR) Compare Period report • Active Session History (ASH) report for good and problem period • OSWatcher • Incident Packaging Service (IPS) package (if there are any errors during problem period) • Oracle ORAchk (performance-related checks)

Oracle Trace File Analyzer prompts you to enter the information required based on the SRDC type.

For example, when you run `ORA-4031` SRDC:

```
$ tfactl diagcollect -srdc ORA-04031
```

Oracle Trace File Analyzer:

1. Prompts to enter event date, time, and database name.
2. Scans the system to identify recent events in the system (up to 10).
3. Proceeds with diagnostic collection after you choose the relevant event.
4. Identifies all the required files.
5. Trims all the files where applicable.
6. Packages all data in a zip file ready to provide to support.

You can also run an SRDC collection in non-interactive silent mode. Provide all the required parameters up front as follows:

```
$ tfactl diagcollect -srdc srdc_type -database db -from "date time" -to
"date time"
```

Related Topics

- https://support.oracle.com/rs?type=doc&id=1918781.1
- https://support.oracle.com/rs?type=doc&id=2560291.1
- https://support.oracle.com/rs?type=doc&id=2560286.1
- https://support.oracle.com/rs?type=doc&id=2500734.1
- https://support.oracle.com/rs?type=doc&id=1914153.1
- https://support.oracle.com/rs?type=doc&id=2383662.1
- https://support.oracle.com/rs?type=doc&id=1682741.1
- https://support.oracle.com/rs?type=doc&id=1682723.1
- https://support.oracle.com/rs?type=doc&id=1928047.1

4.3.7 Diagnostic Upload

Diagnostic upload eliminates the need for different set of commands to upload Oracle ORAchk, Oracle EXAchk, and Oracle Trace File Analyzer diagnostic collections to AHF Service, database, and Oracle Support.

Diagnostic upload enables you to manage configurations of different types of uploads in a generic way. Through `ahfctl` command-line interface, you use generic upload commands to set, get, unset, and check configurations. Configurations are uniquely identified using configuration name so that you can pass the configuration name in command-line to perform upload and other operations.

AHF synchronizes the configuration automatically across the cluster nodes. If you find any sync issues, then run the `tfactl syncahfconfig -c` command to sync configuration across the cluster nodes.

Diagnostic upload supports multiple operating system users to run the diagnostic upload commands if you install AHF as `root`. If you install AHF as a non-root user, then you cannot benefit from the multiple operating system users support.

> **Note:**
>
> Currently not supported on Microsoft Windows.

Currently, AHF supports HTTP, SQLNET, and SFTP types or protocols, or end points. Following sections list the parameters or arguments supported by different end points while setting the configuration.

HTTP

Set Parameters: `url`, `user`, `password`, `proxy`, `noauth`, `https_token`, `header`, `secure`, and `storetype`

Upload Parameters: id, file, and https_token

SQLNET

Set Parameters: user, password, connectstring, and uploadtable

Upload Parameters: file

SFTP

Set Parameters: server, user, and password

Upload Parameters: (optional) id and file

Parameters or arguments Supported by Different Endpoints

Table 4-9 Parameters or Arguments Supported by Different Endpoints

Parameter	Description
url	The target URL to upload files in case of HTTPS type. For example, *https://samplehost.com*.
server	The name of the server to which you want to upload files. For example, *sftpserver.domain.com*.
user	The user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
password	Password of the user.
proxy	The URL of the proxy server. For example, *www.example.com:80*.
id	The location or target where you want to upload your files to.
file	The name of the file to upload.
noauth	Specify true and false. Default value is false. If noauth is set to true, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/password authentication is required.
https_token	Any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. For example, ahfctl setupload -name config -type https -https_token 'abc:13'. You can also pass dynamic headers at upload time by passing the -https_token headers command option to tfactl upload command. For example: -H 'X-TFA-REQUESTID: 1'.

Table 4-9 (Cont.) Parameters or Arguments Supported by Different Endpoints

Parameter	Description
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`ahfctl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.
`connectstring`	The database connect string to log in to the database where you want to upload files. For example, `(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl))).`
`uploadtable`	Specify the name of the table where you want to upload files as `BLOB` type. For example, for uploading Oracle ORAchk collections to the Collection Manager it is set to `RCA13_DOCS`.

Example 4-2 Diagnostic Upload Examples To upload files to My Oracle Support

To setup MOS configuration:

```
ahfctl setupload -name mos -type https

Enter mos.https.user: user_id
Enter mos.https.password: ########
Enter mos.https.url: https://transport.oracle.com/upload/issue

Upload configuration set for: mos
type: https
user: user_id
password: ########
url: https://transport.oracle.com/upload/issue
```

To set proxy:

```
ahfctl setupload -name mos -type https -proxy www-proxy.example.com:80
```

Single-line command:

```
ahfctl setupload -name mos -type https -user user_id -url https://
transport.oracle.com/upload/issue -proxy www-proxy.example.com:80
```

> **Note:**
>
> Instead of `mos`, you can specify any configuration name of your choice.

To upload collections or files to MOS: There are multiple ways you can upload files to MOS after configuring MOS.

- Upload files as part of Oracle Trace File Analyzer diagnostic collection:

  ```
  tfactl diagcollect -last 1h -upload mos -id 3-23104325631
  ```

- Upload files standalone:

  ```
  tfactl upload -name mos -id 3-23104325631 -file /tmp/generated.zip
  ```

- Backward compatibility or upload using `-sr` flag with `diagcollcet` command:

  ```
  tfactl diagcollect -last 1h -sr 3-23104325631
  ```

  > **Note:**
  >
  > In this case, upload configuration name should be `mos` as internally Oracle Trace File Analyzer looks for this name. It works even if MOS configuration is set using the `tfactl setupmos` command in versions earlier than 20.2.

Example 4-3 Uploading a File Using SFTP

```
ahfctl upload -name sftp1 -file test_sftp_upload.log
Upload for: sftp1
Uploading file using pexpect
sftp> put test_sftp_upload.log
put test_sftp_upload.log
Uploading test_sftp_upload.log to /root/test_sftp_upload.log
test_sftp_upload.log                          100%   17     0.0KB/s
00:00
sftp> quit
type: sftp
file: test_sftp_upload.log
Upload completed successfully
```

Example 4-4 Diagnostic Upload Examples

To set configuration parameters for the specified configuration name and SQLNET configuration type:

```
ahfctl setupload -name mysqlnetconfig -type sqlnet
```

```
[root@myserver1]# ahfctl setupload -name mysqlnetconfig -type sqlnet
Enter mysqlnetconfig.sqlnet.user: testuser
Enter mysqlnetconfig.sqlnet.password: ########
Enter mysqlnetconfig.sqlnet.connectstring: (DESCRIPTION = (ADDRESS =
(PROTOCOL = TCP)(HOST = testhost)(PORT = 1521))(CONNECT_DATA =(SERVER =
DEDICATED)(SERVICE_NAME = testservice)))
Enter mysqlnetconfig.sqlnet.uploadtable: RCA13_DOCS

Upload configuration set for: mysqlnetconfig
type: sqlnet
user: testuser
password: ########

connectstring: (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testhost)
(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME =
testservice)))
uploadtable: RCA13_DOCS
```

To set individual parameters for the specified configuration name and SQLNET configuration type:

```
ahfctl setupload -name mysqlnetconfig2 -type sqlnet -user
user_name@example.com
```

This omits the `-password` option and therefore reports:

```
Database upload parameter(s) successfully stored.
AHF will not upload collections into the database until the following
parameters are also set:
['password', 'connectstring', 'uploadtable']
```

When you specify the `-user` command option, `ahfctl` does NOT prompt for the other required parameters so you must explicitly specify them at the command line as follows:

```
ahfctl setupload -type sqlnet -name orachkcm -user testuser -password  -
connectstring sqlnet connect string -uploadtable RCA13_DOCS
```

The `-password` command option DOES NOT take any arguments. When specified, `ahfctl` prompts you to provide the password for the user you specified using the `-user` command option.

To get the list of all configured names in the `AHF.properties` file:

```
ahfctl getupload
```

```
# ahfctl getupload
Upload configurations available:
1. mysftpconfig
2. myhttpsconfig
3. mysqlnetconfig
```

To get all configuration parameters for the specified configuration name:

```
ahfctl getupload -name mysftpconfig
```

```
# ahfctl getupload -name mysftpconfig
Upload configuration get for: mysftpconfig
type: sftp
user: testuser1@example.com
password: #########
server: sftphost.example.com
```

To get individual parameter for the specified configuration name:

```
ahfctl getupload -name mysftpconfig -user
```

```
[root@myserver1]# ahfctl getupload -name mysftpconfig -user
Upload configuration get for: mysftpconfig
type: sftp
user: testuser1@example.com
```

To check or validate configuration of the specified configuration name:

```
ahfctl checkupload -name mysftpconfig
```

```
# ahfctl checkupload -name mysftpconfig -type sftp
Upload configuration check for: mysftpconfig
Parameters are configured correctly to upload files to sftp end point
mysftpconfig
```

To upload to target using the configuration name specified:

```
tfactl upload -name mysftpconfig -id 30676598 -file /tmp/temp.txt
```

```
# tfactl upload -name mysftpconfig -id 30676598 -file /tmp/filename.txt
Upload for: mysftpconfig
type: sftp
file: /tmp/filename.txt
```

```
id: 30676598
Upload completed successfully.
```

To unset individual parameter of the specified configuration name:

```
ahfctl unsetupload -name mysftpconfig -user
```

```
# ahfctl unsetupload -name mysftpconfig -user
Upload configuration successfully unset for: mysftpconfig
```

To unset all parameters of the specified configuration name:

```
ahfctl unsetupload -name mysftpconfig -all
```

```
# ahfctl unsetupload -name mysftpconfig -all
Upload configuration successfully unset for: mysftpconfig
```

To auto upload generated zip file to the database using Oracle ORAchk:

```
exachk -showpass -localonly -check BF7AE780E1252F69E0431EC0E50AE447
```

```
# exachk -showpass -localonly -check BF7AE780E1252F69E0431EC0E50AE447
Orachk.zip successfully uploaded to RCA13_DOCS table
```

To auto upload generated zip file to MOS using `tfactl diagcollect`:

```
$ tfactl diagcollect -since 1h -upload mos -id 3-123456789
```

To upload generated zip to the database with the configurations set by AHF with the specified database config name:

```
exachk -showpass -localonly -check BF7AE780E1252F69E0431EC0E50AE447 -
db_config_name user_dbconf
```

```
# exachk -showpass -localonly -check BF7AE780E1252F69E0431EC0E50AE447 -
db_config_name user_dbconf
Orachk.zip successfully uploaded to RCA13_DOCS table
```

Related Topics

- tfactl setupload
  Use the `tfactl setupload` command to set upload parameters.
- tfactl getupload
  Use the `tfactl getupload` command to fetch the details of configured upload parameters.

- tfactl unsetupload
  Use the `tfactl unsetupload` command to unset the configured upload parameters.
- tfactl checkupload
  Use the `tfactl checkupload` command to validate the configured upload parameters.
- tfactl upload
  Use the `tfactl upload` command to upload collections or files on demand.

4.3.8 Changing Oracle Grid Infrastructure Trace Levels

Enable trace levels to collect enough diagnostics to diagnose the cause of the problem.

Oracle Support asks you to enable certain trace levels when reproducing a problem. You can enable and then disable the trace levels. Use the `dbglevel` option to set the trace level. You can find the required trace level settings grouped by problem trace profiles.

To set trace levels:

1. To set a trace profile:

   ```
   tfactl dbglevel -set profile
   ```

2. To list all available profiles:

   ```
   tfactl dbglevel -help
   ```

- tfactl dbglevel
  Use the `tfactl dbglevel` command to set Oracle Grid Infrastructure trace levels.

4.3.8.1 tfactl dbglevel

Use the `tfactl dbglevel` command to set Oracle Grid Infrastructure trace levels.

Syntax

```
tfactl [run] dbglevel
[ {-set|-unset} profile_name
-dependency [dep1,dep2,...|all]
-dependency_type [type1,type2,type3,...|all]
| {-view|-drop} profile_name
| -lsprofiles
| -lsmodules
| -lscomponents [module_name]
| -lsres
| -create profile_name [ -desc description
| [-includeunset] [-includetrace]
| -debugstate | -timeout time ]
| -modify profile_name [-includeunset] [-includetrace]
| -getstate [ -module module_name ]
```

```
| -active [profile_name]
| -describe [profile_name] ] ]
```

Parameters

Table 4-10 tfactl dbglevel Command Parameters

Parameter	Description
`profile_name`	Specify the name of the profile.
`active`	Displays the list of active profiles.
`set`	Sets the trace or log levels for the profile specified.
`unset`	Unsets the trace or log levels for the profile specified.
`view`	Displays the trace or log entries for the profile specified.
`create`	Creates a profile.
`drop`	Drops the profile specified.
`modify`	Modifies the profile specified.
`describe`	Describes the profiles specified.
`lsprofiles`	Lists all the available profiles.
`lsmodules`	Lists all the discovered Oracle Clusterware modules.
`lscomponents`	Lists all the components associated with the Oracle Clusterware module.
`lsres`	Lists all the discovered Oracle Clusterware resources.
`getstate`	Displays the current trace or log levels for the Oracle Clusterware components or resources.
`module`	Specify the Oracle Clusterware module.
`dependency`	Specify the dependencies to consider, start, or stop dependencies, or both.
`dependency_type`	Specify the type of dependencies to be consider.
`debugstate`	Generates a System State Dump for all the available levels.
`includeunset`	Adds or modifies an unset value for the Oracle Clusterware components or resources.
`includetrace`	Adds or modifies a trace value for the Oracle Clusterware components.

> **WARNING:**
>
> Set the profiles only at the direction of Oracle Support.

4.3.9 Performing Custom Collections

Use the custom collection options to change the diagnostic collections from the default.

- Adjusting the Diagnostic Data Collection Period
  Oracle Trace File Analyzer trims and collects any important logs updated in the past one hour.

- Collecting for Specific Events
  Perform default diagnostic collection or choose an event from the list of recent incidents to collect diagnostic data for that event alone.
- Excluding Large Files from Diagnostic Collection
  Prevent excessively large files from delaying or stalling collections.
- Collecting from Specific Nodes
- Collecting from Specific Components
- Collecting from Specific Directories
- Changing the Collection Name
- Preventing Copying Zip Files and Trimming Files
- Performing Silent Collection
- Collecting Core Files
- Collecting Incident Packaging Service (IPS) Packages
  Incident Packaging Service packages details of problems stored by Oracle Database in ADR for later diagnosis.

4.3.9.1 Adjusting the Diagnostic Data Collection Period

Oracle Trace File Analyzer trims and collects any important logs updated in the past one hour.

If you know that you only want logs for a smaller window, then you can cut this collection period. Cutting the collection period helps you make collections as small and quick as possible.

There are four different ways you can specify the period for collection:

Table 4-11 Ways to Specify the Collection Period

Command	Description
`tfactl diagcollect -last` *n* `h|d`	Collects since the previous *n* hours or days. • Number of days must be less than or equal to 7 • Number of hours must be less than or equal to 168

`tfactl diagcollect -from` “*yyyy-mm-dd*”	Collects from the date and optionally time specified.
	Valid date and time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`

`tfactl diagcollect -from` "*yyyy-mm-dd*" `-to` "*yyyy-mm-dd*"	Collects between the date and optionally time specified.
	Valid date and time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`

Table 4-11 (Cont.) Ways to Specify the Collection Period

Command	Description

`tfactl diagcollect -for "`*`yyyy-mm-dd`*`"`	Collects for the specified date.
	Valid date formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`

4.3.9.2 Collecting for Specific Events

Perform default diagnostic collection or choose an event from the list of recent incidents to collect diagnostic data for that event alone.

Choose to run:

- A diagnostic collection for a specific recent event
- A default time range diagnostic collection

To collect for specific events:

1. To run a default diagnostic collection:

   ```
   tfactl diagcollect
   ```

   For example:

   ```
   $ tfactl diagcollect
   Choose the event you want to perform a diagnostic collection for:
   1. Mar/12/2019 16:08:20 [ db.orcl.orcl ]  ORA-04030: out of process
   memory when trying to allocate
   2. Mar/12/2019 16:08:18 [ db.orcl.orcl ]  ORA-04031: unable to allocate 8
   bytes of shared memory
   3. Mar/12/2019 16:08:16 [ db.orcl.orcl ]  ORA-00494: enqueue held for too
   long more than seconds by osid
   4. Mar/12/2019 16:08:14 [ db.orcl.orcl ]  ORA-29709: Communication
   failure with Cluster Synchronization
   5. Mar/12/2019 16:08:04 [ db.orcl.orcl ]  ORA-29702: error occurred in
   Cluster Group Service operation
   6. Mar/12/2019 16:07:59 [ db.orcl.orcl ]  ORA-32701: Possible hangs up to
   hang ID= detected
   7. Mar/12/2019 16:07:51 [ db.orcl.orcl ]  ORA-07445: exception
   encountered: core dump [] [] [] [] [] []
   8. Mar/12/2019 16:07:49 [ db.orcl.orcl ]  ORA-00700: soft internal error,
   arguments: [700], [], [],[]
   9. Mar/11/2019 22:02:19 [ db.oradb.oradb ]  DIA0 Critical Database
   Process Blocked: Hang ID 1 blocks 5 sessions
   10. Default diagnostic collection, for no specific event

   Please choose the event : 1-10 [] 10

   By default TFA will collect diagnostics for the last 12 hours. This can
   result in large collections
   ```

```
For more targeted collections enter the time of the incident,
otherwise hit <RETURN> to collect for the last 12 hours
[YYYY-MM-DD HH24:MI:SS,<RETURN>=Collect for last 12 hours] :

Collecting data for the last 12 hours for all components...
Collecting data for all nodes

Collection Id : 20190312163846node1

Detailed Logging at : /scratch/app/product/19c/tfa/repository/
collection_Tue_Mar_12_16_38_47_PDT_2019_node_all/
diagcollect_20190312163846_node1.log
2019/03/12 16:38:50 PDT : NOTE : Any file or directory name
containing the string .com will be renamed to replace .com with
dotcom
2019/03/12 16:38:50 PDT : Collection Name :
tfa_Tue_Mar_12_16_38_47_PDT_2019.zip
2019/03/12 16:38:50 PDT : Collecting diagnostics from hosts :
[node1]
2019/03/12 16:38:50 PDT : Scanning of files for Collection in
progress...
2019/03/12 16:38:50 PDT : Collecting additional diagnostic
information...
2019/03/12 16:38:55 PDT : Getting list of files satisfying time
range [03/12/2019 04:38:50 PDT, 03/12/2019 16:38:55 PDT]
2019/03/12 16:39:02 PDT : Collecting ADR incident files...
2019/03/12 16:39:06 PDT : Completed collection of additional
diagnostic information...
2019/03/12 16:39:07 PDT : Completed Local Collection
.------------------------------------.
|         Collection Summary         |
+----------+-----------+------+------+
| Host     | Status    | Size | Time |
+----------+-----------+------+------+
| node1 | Completed | 21MB |  17s |  |
'----------+-----------+------+------'

Logs are being collected to: /scratch/app/product/19c/tfa/
repository/collection_Tue_Mar_12_16_38_47_PDT_2019_node_all
/scratch/app/product/19c/tfa/repository/
collection_Tue_Mar_12_16_38_47_PDT_2019_node_all/
node1.tfa_Tue_Mar_12_16_38_47_PDT_2019.zip


$ tfactl diagcollect
Choose the event you want to perform a diagnostic collection for:
1. Mar/12/2019 16:08:20 [ db.orcl.orcl ]  ORA-04030: out of process
memory when trying to allocate
2. Mar/12/2019 16:08:18 [ db.orcl.orcl ]  ORA-04031: unable to
allocate 8 bytes of shared memory
3. Mar/12/2019 16:08:16 [ db.orcl.orcl ]  ORA-00494: enqueue held
for too long more than seconds by osid
4. Mar/12/2019 16:08:14 [ db.orcl.orcl ]  ORA-29709: Communication
failure with Cluster Synchronization
5. Mar/12/2019 16:08:04 [ db.orcl.orcl ]  ORA-29702: error occurred
```

```
in Cluster Group Service operation
6. Mar/12/2019 16:07:59 [ db.orcl.orcl ]  ORA-32701: Possible hangs up to
hang ID= detected
7. Mar/12/2019 16:07:51 [ db.orcl.orcl ]  ORA-07445: exception
encountered: core dump [] [] [] [] [] []
8. Mar/12/2019 16:07:49 [ db.orcl.orcl ]  ORA-00700: soft internal error,
arguments: [700], [], [],[]
9. Mar/11/2019 22:02:19 [ db.oradb.oradb ]  DIA0 Critical Database
Process Blocked: Hang ID 1 blocks 5 sessions
10. Default diagnostic collection, for no specific event

Please choose the event : 1-10 [] 1
User root does not have permissions to run SRDC 'ora4030' for database
'orcl'.
```

2. To run a diagnostic collection for a specific event that does not have an SRDC:

   ```
   tfactl diagcollect
   ```

   For example:

   ```
   $ tfactl diagcollect
   Choose the event you want to perform a diagnostic collection for:
   1. Mar/12/2019 16:08:20 [ db.orcl.orcl ]  ORA-04030: out of process
   memory when trying to allocate
   2. Mar/12/2019 16:08:18 [ db.orcl.orcl ]  ORA-04031: unable to allocate 8
   bytes of shared memory
   3. Mar/12/2019 16:08:16 [ db.orcl.orcl ]  ORA-00494: enqueue held for too
   long more than seconds by osid
   4. Mar/12/2019 16:08:14 [ db.orcl.orcl ]  ORA-29709: Communication
   failure with Cluster Synchronization
   5. Mar/12/2019 16:08:04 [ db.orcl.orcl ]  ORA-29702: error occurred in
   Cluster Group Service operation
   6. Mar/12/2019 16:07:59 [ db.orcl.orcl ]  ORA-32701: Possible hangs up to
   hang ID= detected
   7. Mar/12/2019 16:07:51 [ db.orcl.orcl ]  ORA-07445: exception
   encountered: core dump [] [] [] [] [] []
   8. Mar/12/2019 16:07:49 [ db.orcl.orcl ]  ORA-00700: soft internal error,
   arguments: [700], [], [],[]
   9. Mar/11/2019 22:02:19 [ db.oradb.oradb ]  DIA0 Critical Database
   Process Blocked: Hang ID 1 blocks 5 sessions
   10. Default diagnostic collection, for no specific event

   Please choose the event : 1-10 [] 9
   Collecting data for all nodes
   Scanning files from mar/11/2019 18:02:19 to mar/11/2019 23:02:19

   Collection Id : 20190312162708node1

   Detailed Logging at : /scratch/app/product/19c/tfa/repository/
   collection_Tue_Mar_12_16_27_09_PDT_2019_node_all/
   diagcollect_20190312162708_node1.log
   2019/03/12 16:27:12 PDT : NOTE : Any file or directory name containing
   the string .com will be renamed to replace .com with dotcom
   ```

```
2019/03/12 16:27:12 PDT : Collection Name :
tfa_Tue_Mar_12_16_27_09_PDT_2019.zip
2019/03/12 16:27:12 PDT : Collecting diagnostics from hosts :
[node1]
2019/03/12 16:27:12 PDT : Scanning of files for Collection in
progress...
2019/03/12 16:27:12 PDT : Collecting additional diagnostic
information...
2019/03/12 16:27:17 PDT : Getting list of files satisfying time
range [03/11/2019 18:02:19 PDT, 03/11/2019 23:02:19 PDT]
2019/03/12 16:27:23 PDT : Collecting ADR incident files...
2019/03/12 16:27:28 PDT : Completed collection of additional
diagnostic information...
2019/03/12 16:27:33 PDT : Completed Local Collection
.-------------------------------------.
|         Collection Summary          |
+----------+-----------+------+------+
| Host     | Status    | Size | Time |
+----------+-----------+------+------+
| node1 | Completed | 10MB |  21s |
'----------+-----------+------+------'

Logs are being collected to: /scratch/app/product/19c/tfa/
repository/collection_Tue_Mar_12_16_27_09_PDT_2019_node_all
/scratch/app/product/19c/tfa/repository/
collection_Tue_Mar_12_16_27_09_PDT_2019_node_all/
node1.tfa_Tue_Mar_12_16_27_09_PDT_2019.zip
```

3. To run a diagnostic collection for a specific event that has an SRDC:

> **Note:**
>
> When choosing an SRDC the user running the collection needs to be in the `dba` group of the database chosen in the event.

```
tfactl diagcollect
```

For example:

```
$ tfactl diagcollect
Choose the event you want to perform a diagnostic collection for:
1. Mar/12/2019 16:08:20 [ db.orcl.orcl ]  ORA-04030: out of process
memory when trying to allocate
2. Mar/12/2019 16:08:18 [ db.orcl.orcl ]  ORA-04031: unable to
allocate 8 bytes of shared memory
3. Mar/12/2019 16:08:16 [ db.orcl.orcl ]  ORA-00494: enqueue held
for too long more than seconds by osid
4. Mar/12/2019 16:08:14 [ db.orcl.orcl ]  ORA-29709: Communication
failure with Cluster Synchronization
5. Mar/12/2019 16:08:04 [ db.orcl.orcl ]  ORA-29702: error occurred
in Cluster Group Service operation
6. Mar/12/2019 16:07:59 [ db.orcl.orcl ]  ORA-32701: Possible hangs
```

```
up to hang ID= detected
7. Mar/12/2019 16:07:51 [ db.orcl.orcl ]  ORA-07445: exception
encountered: core dump [] [] [] [] [] []
8. Mar/12/2019 16:07:49 [ db.orcl.orcl ]  ORA-00700: soft internal error,
arguments: [700], [], [],[]
9. Mar/11/2019 22:02:19 [ db.oradb.oradb ]  DIA0 Critical Database
Process Blocked: Hang ID 1 blocks 5 sessions
10. Default diagnostic collection, for no specific event

Please choose the event : 1-10 [] 1
Scripts to be run by this srdc: srdc_db_sid_memorysizes_10glower.sql
srdc_db_sid_memorysizes_11gplus.sql ipspack
Components included in this srdc: OS DATABASE CHMOS
Collecting data for local node(s)
Scanning files from Mar/12/2019 14:08:20 to Mar/12/2019 18:08:20
WARNING: End time entered is after the current system time.

Collection Id : 20190312163524node1

Detailed Logging at : /scratch/app/product/19c/tfa/repository/
srdc_ora4030_collection_Tue_Mar_12_16_35_25_PDT_2019_node_local/
diagcollect_20190312163524_node1.log
2019/03/12 16:35:30 PDT : NOTE : Any file or directory name containing
the string .com will be renamed to replace .com with dotcom
2019/03/12 16:35:30 PDT : Collection Name :
tfa_srdc_ora4030_Tue_Mar_12_16_35_25_PDT_2019.zip
2019/03/12 16:35:30 PDT : Scanning of files for Collection in progress...
2019/03/12 16:35:30 PDT : Collecting additional diagnostic information...
2019/03/12 16:35:35 PDT : Getting list of files satisfying time range
[03/12/2019 14:08:20 PDT, 03/12/2019 16:35:30 PDT]
2019/03/12 16:35:49 PDT : Collecting ADR incident files...
2019/03/12 16:35:52 PDT : Completed collection of additional diagnostic
information...
2019/03/12 16:35:54 PDT : Completed Local Collection
.-------------------------------------.
|          Collection Summary          |
+-----------+-----------+-------+------+
| Host      | Status    | Size  | Time |
+-----------+-----------+-------+------+
| node1 | Completed | 2.9MB |  24s |
'-----------+-----------+-------+------'

Logs are being collected to: /scratch/app/product/19c/tfa/repository/
srdc_ora4030_collection_Tue_Mar_12_16_35_25_PDT_2019_node_local
/scratch/app/product/19c/tfa/repository/
srdc_ora4030_collection_Tue_Mar_12_16_35_25_PDT_2019_node_local/
node1.tfa_srdc_ora4030_Tue_Mar_12_16_35_25_PDT_2019.zip
```

4.3.9.3 Excluding Large Files from Diagnostic Collection

Prevent excessively large files from delaying or stalling collections.

Run the `tfactl set` *`maxfilecollectionsize`* for the diagnostic collection command to consider only the last 200 KB for the files that are larger than the size specified.

1. To set the maximum file size:

   ```
   tfactl set maxfilecollectionsize=size_in_MB
   ```

2. To collect diagnostic data:

   ```
   tfactl diagcollect
   ```

4.3.9.4 Collecting from Specific Nodes

To collect from specific nodes:

- To collect from specific nodes:

  ```
  tfactl diagcollect -node list of nodes
  ```

  For example:

  ```
  $ tfactl diagcollect -last 1d -node myserver65
  ```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.5 Collecting from Specific Components

To collect from specific components:

- To collect from specific components:

  ```
  tfactl diagcollect component
  ```

  For example:

  To trim and collect all files from the databases *hrdb* and *fdb* in the last 1 day:

  ```
  tfactl -diagcollect -database hrdb,fdb -last 1d
  ```

  To trim and collect all Oracle Clusterware files, operating system logs, and CHMOS/OSW data from *node1* and *node2* updated in the last 6 hours:

  ```
  tfactl diagcollect -crs -os -node node1,node2 -last 6h
  ```

To trim and collect all Oracle ASM logs from *node1* updated between from and to time:

```
tfactl diagcollect -asm -node node1 -from "2016-08-15" -to "2016-08-17"
```

Following are the available component options.

Table 4-12 Component Options

Component Option	Description
`-cha`	Collects Oracle Cluster Health Advisor logs.
`-ips`	Collects Incident Packaging Service logs.
`-database` *database_names*	Collects database logs from databases specified in a comma-separated list.
`-asm`	Collects Oracle ASM logs.
`-crsclient`	Collects Client Logs that are under `GIBASE/diag/clients`.
`-dbclient`	Collects Client Logs that are under `DB ORABASE/diag/clients`.
`-dbwlm`	Collects Database Workload Management (DBWLM) logs.
`-tns`	Collects TNS logs.
`-rhp`	Collects Rapid Home Provisioning (RHP) logs.
`-procinfo`	Collects `Gathers stack` and `fd` from `/proc` for all processes.
`-afd`	Collects AFD logs.
`-crs`	Collects Oracle Clusterware logs.
`-wls`	Collects Oracle WebLogic Server (WLS) logs.
`-emagent`	Collects Oracle Enterprise Manager Agent (EMAGENT) logs.
`-oms`	Collects Oracle Management Service (OMS) logs.
`-ocm`	Collects Oracle Configuration Manager (OCM) logs.
`-emplugins`	Collects Oracle Enterprise Manager Plug-ins (EMPLUGINS) logs.
`-em`	Collects Oracle Enterprise Manager (EM) logs.
`-acfs`	Oracle Advanced Cluster File System (Oracle ACFS).
`-install`	Collects Oracle Installation related files.
`-cfgtools`	Collects configuration tools logs.
`-os`	Collects operating system files such as `/var/log/messages` and `/var/log/exadatatmp/*netdiag*` files only on Exadata systems.
`-ashhtml`	Collects Generate Active Session History (ASH) HTML report.
`-ashtext`	Collects Generate Active Session History (ASH) text report.
`-awrhtml`	Collects Automatic Workload Repository (AWR) HTML logs.
`-awrtext`	Collects Automatic Workload Repository (AWR) text report.
`-avs`	Collects Audit Vault Server logs.

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.6 Collecting from Specific Directories

Oracle Trace File Analyzer discovers all Oracle diagnostics and collects relevant files based on the type and last time updated.

If you want to collect other files, then you can specify extra directories. Oracle Trace File Analyzer collects only the files updated in the relevant time range (one hour by default).

You can configure collection of all files irrespective of the time last updated. Configure on a directory by directory basis using the `-collectall` option.

To collect from specific directories:

1. To include all files updated in the last one hour:

   ```
   tfactl diagcollect -collectdir dir1,dir2,...dirn
   ```

   For example:

   To trim and collect all Oracle Clusterware files updated in the last one hour as well as all files from `/tmp_dir1` and `/tmp_dir2` at the initiating node:

   ```
   $ tfactl diagcollect -crs -collectdir /tmp_dir1,/tmpdir_2
   ```

2. To configure Oracle Trace File Analyzer to collect all files from a directory, first configure it with the `-collectall` option:

   ```
   $ tfactl add dir -collectall
   ```

   or

   ```
   tfactl modify dir -collectall
   ```

   Start a diagnostic collection using the `-collectalldirs` option:

   ```
   $ tfactl diagcollect -collectalldirs
   ```

   > **Note:**
   >
   > If the `-collectalldirs` option is not used normal, then the file type, name, and time range restrictions are applied.

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.7 Changing the Collection Name

Oracle Trace File Analyzer zips collections and puts the zip files in the repository directory using the following naming format:

```
repository/collection_date_time/node_all/node.tfa_date_time.zip
```

You must only change the name of the zipped files using the following options. Manually changing the file name prevents you from using collections with various Oracle Support self-service tools.

To change the collection name:

1. To use your own naming to organize collections:

   ```
   -tag tagname
   ```

   The files are collected into *tagname* directory inside the repository.
2. To rename the `zip` file:

   ```
   -z zip name
   ```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.8 Preventing Copying Zip Files and Trimming Files

By default, Oracle Trace File Analyzer Collector:

- Copies back all zip files from remote notes to the initiating node
- Trims files around the relevant time

To prevent copying zip files and trimming files:

1. To prevent copying the zip file back to the initiating node:

   ```
   -nocopy
   ```

   For example:

   ```
   $ tfactl diagcollect -last 1d -nocopy
   ```

2. To avoid trimming files:

   ```
   -notrim
   ```

   For example:

   ```
   $ tfactl diagcollect -last 1d -notrim
   ```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.9 Performing Silent Collection

- To initiate a silent collection:

  ```
  -silent
  ```

  The `diagcollect` command is submitted as a background process.

  For example:

  ```
  $ tfactl diagcollect -last 1d -silent
  ```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.10 Collecting Core Files

- To collect core files:

  ```
  -cores
  ```

  For example:

  ```
  $ tfactl diagcollect -last 1d -cores
  ```

Related Topics

- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

4.3.9.11 Collecting Incident Packaging Service (IPS) Packages

Incident Packaging Service packages details of problems stored by Oracle Database in ADR for later diagnosis.

Oracle Trace File Analyzer runs IPS to query and collect these packages.

Syntax

```
tfactl ips option
```

Table 4-13 tfactl ips Command Parameters

Command	Description
`tfactl ips`	Runs the IPS.
`tfactl ips show incidents`	Shows all IPS incidents.
`tfactl ips show problems`	Shows all IPS problems.
`tfactl ips show package`	Shows all IPS Packages.
`tfactl diagcollect -ips -h`	Shows all available `diagcollect` IPS options.
`tfactl diagcollect -ips`	Performs an IPS collection following prompts. You can use all the standard `diagcollect` options to limit the scope of IPS collection.
`tfactl diagcollect -ips -adrbasepath adr_base -adrhomepath adr_home`	Performs an IPS collection in silent mode.
`tfactl diagcollect -ips -incident incident_id`	Collects ADR details about a specific incident id.
`tfactl diagcollect -ips -problem problem_id`	Collect ADR details about a specific problem id.

You can change the contents of the IPS package. Use the following options:

1. Start the collection.
2. Suspend the collection using the `-manageips` option.

   For example:

   ```
   $ tfactl diagcollect -ips -incident incident_id -manageips -node local
   ```

3. Find the suspended collection using the `print suspendedips` option.

   For example:

   ```
   $ tfactl print suspendedips
   ```

4. Manipulate the package.
5. Resume the collection using the `-resumeips` option.

For example:

```
$ tfactl diagcollect -resumeips collection_id
```

Related Topics

- tfactl ips
  Use the `tfactl ips` command to collect Automatic Diagnostic Repository diagnostic data.

4.3.10 Limit the Maximum Amount of Memory Used by Oracle Trace File Analyzer

You can now limit the amount of memory used by Oracle Trace File Analyzer.

> **Note:**
>
> This feature is available only on Linux and only when Autonomous Health Framework is installed using a full installation by the `root` user.

Memory can be limited between 150 MB and 2GB or 25% of system memory, whichever is lower. By default, memory limits are enabled and set to the maximum.

There are various use cases including the following when Oracle Trace File Analyzer resource limits apply:

- When Oracle Trace File Analyzer is performing automatic diagnostic collections, for example, when Oracle Trace File Analyzer detects an `ORA-600` error has occurred and collects diagnostics for it.
- When running on-demand collections, for example, if you run an SRDC collection at the request of support.
- During any other Oracle Trace File Analyzer analysis such as using the `tfactl analyze` command to search logs for recent errors.

Memory can be limited at either the system level using `ahfctl setresourcelimit -resource kmem` or combined system and swap memory using `ahfctl setresourcelimit -resource swmem`

For example:

To limit the memory usage to only 1 GB of system memory run:

```
ahfctl setresourcelimit -resource kmem -value 1024
```

Alternatively, to limit the combined total of system memory and the swap memory to 2 GB run:

```
ahfctl setresourcelimit -resource swmem -value 2048
```

Related Topics

- ahfctl getresourcelimit
  Use the `ahfctl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.
- ahfctl setresourcelimit
  Use the `ahfctl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.
- ahfctl unsetresourcelimit
  Use the `ahfctl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.

4.3.11 Limit Oracle Trace File Analyzer's CPU Usage

On Linux the CPU usage of Oracle Trace File Analyzer can be limited with the command `ahfctl setresourcelimit [-value value]`

For example to limit Oracle Trace File Analyzer to a maximum of 50% of a single CPU use: `ahfctl setresourcelimit -value 0.5`

CPU resource limits for Oracle Trace File Analyzer can be set between a minimum of 0.5 and maximum of 4 or 75% of available CPUs, whichever is lower. By default, the Oracle Trace File Analyzer CPU limit is set to the maximum.

Related Topics

- ahfctl getresourcelimit
  Use the `ahfctl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.
- ahfctl setresourcelimit
  Use the `ahfctl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.
- ahfctl unsetresourcelimit
  Use the `ahfctl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.

Related Topics

- tfactl setresourcelimit
  Use the `tfactl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.
- tfactl getresourcelimit
  Use the `tfactl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.
- tfactl unsetresourcelimit
  Use the `tfactl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.

4.4 Proactively Detecting and Diagnosing Performance Issues for Oracle RAC

Oracle Cluster Health Advisor provides system and database administrators with early warning of pending performance issues, and root causes and corrective actions for Oracle RAC databases and cluster nodes. Use Oracle Cluster Health Advisor to increase availability and performance management.

Oracle Cluster Health Advisor estimates an expected value of an observed input based on the default model, which is a trained calibrated model based on a normal operational period of the target system. Oracle Cluster Health Advisor then performs anomaly detection for each input based on the difference between observed and expected values. If sufficient inputs associated with a specific problem are abnormal, then Oracle Cluster Health Advisor raises a warning and generates an immediate targeted diagnosis and corrective action.

Oracle Cluster Health Advisor also sends warning messages to Enterprise Manager Cloud Control using the Oracle Clusterware event notification protocol.

The ability of Oracle Cluster Health Advisor to detect performance and availability issues on Oracle Exadata systems has been improved in this release.

With the Oracle Cluster Health Advisor support for Oracle Solaris, you can now get early detection and prevention of performance and availability issues in your Oracle RAC database deployments.

For more information on *Installing Grid Infrastructure Management Repository*, see *Oracle® Grid Infrastructure Grid Infrastructure Installation and Upgrade Guide 20c for Linux*.

- Oracle Cluster Health Advisor Architecture
  Oracle Cluster Health Advisor runs as a highly available cluster resource, `ochad`, on each node in the cluster.
- Removing Grid Infrastructure Management Repository
  GIMR is desupported in Oracle Database 23c. If GIMR is configured in your existing Oracle Grid Infrastructure installation, then remove the GIMR.
- Monitoring the Oracle Real Application Clusters (Oracle RAC) Environment with Oracle Cluster Health Advisor
  Oracle Cluster Health Advisor is automatically provisioned on each node by default when Oracle Grid Infrastructure is installed for Oracle Real Application Clusters (Oracle RAC) or Oracle RAC One Node database.
- Using Cluster Health Advisor for Health Diagnosis
  Oracle Cluster Health Advisor raises and clears problems autonomously.
- Calibrating an Oracle Cluster Health Advisor Model for a Cluster Deployment
  As shipped with default node and database models, Oracle Cluster Health Advisor is designed not to generate false warning notifications.
- Viewing the Details for an Oracle Cluster Health Advisor Model
  Use the `chactl query model` command to view the model details.

- Managing the Oracle Cluster Health Advisor Repository
  Oracle Cluster Health Advisor repository stores the historical records of cluster host problems, database problems, and associated metric evidence, along with models.
- Viewing the Status of Cluster Health Advisor
  SRVCTL commands are the tools that offer total control on managing the life cycle of Oracle Cluster Health Advisor as a highly available service.
- Enhanced Cluster Health Advisor Support for Oracle Pluggable Databases
  The Cluster Health Advisor (CHA) diagnostic capabilities have been extended to support 4K PDBs, up from 256 in Oracle Database 23c.

Related Topics

- Installing Grid Infrastructure Management Repository

4.4.1 Oracle Cluster Health Advisor Architecture

Oracle Cluster Health Advisor runs as a highly available cluster resource, `ochad`, on each node in the cluster.

Each Oracle Cluster Health Advisor daemon (`ochad`) monitors the operating system on the cluster node and optionally, each Oracle Real Application Clusters (Oracle RAC) database instance on the node.

The `ochad` daemon receives operating system metric data from the Cluster Health Monitor and gets Oracle RAC database instance metrics from a memory-mapped file. The daemon does not require a connection to each database instance. This data, along with the selected model, is used in the Health Prognostics Engine of Oracle Cluster Health Advisor for both the node and each monitored database instance in order to analyze their health multiple times a minute.

4.4.2 Removing Grid Infrastructure Management Repository

GIMR is desupported in Oracle Database 23c. If GIMR is configured in your existing Oracle Grid Infrastructure installation, then remove the GIMR.

1. As the `grid` user, log in to any cluster node and create a new directory owned by `grid` to store the GIMR deletion script.

   ```
   mkdir -p $ORACLE_HOME/gimrdel
   chown grid:oinstall $ORACLE_HOME/gimrdel
   ```

2. Download `scriptgimr.zip` from the My Oracle Support Note 2972418.1 to the `$ORACLE_HOME/gimrdel` directory.
3. Extract the `reposScript.sh` script from the `scriptgimr.zip` and ensure that the `grid` user has read and execute permissions on the `reposScript.sh` script.

   ```
   unzip -q $ORACLE_HOME/gimrdel/scriptgimr.zip
   ```

4. Query and export the CHA user models.

   ```
   Grid_home/bin/chactl query model
   Grid_home/bin/chactl export model -name model_name -file model_name.svm
   ```

5. Run the `reposScript.sh` script, in delete mode, from the `/gimrdel` directory.

   ```
   $ORACLE_HOME/gimrdel/reposScript.sh -mode="Delete"
   ```

Related Topics

- My Oracle Support Note 2972418.1

4.4.3 Monitoring the Oracle Real Application Clusters (Oracle RAC) Environment with Oracle Cluster Health Advisor

Oracle Cluster Health Advisor is automatically provisioned on each node by default when Oracle Grid Infrastructure is installed for Oracle Real Application Clusters (Oracle RAC) or Oracle RAC One Node database.

Oracle Cluster Health Advisor does not require any additional configuration.

When Oracle Cluster Health Advisor detects an Oracle Real Application Clusters (Oracle RAC) or Oracle RAC One Node database instance as running, Oracle Cluster Health Advisor autonomously starts monitoring the cluster nodes. Use CHACTL while logged in as the Grid user to turn on monitoring of the database.

To monitor the Oracle Real Application Clusters (Oracle RAC) environment:

1. To monitor a database, run the following command:

   ```
   $ chactl monitor database -db db_unique_name
   ```

   Oracle Cluster Health Advisor monitors all instances of the Oracle Real Application Clusters (Oracle RAC) or Oracle RAC One Node database using the default model. Oracle Cluster Health Advisor cannot monitor single-instance Oracle databases, even if the single-instance Oracle databases share the same cluster as Oracle Real Application Clusters (Oracle RAC) databases.

   Each database instance is monitored independently both across Oracle Real Application Clusters (Oracle RAC) database nodes and when more than one database run on a single node.

2. To stop monitoring a database, run the following command:

   ```
   $ chactl unmonitor database -db db_unique_name
   ```

   Oracle Cluster Health Advisor stops monitoring all instances of the specified database. However, Oracle Cluster Health Advisor does not delete any data or problems until it is aged out beyond the retention period.

3. To check monitoring status of all cluster nodes and databases, run the following command:

   ```
   $ chactl status
   ```

   Use the `-verbose` option to see more details, such as the models used for the nodes and each database.

4.4.4 Using Cluster Health Advisor for Health Diagnosis

Oracle Cluster Health Advisor raises and clears problems autonomously.

The Oracle Grid Infrastructure user can query the stored information using CHACTL.

To query the diagnostic data:

1. To query currently open problems, run the following command:

   ```
   chactl query diagnosis -db db_unique_name -start time -end time
   ```

   In the syntax example, *db_unique_name* is the name of your database instance. You also specify the start time and end time for which you want to retrieve data. Specify date and time in the `YYYY-MM-DD HH24:MI:SS` format.

2. Use the `-htmlfile` *`file_name`* option to save the output in HTML format.

Example 4-5 Cluster Health Advisor Output Examples in Text and HTML Format

This example shows the default text output for the `chactl query diagnosis` command for a database named *`oltpacbd`*.

```
$ chactl query diagnosis -db oltpacdb -start "2016-02-01 02:52:50" -end
"2016-02-01 03:19:15"
2016-02-01 01:47:10.0  Database oltpacdb  DB Control File IO Performance
(oltpacdb_1) [detected]
2016-02-01 01:47:10.0  Database oltpacdb  DB Control File IO Performance
(oltpacdb_2) [detected]
2016-02-01 02:52:15.0  Database oltpacdb  DB CPU Utilization (oltpacdb_2)
[detected]
2016-02-01 02:52:50.0  Database oltpacdb  DB CPU Utilization (oltpacdb_1)
[detected]
2016-02-01 02:59:35.0  Database oltpacdb  DB Log File Switch (oltpacdb_1)
[detected]
2016-02-01 02:59:45.0  Database oltpacdb  DB Log File Switch (oltpacdb_2)
[detected]

Problem: DB Control File IO Performance
Description: CHA has detected that reads or writes to the control files are
slower than expected.
Cause: The Cluster Health Advisor (CHA) detected that reads or writes to the
control files were slow
because of an increase in disk IO.
The slow control file reads and writes may have an impact on checkpoint and
Log Writer (LGWR) performance.
Action: Separate the control files from other database files and move them
to faster disks or Solid State Devices.

Problem: DB CPU Utilization
Description: CHA detected larger than expected CPU utilization for this
database.
Cause: The Cluster Health Advisor (CHA) detected an increase in database CPU
utilization
```

```
because of an increase in the database workload.
Action: Identify the CPU intensive queries by using the Automatic
Diagnostic and Defect Manager (ADDM) and
follow the recommendations given there. Limit the number of CPU
intensive queries or
relocate sessions to less busy machines. Add CPUs if the CPU capacity
is insufficent to support
the load without a performance degradation or effects on other
databases.

Problem: DB Log File Switch
Description: CHA detected that database sessions are waiting longer
than expected for log switch completions.
Cause: The Cluster Health Advisor (CHA) detected high contention
during log switches
because the redo log files were small and the redo logs switched
frequently.
Action: Increase the size of the redo logs.
```

The timestamp displays date and time when the problem was detected on a specific host or database.

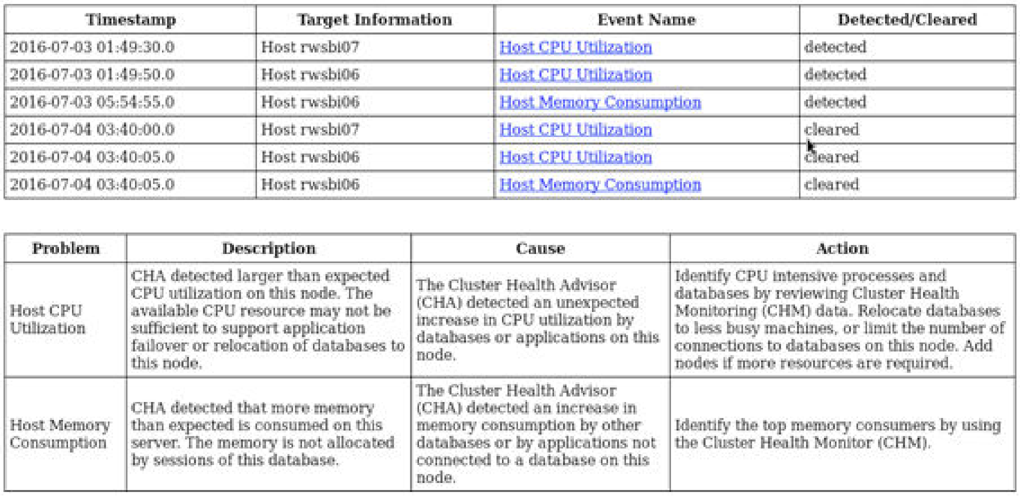
Note:

The same problem can occur on different hosts and at different times, yet the diagnosis shows complete details of the problem and its potential impact. Each problem also shows targeted corrective or preventive actions.

Here is an example of what the output looks like in the HTML format.

```
$ chactl query diagnosis -start "2016-07-03 20:50:00" -end "2016-07-04
03:50:00" -htmlfile ~/chaprob.html
```

Figure 4-5 Cluster Health Advisor Diagnosis HTML Output



Timestamp	Target Information	Event Name	Detected/Cleared
2016-07-03 01:49:30.0	Host rwsbi07	Host CPU Utilization	detected
2016-07-03 01:49:50.0	Host rwsbi06	Host CPU Utilization	detected
2016-07-03 05:54:55.0	Host rwsbi06	Host Memory Consumption	detected
2016-07-04 03:40:00.0	Host rwsbi07	Host CPU Utilization	cleared
2016-07-04 03:40:05.0	Host rwsbi06	Host CPU Utilization	cleared
2016-07-04 03:40:05.0	Host rwsbi06	Host Memory Consumption	cleared

Problem	Description	Cause	Action
Host CPU Utilization	CHA detected larger than expected CPU utilization on this node. The available CPU resource may not be sufficient to support application failover or relocation of databases to this node.	The Cluster Health Advisor (CHA) detected an unexpected increase in CPU utilization by databases or applications on this node.	Identify CPU intensive processes and databases by reviewing Cluster Health Monitoring (CHM) data. Relocate databases to less busy machines, or limit the number of connections to databases on this node. Add nodes if more resources are required.
Host Memory Consumption	CHA detected that more memory than expected is consumed on this server. The memory is not allocated by sessions of this database.	The Cluster Health Advisor (CHA) detected an increase in memory consumption by other databases or by applications not connected to a database on this node.	Identify the top memory consumers by using the Cluster Health Monitor (CHM).

4.4.5 Calibrating an Oracle Cluster Health Advisor Model for a Cluster Deployment

As shipped with default node and database models, Oracle Cluster Health Advisor is designed not to generate false warning notifications.

You can increase the sensitivity and accuracy of the Oracle Cluster Health Advisor models for a specific workload using the `chactl calibrate` command.

Oracle recommends that a minimum of 6 hours of data be available and that both the cluster and databases use the same time range for calibration.

The `chactl calibrate` command analyzes a user-specified time interval that includes all workload phases operating normally. This data is collected while Oracle Cluster Health Advisor is monitoring the cluster and all the databases for which you want to calibrate.

1. To check if sufficient data is available, run the `query calibration` command.

   > **Note:**
   >
   > The `query calibration` command is supported only with GIMR. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.

   If 720 or more records are available, then Oracle Cluster Health Advisor successfully performs the calibration. The calibration function may not consider some data records to be normally occurring for the workload profile being used. In this case, filter the data by using the `KPISET` parameters in both the `query calibration` command and the `calibrate` command.

   For example:

   ```
   $ chactl query calibration -db oltpacdb -timeranges
   'start=2016-07-26 01:00:00,end=2016-07-26 02:00:00,start=2016-07-26
   03:00:00,end=2016-07-26 04:00:00'
   -kpiset 'name=CPUPERCENT min=20 max=40, name=IOTHROUGHPUT min=500
   max=9000' -interval 2
   ```

2. Start the calibration and store the model under a user-specified name for the specified date and time range.

   For example:

   ```
   $ chactl calibrate cluster -model weekday -timeranges ‘start=2016-07-03
   20:50:00,end=2016-07-04 15:00:00’
   ```

3. Use the new model to monitor the cluster as follows:

   For example:

   ```
   $ chactl monitor cluster -model weekday
   ```

Example 4-6 Output for the chactl query calibrate command

```
Database name : oltpacdb
Start time : 2016-07-26 01:03:10
End time : 2016-07-26 01:57:25
Total Samples : 120
Percentage of filtered data : 8.32%
The number of data samples may not be sufficient for calibration.

1) Disk read (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
4.96      0.20      8.98      0.06      25.68

<25       <50       <75       <100      >=100
97.50%    2.50%     0.00%     0.00%     0.00%

2) Disk write (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
27.73     9.72      31.75     4.16      109.39

<50       <100      <150      <200      >=200
73.33%    22.50%    4.17%     0.00%     0.00%

3) Disk throughput (ASM) (IO/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
2407.50   1500.00   1978.55   700.00    7800.00

<5000     <10000    <15000    <20000    >=20000
83.33%    16.67%    0.00%     0.00%     0.00%

4) CPU utilization (total) (%)

MEAN      MEDIAN    STDDEV    MIN       MAX
21.99     21.75     1.36      20.00     26.80

<20       <40       <60       <80       >=80
0.00%     100.00%   0.00%     0.00%     0.00%

5) Database time per user call (usec/call)

MEAN      MEDIAN    STDDEV    MIN       MAX
267.39    264.87    32.05     205.80    484.57

<10000000  <20000000  <30000000  <40000000  <50000000  <60000000
<70000000  >=70000000
100.00%   0.00%     0.00%     0.00%     0.00%     0.00%     0.00%
0.00%

Database name : oltpacdb
Start time : 2016-07-26 03:00:00
End time : 2016-07-26 03:53:30
Total Samples : 342
```

```
Percentage of filtered data : 23.72%
The number of data samples may not be sufficient for calibration.

1) Disk read (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
12.18     0.28      16.07     0.05      60.98

<25       <50       <75       <100      >=100
64.33%    34.50%    1.17%     0.00%     0.00%

2) Disk write (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
57.57     51.14     34.12     16.10     135.29

<50       <100      <150      <200      >=200
49.12%    38.30%    12.57%    0.00%     0.00%

3) Disk throughput (ASM) (IO/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
5048.83   4300.00   1730.17   2700.00   9000.00

<5000     <10000    <15000    <20000    >=20000
63.74%    36.26%    0.00%     0.00%     0.00%

4) CPU utilization (total) (%)

MEAN      MEDIAN    STDDEV    MIN       MAX
23.10     22.80     1.88      20.00     31.40

<20       <40       <60       <80       >=80
0.00%     100.00%   0.00%     0.00%     0.00%

5) Database time per user call (usec/call)

MEAN      MEDIAN    STDDEV    MIN       MAX
744.39    256.47    2892.71   211.45    45438.35

<10000000  <20000000  <30000000  <40000000  <50000000  <60000000  <70000000
>=70000000
100.00%   0.00%     0.00%     0.00%     0.00%     0.00%     0.00%     0.00%
```

4.4.6 Viewing the Details for an Oracle Cluster Health Advisor Model

Use the `chactl query model` command to view the model details.

- You can review the details of an Oracle Cluster Health Advisor model at any time using the `chactl query model` command.

For example:

```
$ chactl query model -name weekday
Model: weekday
Target Type: CLUSTERWARE
Version: OS12.2_V14_0.9.8
OS Calibrated on: Linux amd64
Calibration Target Name: MYCLUSTER
Calibration Date: 2016-07-05 01:13:49
Calibration Time Ranges: start=2016-07-03 20:50:00,end=2016-07-04 
15:00:00
Calibration KPIs: not specified
```

You can also rename, import, export, and delete the models.

4.4.7 Managing the Oracle Cluster Health Advisor Repository

Oracle Cluster Health Advisor repository stores the historical records of cluster host problems, database problems, and associated metric evidence, along with models.

> **Note:**
>
> Applicable only if GIMR is configured. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.

The Oracle Cluster Health Advisor repository is used to diagnose and triage periodic problems. By default, the repository is sized to retain data for 16 targets (nodes and database instances) for 72 hours. If the number of targets increase, then the retention time is automatically decreased. Oracle Cluster Health Advisor generates warning messages when the retention time goes below 72 hours, and stops monitoring and generates a critical alert when the retention time goes below 24 hours.

Use CHACTL commands to manage the repository and set the maximum retention time.

1. To retrieve the repository details, use the following command:

   ```
   $ chactl query repository
   ```

   For example, running the command mentioned earlier shows the following output:

   ```
   specified max retention time(hrs) : 72
   available retention time(hrs)     : 212
   available number of entities      : 2
   allocated number of entities      : 0
   total repository size(gb)         : 2.00
   allocated repository size(gb)     : 0.07
   ```

2. To set the maximum retention time in hours, based on the current number of targets being monitored, use the following command:

   ```
   $ chactl set maxretention -time number_of_hours
   ```

   For example:

   ```
   $ chactl set maxretention -time 80
   max retention successfully set to 80 hours
   ```

   > **Note:**
   >
   > The `maxretention` setting limits the oldest data retained in the repository, but is not guaranteed to be maintained if the number of monitored targets increase. In this case, if the combination of monitored targets and number of hours are not sufficient, then increase the size of the Oracle Cluster Health Advisor repository.

3. To increase the size of the Oracle Cluster Health Advisor repository, use the `chactl resize repository` command.

   For example, to resize the repository to support 32 targets using the currently set maximum retention time, you would use the following command:

   ```
   $ chactl resize repository –entities 32
   repository successfully resized for 32 targets
   ```

4.4.8 Viewing the Status of Cluster Health Advisor

SRVCTL commands are the tools that offer total control on managing the life cycle of Oracle Cluster Health Advisor as a highly available service.

Use SRVCTL commands to the check the status and configuration of Oracle Cluster Health Advisor service on any active hub or leaf nodes of the Oracle RAC cluster.

> **Note:**
>
> A target is monitored only if it is running and the Oracle Cluster Health Advisor service is also running on the host node where the target exists.

1. To check the status of Oracle Cluster Health Advisor service on all nodes in the Oracle RAC cluster:

   ```
   srvctl status cha [-help]
   ```

For example:

```
# srvctl status cha
Cluster Health Advisor is running on nodes racNode1, racNode2.
Cluster Health Advisor is not running on nodes racNode3, racNode4.
```

2. To check if Oracle Cluster Health Advisor service is enabled or disabled on all nodes in the Oracle RAC cluster:

   ```
   srvctl config cha [-help]
   ```

   For example:

   ```
   # srvctl config cha
   Cluster Health Advisor is enabled on nodes racNode1, racNode2.
   Cluster Health Advisor is not enabled on nodes racNode3, racNode4.
   ```

4.4.9 Enhanced Cluster Health Advisor Support for Oracle Pluggable Databases

The Cluster Health Advisor (CHA) diagnostic capabilities have been extended to support 4K PDBs, up from 256 in Oracle Database 23c.

Going forward, this is crucial for Oracle Autonomous Database deployments. CHA's problem detection and root cause analysis will be improved by considering DB events such as reconfiguration. This improves detection, analysis, and targeted preventative actions for problems such as instance evictions.

4.5 Collecting Operating System Resources Metrics

CHM is a high-performance, lightweight daemon that collects, analyzes, aggregates, and stores a large set of operating system metrics to help you diagnose and troubleshoot system issues.

Supported Platforms

Linux, Microsoft Windows, Solaris, AIX, IBM Z Series, and ARM

Why CHM is unique

CHM	Typical OS Collector
Last man standing - daemon runs memory locked, RT scheduling class ensuring consistent data collection under system load.	Inconsistent data dropouts due to scheduling delays under system load.
High fidelity data sampling rate, 5 seconds. Very low resource usage profile at 5-second sampling rates.	Running multiple utilities creates additional overhead on the system being monitored, and worsens with higher sampling rates.

CHM	Typical OS Collector
High Availability daemon, collated data collections across multiple resource categories. Highly optimized collector (data read directly from the operating system, same source as utilities).	Set of scripts/command-line utilities, for example, `top`, `ps`, `vmstat`, `iostat`, and so on re-directing their output to one or more files for every collection sample.
Collected data is collated into a system snapshot overview (**Nodeview**) on every sample, Nodeview also contains additional summarization and analysis of the collected data across multiple resource categories.	System snapshot overviews across different resource categories are very tedious to collate.
Significant inline analysis and summarization during data collection and collation into the Nodeview greatly reduces tedious, manual, time-consuming analysis to drive meaningful insights.	The analysis is time-consuming and processing-intensive as the output of various utilities across multiple files needs to be collated, parsed, interpreted, and then analyzed for meaningful insights.
Performs Clusterware-aware specific metrics collection (Process Aggregates, ASM/OCR/VD disk tagging, Private/Public NIC tagging). Also provides an extensive toolset for in-depth data analysis and visualization.	None

- Understanding Cluster Health Monitor Services
  Cluster Health Monitor uses system monitor (`osysmond`) service to collect operating system metrics.
- Collecting Cluster Health Monitor Data
  Collect Cluster Health Monitor data from any node in the cluster.
- Operating System Metrics Collected by Cluster Health Monitor
  Review the metrics collected by CHM.
- Detecting Component Failures and Self-healing Autonomously
  Improved ability to detect component failures and self-heal autonomously improves business continuity.
- Using Cluster Health Monitor from Enterprise Manager Cloud Control
  Histograms presented in real-time and historical modes enable you to understand precisely what was happening at the time of degradation or failure.

4.5.1 Understanding Cluster Health Monitor Services

Cluster Health Monitor uses system monitor (`osysmond`) service to collect operating system metrics.

About the System Monitor Service

The system monitor service (`osysmond`) is a real-time monitoring and operating system metric collection service that runs on each cluster node. The system monitor service is managed as a High Availability Services (HAS) resource.

`osysmond` persists the collected operating system metrics under a directory in ORACLE_BASE.

Metric Repository is auto-managed on the local filesystem. You can change the location and size of the repository.

- Nodeview samples are continuously written to the repository (JSON record)
- Historical data is auto-archived into hourly zip files
- Archived files are automatically purged once the default retention limit is reached (default: 200 MB)

4.5.2 Collecting Cluster Health Monitor Data

Collect Cluster Health Monitor data from any node in the cluster.

Oracle recommends that you run the `tfactl diagcollect` command to collect diagnostic data when an Oracle Clusterware error occurs.

4.5.3 Operating System Metrics Collected by Cluster Health Monitor

Review the metrics collected by CHM.

Overview of Metrics

CHM groups the operating system data collected into a **Nodeview**. A **Nodeview** is a grouping of metric sets where each metric set contains detailed metrics of a unique system resource.

Brief description of metric sets are as follows:

- **CPU metric set:** Metrics for top 127 CPUs sorted by usage percentage
- **Device metric set:** Metrics for 127 devices that include ASM/VD/OCR along with those having a high average wait time
- **Process metric set:** Metrics for 127 processes
  - Top 25 CPU consumers (idle processes not reported)
  - Top 25 Memory consumers (RSS < 1% of total RAM not reported)
  - Top 25 I/O consumers
  - Top 25 File Descriptors consumers (helps to identify top inode consumers)
  - Process Aggregation: Metrics summarized by foreground and background processes for all Oracle Database and Oracle ASM instances
- **Network metric set:** Metrics for 16 NICS that include public and private interconnects
- **NFS metric set:** Metrics for 32 NFS ordered by round trip time
- **Protocol metric set:** Metrics for protocol groups TCP, UDP, and IP
- **Filesystem metric set:** Metrics for filesystem utilization
- **Critical resources metric set:** Metrics for critical system resource utilization
  - CPU Metrics: system-wide CPU utilization statistics
  - Memory Metrics: system-wide memory statistics
  - Device Metrics: system-wide device statistics distinct from individual device metric set
  - NFS Metrics: Total NFS devices collected every 30 seconds
  - Process Metrics: system-wide unique process metrics

CPU Metric Set

Contains metrics from all CPU cores ordered by usage percentage.

Table 4-14 CPU Metric Set

Metric Name (units)	Description
system [%]	Percentage of CPU utilization occurred while running at the system level (kernel).
user [%]	Percentage of CPU utilization occurred while running at the user level (application).
usage [%]	Total utilization (**system[%]** + **user[%]**).
nice [%]	Percentage of CPU utilization occurred while running at the user level with nice priority.
ioWait [%]	Percentage of time that the CPU was idle during which the system had an outstanding disk I/O request.
steal [%]	Percentage of time spent in involuntary wait by the virtual CPU while the hypervisor was servicing another virtual processor.

Device Metric Set

Contains metrics from all disk devices/partitions ordered by their service time in milliseconds.

Table 4-15 Device Metric Set

Metric Name (units)	Description
ioR [KB/s]	Amount of data read from the device.
ioW [KB/s]	Amount of data written to the device.
numIOs [#/s]	Average disk I/O operations.
qLen [#]	Number of I/O queued requests, that is, in a wait state.
aWait [msec]	Average wait time per I/O.
svcTm [msec]	Average service time per I/O request.
util [%]	Percent utilization of the device (same as `'%util` metric from the `iostat -x` command. Represents the percentage of time device was active).

Process Metric Set

Contains multiple categories of summarized metric data computed across all system processes.

Table 4-16 Process Metric Set

Metric Name (units)	Description
pid	Process ID.

Table 4-16 (Cont.) Process Metric Set

Metric Name (units)	Description
pri	Process priority (raw value from the operating system).
psr	The processor that process is currently assigned to or running on.
pPid	Parent process ID.
nice	Nice value of the process.
state	State of the process. For example, `R->Running`, `S->Interruptible sleep`, and so on.
class	Scheduling class of the process. For example, `RR->RobinRound`, `FF->First in First out`, `B->Batch scheduling`, and so on.
fd [#]	Number of file descriptors opened by this process, which is updated every 30 seconds.
name	Name of the process.
cpu [%]	Process CPU utilization across cores. For example, 50% => 50% of single core, 400% => 100% usage of 4 cores.
thrds [#]	Number of threads created by this process.
vmem [KB]	Process virtual memory usage (KB).
shMem [KB]	Process shared memory usage (KB).
rss [KB]	Process memory-resident set size (KB).
ioR [KB/s]	I/O read in kilobytes per second.
ioW [KB/s]	I/O write in kilobytes per second.
ioT [KB/s]	I/O total in kilobytes per second.
cswch [#/s]	Context switch per second. Collected only for a few critical Oracle Database processes.
nvcswch [#/s]	Non-voluntary context switch per second. Collected only for a few critical Oracle Database processes.
cumulativeCpu [ms]	Amount of CPU used so far by the process in microseconds.

NIC Metric Set

Contains metrics from all network interfaces ordered by their total rate in kilobytes per second.

Table 4-17 NIC Metric Set

Metric Name (units)	Description
name	Name of the interface.
tag	Tag for the interface, for example, **public**, **private**, and so on.
mtu [B]	Size of the maximum transmission unit in bytes supported for the interface.
rx [Kbps]	Average network receive rate.

Table 4-17 (Cont.) NIC Metric Set

Metric Name (units)	Description
tx [Kbps]	Average network send rate.
total [Kbps]	Average network transmission rate (**rx[Kb/s]** + **tx[Kb/s]**).
rxPkt [#/s]	Average incoming packet rate.
txPkt [#/s]	Average outgoing packet rate.
pkt [#/s]	Average rate of packet transmission (**rxPkt[#/s]** + **txPkt[#/s]**).
rxDscrd [#/s]	Average rate of dropped/discarded incoming packets.
txDscrd [#/s]	Average rate of dropped/discarded outgoing packets.
rxUnicast [#/s]	Average rate of unicast packets received.
rxNonUnicast [#/s]	Average rate of multicast packets received.
dscrd [#/s]	Average rate of total discarded packets (**rxDscrd** + **txDscrd**).
rxErr [#/s]	Average error rate for incoming packets.
txErr [#/s]	Average error rate for outgoing packets.
Err [#/s]	Average error rate of total transmission (**rxErr[#/s]** + **txErr[#/s]**).

NFS Metric Set

Contains top 32 NFS ordered by round trip time. This metric set is collected once every 30 seconds.

Table 4-18 NFS Metric Set

Metric Name (units)	Description
op [#/s]	Number of read/write operations issued to a filesystem per second.
bytes [#/sec]	Number of bytes read/write per second from a filesystem.
rtt [s]	This is the duration from the time that the client's kernel sends the RPC request until the time it receives the reply.
exe [s]	This is the duration from that NFS client does the RPC request to its kernel until the RPC request is completed, this includes the RTT time above.
retrains [%]	This is the retransmission's frequency in percentage.

Protocol Metric Set

Contains specific metrics for protocol groups TCP, UDP, and IP. Metric values are cumulative since the system starts.

Table 4-19   TCP Metric Set

Metric Name (units)	Description
failedConnErr [#]	Number of times that TCP connections have made a direct transition to the **CLOSED** state from either the **SYN-SENT** state or the **SYN-RCVD** state, plus the number of times that TCP connections have made a direct transition to the **LISTEN** state from the **SYN-RCVD** state.
estResetErr [#]	Number of times that TCP connections have made a direct transition to the **CLOSED** state from either the **ESTABLISHED** state or the **CLOSE-WAIT** state.
segRetransErr [#]	Total number of TCP segments retransmitted.
rxSeg [#]	Total number of TCP segments received on TCP layer.
txSeg [#]	Total number of TCP segments sent from TCP layer.

Table 4-20   UDP Metric Set

Metric Name (units)	Description
unkPortErr [#]	Total number of received datagrams for which there was no application at the destination port.
rxErr [#]	Number of received datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
rxPkt [#]	Total number of packets received.
txPkt [#]	Total number of packets sent.

Table 4-21   IP Metric Set

Metric Name (units)	Description
ipHdrErr [#]	Number of input datagrams discarded due to errors in their IPv4 headers.
addrErr [#]	Number of input datagrams discarded because the IPv4 address in their IPv4 header's destination field was not a valid address to be received at this entity.
unkProtoErr [#]	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
reasFailErr [#]	Number of failures detected by the IPv4 reassembly algorithm.
fragFailErr [#]	Number of IPv4 discarded datagrams due to fragmentation failures.
rxPkt [#]	Total number of packets received on IP layer.
txPkt [#]	Total number of packets sent from IP layer.

Filesystem Metric Set

Contains metrics for filesystem utilization. Collected only for **GRID_HOME** filesystem.

Table 4-22   Filesystem Metric Set

Metric Name (units)	Description
mount	Mount point.
type	Filesystem type, for example, **etx4**.
tag	Filsystem tag, for example, **GRID_HOME**.
total [KB]	Total amount of space (KB).
used [KB]	Amount of used space (KB).
avbl [KB]	Amount of available space (KB).
used [%]	Percentage of used space.
ifree [%]	Percentage of free file nodes.

System Metric Set

Contains a summarized metric set of critical system resource utilization.

Table 4-23   CPU Metrics

Metric Name (units)	Description
pCpus [#]	Number of physical processing units in the system.
Cores [#]	Number of cores for all CPUs in the system.
vCpus [#]	Number of logical processing units in the system.
cpuHt	CPU Hyperthreading enabled (**Y**) or disabled (**N**).
osName	Name of the operating system.
chipName	Name of the chip of the processing unit.
system [%]	Percentage of CPUs utilization that occurred while running at the system level (kernel).
user [%]	Percentage of CPUs utilization that occurred while running at the user level (application).
usage [%]	Total CPU utilization (**system[%]** + **user[%]**).
nice [%]	Percentage of CPUs utilization occurred while running at the user level with **NICE** priority.
ioWait [%]	Percentage of time that the CPUs were idle during which the system had an outstanding disk I/O request.
Steal [%]	Percentage of time spent in involuntary wait by the virtual CPUs while the hypervisor was servicing another virtual processor.
cpuQ [#]	Number of processes waiting in the run queue within the current sample interval.
loadAvg1	Average system load calculated over time of one minute.
loadAvg5	Average system load calculated over of time of five minutes.

Table 4-23 (Cont.) CPU Metrics

Metric Name (units)	Description
loadAvg15	Average system load calculated over of time of 15 minutes. High load averages imply that a system is overloaded; many processes are waiting for CPU time.
Intr [#/s]	Number of interrupts occurred per second in the system.
ctxSwitch [#/s]	Number of context switches that occurred per second in the system.

Table 4-24 Memory Metrics

Metric Name (units)	Description
totalMem [KB]	Amount of total usable RAM (KB).
freeMem [KB]	Amount of free RAM (KB).
avblMem [KB]	Amount of memory available to start a new process without swapping.
shMem [KB]	Memory used (mostly) by **tmpfs**.
swapTotal [KB]	Total amount of physical swap memory (KB).
swapFree [KB]	Amount of swap memory free (KB).
swpIn [KB/s]	Average swap in rate within the current sample interval (KB/sec).
swpOut [KB/s]	Average swap-out rate within the current sample interval (KB/sec).
pgIn [#/s]	Average page in rate within the current sample interval (pages/sec).
pgOut [#/s]	Average page out rate within the current sample interval (pages/sec).
slabReclaim [KB]	The part of the slab that might be reclaimed such as caches.
buffer [KB]	Memory used by kernel buffers.
Cache [KB]	Memory used by the page cache and slabs.
bufferAndCache [KB]	Total size of buffer and cache (**buffer[KB]** + **Cache[KB]**).
hugePageTotal [#]	Total number of huge pages present in the system for the current sample interval.
hugePageFree [KB]	Total number of free huge pages in the system for the current sample interval.
hugePageSize [KB]	Size of one huge page in KB, depends on the operating system version. Typically the same for all samples for a particular host.

Table 4-25 Device Metrics

Metric Name (units)	Description
disks [#]	Number of disks configured in the system.
ioR [KB/s]	Aggregate read rate across all devices.

Table 4-25 (Cont.) Device Metrics

Metric Name (units)	Description
ioW [KB/s]	Aggregate write rate across all devices.
numIOs [#/s]	Aggregate I/O operation rate across all devices.

Table 4-26 NFS Metrics

Metric Name (units)	Description
nfs [#]	Total NFS devices.

Table 4-27 Process Metrics

Metric Name (units)	Description
fds [#]	Number of open file structs in system.
procs [#]	Number of processes.
rtProcs [#]	Number of real-time processes.
procsInDState	Number of processes in uninterruptible sleep.
sysFdLimit [#]	System limit on a number of file structs.
procsOnCpu [#]	Number of processes currently running on CPU.
procsBlocked [#]	Number of processes waiting for some event/ resource becomes available, such as for the completion of an I/O operation.

Process Aggregates Metric Set

Contains aggregated metrics for all processes by process groups.

Table 4-28 Process Aggregates Metric Set

Metric Name (units)	Description
DBBG	User Oracle Database background process group.
DBFG	User Oracle Database foreground process group.
MDBBG	MGMTDB background processes group.
MDBFG	MGMTDB foreground processes group.
ASMBG	ASM background processes group.
ASMFG	ASM foreground processes group.
IOXBG	IOS background processes group.
IOXFG	IOS foreground processes group.
APXBG	APX background processes group.
APXFG	APX foreground processes group.
CLUST	Clusterware processes group.
OTHER	Default group.

For each group, the below metrics are aggregated to report a group summary.

Metric Name (units)	Description
processes [#]	Total number of processes in the group.
cpu [%]	Aggregated CPU utilization.
rss [KB]	Aggregated resident set size.
shMem [KB]	Aggregated shared memory usage.
thrds [#]	Aggregated thread count.
fds [#]	Aggregated open file-descriptor.
cpuWeight [%]	Contribution of the group in overall CPU utilization of the machine.

4.5.4 Detecting Component Failures and Self-healing Autonomously

Improved ability to detect component failures and self-heal autonomously improves business continuity.

Cluster Health Monitor introduces a new diagnostic feature that identifies critical component events that indicate pending or actual failures and provides recommendations for corrective action. These actions may sometimes be performed autonomously. Such events and actions are then captured and admins are notified through components such as Oracle Trace File Analyzer.

Terms Associated with Diagnosability

CHMDiag: `CHMDiag` is a python daemon managed by `osysmond` that listens for events and takes actions. Upon receiving various events/actions, `CHMDiag` validates them for correctness, does flow control, and schedules the actions for runs. `CHMDiag` monitors each action to its completion, and kills an action if it takes longer than pre-configured time specific to that action.

This JSON file describes all events/actions and their respective attributes. All events/ actions have uniquely identifiable IDs. This file also contains various configurable properties for various actions/events. `CHMDiag` loads this file during its startup.

CRFE API: CRFE API is used by all C clients to send events to `CHMDiag`. This API is used by internal clients like components (RDBMS/CSS/GIPC) to publish events/ actions.

This API also provides support for both synchronous and asynchronous publication of events. Asynchronous publication of events is done through a background thread which will be shared by all CRFE API clients within a process.

CHMDIAG_BASE: This directory resides in `ORACLEB_BASE/`*`hostname`*`/crf/chmdiag`. This directory path contains following directories, which are populated or managed by `CHMDiag`.

- **ActionsResults:** Contains all results for all of the invoked actions with a subdirectory for each action.
- **EventsLog:** Contains a log of all the events/actions received by `CHMDiag` and the location of their respective action results. These log files are also auto-rotated after reaching a fixed size.

- **CHMDiagLog:** Contains `CHMDiag` daemon logs. Log files are auto-rotated and once they reach a specific size. Logs should have sufficient debug information to diagnose any problems that `CHMDiag` could run into.
- **Config:** Contains a run sub-directory for `CHMDiag` process `pid` file management.

New commands to query, collect, and describe CHMDiag events/actions sent by various components:

- **oclumon chmdiag description:** Use the `oclumon chmdiag description` command to get a detailed description of all the supported events and actions.
- **oclumon chmdiag query:** Use the `oclumon chmdiag query` command to query CHMDiag events/actions sent by various components and generate an HTML or a text report.
- **oclumon chmdiag collect:** Use the `oclumon chmdiag collect` command to collect all events/actions data generated by `CHMDiag` into the specified output directory location.

Related Topics

- oclumon chmdiag description
  Use the `oclumon chmdiag description` command to get a detailed description of all the supported events and actions.
- oclumon chmdiag query
  Use the `oclumon chmdiag query` command to query CHMDiag events/actions sent by various components and generate an HTML or a text report.
- oclumon chmdiag collect
  Use the `oclumon chmdiag collect` command to collect all events/actions data generated by CHMDiag into the specified output directory location. This command will primarily be used by Oracle Trace File Analyzer to collect all events/actions that fall within a problematic window.

4.5.5 Using Cluster Health Monitor from Enterprise Manager Cloud Control

Histograms presented in real-time and historical modes enable you to understand precisely what was happening at the time of degradation or failure.

The metric data from Cluster Health Monitor is available in graphical display within Enterprise Manager Cloud Control. Complete cluster views of this data are accessible from the cluster target page. Selecting the **Cluster Health Monitoring** menu item from the **Cluster** menu presents a log-in screen prompting for the Cluster Health Monitor credentials. There is a fixed EMUSER and the password is user-specified. Once the credentials are saved, you then can view Cluster Health Monitor data for the last day in overview format for the entire cluster. Metric categories are CPU, Memory, and Network.

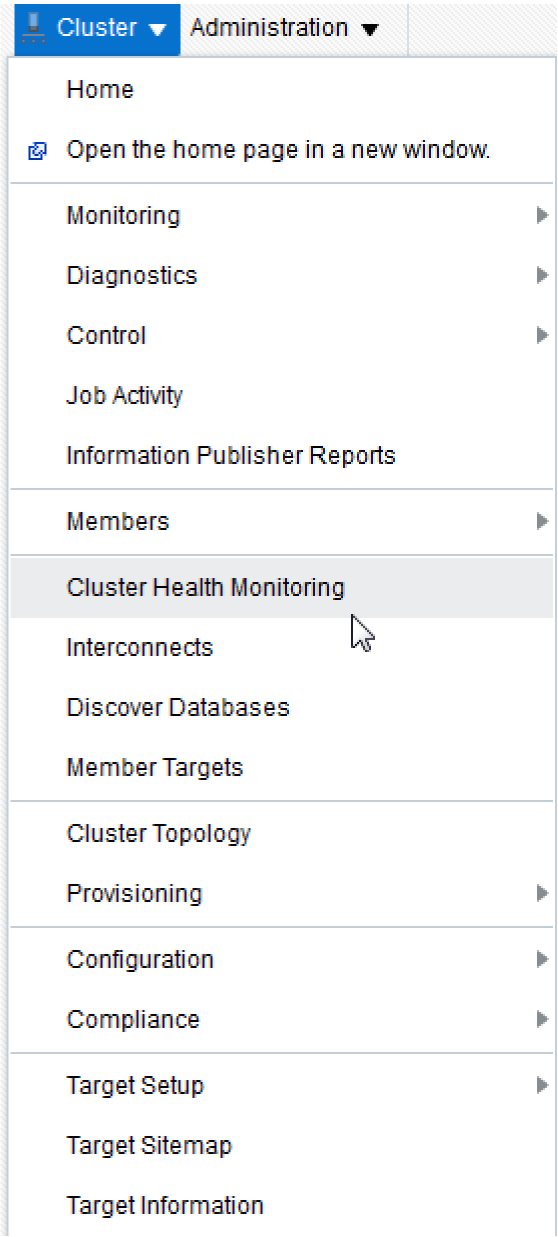
Each category is able to be separately display in greater detail showing more metrics. For example, selecting CPU results in cluster graphs detailing CPU System Usage, CPU User Usage, and CPU Queue Length. From any cluster view, you can select individual node views to more closely examine performance of a single server. As in the case of CPU, the performance of each core is displayed. Move your cursor along the graph to see a tool-tip displaying the numerical values and time stamp of that point.

Besides examining the performance of the current day, you can also review historical data. The amount of historical data is governed by the retention time configured in the Cluster Health Monitor repository in the Gird Infrastructure Management Repository and defaults to 72 hours. This view is selectable at any time by using the **View Mode** drop-down menu and selecting **Historical**. A previous date can then be entered or selected from a pop-up calendar that has dates where data is available bolded. Selecting **Show Chart** then displays the associated metrics graphs.

To view Cluster Health Monitor data:

1. Log in to Enterprise Manager Cloud Control.
2. Select the Cluster Target you want to view.
3. From the **Cluster** drop-down list, select the **Cluster Health Monitoring** option.

Figure 4-6 EMCC - Cluster Health Monitoring



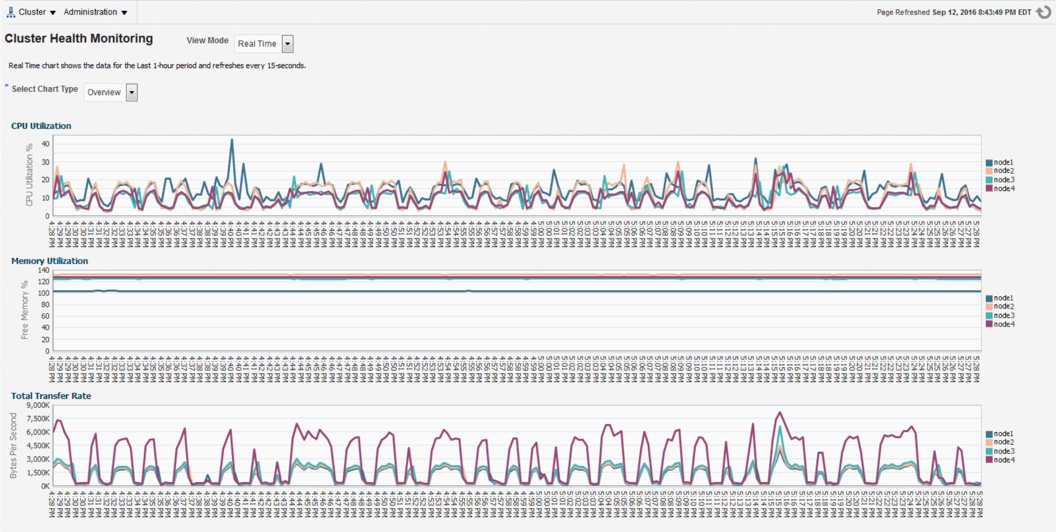
4. Enter Cluster Health Monitor login credentials.

5. From the **View Mode** drop-down list, select the **Real Time** option to view the current data.

   By default, EMCC displays the **Overview** of resource utilization. You can filter by **CPU**, **Memory**, and **Network** by selecting an appropriate option from the **Select Chart Type** drop-down list.

   While viewing CPU and Network metric graphs, click a node name on the legend to view more details.

Figure 4-7 Cluster Health Monitoring - Real Time Data



Cluster ▾ Administration ▾

Page Refreshed Sep 12, 2016 8:43:49 PM EDT

Cluster Health Monitoring

View Mode: Real Time

Real Time chart shows the data for the Last 1-hour period and refreshes every 15-seconds.

* Select Chart Type: Overview

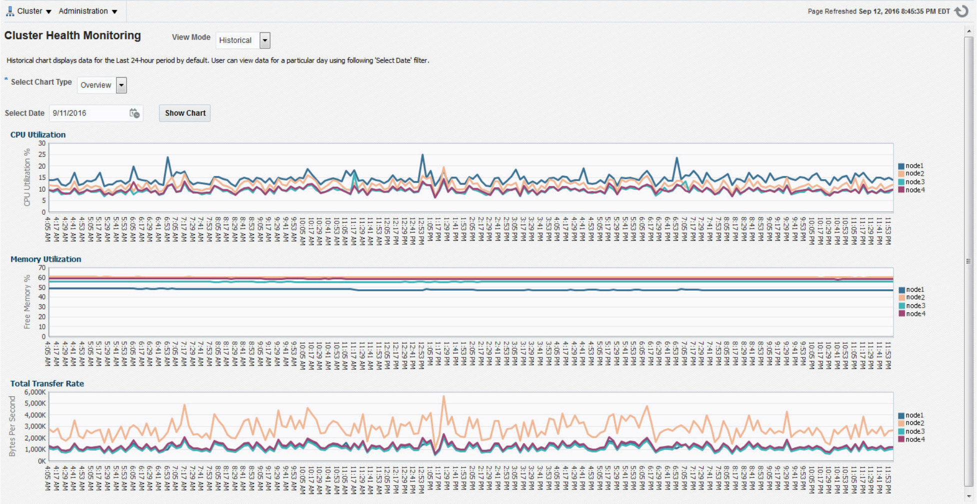
6. From the **View Mode** drop-down list, select the **Historical** option to view data for the last 24 hours.

   - To filter historical data by date, select a day on the **Select Date** calendar control and then click **Show Chart**.

   By default, EMCC displays the **Overview** of resource utilization. You can filter by **CPU**, **Memory**, and **Network** by selecting an appropriate option from the **Select Chart Type** drop-down list.

   While viewing CPU and Network metric graphs, click a node name on the legend to view more details.

Figure 4-8   Cluster Health Monitoring - Historical Data



Cluster ▾ Administration ▾

Page Refreshed **Sep 12, 2016 8:45:35 PM EDT**

Cluster Health Monitoring

View Mode: Historical

Historical chart displays data for the Last 24-hour period by default. User can view data for a particular day using following 'Select Date' filter.

* Select Chart Type: Overview

Select Date: 9/11/2016

Show Chart

CPU Utilization
CPU Utilization %
30
25
20
15
10
5
0
node1
node2
node3
node4
4:05 AM 4:17 AM 4:29 AM 4:41 AM 4:53 AM 5:05 AM 5:17 AM 5:29 AM 5:41 AM 5:53 AM 6:05 AM 6:17 AM 6:29 AM 6:41 AM 6:53 AM 7:05 AM 7:17 AM 7:29 AM 7:41 AM 7:53 AM 8:05 AM 8:17 AM 8:29 AM 8:41 AM 8:53 AM 9:05 AM 9:17 AM 9:29 AM 9:41 AM 9:53 AM 10:05 AM 10:17 AM 10:29 AM 10:41 AM 10:53 AM 11:05 AM 11:17 AM 11:29 AM 11:41 AM 11:53 AM 12:05 PM 12:17 PM 12:29 PM 12:41 PM 12:53 PM 1:05 PM 1:17 PM 1:29 PM 1:41 PM 1:53 PM 2:05 PM 2:17 PM 2:29 PM 2:41 PM 2:53 PM 3:05 PM 3:17 PM 3:29 PM 3:41 PM 3:53 PM 4:05 PM 4:17 PM 4:29 PM 4:41 PM 4:53 PM 5:05 PM 5:17 PM 5:29 PM 5:41 PM 5:53 PM 6:05 PM 6:17 PM 6:29 PM 6:41 PM 6:53 PM 7:05 PM 7:17 PM 7:29 PM 7:41 PM 7:53 PM 8:05 PM 8:17 PM 8:29 PM 8:41 PM 8:53 PM 9:05 PM 9:17 PM 9:29 PM 9:41 PM 9:53 PM 10:05 PM 10:17 PM 10:29 PM 10:41 PM 10:53 PM 11:05 PM 11:17 PM 11:29 PM 11:41 PM 11:53 PM
Memory Utilization
Free Memory %
70
60
50
40
30
20
10
0
node1
node2
node3
node4
4:05 AM 4:17 AM 4:29 AM 4:41 AM 4:53 AM 5:05 AM 5:17 AM 5:29 AM 5:41 AM 5:53 AM 6:05 AM 6:17 AM 6:29 AM 6:41 AM 6:53 AM 7:05 AM 7:17 AM 7:29 AM 7:41 AM 7:53 AM 8:05 AM 8:17 AM 8:29 AM 8:41 AM 8:53 AM 9:05 AM 9:17 AM 9:29 AM 9:41 AM 9:53 AM 10:05 AM 10:17 AM 10:29 AM 10:41 AM 10:53 AM 11:05 AM 11:17 AM 11:29 AM 11:41 AM 11:53 AM 12:05 PM 12:17 PM 12:29 PM 12:41 PM 12:53 PM 1:05 PM 1:17 PM 1:29 PM 1:41 PM 1:53 PM 2:05 PM 2:17 PM 2:29 PM 2:41 PM 2:53 PM 3:05 PM 3:17 PM 3:29 PM 3:41 PM 3:53 PM 4:05 PM 4:17 PM 4:29 PM 4:41 PM 4:53 PM 5:05 PM 5:17 PM 5:29 PM 5:41 PM 5:53 PM 6:05 PM 6:17 PM 6:29 PM 6:41 PM 6:53 PM 7:05 PM 7:17 PM 7:29 PM 7:41 PM 7:53 PM 8:05 PM 8:17 PM 8:29 PM 8:41 PM 8:53 PM 9:05 PM 9:17 PM 9:29 PM 9:41 PM 9:53 PM 10:05 PM 10:17 PM 10:29 PM 10:41 PM 10:53 PM 11:05 PM 11:17 PM 11:29 PM 11:41 PM 11:53 PM
Total Transfer Rate
Bytes Per Second
6,000K
5,000K
4,000K
3,000K
2,000K
1,000K
0K
node1
node2
node3
node4
4:05 AM 4:17 AM 4:29 AM 4:41 AM 4:53 AM 5:05 AM 5:17 AM 5:29 AM 5:41 AM 5:53 AM 6:05 AM 6:17 AM 6:29 AM 6:41 AM 6:53 AM 7:05 AM 7:17 AM 7:29 AM 7:41 AM 7:53 AM 8:05 AM 8:17 AM 8:29 AM 8:41 AM 8:53 AM 9:05 AM 9:17 AM 9:29 AM 9:41 AM 9:53 AM 10:05 AM 10:17 AM 10:29 AM 10:41 AM 10:53 AM 11:05 AM 11:17 AM 11:29 AM 11:41 AM 11:53 AM 12:05 PM 12:17 PM 12:29 PM 12:41 PM 12:53 PM 1:05 PM 1:17 PM 1:29 PM 1:41 PM 1:53 PM 2:05 PM 2:17 PM 2:29 PM 2:41 PM 2:53 PM 3:05 PM 3:17 PM 3:29 PM 3:41 PM 3:53 PM 4:05 PM 4:17 PM 4:29 PM 4:41 PM 4:53 PM 5:05 PM 5:17 PM 5:29 PM 5:41 PM 5:53 PM 6:05 PM 6:17 PM 6:29 PM 6:41 PM 6:53 PM 7:05 PM 7:17 PM 7:29 PM 7:41 PM 7:53 PM 8:05 PM 8:17 PM 8:29 PM 8:41 PM 8:53 PM 9:05 PM 9:17 PM 9:29 PM 9:41 PM 9:53 PM 10:05 PM 10:17 PM 10:29 PM 10:41 PM 10:53 PM 11:05 PM 11:17 PM 11:29 PM 11:41 PM 11:53 PM

4.6 Monitoring System Metrics for Cluster Nodes

This chapter explains the methods to monitor Oracle Clusterware.

Oracle recommends that you use Oracle Enterprise Manager to monitor everyday operations of Oracle Clusterware.

Cluster Health Monitor monitors the complete technology stack, including the operating system, ensuring smooth cluster operations. Both the components are enabled, by default, for any Oracle cluster. Oracle strongly recommends that you use both the components. Also, monitor Oracle Clusterware-managed resources using the Clusterware resource activity log.

- Monitoring Oracle Clusterware with Oracle Enterprise Manager
  Use Oracle Enterprise Manager to monitor the Oracle Clusterware environment.
- Monitoring Oracle Clusterware with Cluster Health Monitor
  You can use the OCLUMON command-line tool to interact with Cluster Health Monitor.

4.6.1 Monitoring Oracle Clusterware with Oracle Enterprise Manager

Use Oracle Enterprise Manager to monitor the Oracle Clusterware environment.

When you log in to Oracle Enterprise Manager using a client browser, the **Cluster Database Home** page appears where you can monitor the status of both Oracle Database and Oracle Clusterware environments. Oracle Clusterware monitoring includes the following details:

- Notifications if there are any VIP relocations
- Status of the Oracle Clusterware on each node of the cluster using information obtained through the Cluster Verification Utility (CVU)
- Notifications if node applications (`nodeapps`) start or stop
- Notification of issues in the Oracle Clusterware alert log for the Oracle Cluster Registry, voting file issues (if any), and node evictions

The **Cluster Database Home** page is similar to a single-instance Database Home page. However, on the Cluster Database Home page, Oracle Enterprise Manager displays the system state and availability. The system state and availability includes a summary about alert messages and job activity, and links to all the database and Oracle Automatic Storage Management (Oracle ASM) instances. For example, track problems with services on the cluster including when a service is not running on all the preferred instances or when a service response time threshold is not being met.

Use the Oracle Enterprise Manager **Interconnects** page to monitor the Oracle Clusterware environment. The Interconnects page displays the following details:

- Public and private interfaces on the cluster
- Overall throughput on the private interconnect
- Individual throughput on each of the network interfaces
- Error rates (if any)
- Load contributed by database instances on the interconnect
- Notifications if a database instance is using public interface due to misconfiguration
- Throughput contributed by individual instances on the interconnect

All the information listed earlier is also available as collections that have a historic view. The historic view is useful with cluster cache coherency, such as when diagnosing problems related to cluster wait events. Access the Interconnects page by clicking the **Interconnect** tab on the Cluster Database home page.

Also, the Oracle Enterprise Manager **Cluster Database Performance** page provides a quick glimpse of the performance statistics for a database. Statistics are rolled up across all the instances in the cluster database in charts. Using the links next to the charts, you can get more specific information and perform any of the following tasks:

- Identify the causes of performance issues
- Decide whether resources must be added or redistributed
- Tune your SQL plan and schema for better optimization
- Resolve performance issues

The charts on the Cluster Database Performance page include the following:

- **Chart for Cluster Host Load Average**: The **Cluster Host Load Average** chart in the Cluster Database Performance page shows potential problems that are outside the database. The chart shows maximum, average, and minimum load values for available nodes in the cluster for the previous hour.
- **Chart for Global Cache Block Access Latency**: Each cluster database instance has its own buffer cache in its System Global Area (SGA). Using Cache Fusion, Oracle RAC environments logically combine buffer cache of each instance to enable the database instances to process data as if the data resided on a logically combined, single cache.
- **Chart for Average Active Sessions**: The **Average Active Sessions** chart in the Cluster Database Performance page shows potential problems inside the database. Categories, called wait classes, show how much of the database is using a resource, such as CPU or disk I/O. Comparing CPU time to wait time helps to determine how much of the response time is consumed with useful work rather than waiting for resources that are potentially held by other processes.
- **Chart for Database Throughput**: The **Database Throughput** charts summarize any resource contention that appears in the Average Active Sessions chart, and also show

how much work the database is performing on behalf of the users or applications. The **Per Second** view shows the number of transactions compared to the number of logons, and the amount of physical reads compared to the redo size for each second. The **Per Transaction** view shows the amount of physical reads compared to the redo size for each transaction. Logons is the number of users that are logged on to the database.

In addition, the **Top Activity** drop-down menu on the **Cluster Database Performance** page enables you to see the activity by wait events, services, and instances. In addition, you can see the details about SQL/sessions by going to a prior point in time by moving the slider on the chart.

4.6.2 Monitoring Oracle Clusterware with Cluster Health Monitor

You can use the OCLUMON command-line tool to interact with Cluster Health Monitor.

OCLUMON is included with Cluster Health Monitor. You can use it to query the Cluster Health Monitor repository to display node-specific metrics for a specified time period. You can also use OCLUMON to perform miscellaneous administrative tasks, such as the following:

- Changing the debug levels with the `oclumon debug` command
- Querying the version of Cluster Health Monitor with the `oclumon version` command
- Viewing the collected information in the form of a node view using the `oclumon dumpnodeview` command
- Changing the metrics datafile size using the `ocloumon manage` command

4.7 Managing Oracle Database and Oracle Grid Infrastructure Logs

This section enables you to manage Oracle Database and Oracle Grid Infrastructure diagnostic data and disk usage snapshots.

- Managing Automatic Diagnostic Repository Log and Trace Files
  Use the `managelogs` command to manage Automatic Diagnostic Repository log and trace files.
- Managing Disk Usage Snapshots
  Use `tfactl` commands to manage Oracle Trace File Analyzer disk usage snapshots.
- Purging Oracle Database and Oracle Grid Infrastructure Logs
  Use these `tfactl` commands to manage log file purge policy for Oracle Database and Oracle Grid Infrastructure logs.
- Securing Access to Diagnostic Collections
  Running `tfactl` commands is restricted to authorized users.

4.7.1 Managing Automatic Diagnostic Repository Log and Trace Files

Use the `managelogs` command to manage Automatic Diagnostic Repository log and trace files.

The `-purge` command option removes files managed by Automatic Diagnostic Repository. This command clears files from “`ALERT`”, "`INCIDENT`", "`TRACE`", "`CDUMP`", "`HM`", "`UTSCDMP`", "`LOG`" under diagnostic destinations. The `-purge` command also provides details about the change in the file system space.

If the diagnostic destinations contain large numbers of files, then the command runs for a while. Check the removal of files in progress from the corresponding directories.

To remove files, you must have operating system privileges over the corresponding diagnostic destinations.

To manage Automatic Diagnostic Repository log and trace files:

1. To limit purge, or show operations to only files older than a specific time:

   ```
   $ tfactl managelogs -older nm|h|d Files from past 'n' [d]ays or 'n'
   [h]ours or 'n' [m]inutes
   ```

   For example:

   ```
   $ tfactl managelogs -purge -older 30d -dryrun
   ```

   ```
   $ tfactl managelogs -purge -older 30d
   ```

2. To get an estimate of how many files are removed and how much space is freed, use the `-dryrun` option:

   For example:

   ```
   $ tfactl managelogs -purge -older 30d -dryrun
   ```

3. To remove files and clean disk space:

   For example:

   ```
   $ tfactl managelogs -purge -older 30d
   ```

   ```
   $ tfactl managelogs -purge -older 30d -gi
   ```

   ```
   $ tfactl managelogs -purge -older 30d -database
   ```

4. To view the space usage of individual diagnostic destinations:

   For example:

   ```
   $ tfactl managelogs -show usage
   ```

   ```
   $ tfactl managelogs -show usage -gi
   ```

```
$ tfactl managelogs -show usage -database
```

Related Topics

- tfactl managelogs
  Use the `tfactl managelogs` command to manage Automatic Diagnostic Repository log and trace files.

4.7.2 Managing Disk Usage Snapshots

Use `tfactl` commands to manage Oracle Trace File Analyzer disk usage snapshots.

Oracle Trace File Analyzer automatically monitors disk usage, records snapshots, and stores the snapshots under `*tfa_install_dir*/tfa/repository/suptools/node/managelogs/usage_snapshot/`

By default, the time interval between snapshots is 60 minutes.

To manage disk usage snapshots:

1. To change the default time interval for snapshots:

   ```
   $ tfactl set diskUsageMonInterval=minutes
   ```

   where *`minutes`* is the number of minutes between snapshots.

2. To turn the disk usage monitor on or off:

   ```
   $ tfactl set diskUsageMon=ON|OFF
   ```

4.7.3 Purging Oracle Database and Oracle Grid Infrastructure Logs

Use these `tfactl` commands to manage log file purge policy for Oracle Database and Oracle Grid Infrastructure logs.

Automatic purging is enabled by default on a Domain Service Cluster (DSC), and disabled by default elsewhere. When automatic purging is enabled, every 60 minutes, Oracle Trace File Analyzer automatically purges logs that are older than 30 days.

To purge Oracle Trace File Analyzer logs automatically:

1. To turn on or off automatic purging:

   ```
   $ tfactl set manageLogsAutoPurge=ON|OFF
   ```

2. To adjust the age of logs to purge:

   ```
   $ tfactl set manageLogsAutoPurgePolicyAge=nd|h
   ```

3. To adjust the frequency of purging:

   ```
   $ tfactl set manageLogsAutoPurgeInterval=minutes
   ```

4.7.4 Securing Access to Diagnostic Collections

Running `tfactl` commands is restricted to authorized users.

`tfactl` provides a command-line interface and shell to do the following:

- Run diagnostics and collect all relevant log data from a time of your choosing
- Trim log files to collect only what is necessary for diagnosis
- Collect and package all trimmed diagnostics from any desired nodes in the cluster and consolidate everything in one package on a single node

Authorized non-root users can run a subset of the `tfactl` commands. All other `tfactl` commands require `root` access. Users who are not authorized cannot run `tfactl` commands.

By default, the following users are authorized to access a subset of `tfactl` commands:

- Oracle Grid Infrastructure home owner
- Oracle Database home owners

User access is applicable only if Oracle Trace File Analyzer is installed as `root` on Linux and UNIX. User access is not applicable if Oracle Trace File Analyzer is installed as non-root, or on Microsoft Windows.

> **Note:**
>
> If an operating system user added to the AHF access control list is deleted without being removed from AHF, then a user created later with the same user name will inherit the deleted user's privileges. To avoid this situation, if an operating system user is deleted, ensure that the user is removed from the AHF access control list.

To provision user access to tfactl:

- To list the users who have access to `tfactl`:

  ```
  tfactl access lsusers
  ```

- To add a user to access `tfactl`:

  ```
  tfactl access add –user user [-local]
  ```

  By default, access commands are applicable to cluster-wide unless you specify the `–local` command option to restrict them to local node.

- To remove a user from accessing `tfactl`:

  ```
  tfactl access remove –user user [-local]
  ```

- To remove all users from accessing `tfactl`:

  ```
  tfactl access removeall [-local]
  ```

- To reset user access to default:

  ```
  tfactl access reset
  ```

Related Topics

- tfactl access
  Use the `tfactl access` command to enable non-root users to have controlled access to Oracle Trace File Analyzer, and to run diagnostic collections.

5

Explore Diagnostic Insights

Autonomous Health Framework Insights (AHF Insights) provides deeper diagnostic insights into Oracle diagnostic collections collected by AHF diagnostic utilities, Oracle Exachk, Oracle Trace File Analyzer, Exawatcher, and Cluster Health Monitor.

AHF Insights is bundled with AHF installer package. You do not need to run a web server to host this site.

> **Note:**
>
> The current version is supported on Linux only.

- Introduction to AHF Insights
  AHF Insights provides a bird's eye view of the entire system with the ability to further drill down for root cause analysis.
- AHF Insights - Home
  Summarizes the System State, System Types, and Time Range the report was generated. As well, it provides a brief overview of the topology of the system and insights into the diagnostics collected by various AHF components.
- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.

5.1 Introduction to AHF Insights

AHF Insights provides a bird's eye view of the entire system with the ability to further drill down for root cause analysis.

> **Note:**
>
> Starting in AHF 23.8, `plotly.js` dependency on CDN has been removed for customers using AHF Insights in restrictive environments.

Previously, results from different AHF components were not available in a single dashboard making it challenging to combine and correlate. To mitigate this, AHF Insights provides a web-based graphical user interface, which does not require a web server to host the web pages, for all diagnostic data collectors and analyzers that are part of AHF Kit.

AHF performs a contextual diagnostic collection for a given period to analyze the performance of database systems. The collection includes diagnostic data from various AHF features such as:

- Configuration
- Environment Topology

- Metrics
- Logs

This diagnostic data collected from the system passes through AHF Insights, which in turn produces an offline report with analysis in the following areas:

- System Configuration
- System State
- Anomalies in the Operating System
- Best Practices Compliance
- System Traces
- Root cause for issues and fixes in some of the anomalous cases

To get started, run the following command:

```
ahf analysis create --type insights
```

Example 5-1 ahf analysis create --type insights

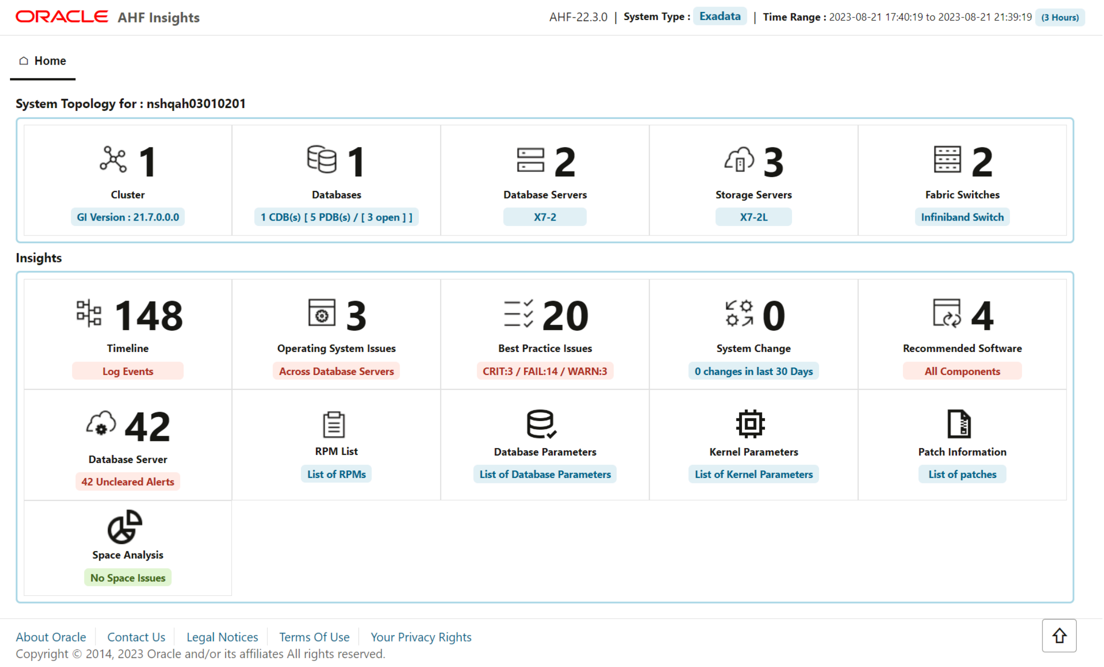
```
[root@node02 ~]# tfactl print status

.----------------------------------------------------------------------
-------------------------.
| Host   | Status of TFA | PID    | Port | Version    | Build
ID              | Inventory Status |
+----------------+---------------+--------+------+------------
+----------------------+----------+
| node02 | RUNNING       | 134679 | 5000 | 22.3.0.0.0 |
22300020221031131221 | COMPLETE         |
| node01 | RUNNING       | 128438 | 5000 | 22.3.0.0.0 |
22300020221031131221 | COMPLETE         |
'----------------+---------------+--------+------+------------
+----------------------+----------'


[root@node02 ~]# ahf analysis create --type insights --last 2h
Starting analysis and collecting data for insights
Collecting data for AHF Insights (This may take a few minutes per node)
AHF Insights report is being generated for the last 2h
From Date : 11/20/2022 01:16:41 UTC - To Date : 11/20/2022 03:17:15 UTC
Report is generated at : /opt/oracle.ahf/data/repository/
collection_Sun_Nov_20_03_16_36_UTC_2022_node_all/cgexa-
ogmn12_insights_2022_11_20_03_18_13.zip
```

5.2 AHF Insights - Home

Summarizes the System State, System Types, and Time Range the report was generated. As well, it provides a brief overview of the topology of the system and insights into the diagnostics collected by various AHF components.

Click on an item on the **Home** page to view details. Concurrently, you can open more than one item. A userscore highlights the item in focus. Use the up/down arrow keys on your keyboard to move the page horizontally. To get to the top of the page, click the **Scroll to top** button. To close an open item, click the **X** mark.

Figure 5-1 Home



ORACLE AHF Insights

AHF-22.3.0 | **System Type :** Exadata | **Time Range :** 2023-08-21 17:40:19 to 2023-08-21 21:39:19 (3 Hours)

⌂ Home

System Topology for : nshqah03010201

1 Cluster GI Version : 21.7.0.0.0	1 Databases 1 CDB(s) [5 PDB(s) / [3 open]]	2 Database Servers X7-2	3 Storage Servers X7-2L	2 Fabric Switches Infiniband Switch

Insights

148 Timeline Log Events	3 Operating System Issues Across Database Servers	20 Best Practice Issues CRIT:3 / FAIL:14 / WARN:3	0 System Change 0 changes in last 30 Days	4 Recommended Software All Components
42 Database Server 42 Uncleared Alerts	RPM List List of RPMs	Database Parameters List of Database Parameters	Kernel Parameters List of Kernel Parameters	Patch Information List of patches
Space Analysis No Space Issues				

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

System Topology

- **Cluster:** Provides a summary of cluster and cluster resources, and ASM details.
- **Databases:** Provides basic and detailed information about Oracle Databases running on the system.
- **Database Servers:** Provides basic information about database servers.
- **Storage Servers:** Provides basic information about storage servers.
- **Fabric Switches:** Provides basic information about RDMA Network Fabric Switches.

Insights

- **Timeline:** Provides Timeline visualization in a graph and provides a table with specific information about each timestamp.
- **Operating System Issues:** Provides details about the metrics collected on the system and a detailed report on operating system anomalies.
- **Best Practice Issues:** Provides the results of Best Practices Compliance checks run on the system, paginated.
- **System Change:** Provides details on the changes applied to the system, paginated.
- **Recommended Software:** Lists recommended software and links to supported versions.
- **Database Server:** Provides details about the Management Server metrics and the alerts recorded in the Management Server.

- **RPM List:** Lists RPMs and the differences between them across nodes, paginated.
- **Database Parameters:** Lists normal and hidden Oracle Database parameters, paginated.
- **Kernel Parameters:** Lists the kernel parameters, paginated.
- **Space Analysis:** Renders **Disk Utilization** and **Diagnostice Space Usage** data in visual and tabular format.
- System Topology
- Insights

5.2.1 System Topology

> **Note:**
>
> **Fabric Switches** and **Storage Servers** sections will not be displayed in a non-Exadata environment.

- Cluster
- Databases
- Database Servers
- Storage Servers
- Fabric Switches

5.2.1.1 Cluster

AHF 23.8

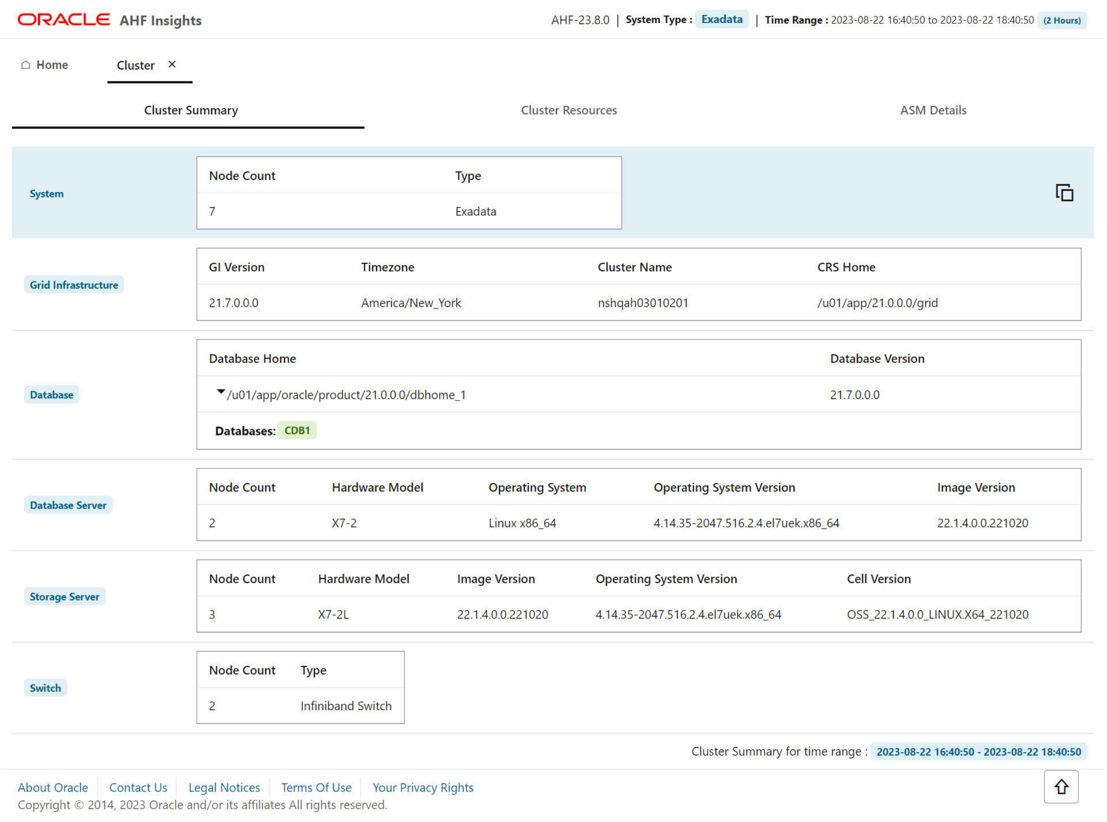
Starting in AHF 23.8, you will be able copy data in text format into the clipboard to post it into SR body while raising a service request.

How does AHF Insights UI render this information

Provides a summary of cluster and cluster resources, and ASM details.

Cluster Summary

Figure 5-2 Cluster Summary



ORACLE AHF Insights AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)

Home Cluster ×

Cluster Summary Cluster Resources ASM Details

System

Node Count	Type
7	Exadata

Grid Infrastructure

GI Version	Timezone	Cluster Name	CRS Home
21.7.0.0.0	America/New_York	nshqah03010201	/u01/app/21.0.0.0/grid

Database

Database Home	Database Version
▾/u01/app/oracle/product/21.0.0.0/dbhome_1	21.7.0.0.0

Databases: CDB1

Database Server

Node Count	Hardware Model	Operating System	Operating System Version	Image Version
2	X7-2	Linux x86_64	4.14.35-2047.516.2.4.el7uek.x86_64	22.1.4.0.0.221020

Storage Server

Node Count	Hardware Model	Image Version	Operating System Version	Cell Version
3	X7-2L	22.1.4.0.0.221020	4.14.35-2047.516.2.4.el7uek.x86_64	OSS_22.1.4.0.0_LINUX.X64_221020

Switch

Node Count	Type
2	Infiniband Switch

Cluster Summary for time range : 2023-08-22 16:40:50 - 2023-08-22 18:40:50

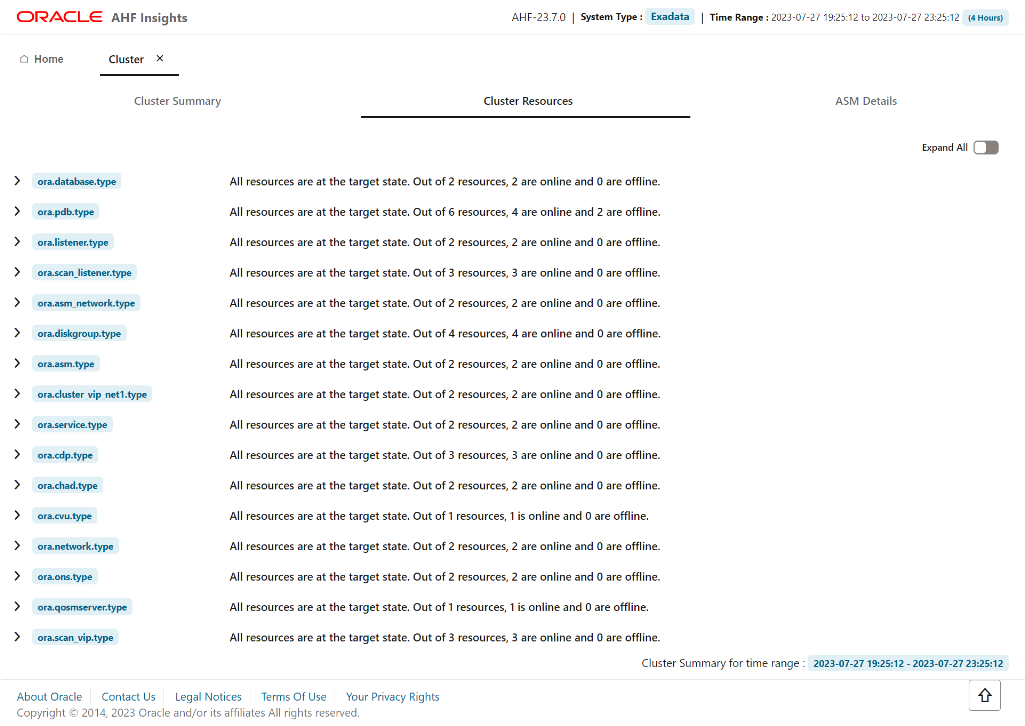
About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides a brief overview on System, Oracle Grid Infrastructure, Incident, Oracle Database, Database Server, Storage Server, and RDMA Network Fabric Switch.

- Click the arrow located inside the **Database Home** section to get Database Home details.
- Click **Copy as text** to copy the cluster summary into the clipboard.

Cluster Resources

Figure 5-3 Cluster Resources



ORACLE AHF Insights

AHF-23.7.0 | **System Type :** Exadata | **Time Range :** 2023-07-27 19:25:12 to 2023-07-27 23:25:12 (4 Hours)

Home | Cluster ×

Cluster Summary | Cluster Resources | ASM Details

Expand All

ora.database.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.pdb.type	All resources are at the target state. Out of 6 resources, 4 are online and 2 are offline.
ora.listener.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.scan_listener.type	All resources are at the target state. Out of 3 resources, 3 are online and 0 are offline.
ora.asm_network.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.diskgroup.type	All resources are at the target state. Out of 4 resources, 4 are online and 0 are offline.
ora.asm.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.cluster_vip_net1.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.service.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.cdp.type	All resources are at the target state. Out of 3 resources, 3 are online and 0 are offline.
ora.chad.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.cvu.type	All resources are at the target state. Out of 1 resources, 1 is online and 0 are offline.
ora.network.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.ons.type	All resources are at the target state. Out of 2 resources, 2 are online and 0 are offline.
ora.qosmserver.type	All resources are at the target state. Out of 1 resources, 1 is online and 0 are offline.
ora.scan_vip.type	All resources are at the target state. Out of 3 resources, 3 are online and 0 are offline.

Cluster Summary for time range : 2023-07-27 19:25:12 - 2023-07-27 23:25:12

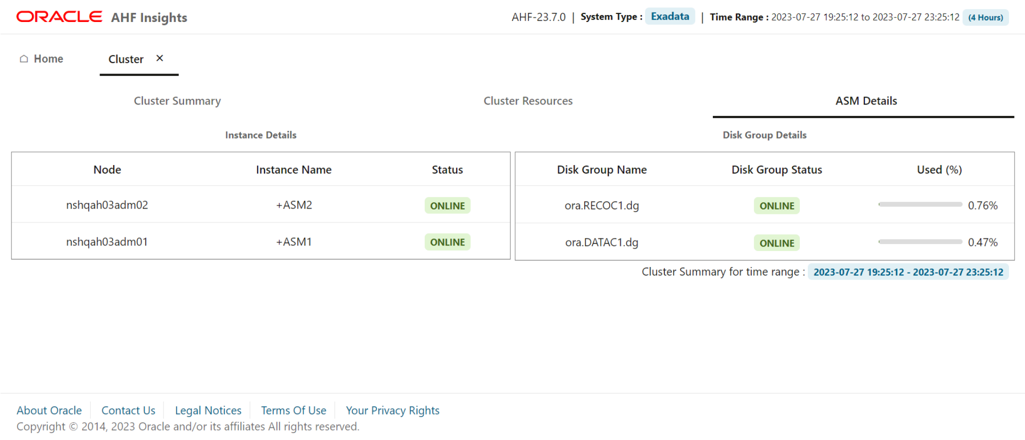
About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides details on the cluster resources, Oracle Database, pluggable database (PDB), and listener, paginated. The details include CRS resource names, online or offline statuses of the targets, state of the resources, and the servers on which the resources are running.

- Click the **Expand All** toggle button to view details of all cluster resources.

ASM Details

Figure 5-4 ASM Details



ORACLE AHF Insights

AHF-23.7.0 | **System Type :** Exadata | **Time Range :** 2023-07-27 19:25:12 to 2023-07-27 23:25:12 (4 Hours)

Home | Cluster ×

Cluster Summary | Cluster Resources | ASM Details

Instance Details

Node	Instance Name	Status
nshqah03adm02	+ASM2	ONLINE
nshqah03adm01	+ASM1	ONLINE

Disk Group Details

Disk Group Name	Disk Group Status	Used (%)
ora.RECOC1.dg	ONLINE	0.76%
ora.DATAC1.dg	ONLINE	0.47%

Cluster Summary for time range : 2023-07-27 19:25:12 - 2023-07-27 23:25:12

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides details on the nodes, instance names, online or offline statuses of the nodes, disk group names, online or offline statuses of the disk groups, and percentage of disk usage, paginated.

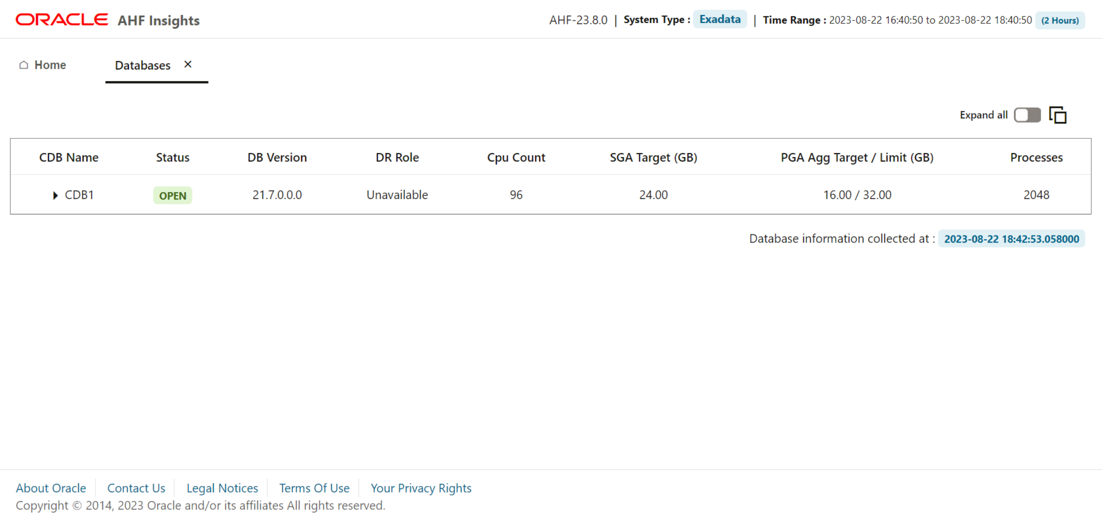
5.2.1.2 Databases

AHF 23.8

Starting in AHF 23.8, you will be able copy data in text format into the clipboard to post it into SR body while raising a service request.

How does AHF Insights UI render this information

Figure 5-5   Databases



AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)

CDB Name	Status	DB Version	DR Role	Cpu Count	SGA Target (GB)	PGA Agg Target / Limit (GB)	Processes
CDB1	OPEN	21.7.0.0.0	Unavailable	96	24.00	16.00 / 32.00	2048

Database information collected at : 2023-08-22 18:42:53.058000

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides basic and detailed information about Oracle Databases running on the system.

- Click **Expand All** to view detailed information on all items or click an arrow button to view detailed information on a specific item.

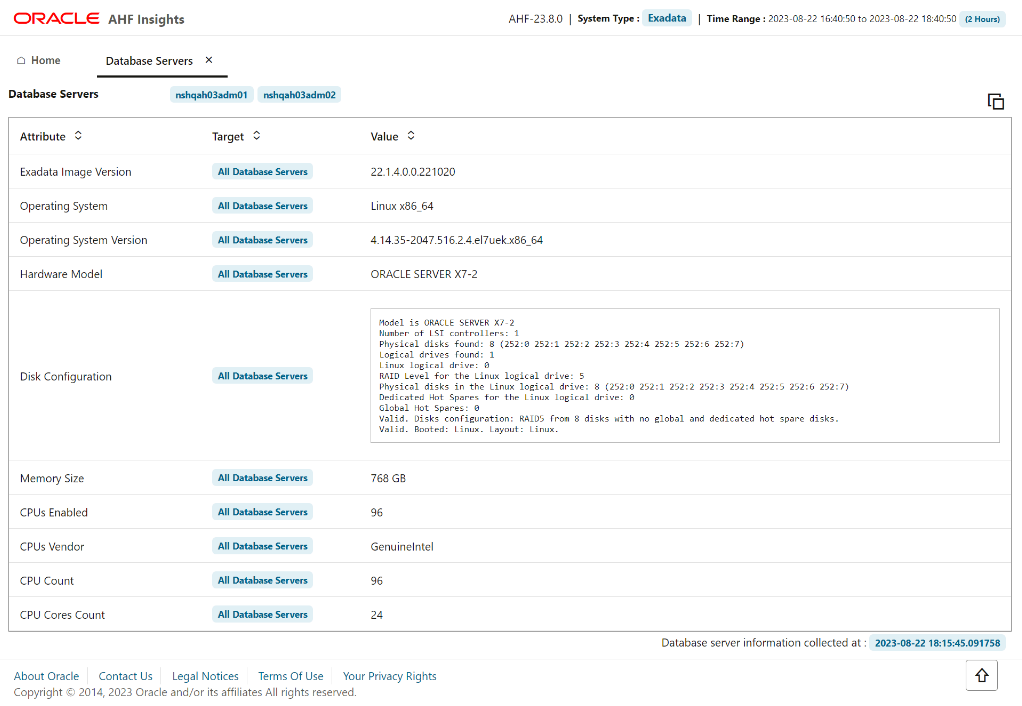
5.2.1.3 Database Servers

AHF 23.8

Starting in AHF 23.8, you will be able copy data in text format into the clipboard to post it into SR body while raising a service request.

How does AHF Insights UI render this information

Figure 5-6 Database Servers



ORACLE AHF Insights
AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)
Home
Database Servers ×

Database Servers nshqah03adm01 nshqah03adm02

Attribute	Target	Value
Exadata Image Version	All Database Servers	22.1.4.0.0.221020
Operating System	All Database Servers	Linux x86_64
Operating System Version	All Database Servers	4.14.35-2047.516.2.4.el7uek.x86_64
Hardware Model	All Database Servers	ORACLE SERVER X7-2
Disk Configuration	All Database Servers	Model is ORACLE SERVER X7-2 Number of LSI controllers: 1 Physical disks found: 8 (252:0 252:1 252:2 252:3 252:4 252:5 252:6 252:7) Logical drives found: 1 Linux logical drive: 0 RAID Level for the Linux logical drive: 5 Physical disks in the Linux logical drive: 8 (252:0 252:1 252:2 252:3 252:4 252:5 252:6 252:7) Dedicated Hot Spares for the Linux logical drive: 0 Global Hot Spares: 0 Valid. Disks configuration: RAID5 from 8 disks with no global and dedicated hot spare disks. Valid. Booted: Linux. Layout: Linux.
Memory Size	All Database Servers	768 GB
CPUs Enabled	All Database Servers	96
CPUs Vendor	All Database Servers	GenuineIntel
CPU Count	All Database Servers	96
CPU Cores Count	All Database Servers	24

Database server information collected at : 2023-08-22 18:15:45.091758

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Provides basic information about database servers.

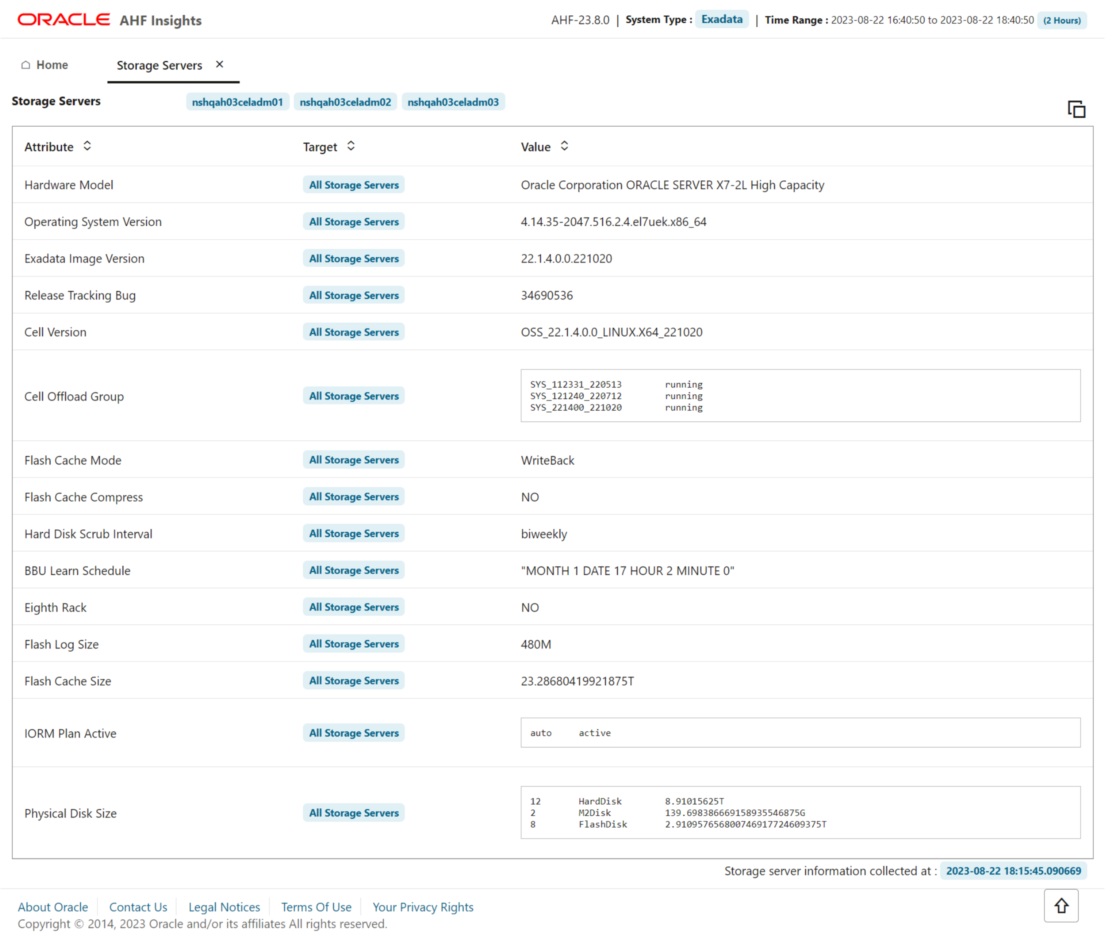
- Sort by **Attribute**, **Target**, and **Value** fields.

5.2.1.4 Storage Servers

AHF 23.8

Starting in AHF 23.8, you will be able copy data in text format into the clipboard to post it into SR body while raising a service request.

How does AHF Insights UI render this information



ORACLE AHF Insights
AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)
⌂ Home
Storage Servers ×

Storage Servers nshqah03celadm01 nshqah03celadm02 nshqah03celadm03

Attribute	Target	Value
Hardware Model	All Storage Servers	Oracle Corporation ORACLE SERVER X7-2L High Capacity
Operating System Version	All Storage Servers	4.14.35-2047.516.2.4.el7uek.x86_64
Exadata Image Version	All Storage Servers	22.1.4.0.0.221020
Release Tracking Bug	All Storage Servers	34690536
Cell Version	All Storage Servers	OSS_22.1.4.0.0_LINUX.X64_221020
Cell Offload Group	All Storage Servers	SYS_112331_220513 running SYS_121240_220712 running SYS_221400_221020 running
Flash Cache Mode	All Storage Servers	WriteBack
Flash Cache Compress	All Storage Servers	NO
Hard Disk Scrub Interval	All Storage Servers	biweekly
BBU Learn Schedule	All Storage Servers	"MONTH 1 DATE 17 HOUR 2 MINUTE 0"
Eighth Rack	All Storage Servers	NO
Flash Log Size	All Storage Servers	480M
Flash Cache Size	All Storage Servers	23.28680419921875T
IORM Plan Active	All Storage Servers	auto active
Physical Disk Size	All Storage Servers	12 HardDisk 8.91015625T 2 M2Disk 139.698386669158935546875G 8 FlashDisk 2.910957656800746917724609375T

Storage server information collected at : 2023-08-22 18:15:45.090669

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-7 Storage Servers

Provides basic information about storage servers.

- Sort by **Attribute**, **Target**, and **Value** fields.

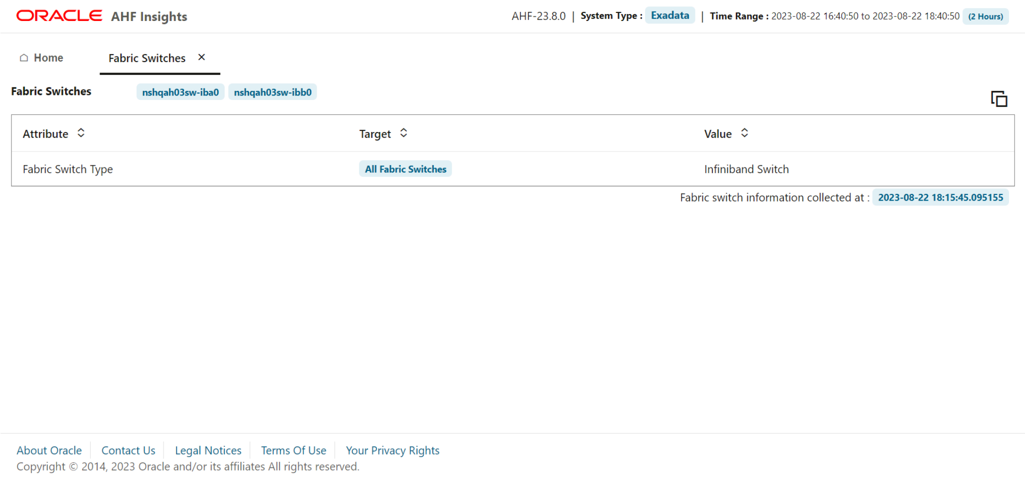
5.2.1.5 Fabric Switches

AHF 23.8

Starting in AHF 23.8, you will be able copy data in text format into the clipboard to post it into SR body while raising a service request.

How does AHF Insights UI render this information

Figure 5-8 Fabric Switches



ORACLE AHF Insights
AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)
⌂ Home
Fabric Switches ✕
Fabric Switches
nshqah03sw-iba0
nshqah03sw-ibb0

Attribute	Target	Value
Fabric Switch Type	All Fabric Switches	Infiniband Switch

Fabric switch information collected at : 2023-08-22 18:15:45.095155

Provides basic information about RDMA Network Fabric Switches.

- Sort by **Attribute**, **Target**, and **Value** fields.

5.2.2 Insights

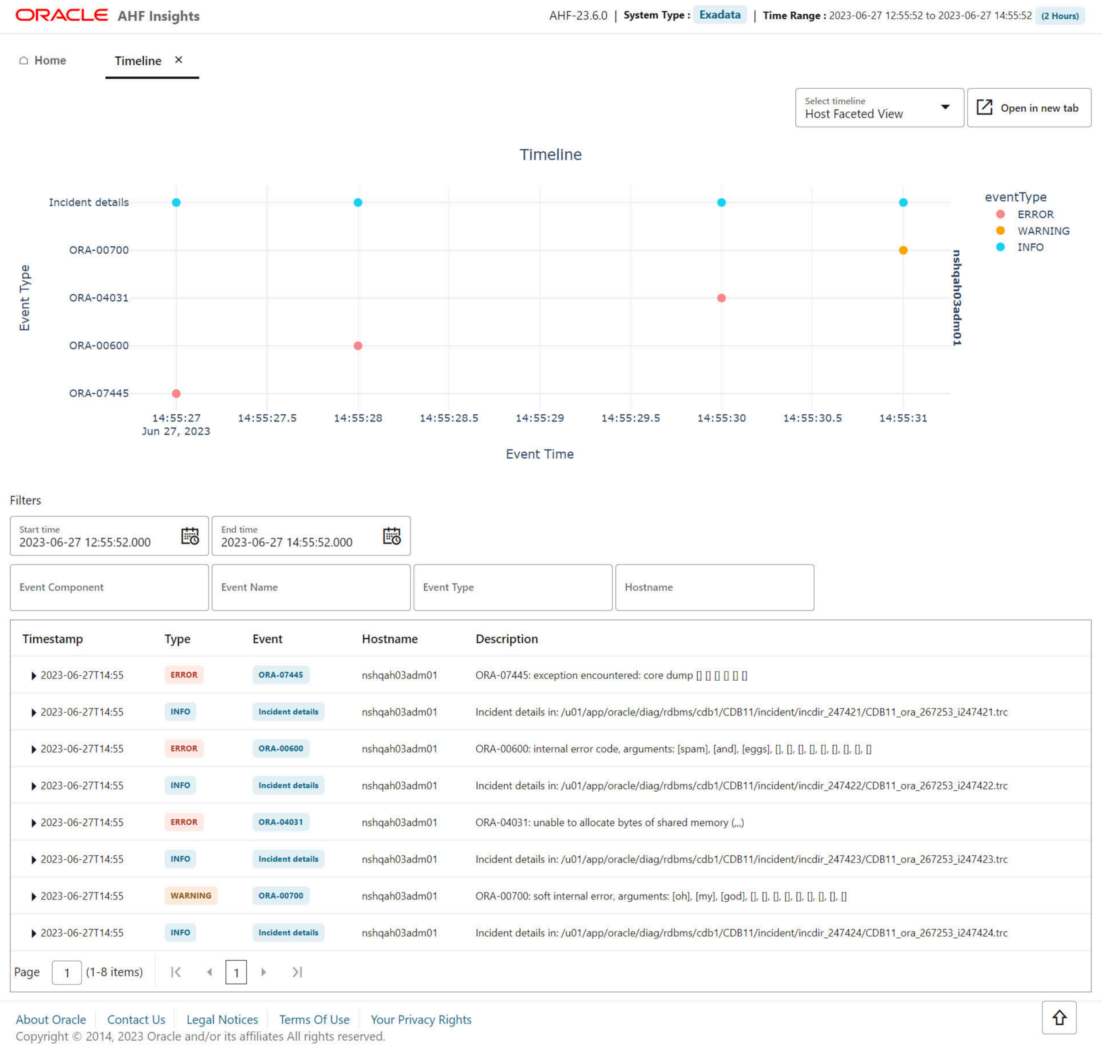
> **Note:**
>
> **Database Server** section will not be displayed in a non-Exadata environment.

- Timeline
- Operating System Issues
- Best Practice Issues
- System Change
- Recommended Software
- Database Server
- RPM List
- Database Parameters
- Kernel Parameters
- Patch Information
- Space Analysis
- Database Anomalies Advisor
  AHF detects database anomalies and identifies the cause and corrective action.

5.2.2.1 Timeline

How does AHF Insights UI render this information

Figure 5-9   Timeline - Host Faceted View



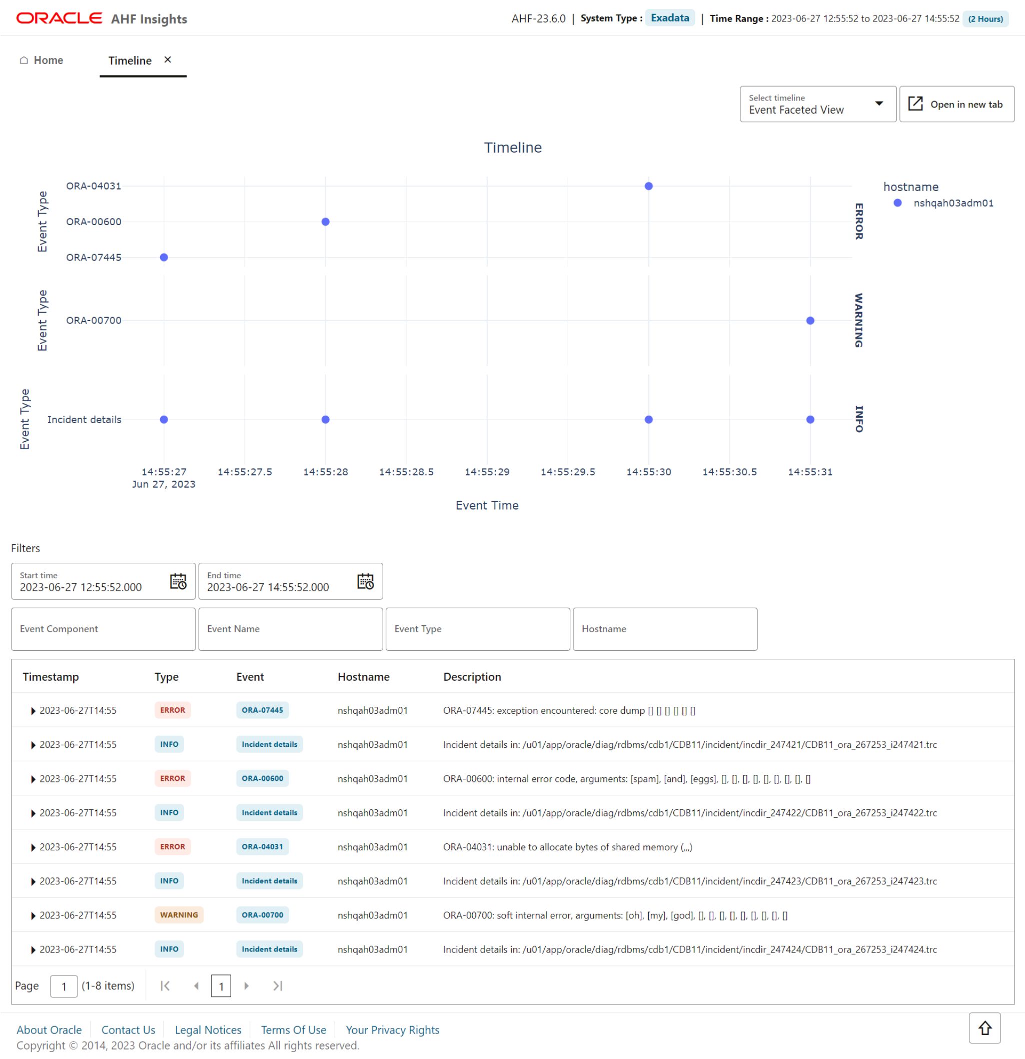
Start time: 2023-06-27 12:55:52.000

End time: 2023-06-27 14:55:52.000

Timestamp	Type	Event	Hostname	Description
2023-06-27T14:55	ERROR	ORA-07445	nshqah03adm01	ORA-07445: exception encountered: core dump [] [] [] [] [] []
2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247421/CDB11_ora_267253_i247421.trc
2023-06-27T14:55	ERROR	ORA-00600	nshqah03adm01	ORA-00600: internal error code, arguments: [spam], [and], [eggs], [], [], [], [], [], [], [], []
2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247422/CDB11_ora_267253_i247422.trc
2023-06-27T14:55	ERROR	ORA-04031	nshqah03adm01	ORA-04031: unable to allocate bytes of shared memory (,,,)
2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247423/CDB11_ora_267253_i247423.trc
2023-06-27T14:55	WARNING	ORA-00700	nshqah03adm01	ORA-00700: soft internal error, arguments: [oh], [my], [god], [], [], [], [], [], [], [], []
2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247424/CDB11_ora_267253_i247424.trc

Page 1 (1-8 items)

Figure 5-10 Timeline - Event Faceted View



AHF-23.6.0 | **System Type :** Exadata | **Time Range :** 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Select timeline: Event Faceted View

Start time: 2023-06-27 12:55:52.000

End time: 2023-06-27 14:55:52.000

Event Component | Event Name | Event Type | Hostname

Timestamp	Type	Event	Hostname	Description
▸ 2023-06-27T14:55	ERROR	ORA-07445	nshqah03adm01	ORA-07445: exception encountered: core dump [] [] [] [] [] []
▸ 2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247421/CDB11_ora_267253_i247421.trc
▸ 2023-06-27T14:55	ERROR	ORA-00600	nshqah03adm01	ORA-00600: internal error code, arguments: [spam], [and], [eggs], [], [], [], [], [], [], [], [], []
▸ 2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247422/CDB11_ora_267253_i247422.trc
▸ 2023-06-27T14:55	ERROR	ORA-04031	nshqah03adm01	ORA-04031: unable to allocate bytes of shared memory (,,,)
▸ 2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247423/CDB11_ora_267253_i247423.trc
▸ 2023-06-27T14:55	WARNING	ORA-00700	nshqah03adm01	ORA-00700: soft internal error, arguments: [oh], [my], [god], [], [], [], [], [], [], [], [], []
▸ 2023-06-27T14:55	INFO	Incident details	nshqah03adm01	Incident details in: /u01/app/oracle/diag/rdbms/cdb1/CDB11/incident/incdir_247424/CDB11_ora_267253_i247424.trc

Page 1 (1-8 items) |< ◂ 1 ▸ >|

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides Timeline visualization in a graph and provides a table with specific information about each timestamp.

- Search values using the filter section.
- Filter by a specific time range.
- Click the arrow located at the left side of a specific date to view detailed information regarding a specific timestamp.
- Hover over a specific data point in the graph to get detailed information about that specific point in time.
- Zoom into the timeline.

5.2.2.2 Operating System Issues

AHF 23.8

AHF 23.8 includes the following enhancements to the user interface to make it more intuitive and easier to use.

You can:

- Spot the disks that have anomalies. In the **Operating System Issues** tab, under **Local IO**, click **Disk** to view **Disk Metrics**. Disks that have anomalies are marked with an **X** mark.
- Explore process aggregate from operating system details in a more intuitive way.
  - Demarcated process aggregates per the instance group like Databases, ASM, APX (Apex), IOS, Clusterware, and so on.
  - Legends specific to individual category rather than single legend for all categories.

AHF 23.10

AHF 23.10 includes the following enhancements to the user interface to make it more intuitive.

You will now be able to view the data in problematic time ranges in plots with more data points.

The problematic time ranges will have the following reading intervals:

- 5 seconds for ranges less than 1 minute
- 30 seconds for ranges more than 1 minute

The number of data points for plots under **Operating System Issues** section are dynamic for optimal time taken to generate report.

The data points for time ranges greater than 4 hours are reduced and have the following reading intervals:

- 1 minute for intervals up to 4 hours
- 3 minutes for intervals greater than 4 hours and less than 12 hours
- 5 minutes for intervals greater than 12 hours.

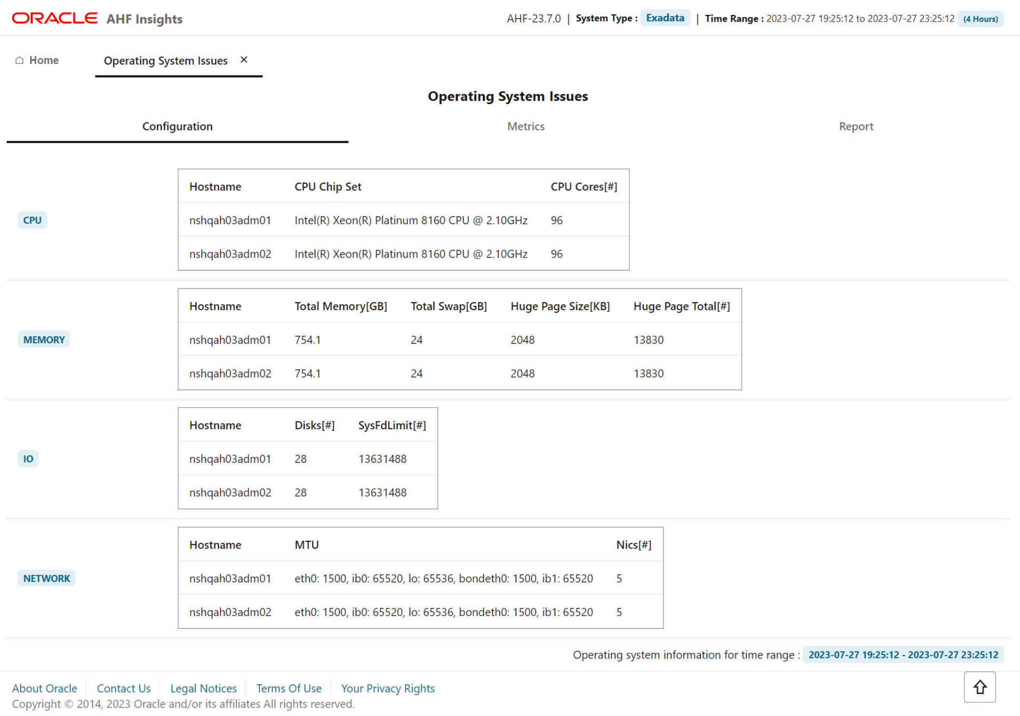
AHF 23.11

Starting in AHF 23.11, you will be able to view data coming from `Exawatcher`.

You can explore data coming from cell nodes in a visual format. You can switch between cell nodes, tagged as (S), and compute nodes, tagged as (D) from a dropdown. You will be able to examine Flash Disks, Flash Disk Aggregates, and Hard Disk Aggregates metrics.

How does AHF Insights UI render this information

Figure 5-11 Operating System Issues - Configuration



ORACLE AHF Insights
AHF-23.7.0 | System Type : Exadata | Time Range : 2023-07-27 19:25:12 to 2023-07-27 23:25:12 (4 Hours)
Home
Operating System Issues ×
Configuration
Metrics
Report

Operating System Issues

CPU

Hostname	CPU Chip Set	CPU Cores[#]
nshqah03adm01	Intel(R) Xeon(R) Platinum 8160 CPU @ 2.10GHz	96
nshqah03adm02	Intel(R) Xeon(R) Platinum 8160 CPU @ 2.10GHz	96

MEMORY

Hostname	Total Memory[GB]	Total Swap[GB]	Huge Page Size[KB]	Huge Page Total[#]
nshqah03adm01	754.1	24	2048	13830
nshqah03adm02	754.1	24	2048	13830

IO

Hostname	Disks[#]	SysFdLimit[#]
nshqah03adm01	28	13631488
nshqah03adm02	28	13631488

NETWORK

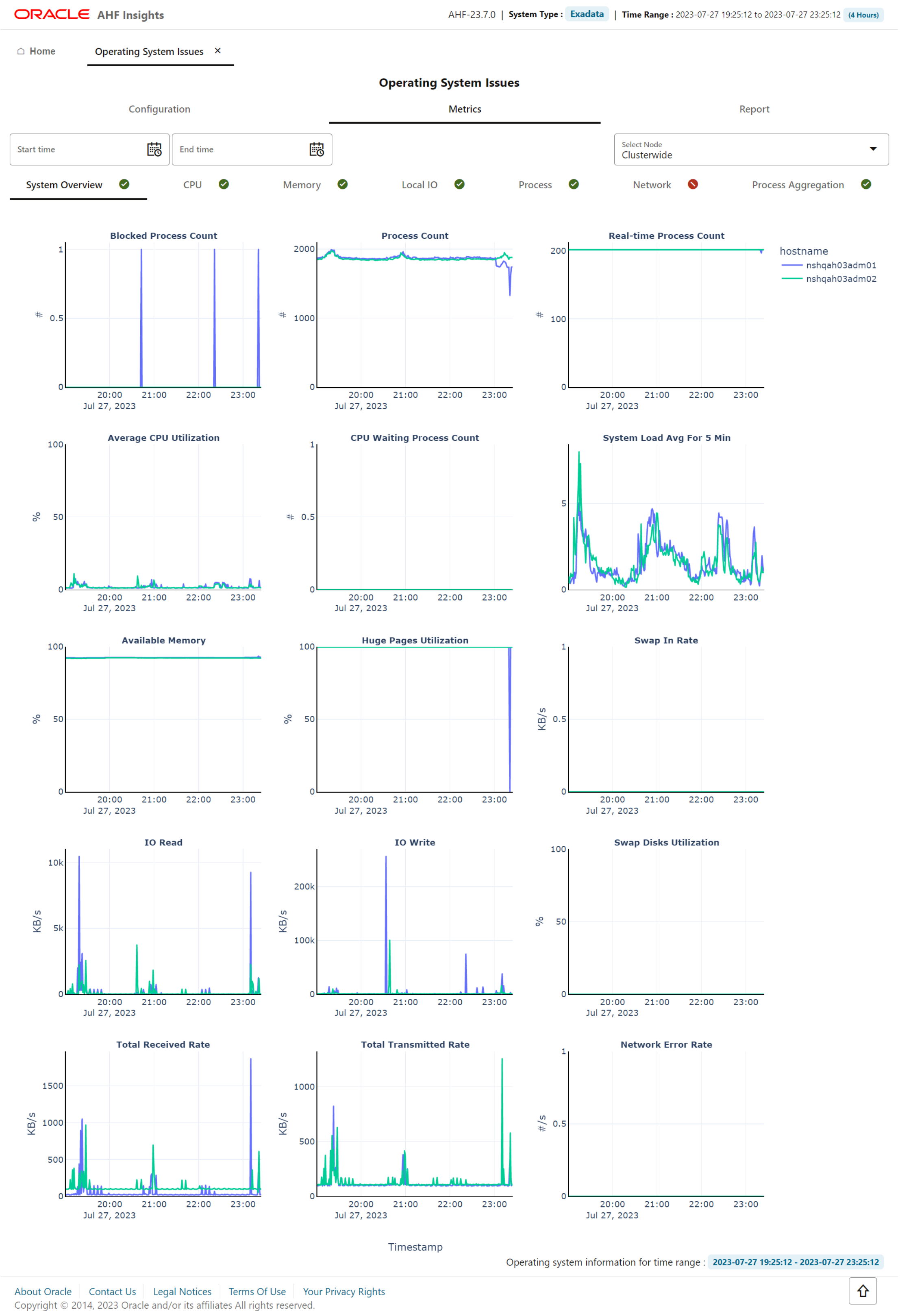
Hostname	MTU	Nics[#]
nshqah03adm01	eth0: 1500, ib0: 65520, lo: 65536, bondeth0: 1500, ib1: 65520	5
nshqah03adm02	eth0: 1500, ib0: 65520, lo: 65536, bondeth0: 1500, ib1: 65520	5

Operating system information for time range : 2023-07-27 19:25:12 - 2023-07-27 23:25:12

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-12 Operating System Issues - Metrics



AHF Insights AHF-23.7.0 | System Type : Exadata | Time Range : 2023-07-27 19:25:12 to 2023-07-27 23:25:12 (4 Hours)

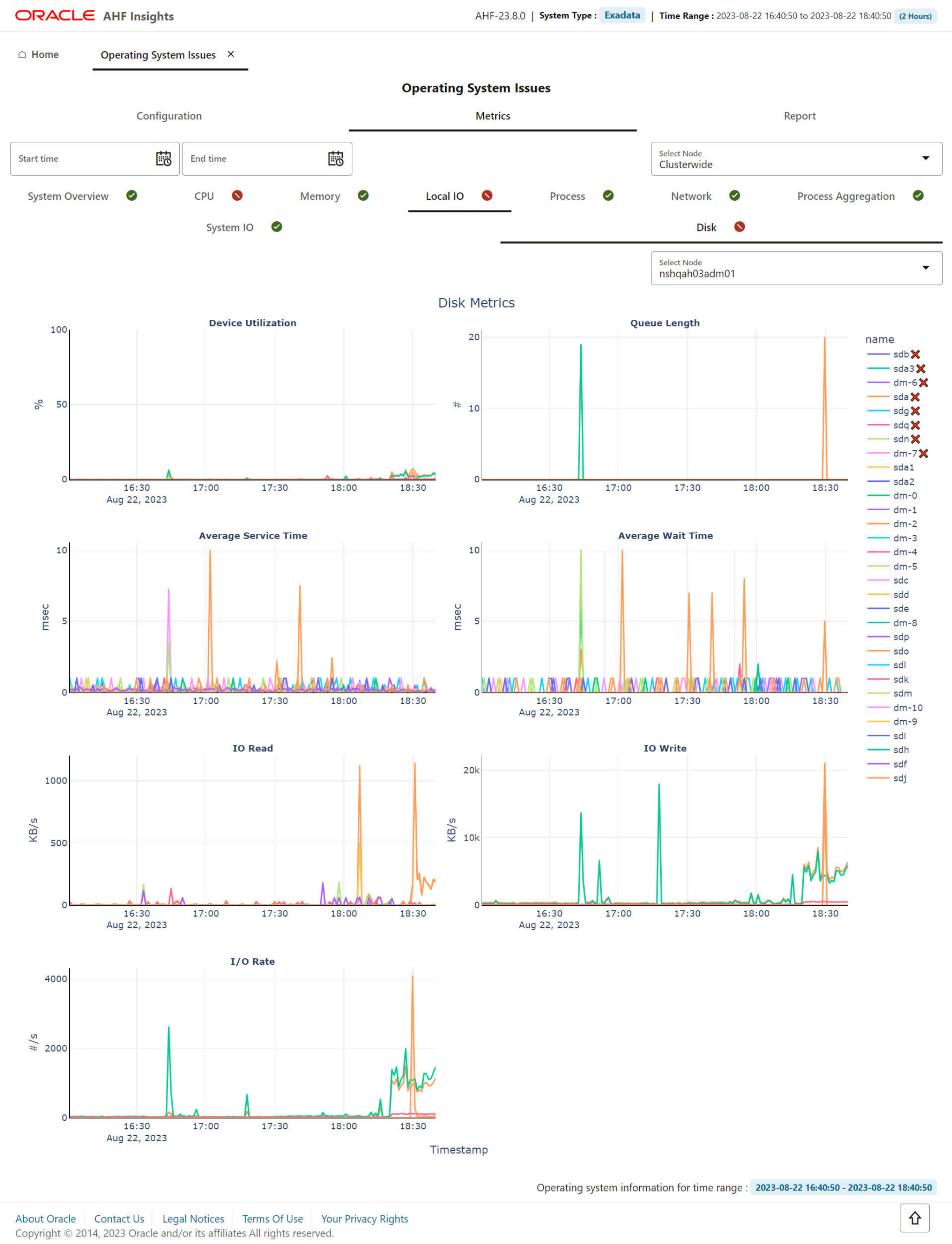
Operating System Issues

Select Node: Clusterwide

Operating system information for time range : 2023-07-27 19:25:12 - 2023-07-27 23:25:12

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Figure 5-13 Operating System Issues - Metrics - Disk Anamolies



ORACLE AHF Insights

AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)

⌂ Home | Operating System Issues ×

Operating System Issues

Configuration | Metrics | Report

Start time | End time | Select Node: Clusterwide

System Overview ✓ | CPU ⊘ | Memory ✓ | Local IO ⊘ | Process ✓ | Network ✓ | Process Aggregation ✓

System IO ✓ | Disk ⊘

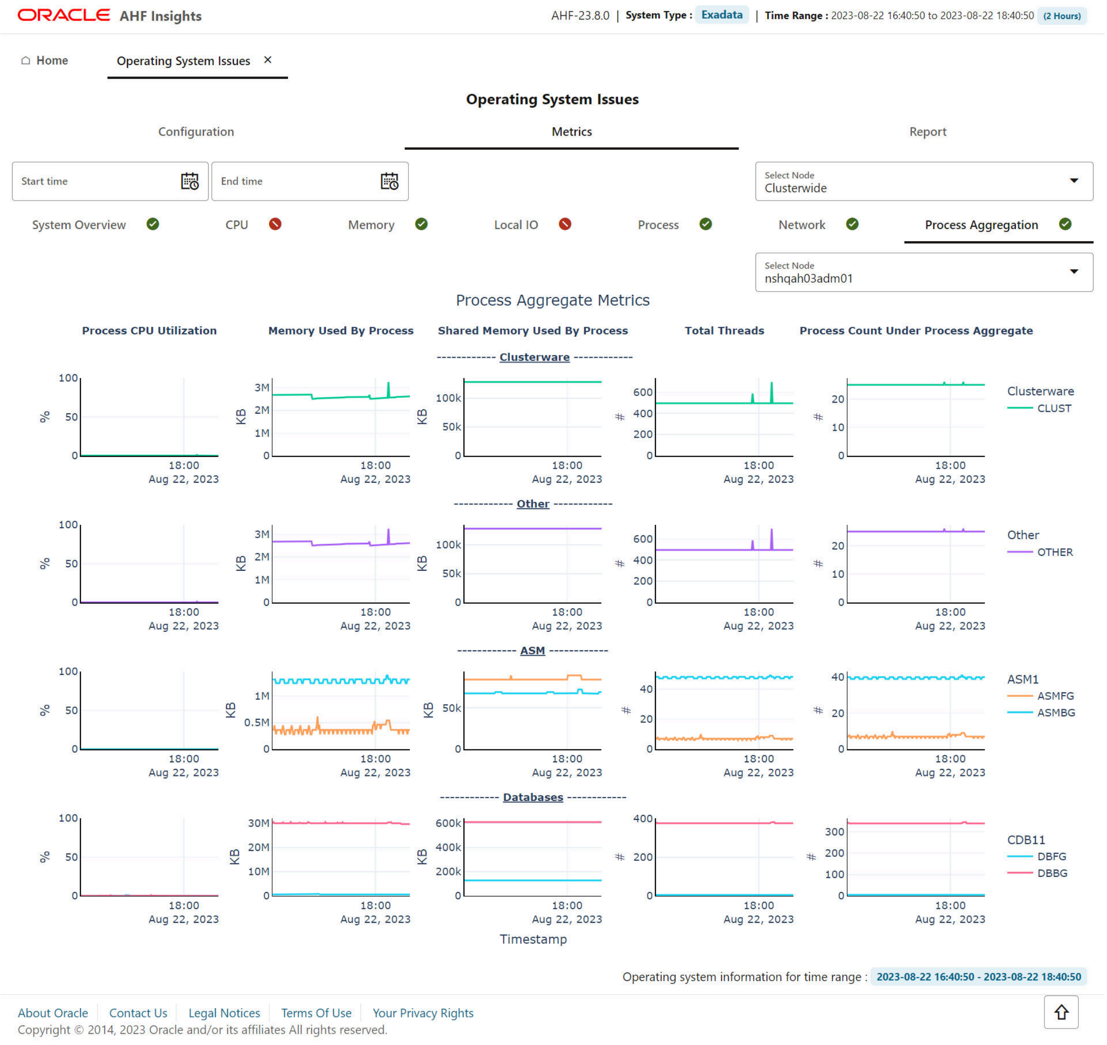
Select Node: nshqah03adm01

Disk Metrics

Operating system information for time range : 2023-08-22 16:40:50 - 2023-08-22 18:40:50

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Figure 5-14 Operating System Issues - Metrics - Process Aggregation



AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)

Start time

End time

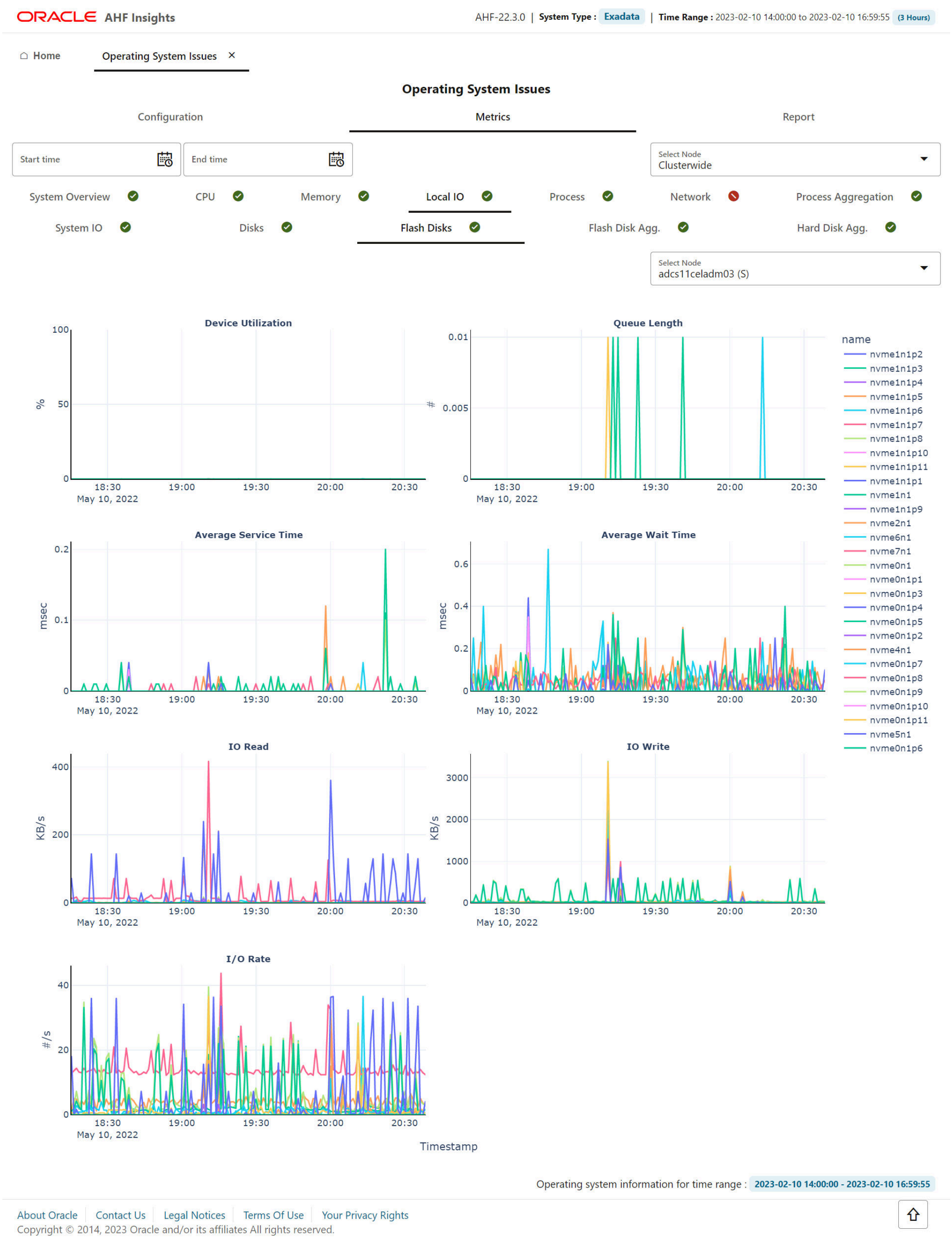
Select Node
Clusterwide

Select Node
nshqah03adm01

Operating system information for time range : 2023-08-22 16:40:50 - 2023-08-22 18:40:50

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-15 Operating System Issues - Metrics - Local I/O - Flash Disks



ORACLE AHF Insights   AHF-22.3.0 | System Type : Exadata | Time Range : 2023-02-10 14:00:00 to 2023-02-10 16:59:55 (3 Hours)

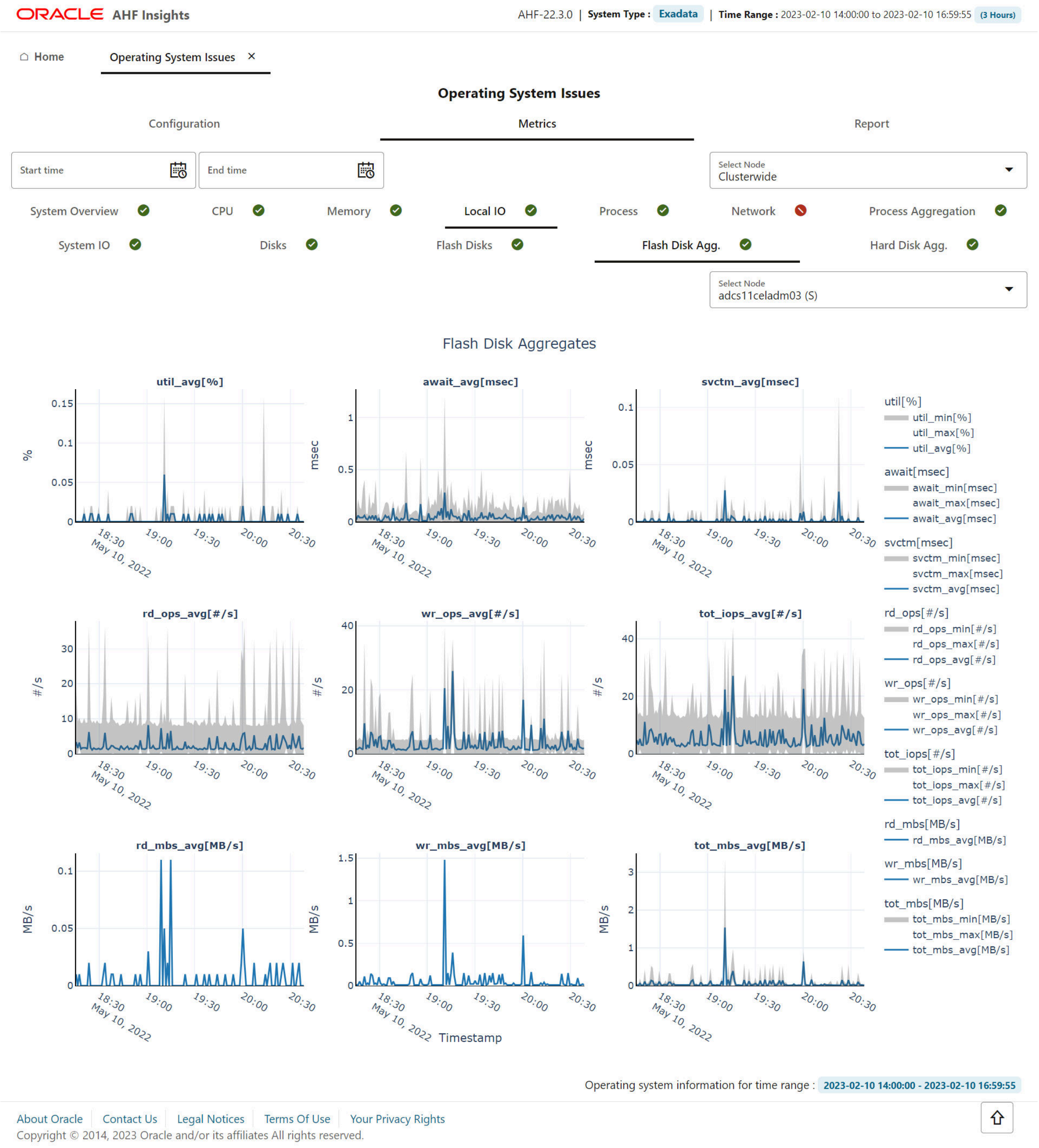
Select Node: Clusterwide

Select Node: adcs11celadm03 (S)

Operating system information for time range : 2023-02-10 14:00:00 - 2023-02-10 16:59:55

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-16 Operating System Issues - Metrics - Local I/O - Flash Disk Aggregation



AHF-22.3.0 | System Type : Exadata | Time Range : 2023-02-10 14:00:00 to 2023-02-10 16:59:55 (3 Hours)

Operating System Issues

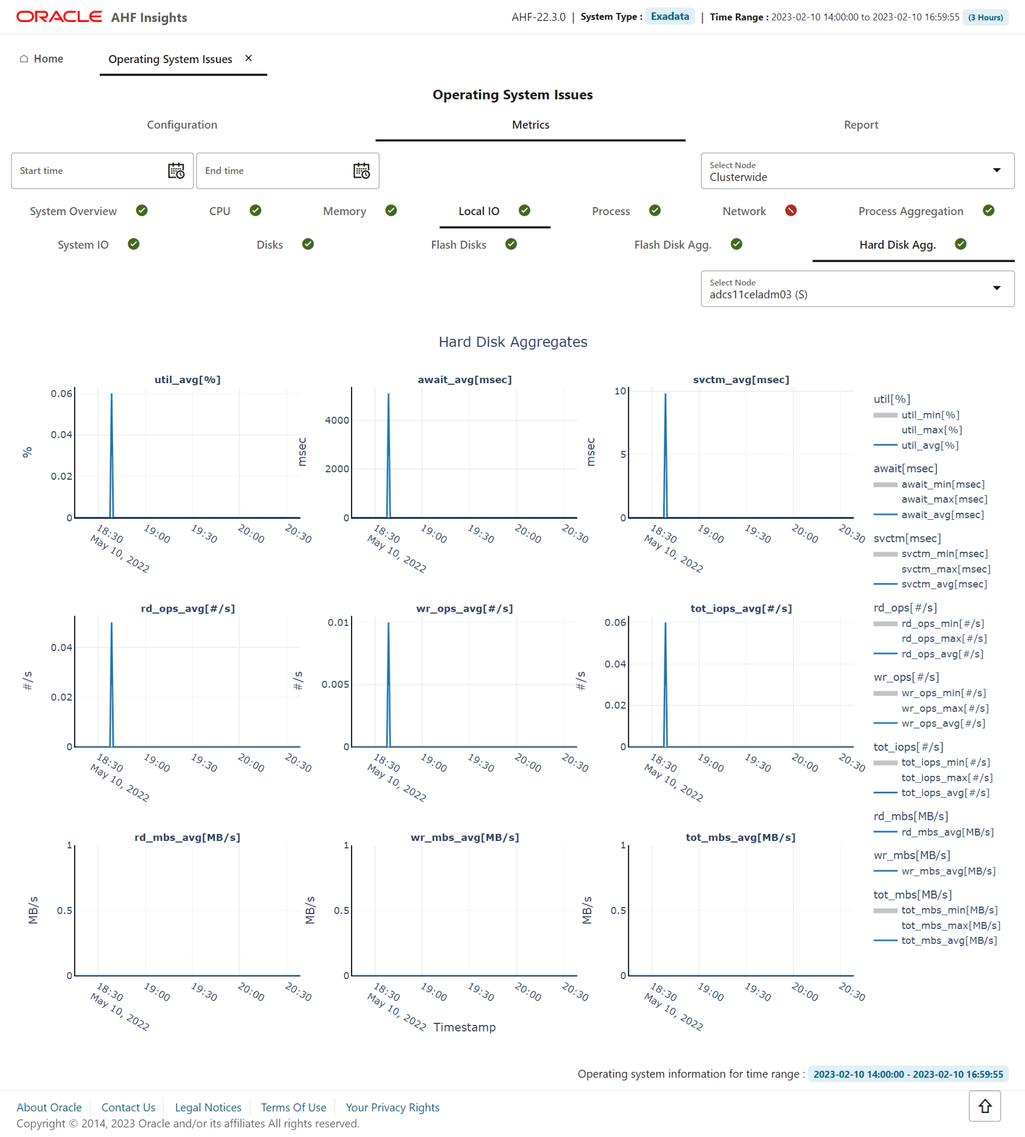
Select Node: Clusterwide

Select Node: adcs11celadm03 (S)

Operating system information for time range : 2023-02-10 14:00:00 - 2023-02-10 16:59:55

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-17 Operating System Issues - Metrics - Local I/O - Hard Disk Aggregation



AHF-22.3.0 | System Type : Exadata | Time Range : 2023-02-10 14:00:00 to 2023-02-10 16:59:55 (3 Hours)

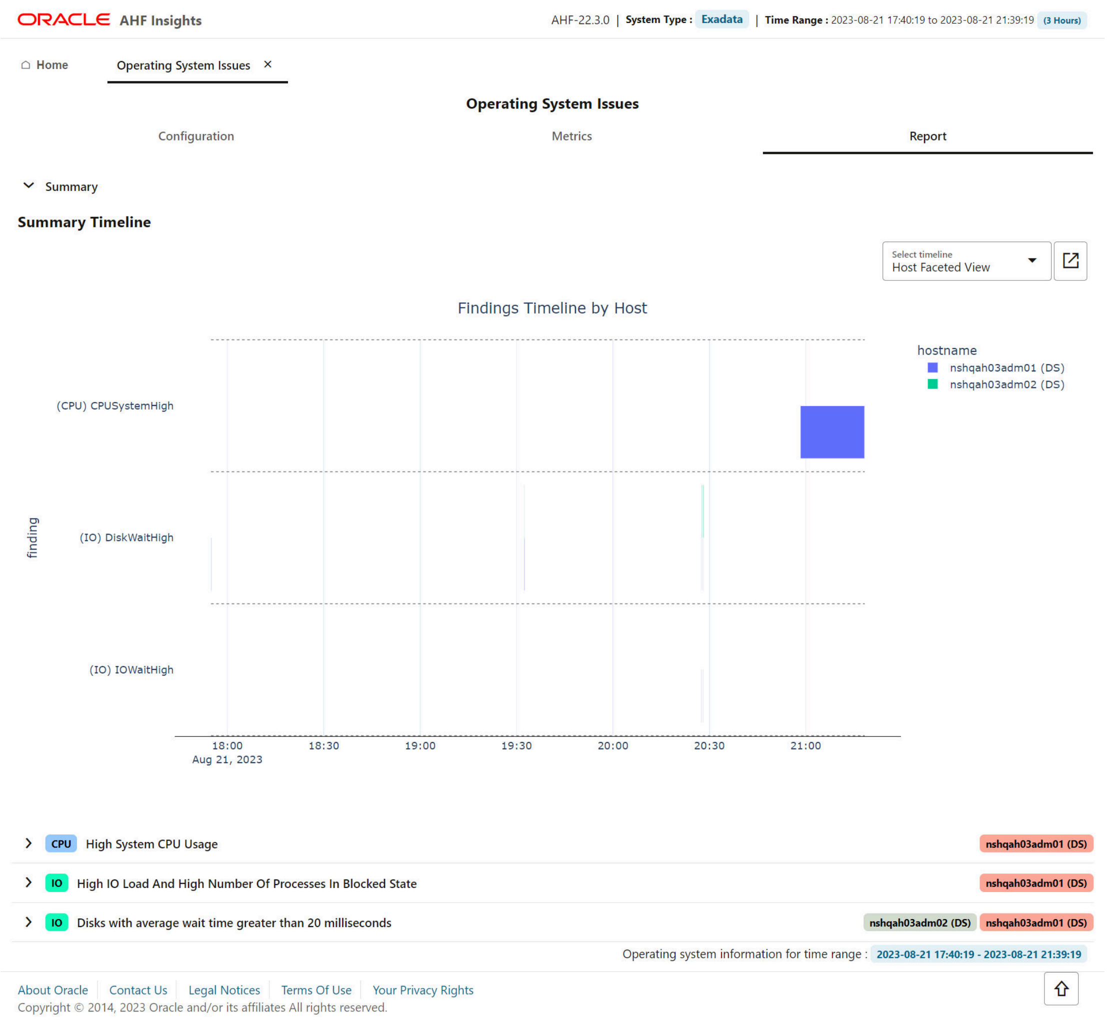
Select Node
Clusterwide

Select Node
adcs11celadm03 (S)

Operating system information for time range : 2023-02-10 14:00:00 - 2023-02-10 16:59:55

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-18 Operating System Issues - Report



CPU	High System CPU Usage	nshqah03adm01 (DS)
IO	High IO Load And High Number Of Processes In Blocked State	nshqah03adm01 (DS)
IO	Disks with average wait time greater than 20 milliseconds	nshqah03adm02 (DS) nshqah03adm01 (DS)

Operating system information for time range : 2023-08-21 17:40:19 - 2023-08-21 21:39:19

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Provides details about the metrics collected on the system and a detailed report on operating system anomalies. This page presents three views, **Configuration**, **Metrics**, and **Report**.

Metrics view has tabs displaying CPU, Memory, System I/O, Process, Network interface, Process aggregation metrics, and green and red icons indicating the statuses. From the drop-down list at the upper-right corner, select a node for which you want to view the metrics. Select a time range from the calendar widget to view metrics for that period.

Report view includes Summary Timeline and Observed Findings.

Configuration

This tab showcases CPU, Memory, IO, and Network configuration details of the systems from where operating system metrics were collected.

Metrics

System Overview

This tab showcases overview of resources such as CPU, memory, processes, and I/O operation.

- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

CPU Metrics

This tab showcases CPU metrics.

- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

Memory Metrics

This tab showcases memory metrics.

- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

Local I/O Metrics

This tab show case System IO metrics.

- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

Process Metrics

This tab showcases process metrics.

- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

Network Metrics

This tab showcases network interface metrics.

- Select different metrics related to network like interface, IP, UDP, and TCP.
- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

Process Aggregation Metrics

This tab showcases aggregation of process metrics.

- Select a node from the Select Node drop-down list to view node-specific process aggregation metrics.
- Hover over a specific point in time of the graph to get detailed information.
- Zoom into the timeline.

Report

With Report view, explore the findings in a drop-down fashion with a full widescreen view.

You can:

- view the Event information in a subplot within the Summary Timeline Gantt Chart

- explore the top ranked metrics in tables under a problem finding in a visual format
- view the metrics associated with the prblem finding in a visual format
- drill down into the detailed state of the system at a specific problematic point in time under 'Problematic Snapshots' section. Problem specific system snapshots are organized into dropdowns ordered by problem timestamp

5.2.2.3 Best Practice Issues

AHF 23.8

Starting in AHF 23.8, AHF compliance checks from Oracle Orachk and Oracle Exachk are integrated into AHF Insights Best Practice Issues section.

AHF has thousands of Best Practice Compliance Checks, which are run automatically by AHF Oracle Orachk and Oracle Exachk. The results of these checks are viewable in HTML reports and output in JSON and XML for consumption into other tools. In addition, all Best Practice Compliance Checks are fully integrated into AHF Insights for running on-demand.

AHF Insights makes it easy to quickly see the Health Score, understand where systems are out of compliance and then take the necessary corrective action.

With this enhancement, you can:

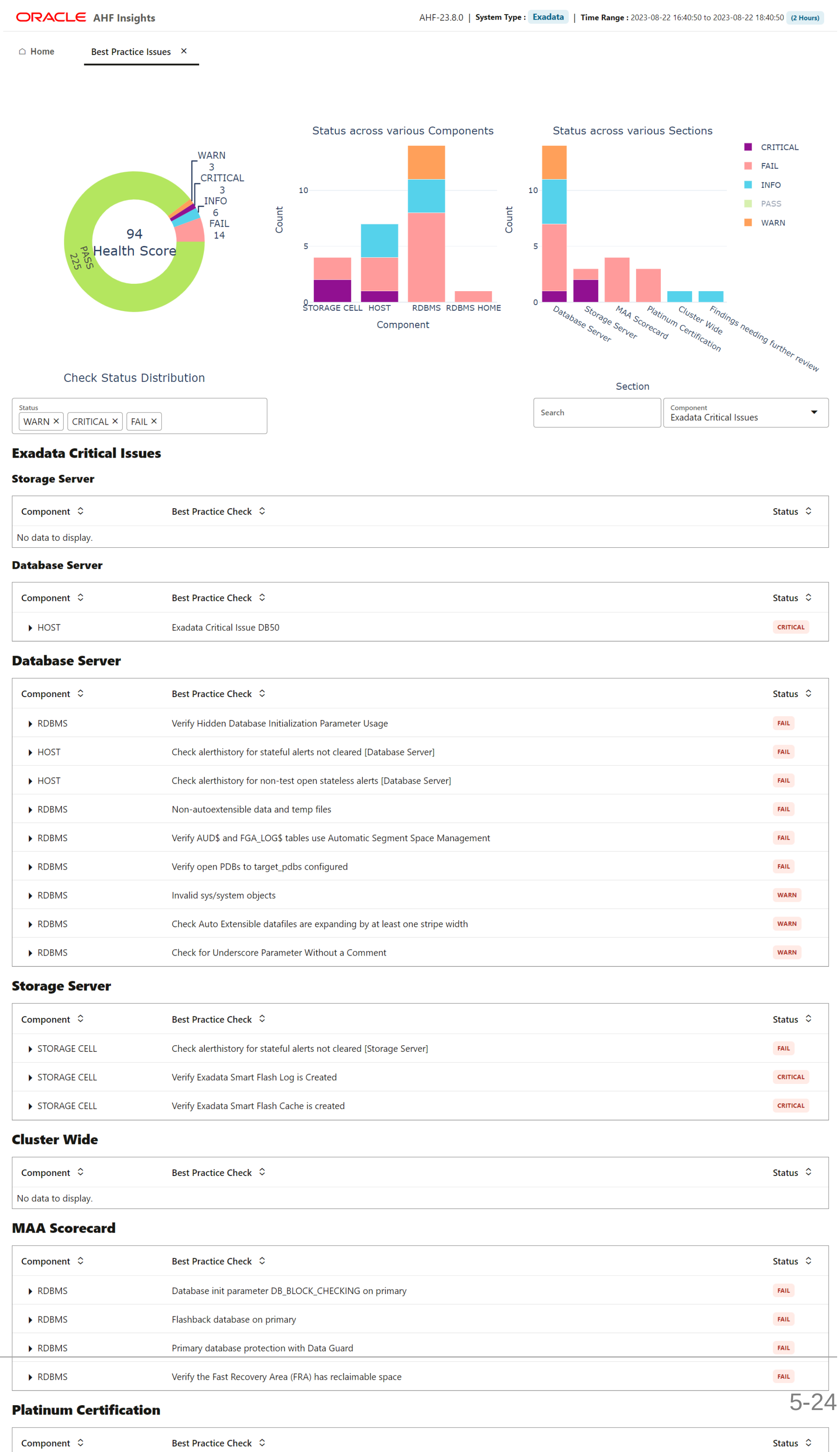
- Explore the best practice data in a visual format.
- Filter best practices across different status through visualization and Status status drop-down.
- Search checks from all sections of best practice report.
- View the best practice report in a vertical fashion.
- See the health score with a visual distribution of checks that have failed.

Continue to use the Oracle Orachk / Oracle Exachk commands for automated scheduled runs, but for on-demand compliance investigation, generate an AHF Insights report:

```
ahf analysis create --type insights
```

How does AHF Insights UI render this information

Figure 5-19   Best Practice Issues



Exadata Critical Issues

Storage Server

Component	Best Practice Check	Status
No data to display.		

Database Server

Component	Best Practice Check	Status
HOST	Exadata Critical Issue DB50	CRITICAL

Database Server

Component	Best Practice Check	Status
RDBMS	Verify Hidden Database Initialization Parameter Usage	FAIL
HOST	Check alerthistory for stateful alerts not cleared [Database Server]	FAIL
HOST	Check alerthistory for non-test open stateless alerts [Database Server]	FAIL
RDBMS	Non-autoextensible data and temp files	FAIL
RDBMS	Verify AUD$ and FGA_LOG$ tables use Automatic Segment Space Management	FAIL
RDBMS	Verify open PDBs to target_pdbs configured	FAIL
RDBMS	Invalid sys/system objects	WARN
RDBMS	Check Auto Extensible datafiles are expanding by at least one stripe width	WARN
RDBMS	Check for Underscore Parameter Without a Comment	WARN

Storage Server

Component	Best Practice Check	Status
STORAGE CELL	Check alerthistory for stateful alerts not cleared [Storage Server]	FAIL
STORAGE CELL	Verify Exadata Smart Flash Log is Created	CRITICAL
STORAGE CELL	Verify Exadata Smart Flash Cache is created	CRITICAL

Cluster Wide

Component	Best Practice Check	Status
No data to display.		

MAA Scorecard

Component	Best Practice Check	Status
RDBMS	Database init parameter DB_BLOCK_CHECKING on primary	FAIL
RDBMS	Flashback database on primary	FAIL
RDBMS	Primary database protection with Data Guard	FAIL
RDBMS	Verify the Fast Recovery Area (FRA) has reclaimable space	FAIL

Platinum Certification

Component	Best Practice Check	Status

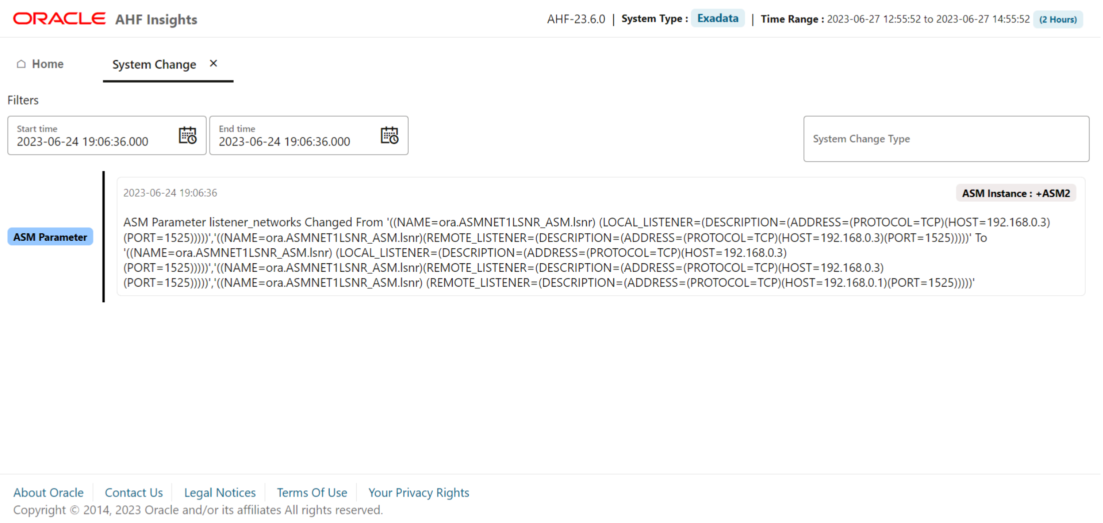
Provides the results of Best Practices Compliance checks run on the system, paginated. The details include the list of Components on which the checks were run, the Best Practice Checks that were run on the components, and Statuses of those checks.

- Hover the mouse pointer over doughnut pie chart and stacked bar chart to view snippets in a tooltip.
- Filter the checks by severity - **CRITICAL**, **FAIL**, **WARN**, **PASS**, and **INFO**.
- Use the **Component** drop-down list to navigate to different sections of the report.
- Click the arrow on each entry in the table to view details of one specific issue.

5.2.2.4 System Change

How does AHF Insights UI render this information

Figure 5-20 System Change



AHF-23.6.0 | **System Type :** Exadata | **Time Range :** 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Start time 2023-06-24 19:06:36.000

End time 2023-06-24 19:06:36.000

System Change Type

ASM Parameter

2023-06-24 19:06:36

ASM Instance : +ASM2

ASM Parameter listener_networks Changed From '((NAME=ora.ASMNET1LSNR_ASM.lsnr) (LOCAL_LISTENER=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.0.3)(PORT=1525)))))','((NAME=ora.ASMNET1LSNR_ASM.lsnr)(REMOTE_LISTENER=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.0.3)(PORT=1525)))))' To '((NAME=ora.ASMNET1LSNR_ASM.lsnr) (LOCAL_LISTENER=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.0.3)(PORT=1525)))))','((NAME=ora.ASMNET1LSNR_ASM.lsnr)(REMOTE_LISTENER=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.0.3)(PORT=1525)))))','((NAME=ora.ASMNET1LSNR_ASM.lsnr) (REMOTE_LISTENER=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.0.1)(PORT=1525)))))'

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides details on the changes applied to the system, paginated.

- Search values using the filter section.
- Filter by a specific time range.

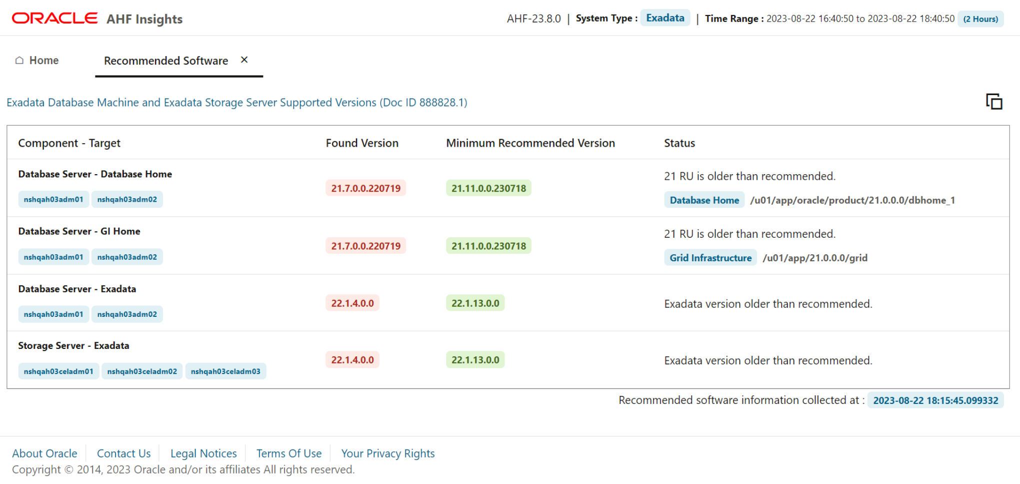
5.2.2.5 Recommended Software

AHF 23.8

Starting in AHF 23.8, you will be able copy data in text format into the clipboard to post it into SR body while raising a service request.

How does AHF Insights UI render this information

Figure 5-21   Recommended Software



ORACLE AHF Insights
AHF-23.8.0 | System Type : Exadata | Time Range : 2023-08-22 16:40:50 to 2023-08-22 18:40:50 (2 Hours)
Home
Recommended Software ×

Exadata Database Machine and Exadata Storage Server Supported Versions (Doc ID 888828.1)

Component - Target	Found Version	Minimum Recommended Version	Status
Database Server - Database Home nshqah03adm01 nshqah03adm02	21.7.0.0.220719	21.11.0.0.230718	21 RU is older than recommended. Database Home /u01/app/oracle/product/21.0.0.0/dbhome_1
Database Server - GI Home nshqah03adm01 nshqah03adm02	21.7.0.0.220719	21.11.0.0.230718	21 RU is older than recommended. Grid Infrastructure /u01/app/21.0.0.0/grid
Database Server - Exadata nshqah03adm01 nshqah03adm02	22.1.4.0.0	22.1.13.0.0	Exadata version older than recommended.
Storage Server - Exadata nshqah03celadm01 nshqah03celadm02 nshqah03celadm03	22.1.4.0.0	22.1.13.0.0	Exadata version older than recommended.

Recommended software information collected at : 2023-08-22 18:15:45.099332

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Lists recommended software and links to supported versions.

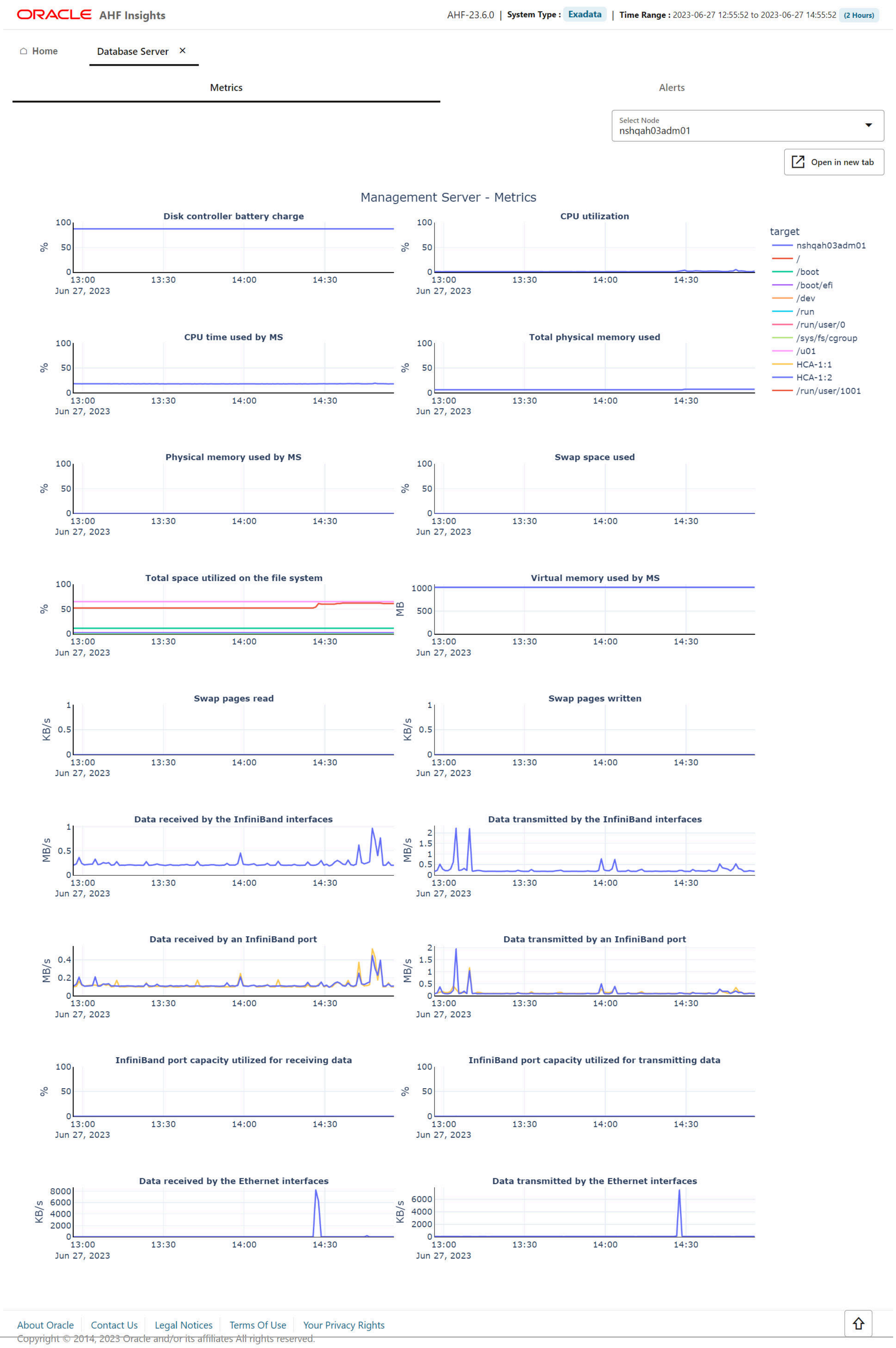
5.2.2.6 Database Server

How does AHF Insights UI render this information

Database Server includes two sections, Management Server **Metrics** and **Alerts** recorded in Management Server across Hardware , Software, and ADR.

Metrics

Figure 5-22 Database Server Metrics



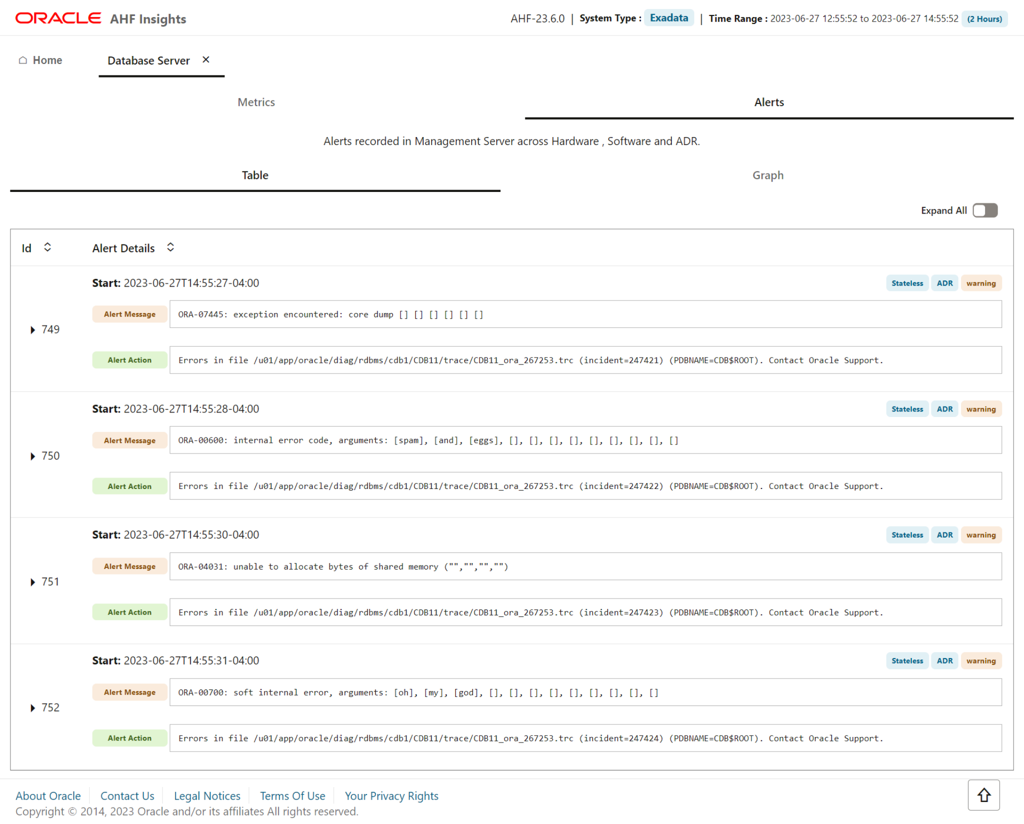
ORACLE AHF Insights
AHF-23.6.0 | System Type : Exadata | Time Range : 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)
Home
Database Server ✕
Metrics
Alerts
Select Node
nshqah03adm01
Open in new tab
Management Server - Metrics
Disk controller battery charge
CPU utilization
CPU time used by MS
Total physical memory used
Physical memory used by MS
Swap space used
Total space utilized on the file system
Virtual memory used by MS
Swap pages read
Swap pages written
Data received by the InfiniBand interfaces
Data transmitted by the InfiniBand interfaces
Data received by an InfiniBand port
Data transmitted by an InfiniBand port
InfiniBand port capacity utilized for receiving data
InfiniBand port capacity utilized for transmitting data
Data received by the Ethernet interfaces
Data transmitted by the Ethernet interfaces
%
MB
KB/s
MB/s
0
50
100
500
1000
0.5
1
1.5
2
0.2
0.4
2000
4000
6000
8000
13:00
13:30
14:00
14:30
Jun 27, 2023
target
nshqah03adm01
/
/boot
/boot/efi
/dev
/run
/run/user/0
/sys/fs/cgroup
/u01
HCA-1:1
HCA-1:2
/run/user/1001
About Oracle
Contact Us
Legal Notices
Terms Of Use
Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Metrics section provdies details about the Management Server metrics such as Disk controller battery charge, CPU utilization, CPU time used by the Management Server, Total space utilized on the file system, and so on.

- From the drop-down list, select a host for which you want to view the metrics.

Alerts

Figure 5-23 Database Server Alerts



AHF-23.6.0 | **System Type :** Exadata | **Time Range :** 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Alerts recorded in Management Server across Hardware , Software and ADR.

Id	Alert Details
749	**Start:** 2023-06-27T14:55:27-04:00 Stateless ADR warning Alert Message: `ORA-07445: exception encountered: core dump [] [] [] [] [] []` Alert Action: `Errors in file /u01/app/oracle/diag/rdbms/cdb1/CDB11/trace/CDB11_ora_267253.trc (incident=247421) (PDBNAME=CDB$ROOT). Contact Oracle Support.`
750	**Start:** 2023-06-27T14:55:28-04:00 Stateless ADR warning Alert Message: `ORA-00600: internal error code, arguments: [spam], [and], [eggs], [], [], [], [], [], [], [], [], []` Alert Action: `Errors in file /u01/app/oracle/diag/rdbms/cdb1/CDB11/trace/CDB11_ora_267253.trc (incident=247422) (PDBNAME=CDB$ROOT). Contact Oracle Support.`
751	**Start:** 2023-06-27T14:55:30-04:00 Stateless ADR warning Alert Message: `ORA-04031: unable to allocate bytes of shared memory ("","","","")` Alert Action: `Errors in file /u01/app/oracle/diag/rdbms/cdb1/CDB11/trace/CDB11_ora_267253.trc (incident=247423) (PDBNAME=CDB$ROOT). Contact Oracle Support.`
752	**Start:** 2023-06-27T14:55:31-04:00 Stateless ADR warning Alert Message: `ORA-00700: soft internal error, arguments: [oh], [my], [god], [], [], [], [], [], [], [], [], []` Alert Action: `Errors in file /u01/app/oracle/diag/rdbms/cdb1/CDB11/trace/CDB11_ora_267253.trc (incident=247424) (PDBNAME=CDB$ROOT). Contact Oracle Support.`

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Alerts section provides details about the Alerts recorded in the Management Server across hardware, software, and ADR. Alert section has two views, **Table** and **Graph**.

Table view provides Alert Details such as description of the alert and the remedial action you can take, in tabular format.

- Click the **Expand All** toggle button to view details of all alerts.
- Click the arrow to view detailed information about an alert.

Graph view categorises the alerts by severity such as Critical and Warning, and type such as Stateful and Stateless.

- Click the **Show open alerts** toggle button to view the list of open alerts. The button is turned on by default.

Related Topics

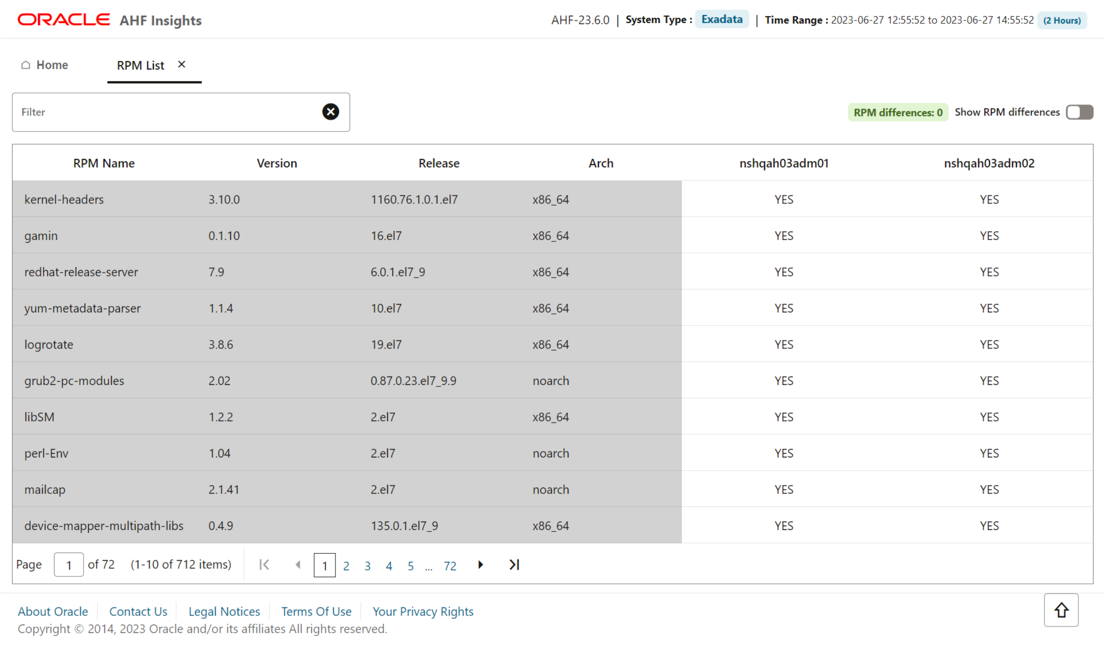
- Using the DBMCLI Utility

- Exadata Metrics
- Exadata Alerts

5.2.2.7 RPM List

How does AHF Insights UI render this information

Figure 5-24 List of RPMs



AHF Insights

AHF-23.6.0 | **System Type :** Exadata | **Time Range :** 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Home | RPM List ×

Filter

RPM differences: 0 | Show RPM differences

RPM Name	Version	Release	Arch	nshqah03adm01	nshqah03adm02
kernel-headers	3.10.0	1160.76.1.0.1.el7	x86_64	YES	YES
gamin	0.1.10	16.el7	x86_64	YES	YES
redhat-release-server	7.9	6.0.1.el7_9	x86_64	YES	YES
yum-metadata-parser	1.1.4	10.el7	x86_64	YES	YES
logrotate	3.8.6	19.el7	x86_64	YES	YES
grub2-pc-modules	2.02	0.87.0.23.el7_9.9	noarch	YES	YES
libSM	1.2.2	2.el7	x86_64	YES	YES
perl-Env	1.04	2.el7	noarch	YES	YES
mailcap	2.1.41	2.el7	noarch	YES	YES
device-mapper-multipath-libs	0.4.9	135.0.1.el7_9	x86_64	YES	YES

Page 1 of 72 (1-10 of 712 items) 1 2 3 4 5 ... 72

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

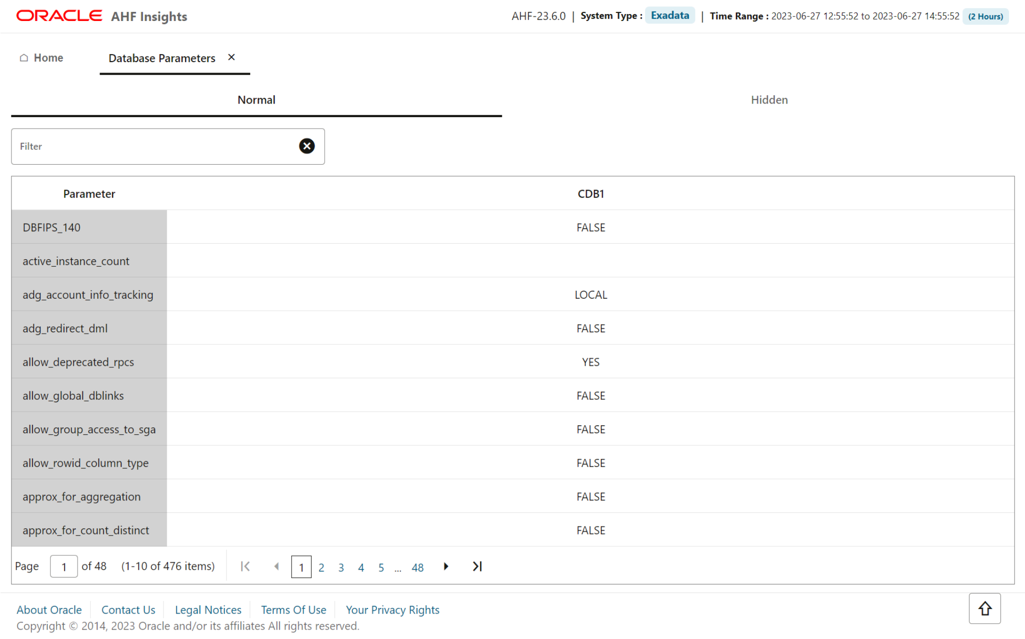
Lists RPMs and the differences between them across nodes, paginated.

- Enter the name of the parameter in the filter field to filter the RPMs.
- The **RPM Name**, **Version**, **Release**, and **Arch** columns remains fixed.
- Click the **Show RPM differences** toggle button to view the differences between the RPMs across nodes.

5.2.2.8 Database Parameters

How does AHF Insights UI render this information

Figure 5-25 Oracle Database Parameters - Normal



ORACLE AHF Insights

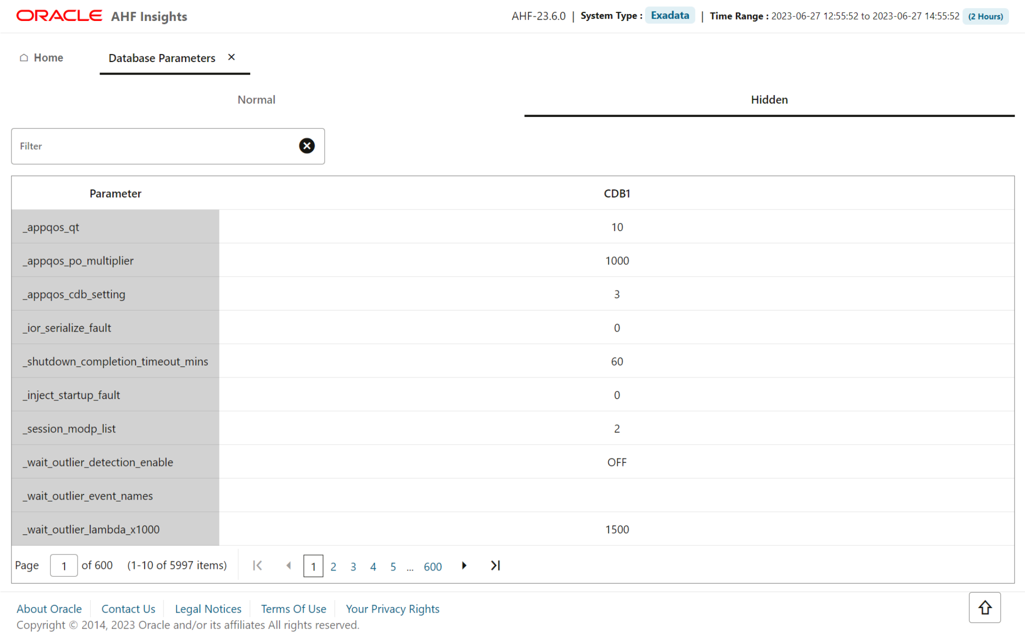
AHF-23.6.0 | System Type : Exadata | Time Range : 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Parameter	CDB1
DBFIPS_140	FALSE
active_instance_count	
adg_account_info_tracking	LOCAL
adg_redirect_dml	FALSE
allow_deprecated_rpcs	YES
allow_global_dblinks	FALSE
allow_group_access_to_sga	FALSE
allow_rowid_column_type	FALSE
approx_for_aggregation	FALSE
approx_for_count_distinct	FALSE

Page 1 of 48 (1-10 of 476 items) 1 2 3 4 5 ... 48

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-26 Oracle Database Parameters - Hidden



ORACLE AHF Insights

AHF-23.6.0 | System Type : Exadata | Time Range : 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Parameter	CDB1
_appqos_qt	10
_appqos_po_multiplier	1000
_appqos_cdb_setting	3
_ior_serialize_fault	0
_shutdown_completion_timeout_mins	60
_inject_startup_fault	0
_session_modp_list	2
_wait_outlier_detection_enable	OFF
_wait_outlier_event_names	
_wait_outlier_lambda_x1000	1500

Page 1 of 600 (1-10 of 5997 items) 1 2 3 4 5 ... 600

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

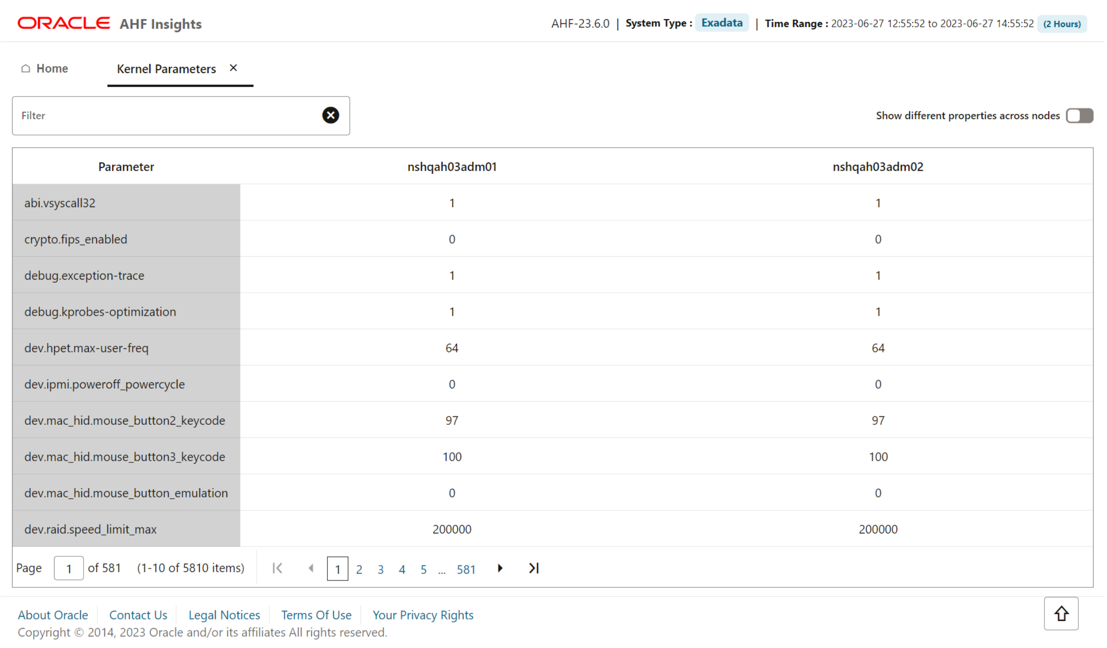
Lists normal and hidden Oracle Database parameters, paginated. This page also provides two views, **Normal** and **Hidden**. Normal view is displayed by default.

- Enter the name of the parameter in the filter field to filter the parameters.
- The **Parameter** column remains fixed and you can view the properties of each parameter across multiple databases.
- Click the **Show different properties across databases** toggle button to view different properties across databases.
- Click **Hidden** to view the hidden parameter.

5.2.2.9 Kernel Parameters

How does AHF Insights UI render this information

Figure 5-27 Kernel Parameters



AHF-23.6.0 | System Type : Exadata | Time Range : 2023-06-27 12:55:52 to 2023-06-27 14:55:52 (2 Hours)

Parameter	nshqah03adm01	nshqah03adm02
abi.vsyscall32	1	1
crypto.fips_enabled	0	0
debug.exception-trace	1	1
debug.kprobes-optimization	1	1
dev.hpet.max-user-freq	64	64
dev.ipmi.poweroff_powercycle	0	0
dev.mac_hid.mouse_button2_keycode	97	97
dev.mac_hid.mouse_button3_keycode	100	100
dev.mac_hid.mouse_button_emulation	0	0
dev.raid.speed_limit_max	200000	200000

Page 1 of 581 (1-10 of 5810 items) 1 2 3 4 5 ... 581

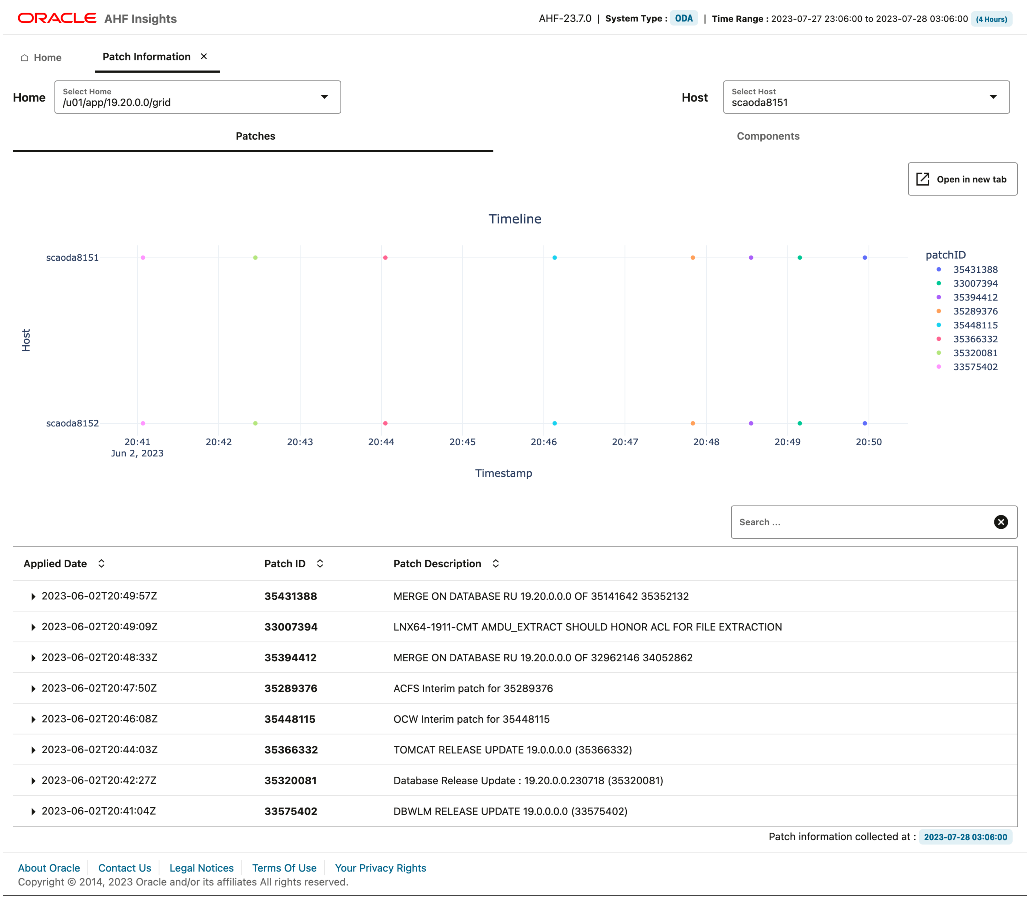
Lists the kernel parameters, paginated.

- Enter the name of the parameter in the filter field to filter the parameters.
- The **Parameter** column remains fixed and you can view the properties of each parameter across multiple hosts/nodes.
- Click the **Show different properties across hosts/nodes** toggle button to view different properties across hosts/nodes.

5.2.2.10 Patch Information

How does AHF Insights UI render this information

Figure 5-28 Patch Information



AHF-23.7.0 | System Type : ODA | Time Range : 2023-07-27 23:06:00 to 2023-07-28 03:06:00 (4 Hours)

Home: Select Home /u01/app/19.20.0.0/grid

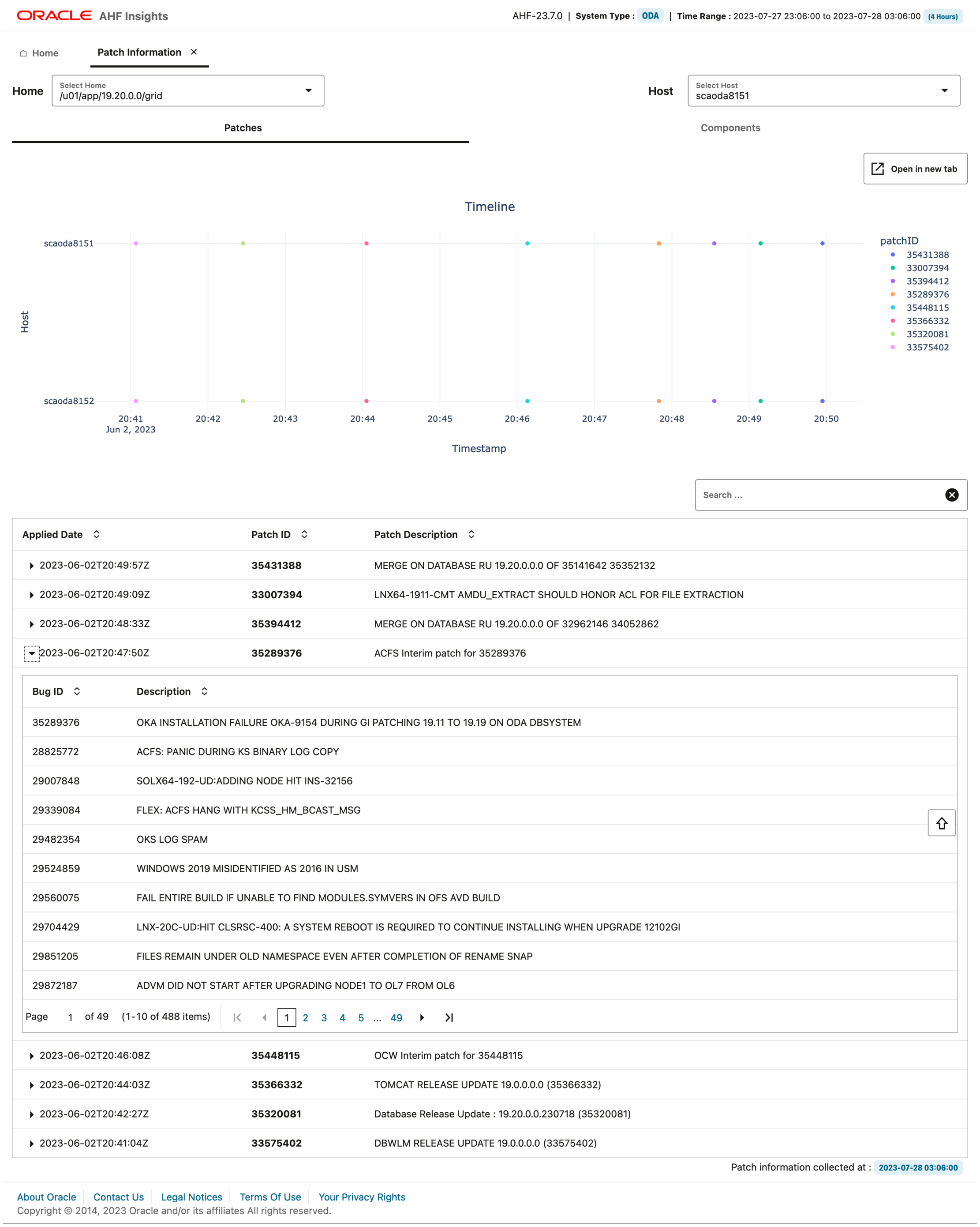
Host: Select Host scaoda8151

Applied Date	Patch ID	Patch Description
2023-06-02T20:49:57Z	**35431388**	MERGE ON DATABASE RU 19.20.0.0.0 OF 35141642 35352132
2023-06-02T20:49:09Z	**33007394**	LNX64-1911-CMT AMDU_EXTRACT SHOULD HONOR ACL FOR FILE EXTRACTION
2023-06-02T20:48:33Z	**35394412**	MERGE ON DATABASE RU 19.20.0.0.0 OF 32962146 34052862
2023-06-02T20:47:50Z	**35289376**	ACFS Interim patch for 35289376
2023-06-02T20:46:08Z	**35448115**	OCW Interim patch for 35448115
2023-06-02T20:44:03Z	**35366332**	TOMCAT RELEASE UPDATE 19.0.0.0.0 (35366332)
2023-06-02T20:42:27Z	**35320081**	Database Release Update : 19.20.0.0.230718 (35320081)
2023-06-02T20:41:04Z	**33575402**	DBWLM RELEASE UPDATE 19.0.0.0.0 (33575402)

Patch information collected at : 2023-07-28 03:06:00

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-29 Patch Information - Timeline



AHF-23.7.0 | **System Type :** ODA | **Time Range :** 2023-07-27 23:06:00 to 2023-07-28 03:06:00 (4 Hours)

Home Select Home: /u01/app/19.20.0.0/grid

Host Select Host: scaoda8151

Applied Date	Patch ID	Patch Description
2023-06-02T20:49:57Z	**35431388**	MERGE ON DATABASE RU 19.20.0.0.0 OF 35141642 35352132
2023-06-02T20:49:09Z	**33007394**	LNX64-1911-CMT AMDU_EXTRACT SHOULD HONOR ACL FOR FILE EXTRACTION
2023-06-02T20:48:33Z	**35394412**	MERGE ON DATABASE RU 19.20.0.0.0 OF 32962146 34052862
2023-06-02T20:47:50Z	**35289376**	ACFS Interim patch for 35289376

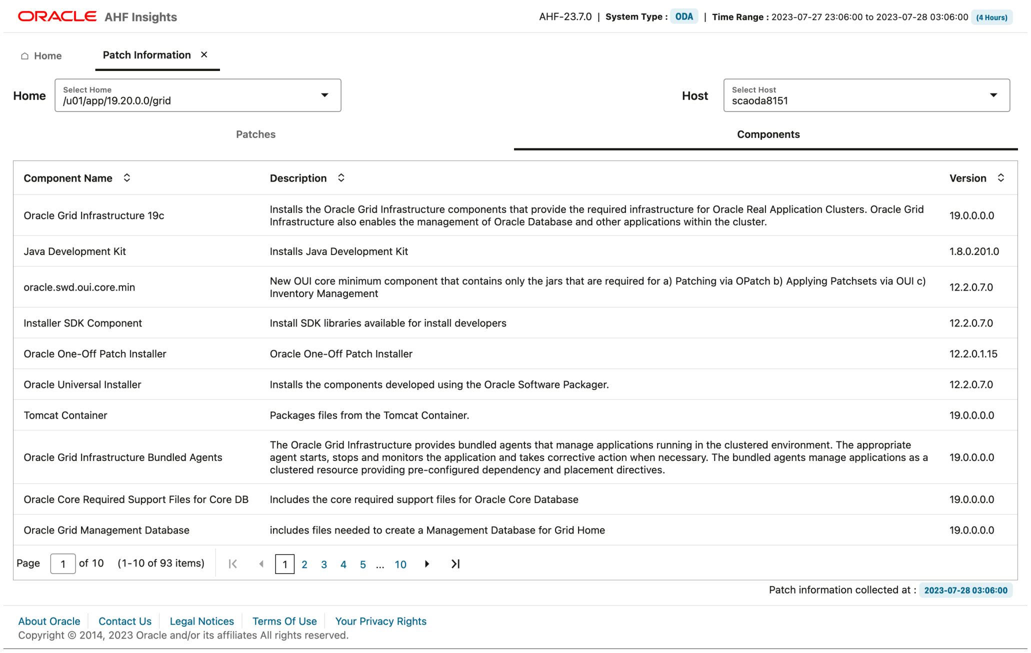
Bug ID	Description
35289376	OKA INSTALLATION FAILURE OKA-9154 DURING GI PATCHING 19.11 TO 19.19 ON ODA DBSYSTEM
28825772	ACFS: PANIC DURING KS BINARY LOG COPY
29007848	SOLX64-192-UD:ADDING NODE HIT INS-32156
29339084	FLEX: ACFS HANG WITH KCSS_HM_BCAST_MSG
29482354	OKS LOG SPAM
29524859	WINDOWS 2019 MISIDENTIFIED AS 2016 IN USM
29560075	FAIL ENTIRE BUILD IF UNABLE TO FIND MODULES.SYMVERS IN OFS AVD BUILD
29704429	LNX-20C-UD:HIT CLSRSC-400: A SYSTEM REBOOT IS REQUIRED TO CONTINUE INSTALLING WHEN UPGRADE 12102GI
29851205	FILES REMAIN UNDER OLD NAMESPACE EVEN AFTER COMPLETION OF RENAME SNAP
29872187	ADVM DID NOT START AFTER UPGRADING NODE1 TO OL7 FROM OL6

Applied Date	Patch ID	Patch Description
2023-06-02T20:46:08Z	**35448115**	OCW Interim patch for 35448115
2023-06-02T20:44:03Z	**35366332**	TOMCAT RELEASE UPDATE 19.0.0.0.0 (35366332)
2023-06-02T20:42:27Z	**35320081**	Database Release Update : 19.20.0.0.230718 (35320081)
2023-06-02T20:41:04Z	**33575402**	DBWLM RELEASE UPDATE 19.0.0.0.0 (33575402)

Patch information collected at : 2023-07-28 03:06:00

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Figure 5-30 Patch Information - Components



Component Name	Description	Version
Oracle Grid Infrastructure 19c	Installs the Oracle Grid Infrastructure components that provide the required infrastructure for Oracle Real Application Clusters. Oracle Grid Infrastructure also enables the management of Oracle Database and other applications within the cluster.	19.0.0.0.0
Java Development Kit	Installs Java Development Kit	1.8.0.201.0
oracle.swd.oui.core.min	New OUI core minimum component that contains only the jars that are required for a) Patching via OPatch b) Applying Patchsets via OUI c) Inventory Management	12.2.0.7.0
Installer SDK Component	Install SDK libraries available for install developers	12.2.0.7.0
Oracle One-Off Patch Installer	Oracle One-Off Patch Installer	12.2.0.1.15
Oracle Universal Installer	Installs the components developed using the Oracle Software Packager.	12.2.0.7.0
Tomcat Container	Packages files from the Tomcat Container.	19.0.0.0.0
Oracle Grid Infrastructure Bundled Agents	The Oracle Grid Infrastructure provides bundled agents that manage applications running in the clustered environment. The appropriate agent starts, stops and monitors the application and takes corrective action when necessary. The bundled agents manage applications as a clustered resource providing pre-configured dependency and placement directives.	19.0.0.0.0
Oracle Core Required Support Files for Core DB	Includes the core required support files for Oracle Core Database	19.0.0.0.0
Oracle Grid Management Database	includes files needed to create a Management Database for Grid Home	19.0.0.0.0

Patch information collected at : 2023-07-28 03:06:00

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Provides a list of patches to keep track of which patch was applied to which hosts, where (Oracle Database home or Grid home), and when (timeline). Gaps or inconsistencies in patching are highlighted across nodes for the same home. Lists bugs that a particular patch provides the fixes for. Bugs and relevant patch information can be quickly searched and viewed via interactive reports.

Patches tab:

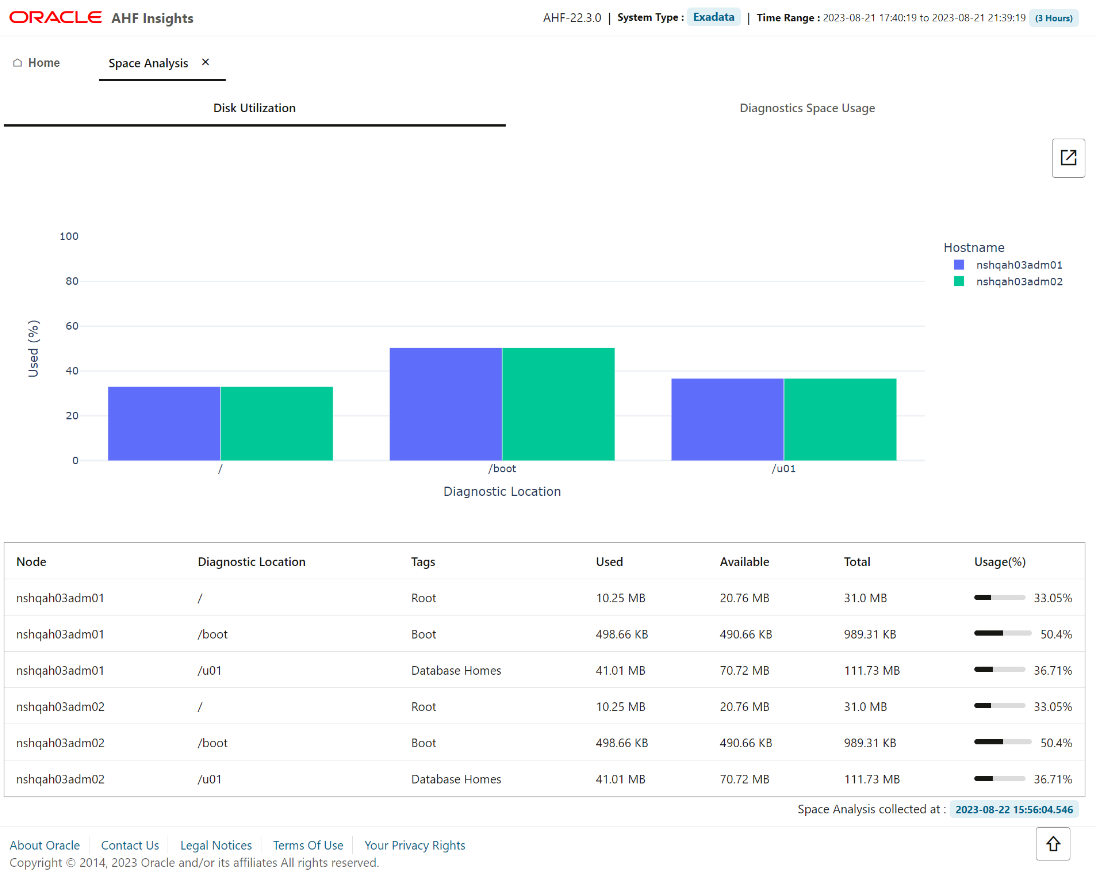
- In the Timeline section, double-click a patch ID to view on which host and when the patch was applied.
- Enter the patch ID in the filter field to filter and view the patch details.
- Under **Applied Date**, click the right arrow key to view list of bugs that a particular patch addresses.
- Click the X mark to clear the filter.

Components tab: Provides a paginated list components and their version affected by applying the patches.

5.2.2.11 Space Analysis

How does AHF Insights UI render this information

Figure 5-31 Disk Utilization



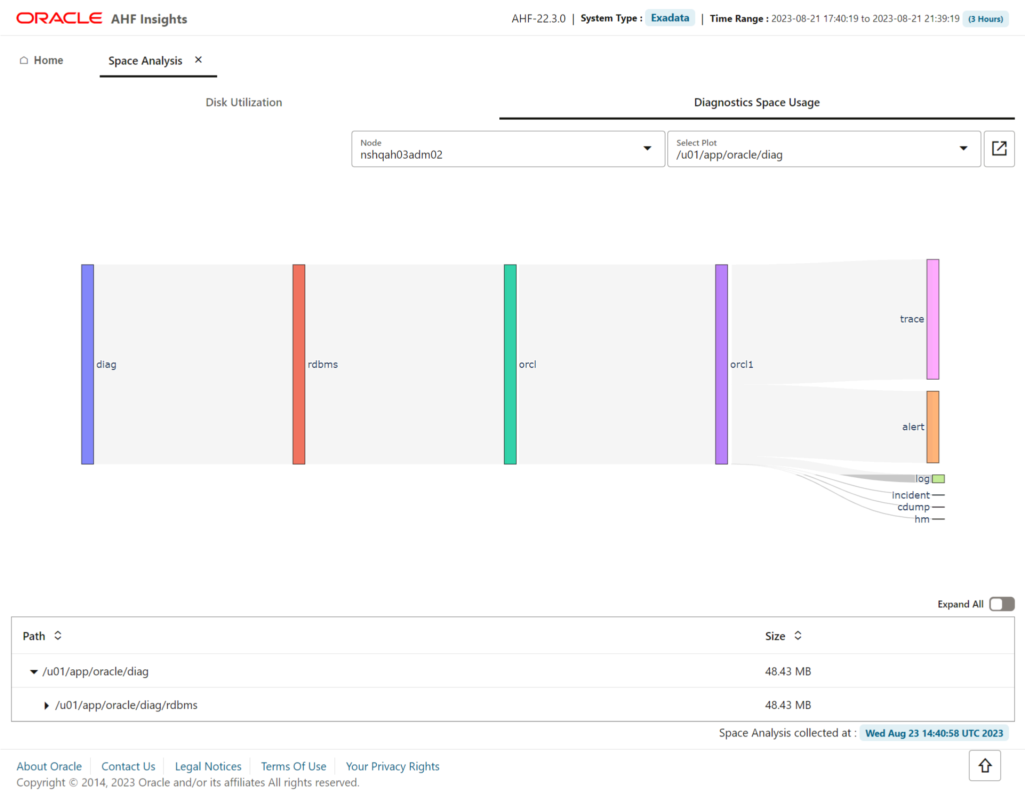
AHF-22.3.0 | System Type : Exadata | Time Range : 2023-08-21 17:40:19 to 2023-08-21 21:39:19 (3 Hours)

Node	Diagnostic Location	Tags	Used	Available	Total	Usage(%)
nshqah03adm01	/	Root	10.25 MB	20.76 MB	31.0 MB	33.05%
nshqah03adm01	/boot	Boot	498.66 KB	490.66 KB	989.31 KB	50.4%
nshqah03adm01	/u01	Database Homes	41.01 MB	70.72 MB	111.73 MB	36.71%
nshqah03adm02	/	Root	10.25 MB	20.76 MB	31.0 MB	33.05%
nshqah03adm02	/boot	Boot	498.66 KB	490.66 KB	989.31 KB	50.4%
nshqah03adm02	/u01	Database Homes	41.01 MB	70.72 MB	111.73 MB	36.71%

Space Analysis collected at : 2023-08-22 15:56:04.546

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights
Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Figure 5-32   Diagnostic Space Usage



ORACLE AHF Insights

AHF-22.3.0 | System Type : Exadata | Time Range : 2023-08-21 17:40:19 to 2023-08-21 21:39:19 (3 Hours)

Node: nshqah03adm02

Select Plot: /u01/app/oracle/diag

Path	Size
▾ /u01/app/oracle/diag	48.43 MB
▸ /u01/app/oracle/diag/rdbms	48.43 MB

Space Analysis collected at : Wed Aug 23 14:40:58 UTC 2023

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Disk Utilization tab: Provides a paginated view of host-wise directory structure, space consumed by directories and files, and available space.

Diagnostic Space Usage tab: Provides a paginated view of disk spave consumed by diagnostics. Use the drop-down lists to filter by nodes and diagnostics collected..

Related Topics

- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.
- tfactl get
  Use the `tfactl get` command to view the details of various Oracle Trace File Analyzer configuration settings.

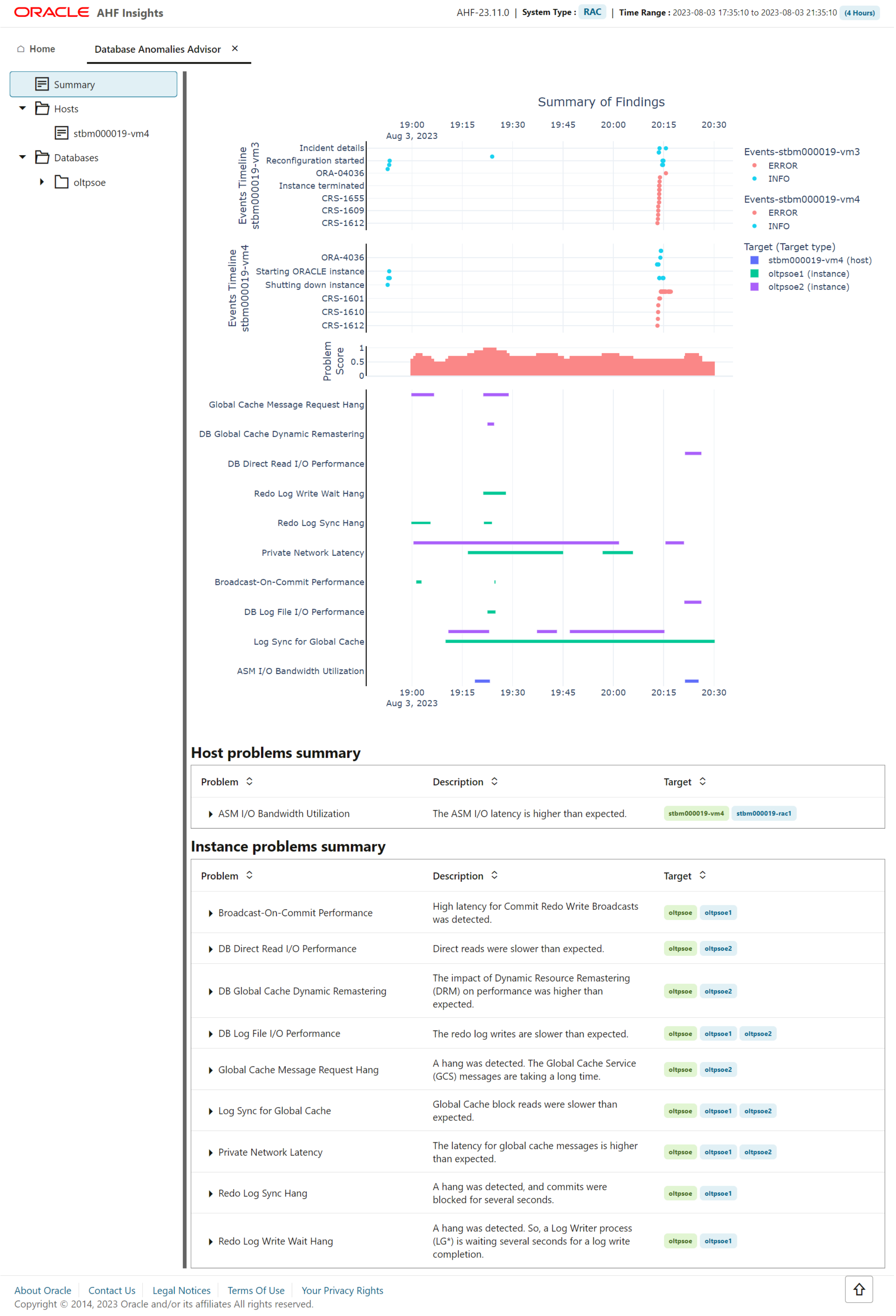
5.2.2.12 Database Anomalies Advisor

AHF detects database anomalies and identifies the cause and corrective action.

The Database Anomalies Advisor shows a summary timeline of anomalies for hosts and database instances. Findings can be drilled into to understand the cause and recommendation action.

To view the Database Anomalies Advisor and it’s recommendations, run `ahf analysis create --type insights`, open the resulting report, and click **Database Anomalies Advisor**.

Figure 5-33 Database Anomalies Advisor



Host problems summary

Problem	Description	Target
ASM I/O Bandwidth Utilization	The ASM I/O latency is higher than expected.	stbm000019-vm4 stbm000019-rac1

Instance problems summary

Problem	Description	Target
Broadcast-On-Commit Performance	High latency for Commit Redo Write Broadcasts was detected.	oltpsoe oltpsoe1
DB Direct Read I/O Performance	Direct reads were slower than expected.	oltpsoe oltpsoe2
DB Global Cache Dynamic Remastering	The impact of Dynamic Resource Remastering (DRM) on performance was higher than expected.	oltpsoe oltpsoe2
DB Log File I/O Performance	The redo log writes are slower than expected.	oltpsoe oltpsoe1 oltpsoe2
Global Cache Message Request Hang	A hang was detected. The Global Cache Service (GCS) messages are taking a long time.	oltpsoe oltpsoe2
Log Sync for Global Cache	Global Cache block reads were slower than expected.	oltpsoe oltpsoe1 oltpsoe2
Private Network Latency	The latency for global cache messages is higher than expected.	oltpsoe oltpsoe1 oltpsoe2
Redo Log Sync Hang	A hang was detected, and commits were blocked for several seconds.	oltpsoe oltpsoe1
Redo Log Write Wait Hang	A hang was detected. So, a Log Writer process (LG*) is waiting several seconds for a log write completion.	oltpsoe oltpsoe1

About Oracle | Contact Us | Legal Notices | Terms Of Use | Your Privacy Rights

Copyright © 2014, 2023 Oracle and/or its affiliates All rights reserved.

Related Topics

- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.

5.3 ahf analysis

Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.

AHF 23.8

Starting in AHF 23.8, you will be able to upload AHF Insights report automatically if Object Store is configured as part of AHF. Uploading AHF Insights reports helps Oracle Cloud Operations to identify, investigate, track, and resolve system health issues and divergences in best practice configurations quickly and effectively.

Oracle Autonomous Database on Dedicated Exadata Infrastructure and Oracle SaaS

To set REST endpoints (Object Store's), run:

```
ahfctl setupload -name oss -type https -user <user> -url
<object_store> -password
```

To upload AHF Insights report to Object Store, run:

```
ahf analysis create --type insights
```

.

ahf analysis create

```
ahf analysis create [-h] [--type {insights|impact}] [[--last n{m|h} [--
refresh] | --for DATETIME | --from DATETIME --to DATETIME] [--tag
TAGNAME] | [--scope SCOPE --name NAME --cluster CLUSTER --clusters
CLUSTER_LIST]][--output-file PATH] [--to-json]
```

Syntax: AHF Balance

```
ahf analysis create [-h] --type impact --scope [fleet|cluster|
database] [--cluster CLUSTER_NAME] [--clusters space-delimited list of
clusters
] --name NAME
```

Parameters

Table 5-1 ahf analysis create --type impact Command Parameters

Parameter	Description
`-h`, `--help`	Show this help and exit.

Table 5-1 (Cont.) ahf analysis create --type impact Command Parameters

Parameter	Description
`--type impact`	Specify the type of report to generate.
`--scope` [`fleet`| `cluster`|`database`]	Specify to generate AHF Balance reports - Fleet Report, Cluster Report, and Database Report Specify the `--scope` and `--name` options to create an impact analysis. The `--cluster` option is required for database impact analysis.
`--output-file` *`PATH`*	Specify to create output file in the specified location.
`--clusters` *`clu1 clu2 clu3`*	Specify a space-delimited list of clusters to include in the fleet scope.
`--name` *`NAME`*	Specify the name of the fleet, cluster, or database to report on.
`--user-name` *`USER_NAME`*	Specify the Oracle Enterprise Manager Repository user name.
`--connect-string` *`CONNECT_STRING`*	Specify the connect string for the Oracle Enterprise Manager Repository.

Syntax: AHF Insights

```
ahf analysis create [-h] --type insights [--last n{m|h} | --for DATETIME | --
from DATETIME --to DATETIME] [--refresh] [--tag TAGNAME
]
```

Parameters

Table 5-2 ahf analysis create --type insights Command Parameters

Parameter	Description
`-h`, `--help`	Show this help and exit.
`--type insights`	Specify the type of report to generate.
`--last` *`n{m|h}`*	Specify the `--last` parameter to analyze data for the past number of minutes (m) or hours (h). `--last` cannot be greater than 12 hours.

`--for` *`<DATETIME>`*	Specify the `--for` parameter to analyze data for a 2 hour period before and after the timestamp specified.
	Supported time formats:
	`"YYYY-MM-DDTHH:MM:SS"`
	`"YYYY-MM-DD HH:MM:SS"`

Table 5-2 (Cont.) ahf analysis create --type insights Command Parameters

Parameter	Description

`--from <DATETIME>`
`--to <DATETIME>`
	Specify the `--from` and `--to` parameters (you must use these two parameters together) to analyze data for a specific time interval.
	Supported time formats:
	`"YYYY-MM-DDTHH:MM:SS"`
	`"YYYY-MM-DD HH:MM:SS"`
	`"YYYY-MM-DD"`
	Time difference between from and to time should not be more than 4 hours.

`--refresh`	Provides fresh data from AHF Insights sources. Specify `--refresh` alone or together with `--last` to provide fresh data from AHF Insights sources.
`--include-cell-data`	Specify to include data from cell into AHF Insights sources.
`--tag TAGNAME`	Specify to collect the files into the *TAGNAME* directory inside the repository.

Syntax: ahf analysis explore

```
ahf analysis explore [-h] [--with scope] [--from-file FILE]
```

Parameters

Table 5-3 ahf analysis explore Command Parameters

Parameter	Description
`-h`, `--help`	Show this help and exit.
`--from-file FILE`	Specify to read from a file. If you do not specify the file extension, then AHF Scope assumes `.mdb` as the file extension.

Example 5-2 AHF Insights Analysis Usage Examples

Specify `[--last | --for | --from --to]` to create an analysis for a given period of time. Maximum time interval allowed is 4 hrs.

Specify `[--refresh]` alone or together with `[--last]` to provide fresh data from AHF Insights sources.

- Create analysis report from the data collected in the last 3 hours:

  ```
  ahf analysis create --type insights --last 3h
  ```

- Create analysis for a 2-hour period centered at the specified timestamp:

  ```
  ahf analysis create --type insights --for 2022-10-10T14:00:00
  ```

- Create analysis for a given time range:

  ```
  ahf analysis create --type insights --from 2022-10-10T14:00:00 --to
  2022-10-10T15:30:00
  ```

- Create analysis specifying a timezone:

  ```
  ahf analysis create --type insights --from 2022-10-10T14:00:00 --to
  2022-10-11T13:30:00
  ```

- Create analysis with most recent data:

  ```
  ahf analysis create --type insights --refresh
  ```

- Create analysis with a tag:

  ```
  ahf analysis create --type insights --tag my_tag
  ```

Example 5-3   AHF Balance Usage Examples

Specify `[--scope]` and `[--name]` options to create an impact analysis.

The `[--cluster]` option is required for database impact analysis.

- Create analysis for a fleet (all clusters):

  ```
  ahf analysis create --type impact --scope fleet --name fleet1
  ```

- Create analysis for a fleet (cluster list):

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --clusters
  clu1 clu2 clu3
  ```

- Create analysis for a cluster:

  ```
  ahf analysis create --type impact --scope cluster --name cluster1
  ```

- Create analysis for a database:

  ```
  ahf analysis create --type impact --scope database --cluster cluster1 --
  name database1
  ```

- Create analysis specifying the output directory:

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --output-
  file /custom_path/custom_name.html
  ```

- Create analysis specifying EM repository user name and password:

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --
  user-name oracle --connect-string <cs>
  ```

6 Analyze Issue Root Cause

Autonomous Health Framework Scope (AHF Scope) is a standalone, interactive, real-time capable front-end to Cluster Health Advisor (CHA). AHF Scope requires a very small foot-print on the monitored system.

CHA continuously monitors cluster nodes and Oracle RAC databases for performance and availability issue precursors to provide early warning of problems before they become critical.

> **Note:**
>
> GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c. For more information, see Removing Grid Infrastructure Management Repository.

- Introduction to AHF Scope
  AHF Scope is a standalone, interactive, real-time capable front-end to Oracle Cluster Health Advisor (CHA). AHF Scope requires a very small foot-print on the monitored system.
- Cluster View: Connecting and Basics of Monitoring
  Start AHF Scope using the script `ahfscope` on Linux/UNIX or `ahfscope.bat` on Microsoft Windows. This script is located in the `/opt/oracle.ahf/ahfscope/bin/` directory.
- Expert Mode
  Expert mode facilitates an advanced analysis of the metrics and their observed values against the predicted ones.
- Live and Passive Sessions
  AHF Scope maintains two separate sessions in parallel, Live Session (Primary) to receive current metrics in real-time and Past (Replay) Session to display statically a situation encountered at an earlier time.
- ahfscope Console Commands
  Use the `ahfscope -i` command option to activate an interactive command-line interface (CLI). Enter a question mark (?) to see the list of available commands.
- List of Hot Keys
  Hot Keys are keyboard shortcuts that provide an alternate way to do something you would typically do with a mouse.
- Set of Persistent Settings
  Review the list of persistent settings that you can reuse.
- Accessibility Aspects
  AHF Scope can be used without the help of the mouse.
- Customizing Java Run Time System
  As AHF Scope is written in Java, it is platform independent.

- Setting Proper Character Encoding Page on Microsoft Windows
  Specify the encoding to interpret the characters dispalyed on the HTML page correctly.
- ahfscope
  Use the `ahfscope` command to manage AHF Scope.

6.1 Introduction to AHF Scope

AHF Scope is a standalone, interactive, real-time capable front-end to Oracle Cluster Health Advisor (CHA). AHF Scope requires a very small foot-print on the monitored system.

AHF Scope is invoked using the `ahfscope` script available in the `/opt/oracle.ahf/ahfscope/bin/` directory. AHF Scope is designed primarily for cluster or database experts. It is capable of handling large amounts of data efficiently. Its layout and mode of operation is designed for functional efficiency. Most of the operations can be executed using a positional pointer and Hot Keys, or a floating menu available at the cursor position.

If Grid Infrastructure Management Repository (GIMR) is configured,, AHF Scope will connect directly to GIMR using a JDBC connection, and read the current data in real-time. AHF Scope can also operate locally with no connection to GIMR using a data archive extracted from GIMR.

6.2 Cluster View: Connecting and Basics of Monitoring

Start AHF Scope using the script `ahfscope` on Linux/UNIX or `ahfscope.bat` on Microsoft Windows. This script is located in the `/opt/oracle.ahf/ahfscope/bin/` directory.

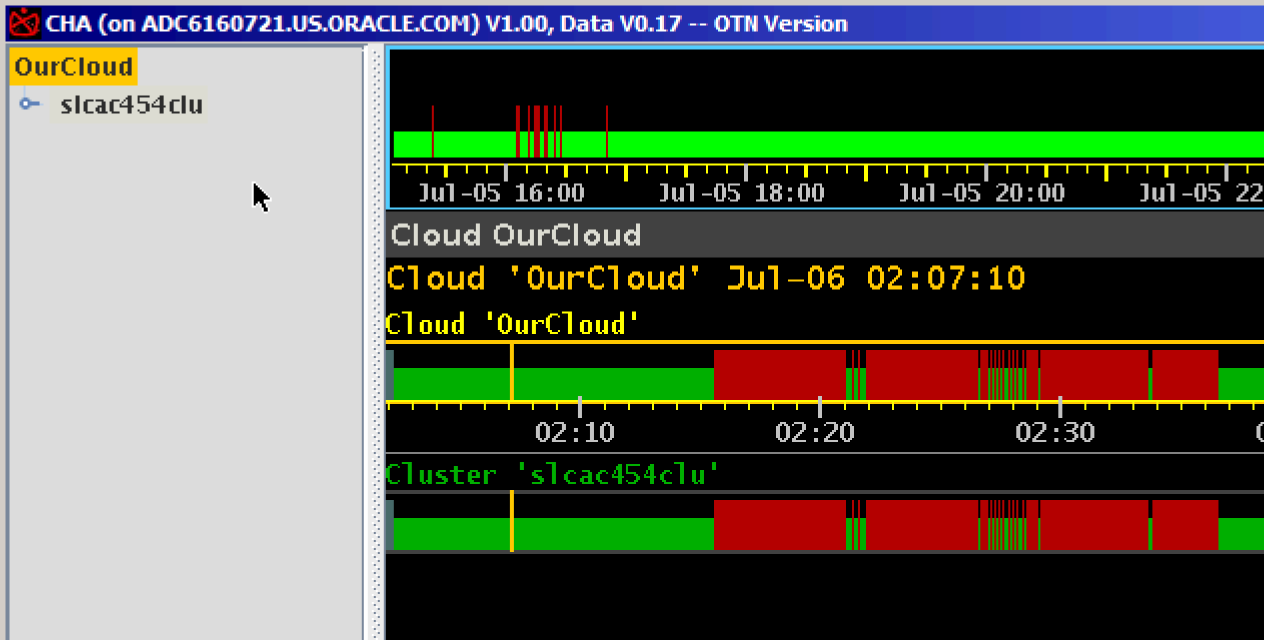
To connect to GIMR, the script obtains connection parameters using Oracle Wallet services. AHF Scope displays a top-level **Cloud View** upon starting and connecting to GIMR. AHF Scope will terminate upon closing the main window.

- Basics of Navigation Through Entity Panels
- Target Entities
- Browsing Through Time and Pin Operation
- Changing the Set of Visible Probes
- Selecting Abnormal Probes in Any Time Range
- Problems or Anomalies
- Browsing through active time of a Problem

6.2.1 Basics of Navigation Through Entity Panels

This is the default window that will appear when AHF Scope is started:

Figure 6-1   AHF Scope default window



The window contains a navigation tree on the left and an analysis panel on the right. The navigation tree always starts in a symbolic top-level system "OurCloud" and displays all components within its connected Cloud. AHF Scope currently connects to only one GIMR, and thus contains data for all monitored nodes and Oracle RAC databases within a single cluster.

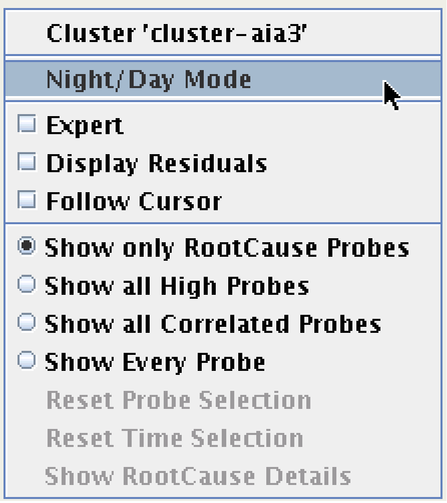
The analysis panel contains three components:

1. A system timeline at the top showing a condensed long term system history.
2. A status line.
3. An entity panel associated with the entity selected in the navigation tree.

The currently selected navigation tree entity is marked with a yellow background.

The analysis panel initially appears with a dark background called "Night Theme". A "Day Theme" displaying dark text on a light background is also available. You can toggle the themes by moving the cursor onto the entity panel and pressing lowercase "w", or by using the right mouse click to access the floating menu and selecting "Night/Day Mode

Figure 6-2 Night/Day mode



Cluster 'cluster-aia3'

Night/Day Mode

☐ Expert
☐ Display Residuals
☐ Follow Cursor

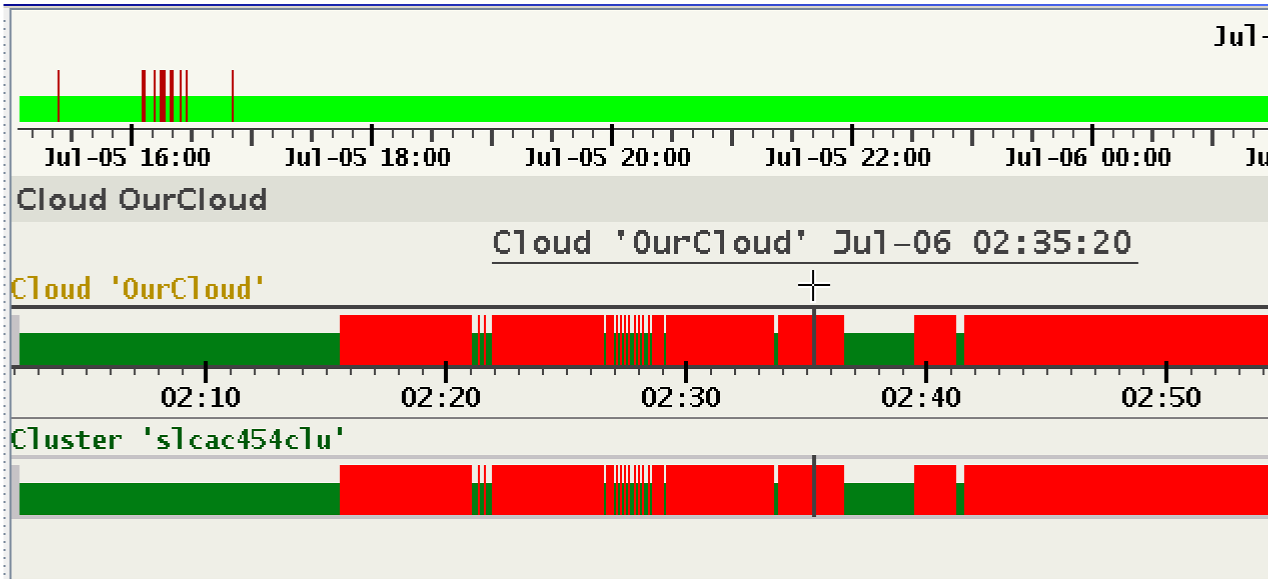
● Show only RootCause Probes
○ Show all High Probes
○ Show all Correlated Probes
○ Show Every Probe

Reset Probe Selection
Reset Time Selection
Show RootCause Details

This is the first example of how to use either a Hot Key or a floating menu to perform the same function. For more information about Hot Keys, see *List of Hot Keys*.

The main panel in Day Theme looks like as follows:

Figure 6-3 Main Panel in Day Theme



This change is persistent. With every consecutive start, the most recent selected theme is used. For more information about the settings that AHF Scope persists, see *Set of Persistent Settings*.

> **Note:**
>
> The persistent storage for these settings is associated with a specific user on a specific host. These settings need to be repeated when using AHF Scope on multiple hosts.

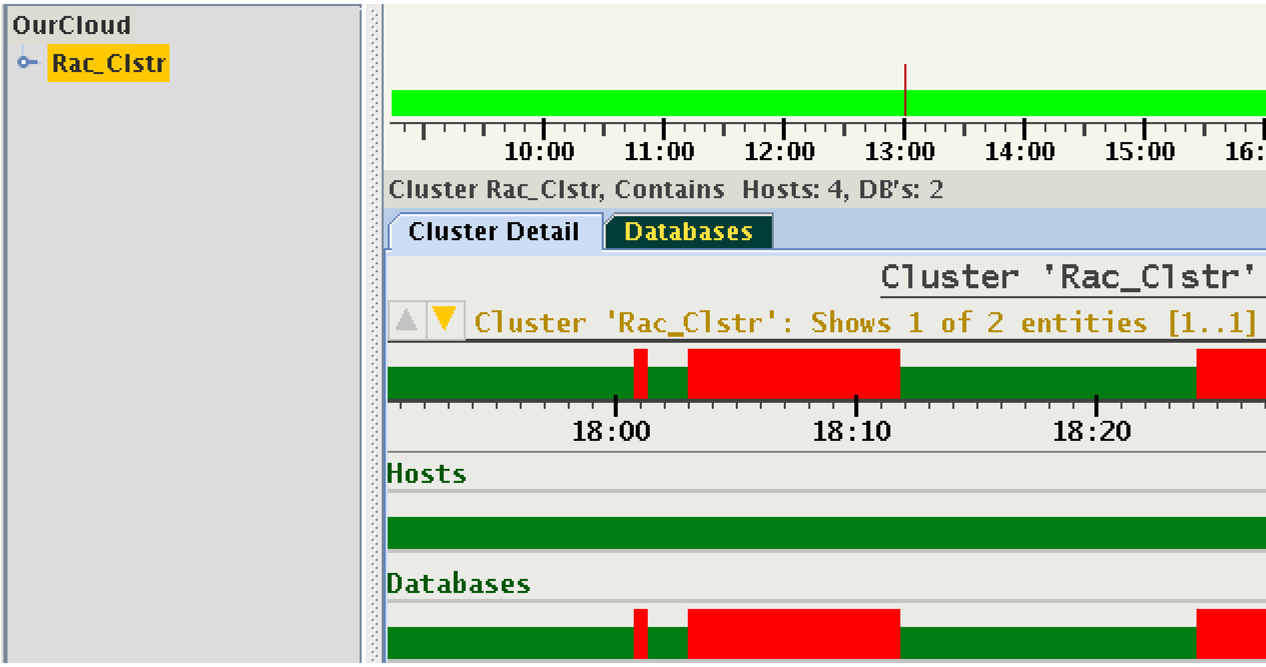
The status timelines in the entity panel display for each timestamp the state of its entity marked either green, red, or gray.

1. Green means that at that point in time, none of its sub-entities indicate any problem flagged as "abnormal".
2. Red means that at least one of its sub-entities is in abnormal state. Mathematically, this means that AHF Scope calculates a union of sets of all sub-entities and propagates its value upward to the top most entity, which is here OurCloud.
3. Gray marks periods in time in which no data was received for any of the sub-entities.
4. Gray over green marks periods in time in which some sub-entities received no data.

Click the cluster entity under OurCloud. AHF Scope now marks the cluster name with a yellow background, and the entity panel changes to display the cluster details.

> **Note:**
>
> When a cluster entity is selected, the status line under the timeline displays the number of hosts and databases in this cluster.

Figure 6-4 Number of hosts and databases in this cluster



Cluster Rac_Clstr, Contains Hosts: 4, DB's: 2

Cluster 'Rac_Clstr': Shows 1 of 2 entities [1..1]

In this hierarchy, the cluster entity contains two sub-entities "Hosts" and "Databases". The above display indicates that all red-marked abnormal states come from one of the databases only.

Any entity in the navigation tree may be expanded to show its sub-entities. Note that expanding the navigation tree does not change the entity panel on the right. This panel changes only when a different entity is selected in the tree.

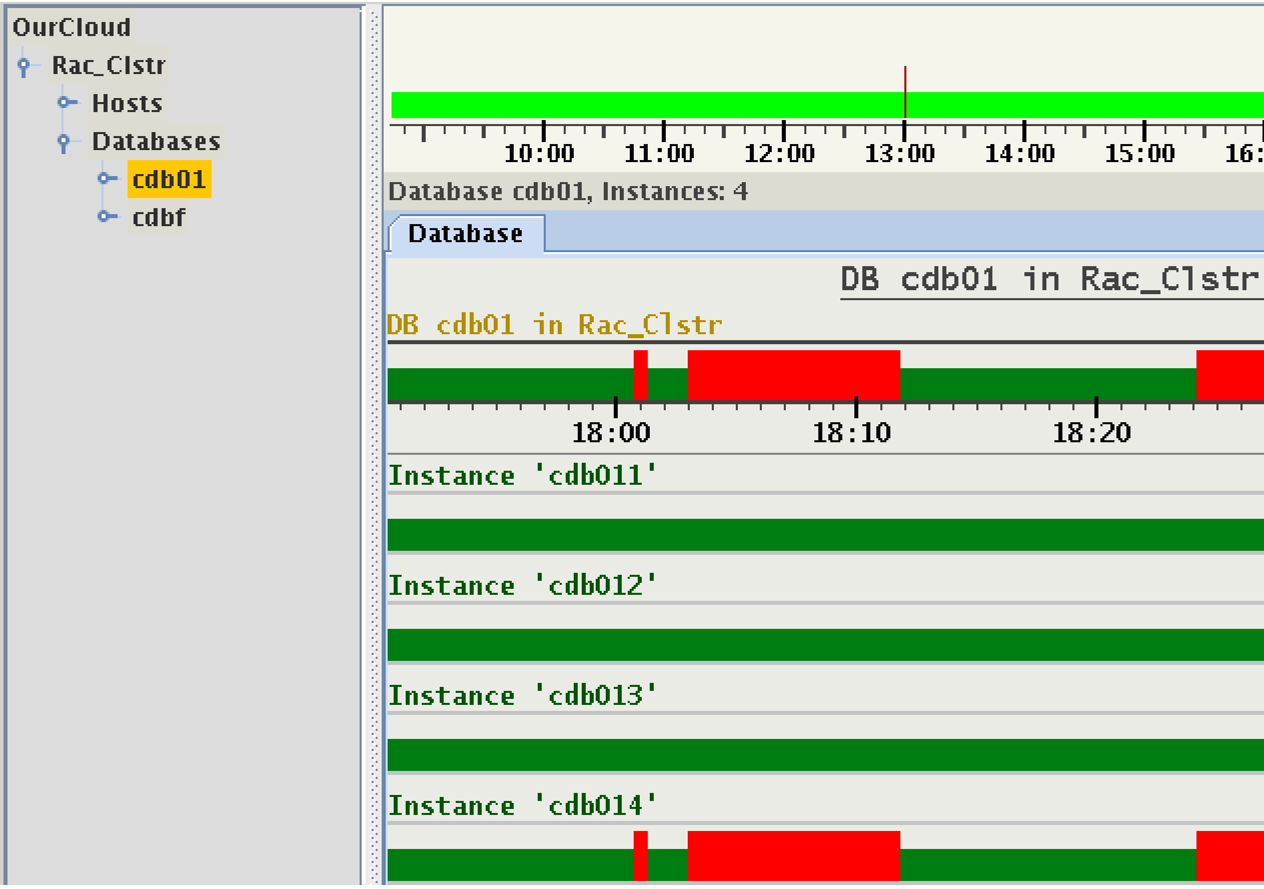
Note the position of the cursor on the status timeline of the cluster. The entity name will change color to indicate that it has focus. Moving the cursor over the "Databases" status timeline switches the highlighting and focus accordingly. Focusing on a specific entity allows you to enter its panel without moving the mouse pointer to the navigation tree. To step down to the panel of any sub-entity, for example, "Databases" in the image above, you can choose between these methods:

1. Select the entity in the navigation tree on the left. This requires a movement of the mouse pointer to the tree.
2. Place the cursor on the entity name and double-click it.
3. Use a Hot Key without moving the mouse pointer. Press Enter on your keyboard. AHF Scope will select the focused entity and enter its panel. The selected entity will be automatically expanded and highlighted in the navigation tree.

This is the second example of how to use Hot Keys. Instead of moving the pointer across distances to expand an entity in the navigation tree, focus the entity using one hand, and then hit the Enter key on your keyboard. This is by far the fastest way to traverse through the entities.

In this example Entity "Databases" contain two databases of which one indicates abnormal state. When you select this database and step down to its panel, you will see timelines of all its instances.

Figure 6-5   Entity 'Databases' containing two databases



From this example, you can clearly see that the state of the database is a union of states of its instances. This example also shows gray areas in the status bars of instances. They indicate absence of monitored values for some periods in time. The entity might have been stopped, terminated, evicted, or non-responsive. The only known fact is that not a single value was recorded for this entity at this point in time.

With the Instances, we reached one of the final Sub-Entities. These are the Target Entities of CHA. Every type of Target entity has its own specialized panel in AHF Scope.

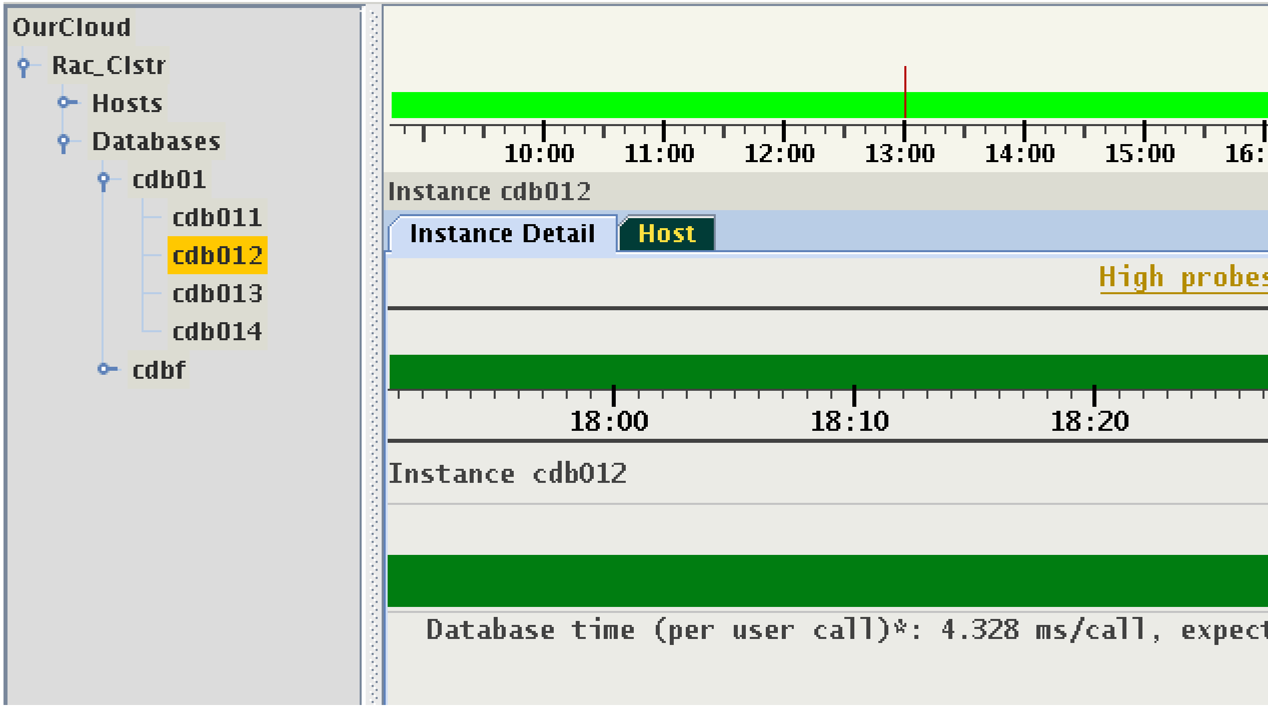
Related Topics

- List of Hot Keys
  Hot Keys are keyboard shortcuts that provide an alternate way to do something you would typically do with a mouse.
- Set of Persistent Settings
  Review the list of persistent settings that you can reuse.

6.2.2 Target Entities

CHA currently supports two types of target entities: "Host" and "Instance". Using the same example above, lets enter the panel of the second from the top instance *cdb012*:

Figure 6-6 Target Entities



Database time (per user call)*: 4.328 ms/call, expect

On the panel of an instance (or a host), the top timeline represents the state of the target entity. Any status timeline below represents a time series of individual metrics collected for the target entity, which are referred to as signals or probes. The state of a target entity is represented by four colors:

1. Green: The state is normal. None of the probes are in abnormal condition.
2. Yellow: Entity state is still normal, but some of the probes are in abnormal condition.
3. Red: Entity is in abnormal state. At least one problem (also called "decision") indicates the reason for the abnormal state. The height of the red bar changes with the number of problems at that point in time.
4. Gray: Data was not received.

Every single point in the timeline of a target entity holds a set of values:

1. State of the entity, which may be green, yellow, red, or gray (missing).
2. Set of problems (if indicating red state).
3. Set of probes in abnormal state (if indicating yellow state).

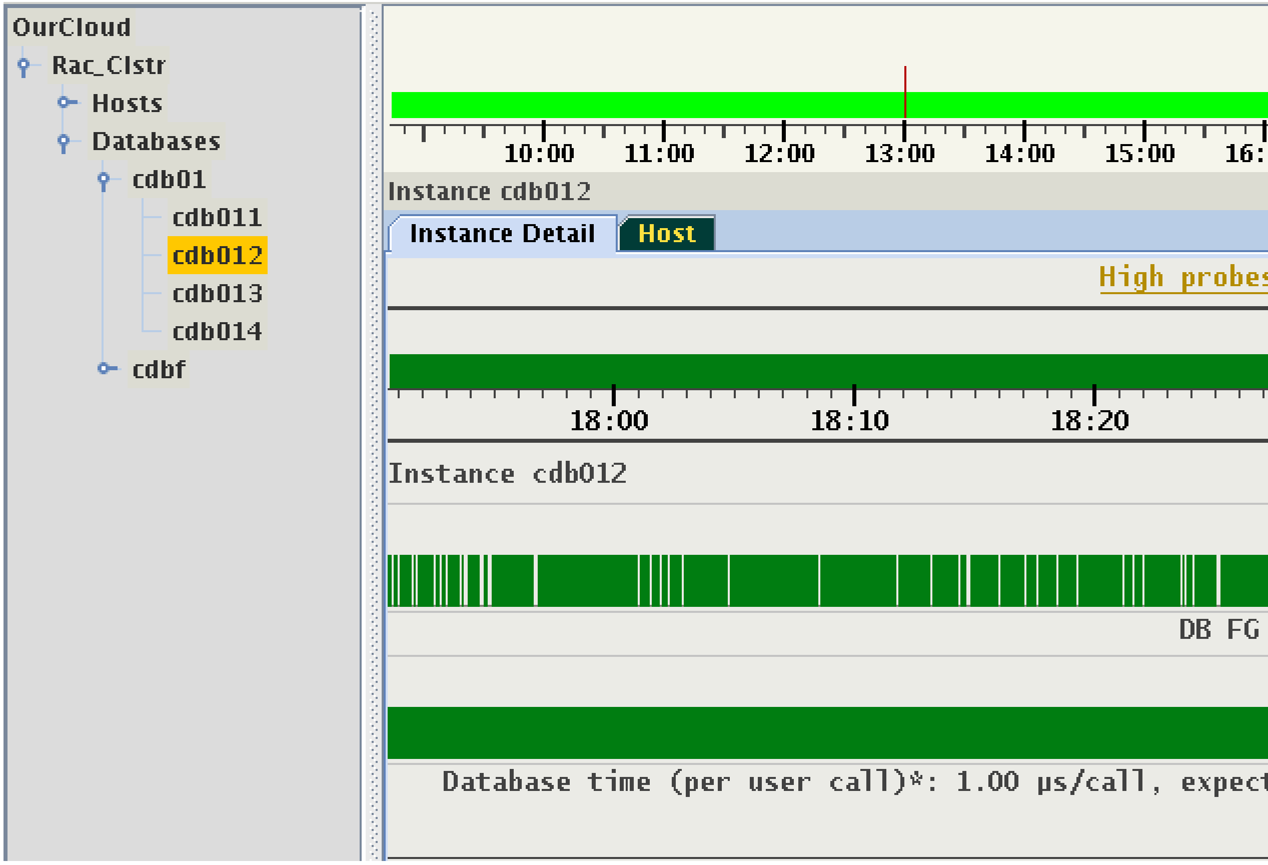
The set of indicated probes may change with every time-point. By default, only probes which are in an abnormal state are shown. When there is no problem indicated, the target entity will be yellow on the timeline. There are a collection of options controlling selection of displayed probes that will be described later.

In the above illustration at the time 18:35:30, the state of the instance is indicated by a yellow bar, and below we see that the probe "Database time" is in an abnormal state. Its value at this point in time is 4.328 ms/call, albeit the predicted (or expected) value in the active calibrated model was 494.719 ms/call. The set of probes in abnormal state and their values may change in every individual point in time. When a probe value is reported in a sample, the data set contains:

1. State of the probe (normal/high/low).
2. Observed value, which may be missing at some points in time.
3. Predicted value, which may also be missing at some points in time, or when no prediction for this probe is available, this value is missing at all points in time.

Not every probe is reported in every sample. Some probes might be reported only at certain points in time. A typical example of such probes are DB wait events. When a probe value is not reported, an empty space is displayed in the timeline denoted as gray. Below is another example for the same Target showing a sample at a different point in time. At this point in time, two probes are indicated as abnormal.

Figure 6-7 DB wait events



Database time (per user call)*: 1.00 μs/call, expect

Notice the numerous gaps in the indication of "DB FG Wait Ratio". This is an example of a probe without expected values and whose observed value is not being reported with every sample. This differs from the indication in timestamps in which no values were reported for an entity. These periods of time are marked by the gray bars.

Every type of target entity has a unique panel with specialized tabs. For example, the panel of an instance has a tab "Host", which shows the host where the instance is running. Similarly, a panel of a host has a tab called "Instances", which shows a set of running database instances.

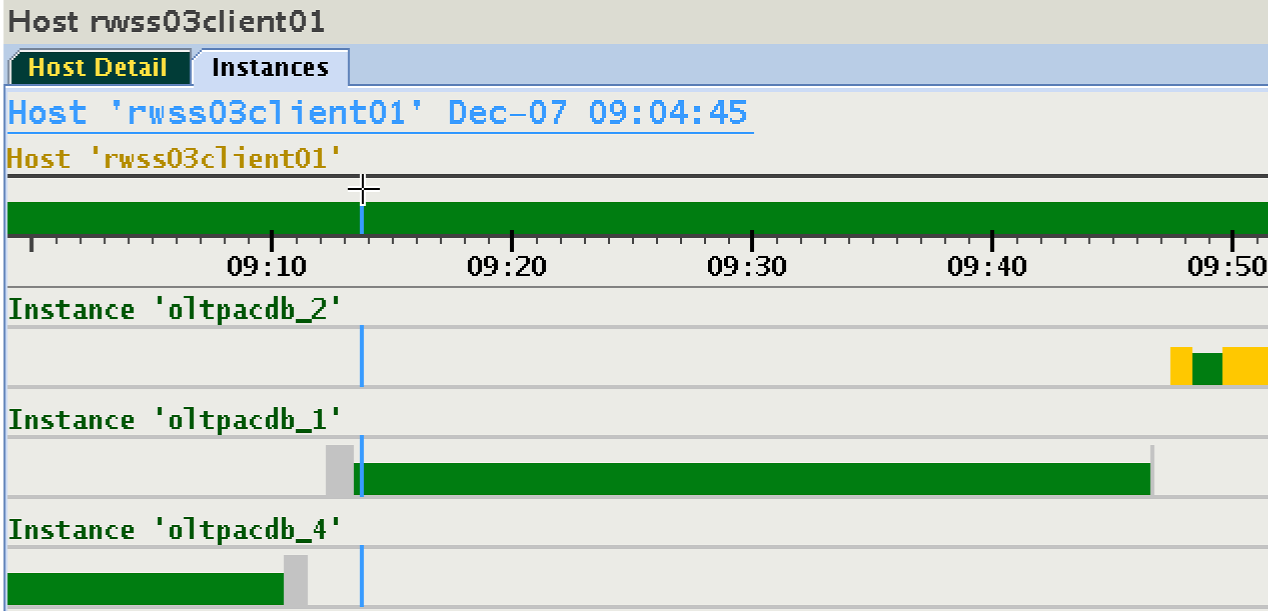
Generally, this panel is used to visualize dynamic dependencies between target entities. The navigation tree depicts only the hierarchy of the logical structure of the installation. The logical structure contains a mix of hardware and software target components in their hierarchical dependency. For example, an entity "Cluster" points to "Hosts", which contains a list of individual hosts. These relationships do not change with time. The dynamic dependencies describe how the target entities relate to each other. These relations may change with time. They are defined by pairs of target entities and ranges of time in which they are valid. Some of these relations may be exclusive. For example, at a specific point in time, an instance is said to run on one host. However, a host can have a number of instances running on it at the same point in time.

- A Host Panel
- An Instance Panel

6.2.2.1 A Host Panel

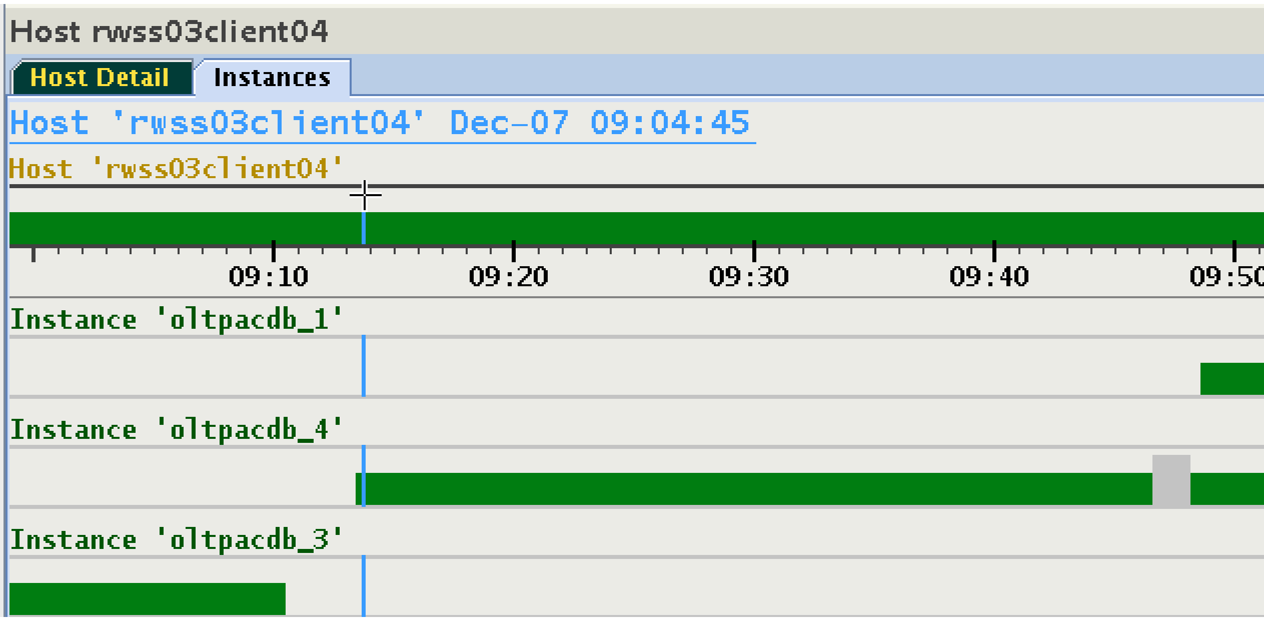
A Host panel has two tabs: "Host Detail" and "Instances".

Figure 6-8 Host Panel



This host is running three different instances between 9 and 10 o'clock. Something happened around 9:11 and 9:46, which caused the instance to shut down, or change its host. As more than one instance from different databases may run on a host, there is a 1:N relationship. After approximately 9:48, two instances are running on this host.

Figure 6-9 Panel of a Host



Host rwss03client04

Host 'rwss03client04' Dec-07 09:04:45

Host 'rwss03client04'

Instance 'oltpacdb_1'

Instance 'oltpacdb_4'

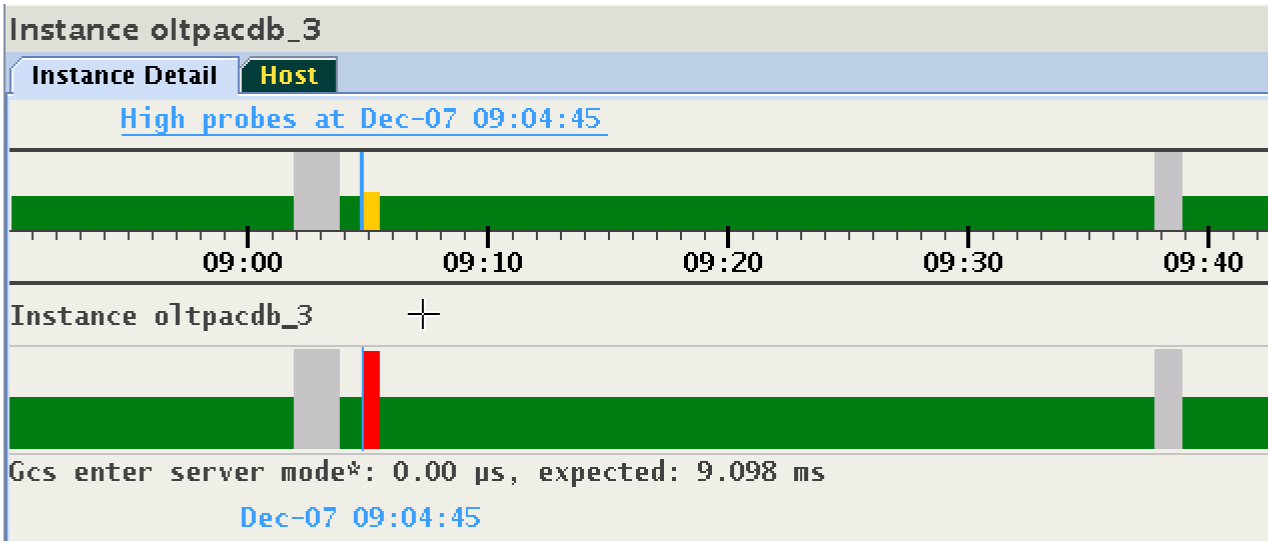
Instance 'oltpacdb_3'

To switch from a host panel to the desired instance panel, move focus to any of the instances using down or up arrow key and hit the Enter key on your keyboard, or double-click any of the instance names. The display will switch to the panel of the chosen instance, select its node in the navigation tree, and expand the navigation tree to make this node visible.

6.2.2.2 An Instance Panel

From the above example, let us switch to the instance `otlpacdb_3`. It is the customary status panel.

Figure 6-10 Instance Panel



Instance oltpacdb_3

High probes at Dec-07 09:04:45

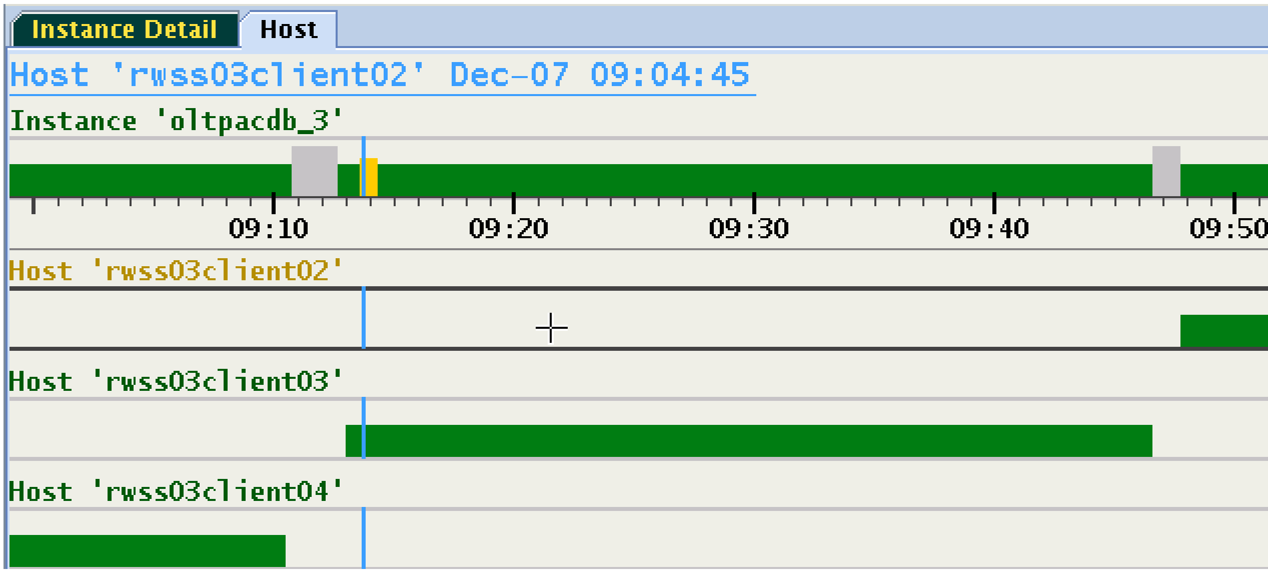
Instance oltpacdb_3

Gcs enter server mode*: 0.00 μs, expected: 9.098 ms

Dec-07 09:04:45

The panel displays two interruptions in service mentioned in the previous section. This display does not indicate that the instance was in fact running on more than one host at different points in time. Click the "Host" tab to visualize where the instance was running. The relationship is 1:1. An instance runs always on only one host at a particular point in time.

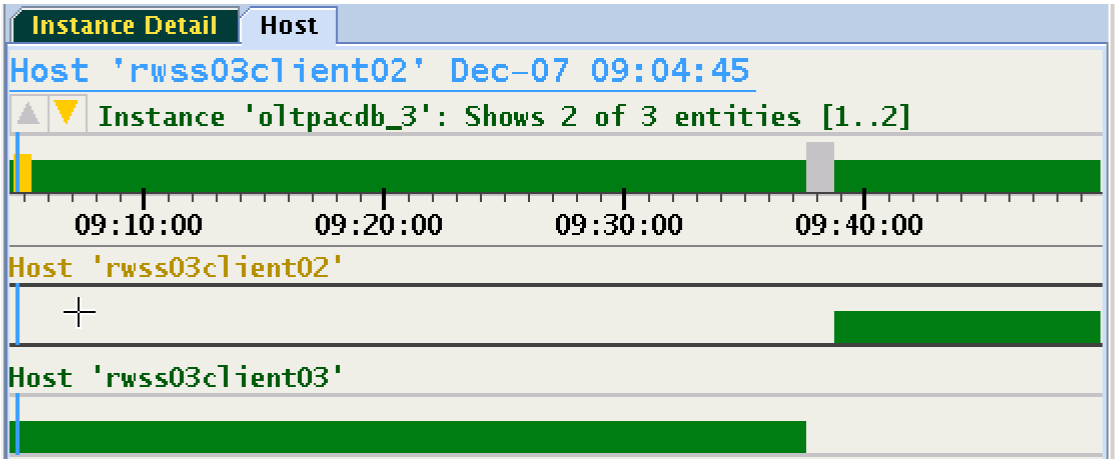
Figure 6-11 Instance Panel



From this display, switching to any of the hosts is performed by either double-clicking its name, or by selecting the timeline and hitting the Enter key on your keyboard. Using this method, you can quickly switch between host and instances. As the image illustrates, this panel displays a form of cascaded time ranges from most recent on top to the oldest on the bottom. When resizing the window, the display may change dynamically causing timelines to be added or removed.

For example:

Figure 6-12 Instance Panel



The run time of the instance on host *rwss03client04* is no longer indicated because it ended prior to 9:04 and this time is not shown in the narrower window.

6.2.3 Browsing Through Time and Pin Operation

AHF Scope display is dynamic when connected to a GIMR and receiving live data in real-time. AHF Scope is receiving new samples and advancing all timelines. With every new sample or with a change of a cursor position, the corresponding time point is automatically displayed with a set of abnormal probes together with their values. This time point is indicated by a vertical marker. Once a time point of interest is identified, it can be "pinned" using

1. Double-click any time at the target status timeline.
2. Press the Hot Ley "p" while hovering over target status timeline.
3. Press the left or right arrow key while hovering over target status timeline.

The pinned time point may be fine-tuned by pressing the left or right arrow keys and observing the displayed timestamp. Once the time point is pinned, the position marker will no longer follow the cursor. Its color changes from orange to blue to indicate this mode of operation. Moving the cursor to any other time and pressing "p" changes the pin point to the new location. Pressing "f" will unpin the time point causing it to again follow the cursor.

Note that pinning to a specific time point selects its corresponding set of probes in abnormal state. When browsing through the visible values of this set, the pin point can be preserved. To achieve this, either hover cursor over the timelines of the probes, or use the down arrow key to move focus to these timelines. Press and hold the Control key and move the timestamp marker sideward using mouse or left or right arrow keys. Besides the light blue pin marker, a second marker is displayed following the cursor position. The bottom information line shows the time point associated with this marker. The floating label at the bottom of each bar graph shows the values at the position of the cursor.

Figure 6-13   Browsing Through Time and Pin Operation

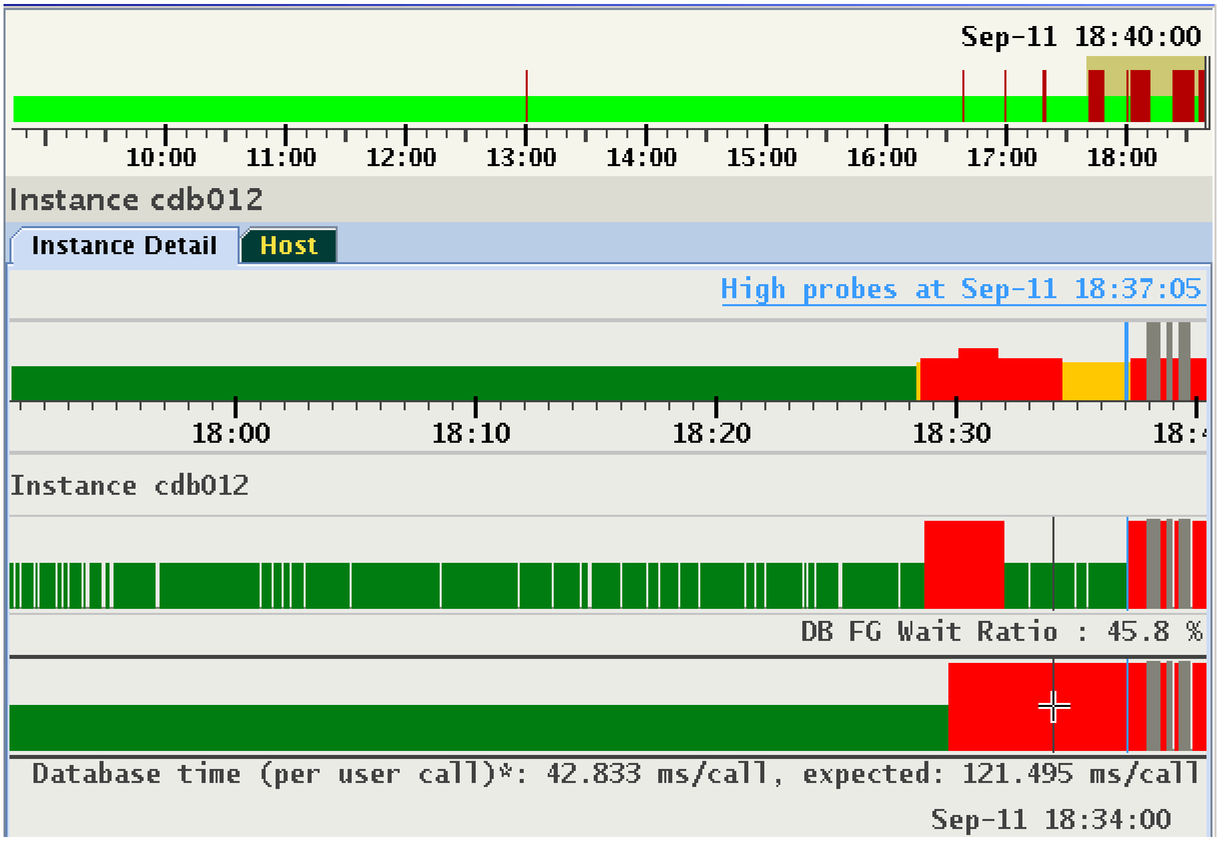


Image shows a set of two probes in abnormal state at pinned time 18:37:05. Press the Control key and move the cursor along the timeline. Each position corresponds to a different point in time. In this example, the values sampled at 18:34:00 of a set of probes selected at 18:37:05 are shown. With the Control key remaining pressed, use the left ot right arrow keys to step through time points one sample at a time.

To activate this feature permanently, select the checkbox "Follow Cursor" in the floating menu.

Pin point is automatically preserved in every entity sharing the same cluster. This feature is used to move between different panels and explore values of probes at the same time point. When viewing live data, the pin will be released when its timestamp reaches the left or right end of the viewport.

6.2.4 Changing the Set of Visible Probes

By default, only probes in abnormal state are displayed in yellow for every time point. When the selected time point is marked red, a set of problems is active (see *Problems or Anomalies*), each with its own set of abnormal probes. At this point, only the description of the problem is displayed. Once a problem is selected, its associated set of abnormal probes are identified and displayed. This will be discussed further in *Problems or Anomalies*.

You may prefer to display all high probes at any time point, or perhaps explore visually the time series of every probe regardless of their state.

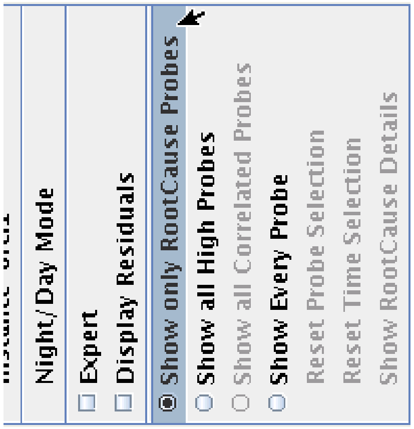
The following are the custom settings for the selection of probes:

1. Display only abnormal probes (the "yellow" marked zone) or probes of a selected problem. This is the default behavior.
2. Display always all abnormal probes (on "yellow" or "red").
3. Display every existing probe regardless its state.
4. Display all probes belonging to the same category (called "correlated probes").
5. Display every abnormal probe in a specific time range. For more information, see *Selecting Abnormal Probes in any Time Range*.
6. Display only a subset of existing probes (3) by their category. For more information, see *Selecting Custom Set of Probes*.

The following examples show how to select options (2), (3) and (4) from the above list. Use either floating menu or a Hot Key to change the mode in which probes are being displayed.

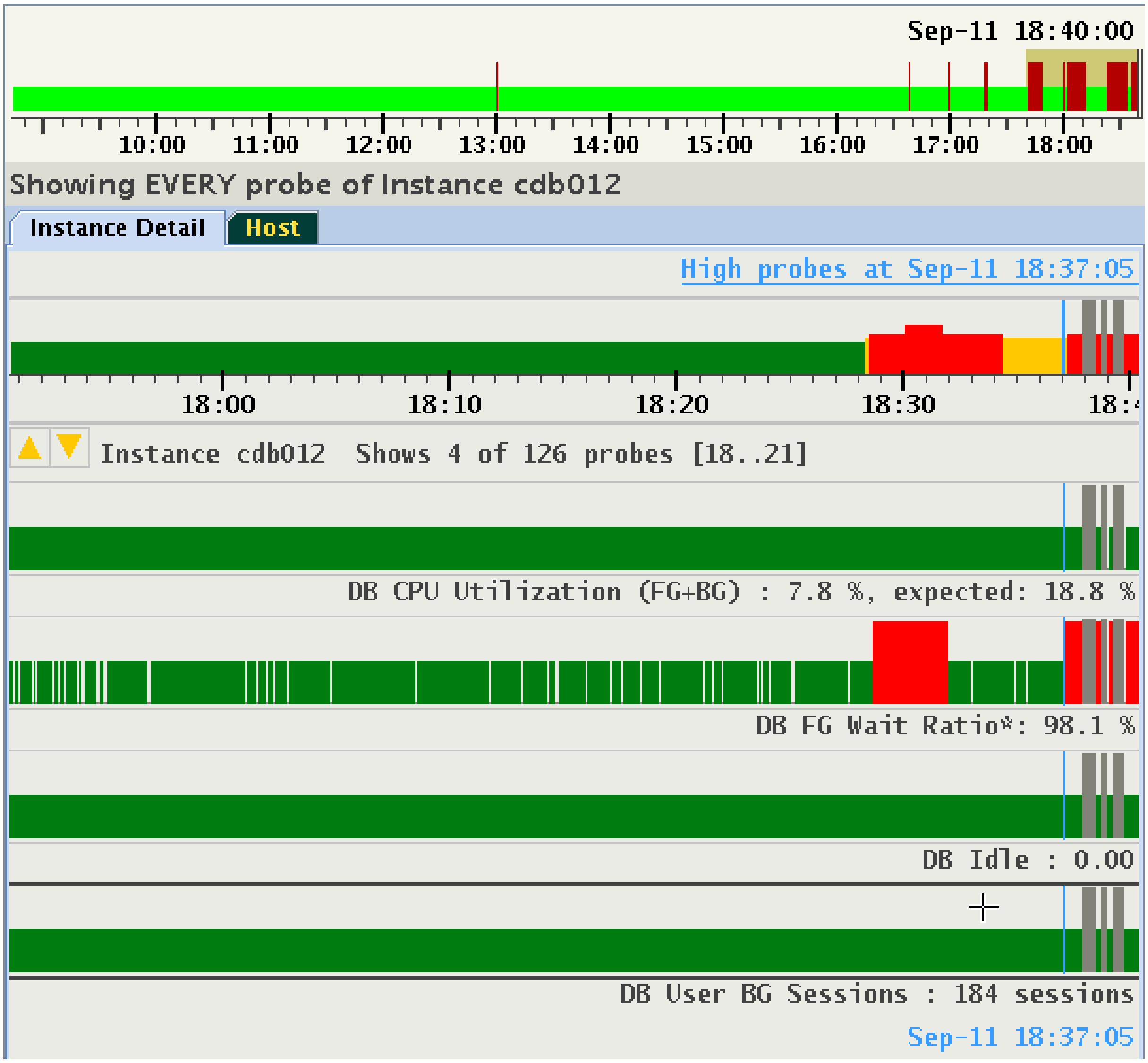
For example:

Figure 6-14 Changing the Set of Visible Probes



Either select "Show all High Probes" or press "a" to display every high probe at any point in time. Select "Show Every Probe" or press "A" to view every probe regardless of its state.

Figure 6-15   Changing the Set of Visible Probes

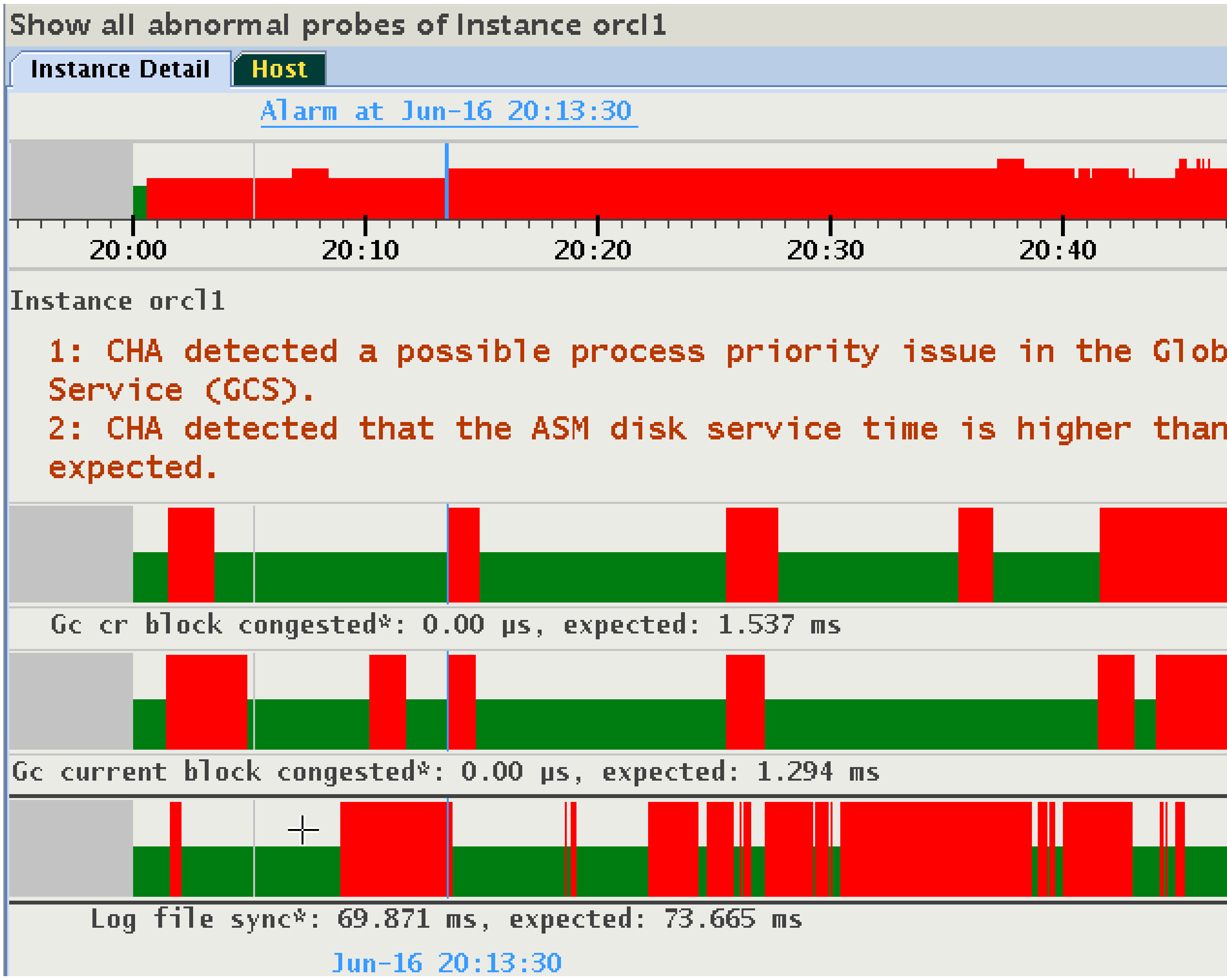

Sep-11 18:40:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
Showing EVERY probe of Instance cdb012
Instance Detail
Host
High probes at Sep-11 18:37:05
18:00
18:10
18:20
18:30
18:4
Instance cdb012 Shows 4 of 126 probes [18..21]
DB CPU Utilization (FG+BG) : 7.8 %, expected: 18.8 %
DB FG Wait Ratio*: 98.1 %
DB Idle : 0.00
DB User BG Sessions : 184 sessions
Sep-11 18:37:05

The number of probes may exceed the size of the display window. In this example, only four probes out of a total of 126 can be displayed. The Status label under the time line indicates which subset of probes is being shown and provides up or down arrows to navigate. In this example, probes 18, 19, 20 and 21 are displayed. Both up/down icons are highlighted indicating that scrolling both directions is available using cursor up/down or page up/down keys or using the mouse wheel.

It is also possible to display all probes belonging to the same category. Categories of probes will be explained in the section devoted to *Expert Mode*. Every probe may belong to one or more pre-defined categories. For example, "Buffer Cache," or "Global Cache Exceptions" are categories of probes associated with database instances.

Note that when the cursor hovers over any probe's timeline, its boundaries are highlighted as it gets focus. Alternatively, use the up or down arrow keys to move focus to a specific probe without moving the mouse pointer. Figure 13-17 focus is on "Log file sync":

Figure 6-16 Changing the Set of Visible Probes



Show all abnormal probes of Instance orcl1

Instance orcl1

1: CHA detected a possible process priority issue in the Glob
Service (GCS).
2: CHA detected that the ASM disk service time is higher than
expected.

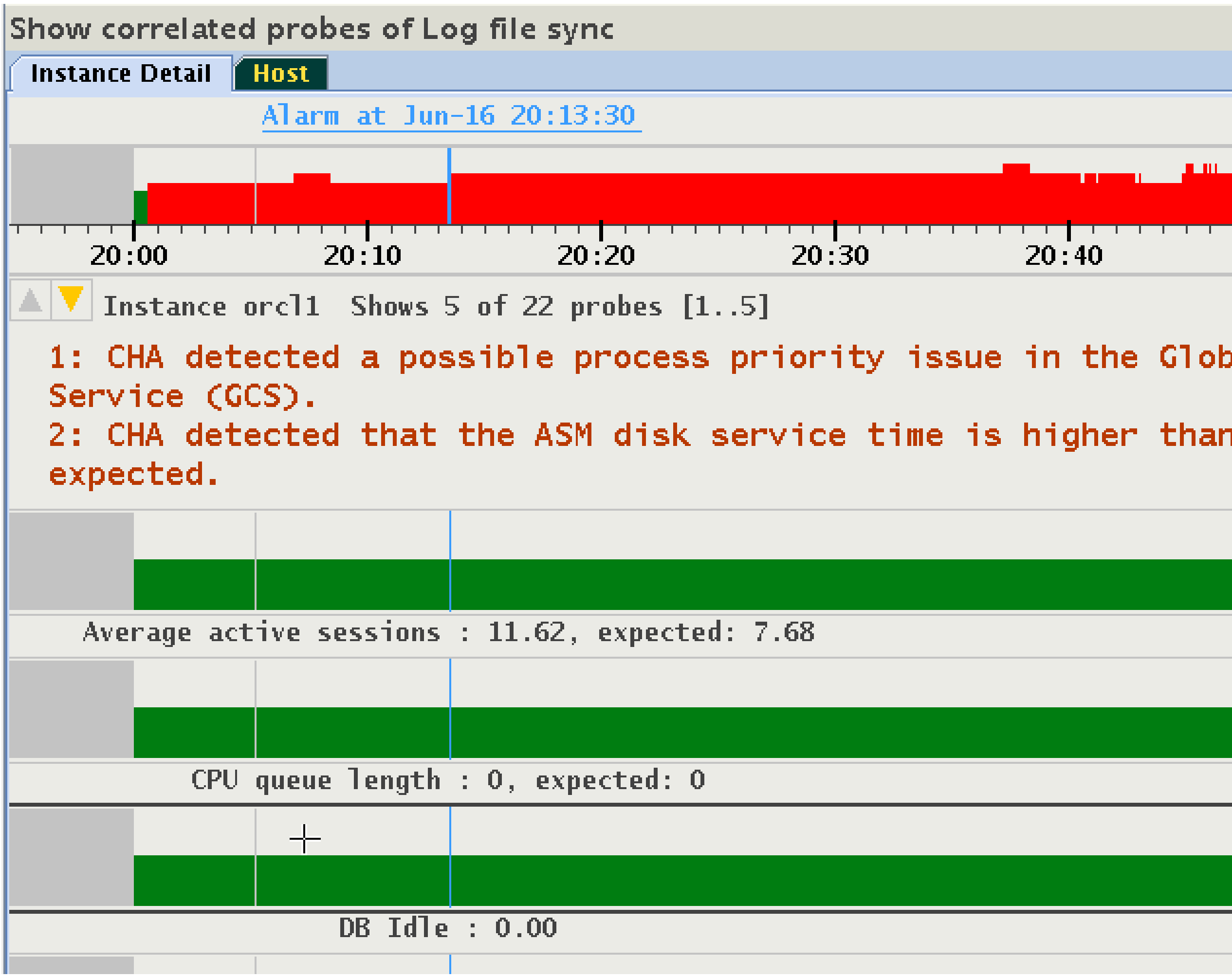
Gc cr block congested*: 0.00 µs, expected: 1.537 ms

Gc current block congested*: 0.00 µs, expected: 1.294 ms

Log file sync*: 69.871 ms, expected: 73.665 ms

Use the right-click popup menu, or press "c" to display all correlated probes belonging to all "Log file sync" member categories.

Figure 6-17   Changing the Set of Visible Probes



Show correlated probes of Log file sync

Instance orcl1   Shows 5 of 22 probes [1..5]

1: CHA detected a possible process priority issue in the Glob
Service (GCS).
2: CHA detected that the ASM disk service time is higher than
expected.

Average active sessions : 11.62, expected: 7.68

CPU queue length : 0, expected: 0

DB Idle : 0.00

Should the number of probes not fit into the display, the up/down cursor icons appear and the status line shows details about visible subset of probes. See *Expert Mode* for the steps to select and create subsets of probes.

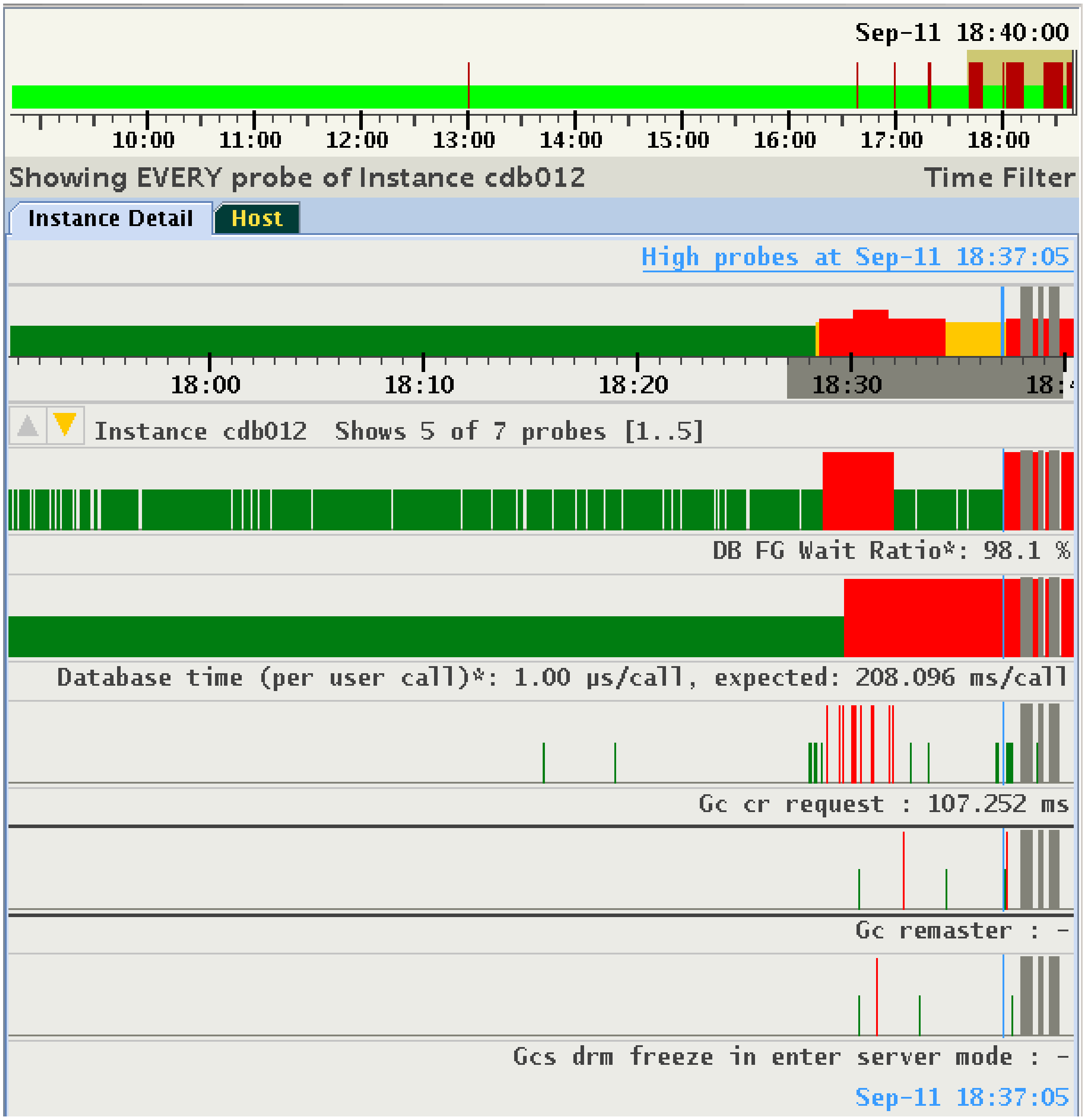
Related Topics

- Problems or Anomalies
- Selecting Abnormal Probes in Any Time Range
- Selecting Custom Set of Probes
- Expert Mode
  Expert mode facilitates an advanced analysis of the metrics and their observed values against the predicted ones.

6.2.5 Selecting Abnormal Probes in Any Time Range

Tracking probes in abnormal state between times points is supported. Move the cursor to the first time point, press the Shift key, press the left mouse key and move the cursor to the second time point, release the mouse button, and then release the Shift key. The selected time range is indicated by a gray bar under the time line. The information strip indicates that a "Time Filter" is active. In the example, a total of 7 probes are indicated high between 18:27 and 18:40, with probes 1 to 5 visible in the display:

Figure 6-18 Selecting Abnormal Probes in any Time Range



Showing EVERY probe of Instance cdb012 Time Filter

High probes at Sep-11 18:37:05

Instance cdb012 Shows 5 of 7 probes [1..5]

DB FG Wait Ratio*: 98.1 %

Database time (per user call)*: 1.00 µs/call, expected: 208.096 ms/call

Gc cr request : 107.252 ms

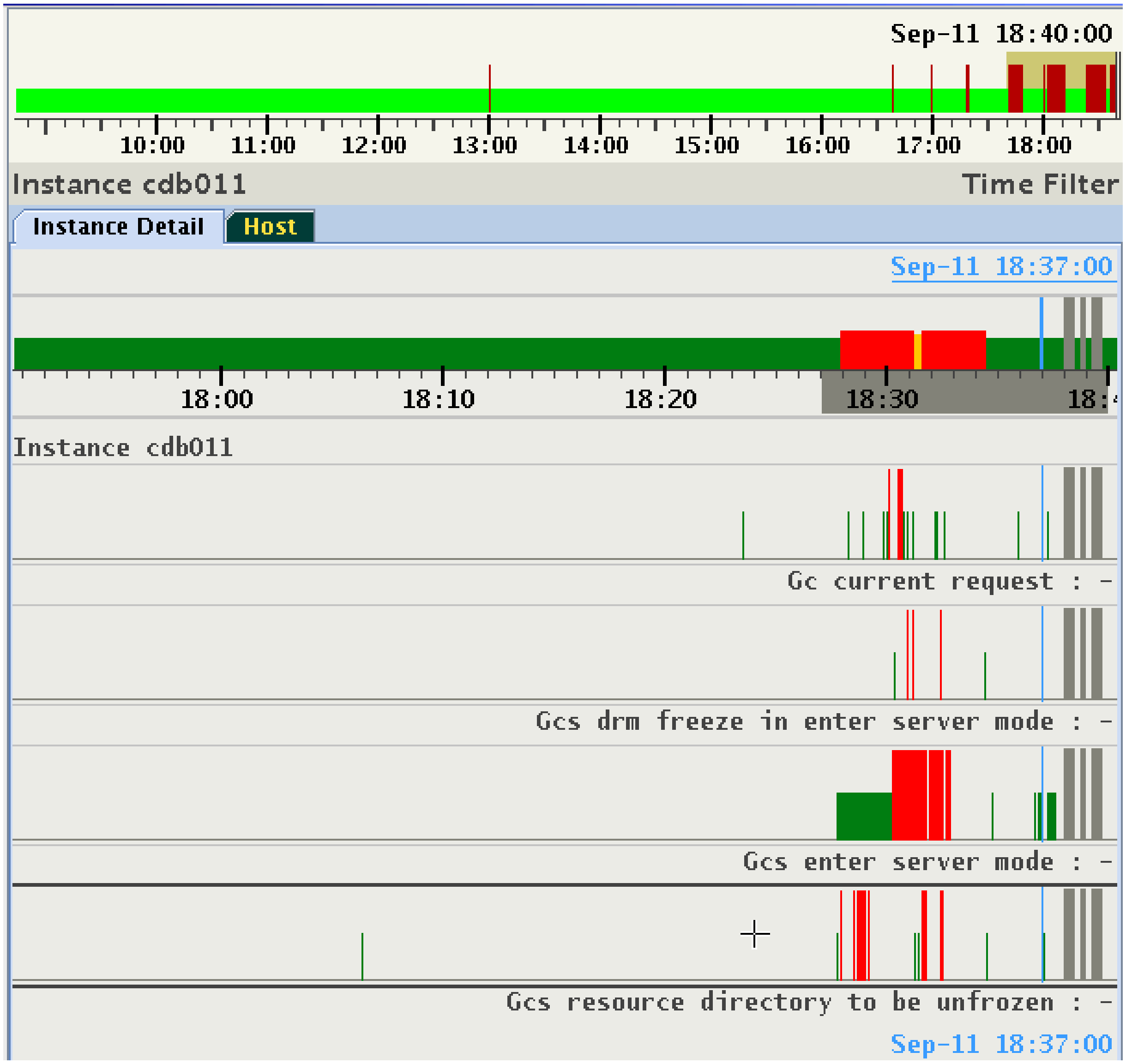
Gc remaster : -

Gcs drm freeze in enter server mode : -

Sep-11 18:37:05

The selection of time range is preserved cluster-wide similar to a selection of pin point. You can change target entities and see the sets of abnormal probes in the selected time range. For example, in the same period in time, only four high probes for another instance of the database are detected.

Figure 6-19   Selecting Abnormal Probes in any Time Range



To deactivate the filter, either select "Reset Time Selection" on the right-click pop-up menu, or hit the Escape key on your keyboard.

6.2.6 Problems or Anomalies

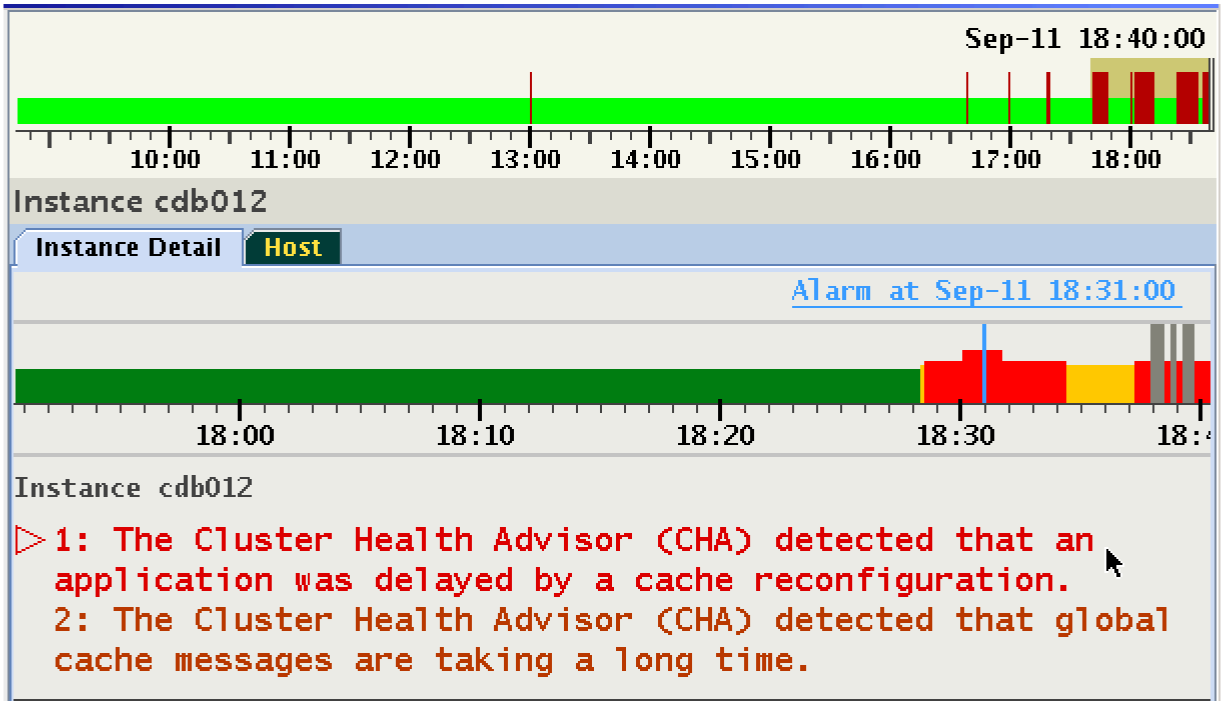
Whenever the timeline of the entity displays red, one or more problems exist at that timestamp. Every problem contains the following information:

1. **Name:** This is an internal identifier.
2. **Description:** An explanation of the nature of the diagnosed problem (displayed by default on the panel).
3. Confidence probability in percentage (may differ at every time point).

4. Root cause and diagnosis of the problem.
5. Suggested corrective actions.
6. Set of probes associated with the problem (may differ at every time point).
7. Set of inference chains in Bayesian Network. One chain per probe associated with the problem.
8. Set of tables with detailed information (optional, calculated per time point).

Portions of this information will be displayed only in the Expert Mode, described in *Expert Mode*. Below is an example of two problems indicated at 18:31:00:

Figure 6-20   Problems or Anomalies



Instance cdb012

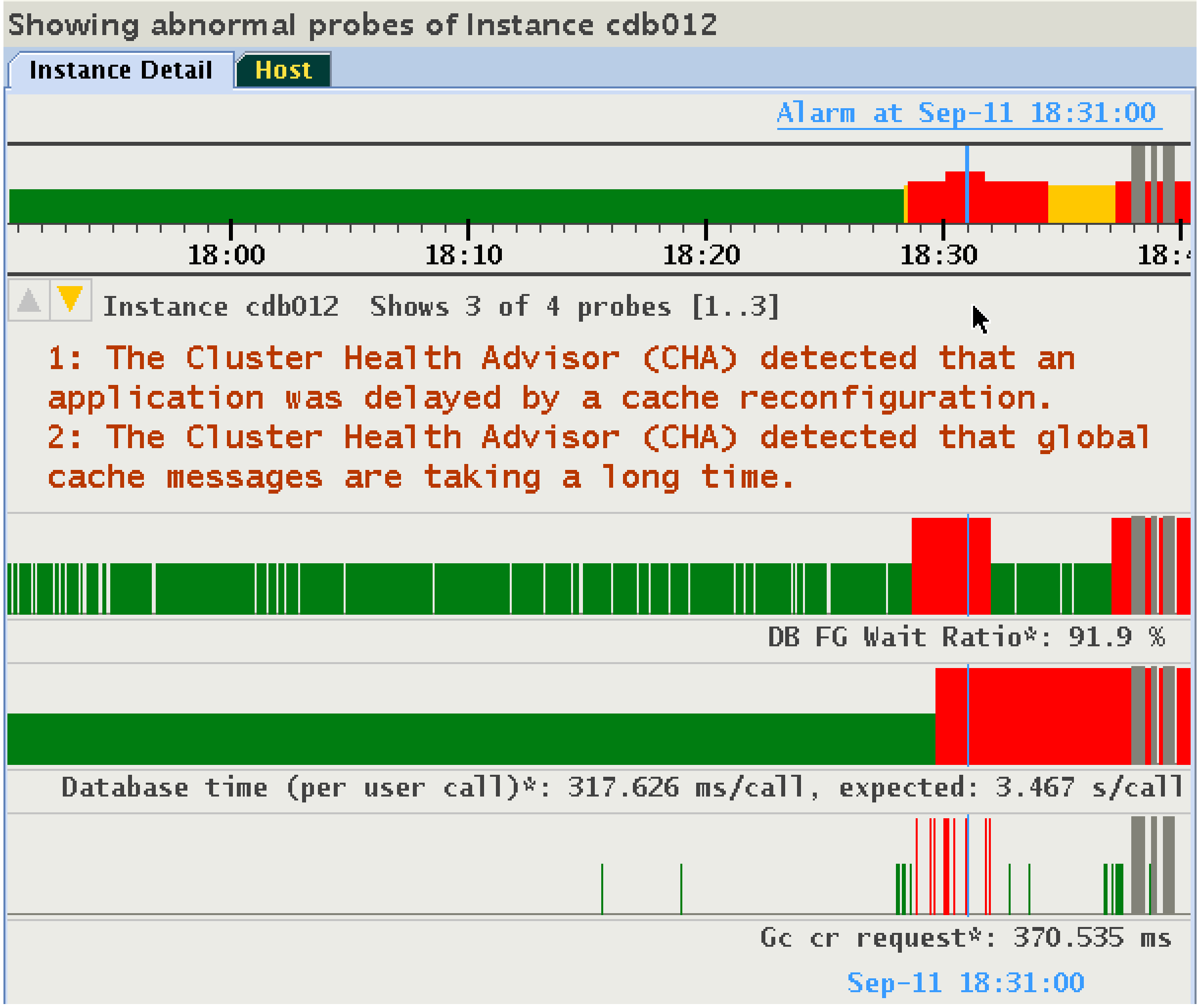
▷ 1: The Cluster Health Advisor (CHA) detected that an application was delayed by a cache reconfiguration.
2: The Cluster Health Advisor (CHA) detected that global cache messages are taking a long time.

Problems are listed in the order of their confidence probability. Problems that have probes that are Key Performance Indicator (KPI) will be displayed at the top of the list regardless of their confidence probability. The order and set of problems may differ at each time point, and a set of probes raised for each problem may vary with every time point.

The problem with a focus is indicated by a color change and a right arrow to the left of its number. Focus may also be changed using the up or down arrow keys.

Each problem has a set of probes in abnormal state. As long a specific Problem is not selected, AHF Scope will not display any probes. This default preference for display of probes may be changed by using the right click pop-up menu, or by using a Hot Key. For example, when selecting radio button "Show all High Probes" or pressing "a", all abnormal probes across all problems at 18:31 are displayed.

Figure 6-21 Problems or Anomalies



Showing abnormal probes of Instance cdb012

Instance cdb012 Shows 3 of 4 probes [1..3]

1: The Cluster Health Advisor (CHA) detected that an application was delayed by a cache reconfiguration.
2: The Cluster Health Advisor (CHA) detected that global cache messages are taking a long time.

DB FG Wait Ratio*: 91.9 %

Database time (per user call)*: 317.626 ms/call, expected: 3.467 s/call

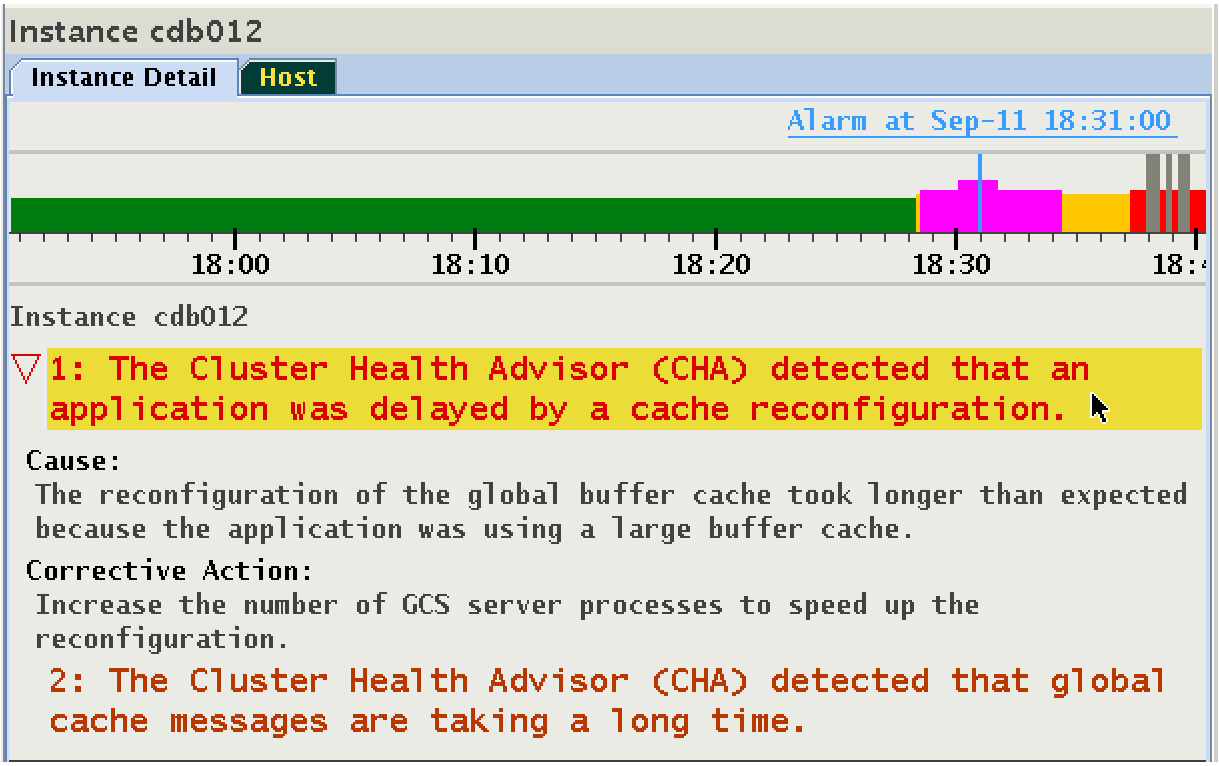
Gc cr request*: 370.535 ms

The highlighted up/down icons in the upper-left side of the panel indicates that not all probes can be displayed. In this example, the information bar displays "Shows 3 of 4 probes [1..3]". Use down/up Arrow or the page up/down keys to scroll through the probes while keeping same time position.

Probes specific to a problem are still available by returning to the default mode, and by selecting the problem of interest. Press "a" again to remove the display of all abnormal probes and return to the default mode.

To step through the analysis of a problem in detail, highlight the problem and either click it, or hit the Enter key on your keyboard. This action selects the highlighted problem and displays the root cause diagnosis and a recommended corrective action. In addition, on the status timeline every occurrence of the same problem is displayed in magenta. In the example below, the top problem was indicated between 18:28 and 18:34:

Figure 6-22   Problems or Anomalies



Instance cdb012

1: The Cluster Health Advisor (CHA) detected that an application was delayed by a cache reconfiguration.

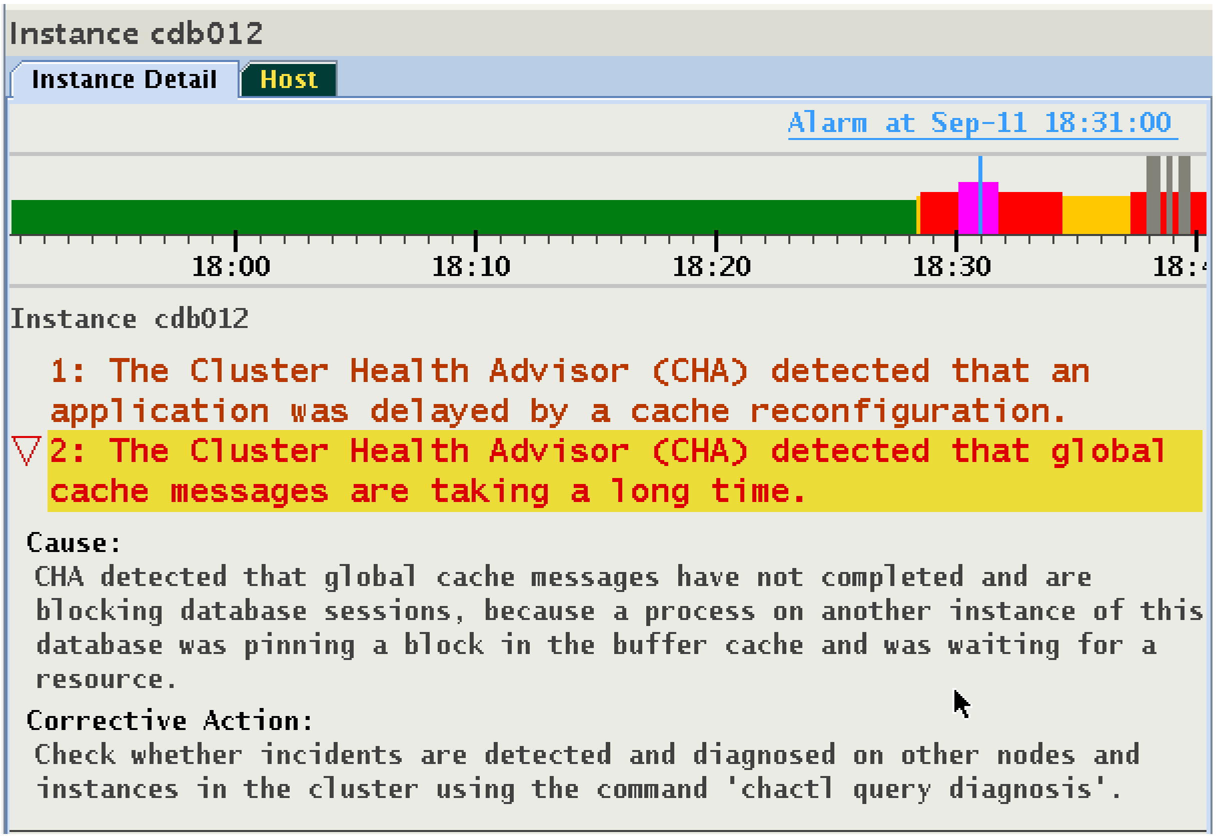
Cause:
The reconfiguration of the global buffer cache took longer than expected because the application was using a large buffer cache.

Corrective Action:
Increase the number of GCS server processes to speed up the reconfiguration.

2: The Cluster Health Advisor (CHA) detected that global cache messages are taking a long time.

To switch to another problem, either click it, or use the up/down arrow to highlight it, and then hit the Enter key on your keyboard. Note how the magenta marked time period has changed on target's status timeline.

Figure 6-23   Problems or Anomalies



Instance cdb012

1: The Cluster Health Advisor (CHA) detected that an application was delayed by a cache reconfiguration.

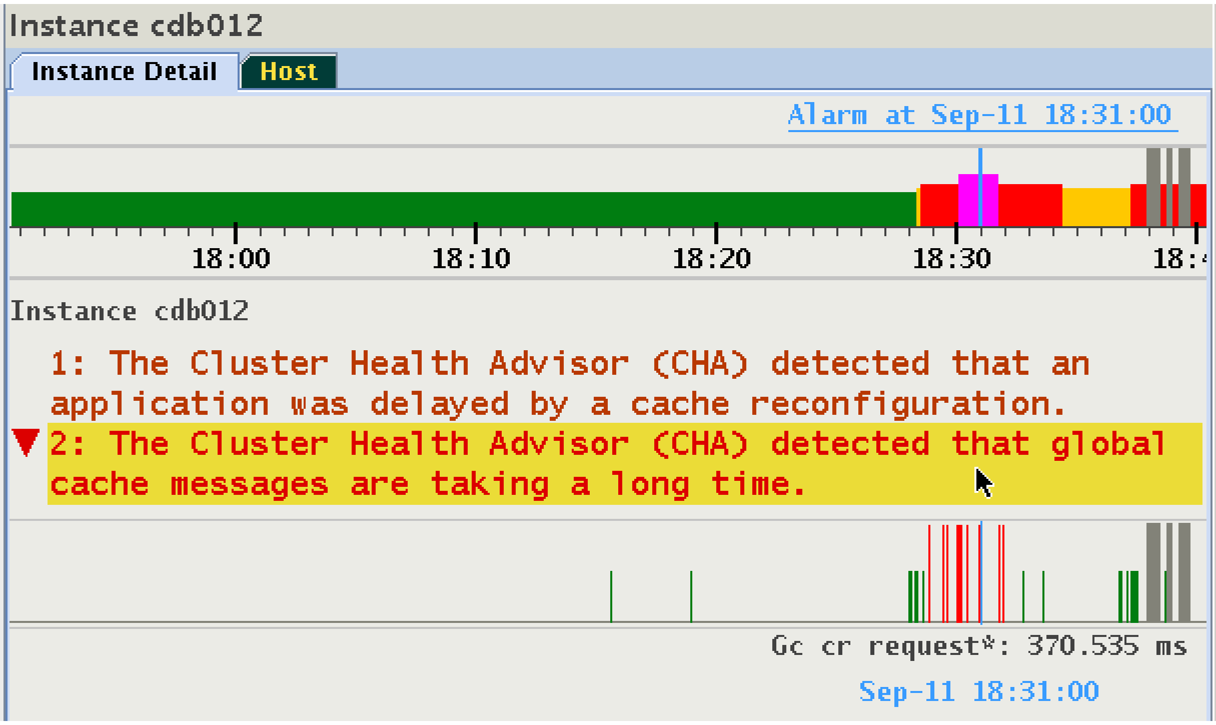
▽ 2: The Cluster Health Advisor (CHA) detected that global cache messages are taking a long time.

Cause:
CHA detected that global cache messages have not completed and are blocking database sessions, because a process on another instance of this database was pinning a block in the buffer cache and was waiting for a resource.

Corrective Action:
Check whether incidents are detected and diagnosed on other nodes and instances in the cluster using the command 'chactl query diagnosis'.

Click once more on the selected problem, or hit the Enter key on your keyboard to display the set of the probes providing evidence supporting the problem determination. In this example, the problem has only one probe, "Gc cr request":

Figure 6-24 Problems or Anomalies



Instance cdb012

1: The Cluster Health Advisor (CHA) detected that an application was delayed by a cache reconfiguration.

2: The Cluster Health Advisor (CHA) detected that global cache messages are taking a long time.

Gc cr request*: 370.535 ms

Sep-11 18:31:00

Hit the Enter key again, and note that the display returns to its list of problems to facilitate analysis of the additional ones. There are the following three problem displays which cycle upon clicking or pressing Enter.

1. Problem is highlighted (empty right arrow points to the problem name).
2. Problem is selected, shows textual descriptions of cause, corrective action (empty down arrow points to the descriptions).
3. Problem is selected, shows status timelines of probes associated with the problem (filled down arrow points to the probe timelines).

Note that when selecting a different problem by a mouse click or using Enter, the display mode stays the same allowing stepping through each problem in the same mode.

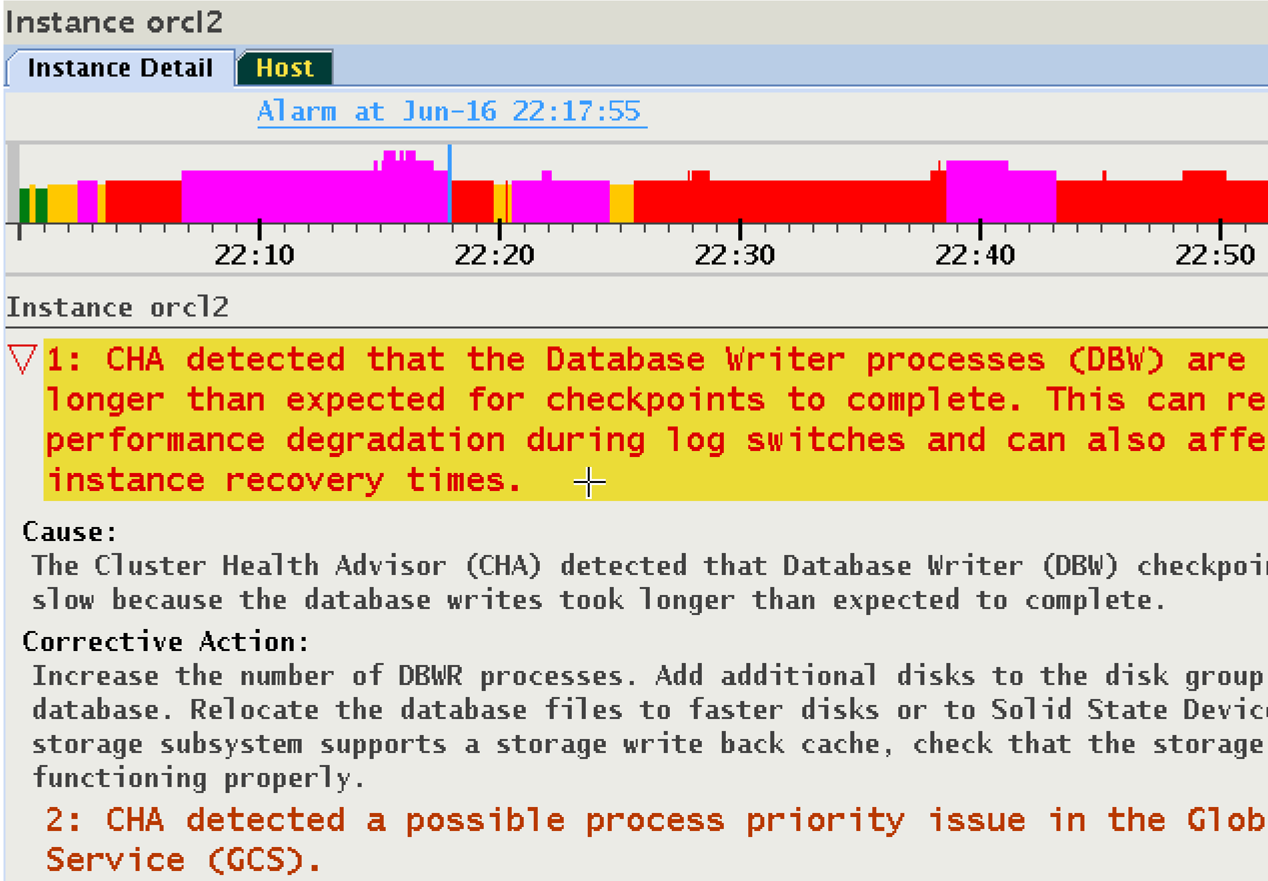
Related Topics

- Expert Mode
  Expert mode facilitates an advanced analysis of the metrics and their observed values against the predicted ones.

6.2.7 Browsing through active time of a Problem

Once a problem is selected, the time periods in which it was active is marked by a magenta color on the status timeline. Press and hold the Shift key and use the left or right arrow key to fast forward to a previous or next active time point in which this problem was indicated. As shown in Figure 13-25, for example, at 22:17:55 a "DB Writer checkpoint" problem is displayed. The magenta color shows several time ranges in which this condition was also diagnosed.

Figure 6-25   Browsing through active time of a Problem



Instance orcl2

1: CHA detected that the Database Writer processes (DBW) are longer than expected for checkpoints to complete. This can re performance degradation during log switches and can also affe instance recovery times.

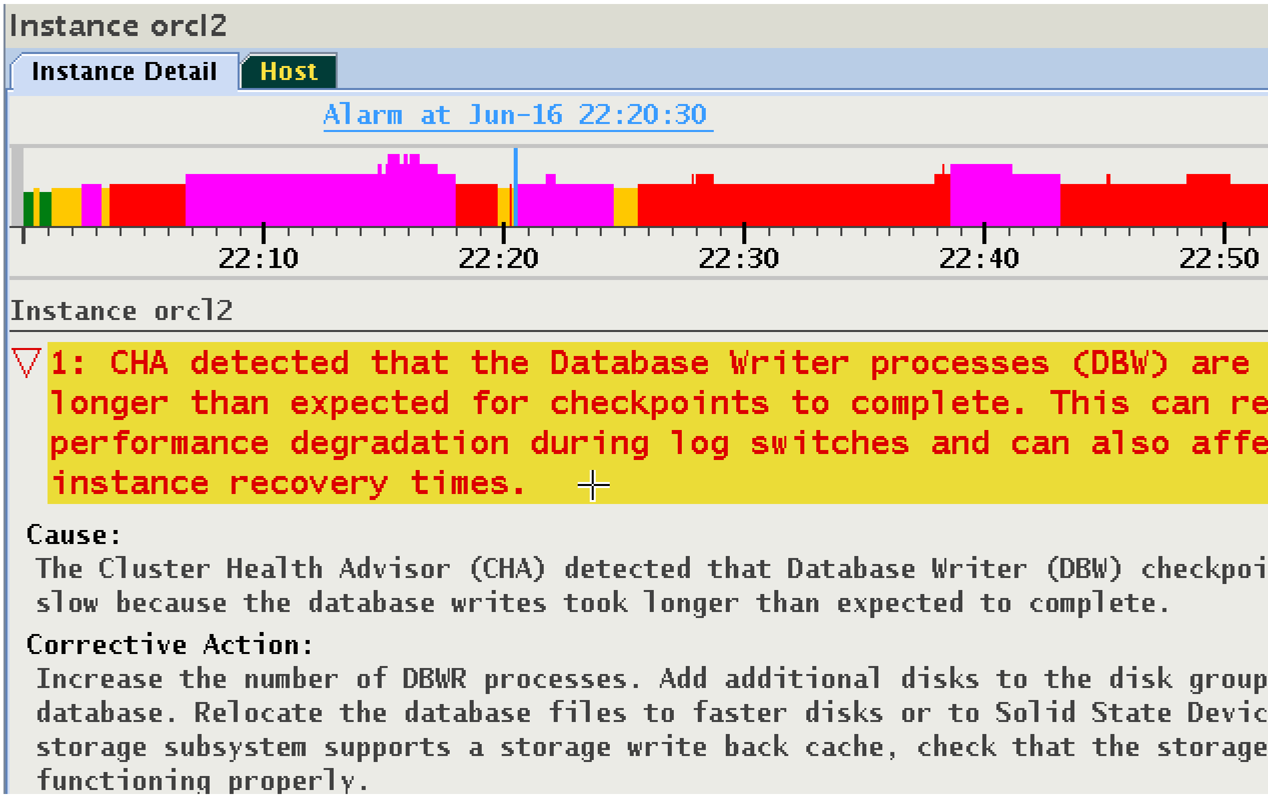
Cause:
The Cluster Health Advisor (CHA) detected that Database Writer (DBW) checkpoi slow because the database writes took longer than expected to complete.

Corrective Action:
Increase the number of DBWR processes. Add additional disks to the disk group database. Relocate the database files to faster disks or to Solid State Devic storage subsystem supports a storage write back cache, check that the storage functioning properly.

2: CHA detected a possible process priority issue in the Glob Service (GCS).

The selected timestamp is at the end of the magenta colored time range. Press Shift+Right Arrow keys and the cursor will move to the next later timestamp in which the same Problem was reported. In this case, it was 22:20:30, approximately two minutes later.

Figure 6-26 Browsing through active time of a Problem



1: CHA detected that the Database Writer processes (DBW) are longer than expected for checkpoints to complete. This can re performance degradation during log switches and can also affe instance recovery times.

Cause:
The Cluster Health Advisor (CHA) detected that Database Writer (DBW) checkpoi slow because the database writes took longer than expected to complete.

Corrective Action:
Increase the number of DBWR processes. Add additional disks to the disk group database. Relocate the database files to faster disks or to Solid State Devic storage subsystem supports a storage write back cache, check that the storage functioning properly.

6.3 Expert Mode

Expert mode facilitates an advanced analysis of the metrics and their observed values against the predicted ones.

Section 2 cover the Standard mode of operation. However, since this diagnosis is based on an applied machine learning model of predicted metric values, there is always a probability that an abnormal condition will not be diagnosed correctly - either raising a warning too late or providing a false one. To facilitate an advanced analysis of the metrics and their observed values against the predicted ones, an Expert mode is provided.

- Activating the Expert Mode
- Resizing Expert Diagrams
- Selecting Custom Set of Probes

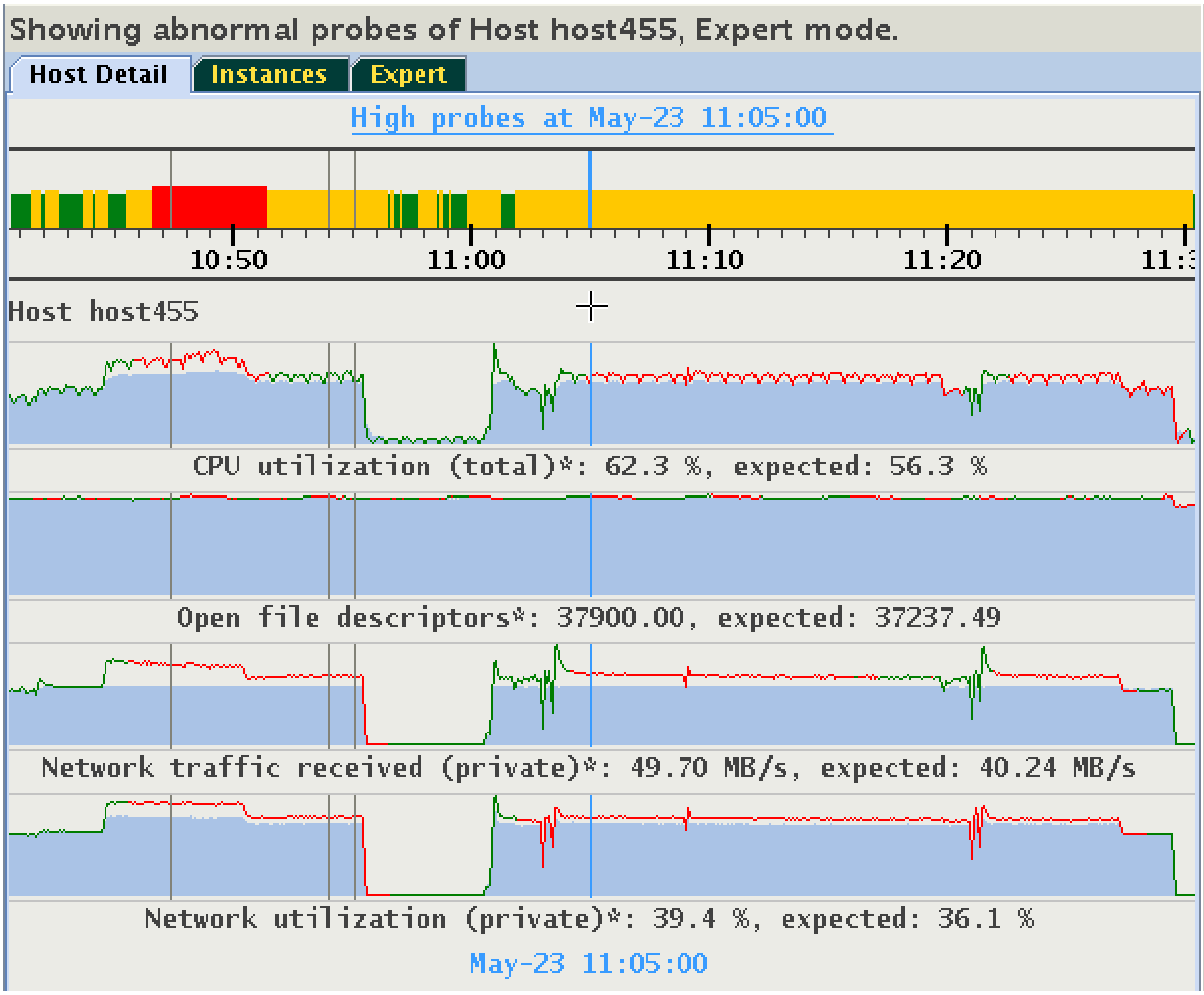
6.3.1 Activating the Expert Mode

Press "e" to toggle the Expert mode, or use the right-click pop-up menu, and then select "Expert". The probe status timelines change their appearance, and an additional "Expert" tab appears. Only the target timeline stays unchanged.

In the Expert mode, timelines of probes contain now an overlapping display of three values:

1. Time series for the expected (or predicted) value displayed as light blue lines from 0 to its value.
2. Time series for the observed value. Plotted on top of the predicted values in green or in red to indicate the state.
3. State of the probe marked in green or red of the observed value plot.

Figure 6-27 Activating Expert Mode



Showing abnormal probes of Host host455, Expert mode.

High probes at May-23 11:05:00

Host host455

CPU utilization (total)*: 62.3 %, expected: 56.3 %

Open file descriptors*: 37900.00, expected: 37237.49

Network traffic received (private)*: 49.70 MB/s, expected: 40.24 MB/s

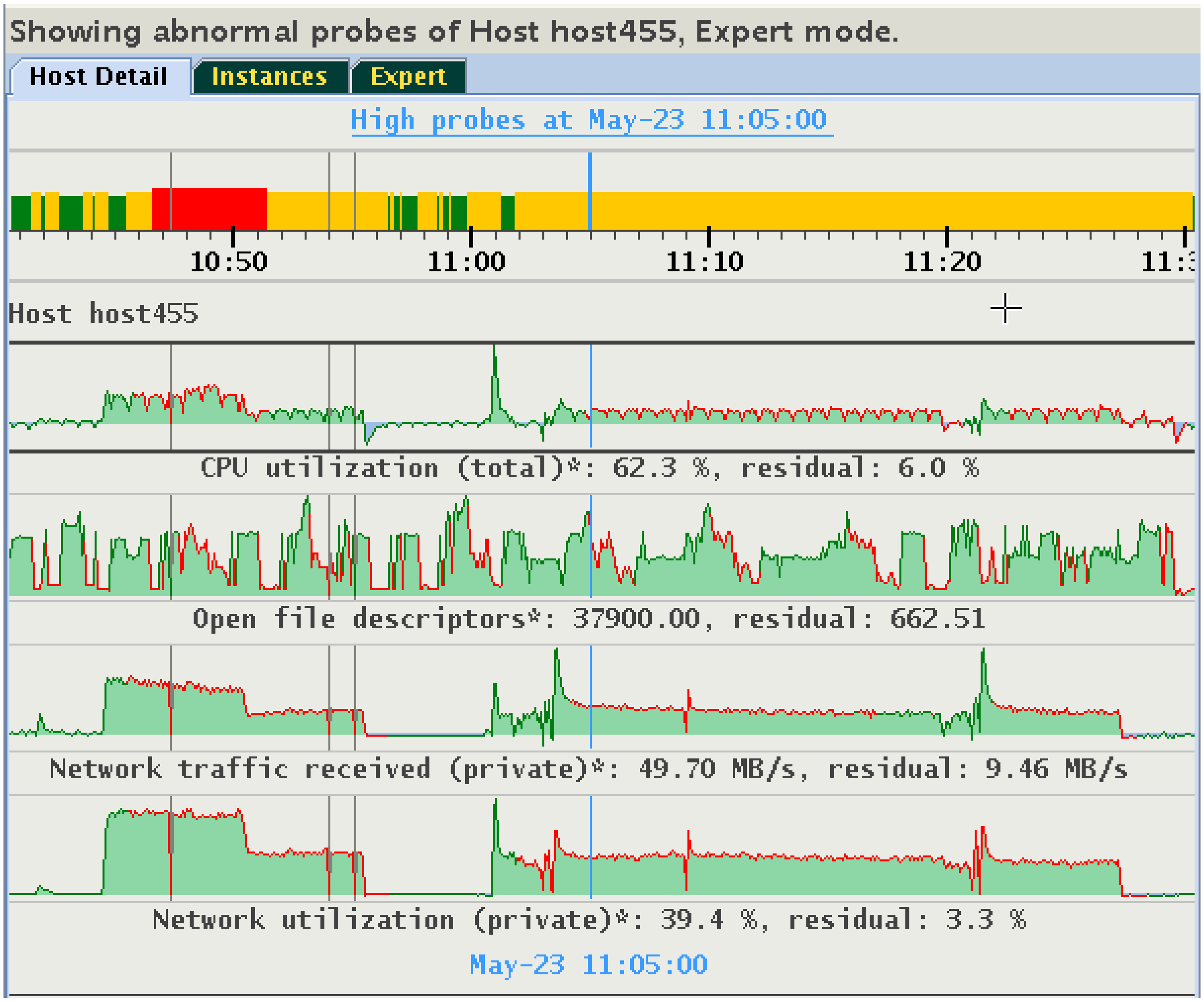
Network utilization (private)*: 39.4 %, expected: 36.1 %

May-23 11:05:00

This display helps to evaluate how well the existing model aligns the actual observed values with the predicted values. If the observed values are consistently and significantly different from predicted values, then it is likely that the model is not well-calibrated to a particular workload. Performing a CHA calibration based on this workload should be considered.

The histograms of the probes are dynamically self-adaptive to the range of values of each metric predicted or observed value. This might cause that parts of the visible time series appear "flat". The predicted and observed values might be so similar to each other that the differences between them would be barely visible. See the "Open file descriptors" in the above image. In such cases, you might prefer to see a plot of a difference between the observed and predicted values, called a "residual". Select "Display Residuals" on the floating menu, or press "r" to toggle between the display of residuals or of the pair predicted/observed. The time series shown originally in Figure 13-27 changes to what is shown in Figure 13-28.

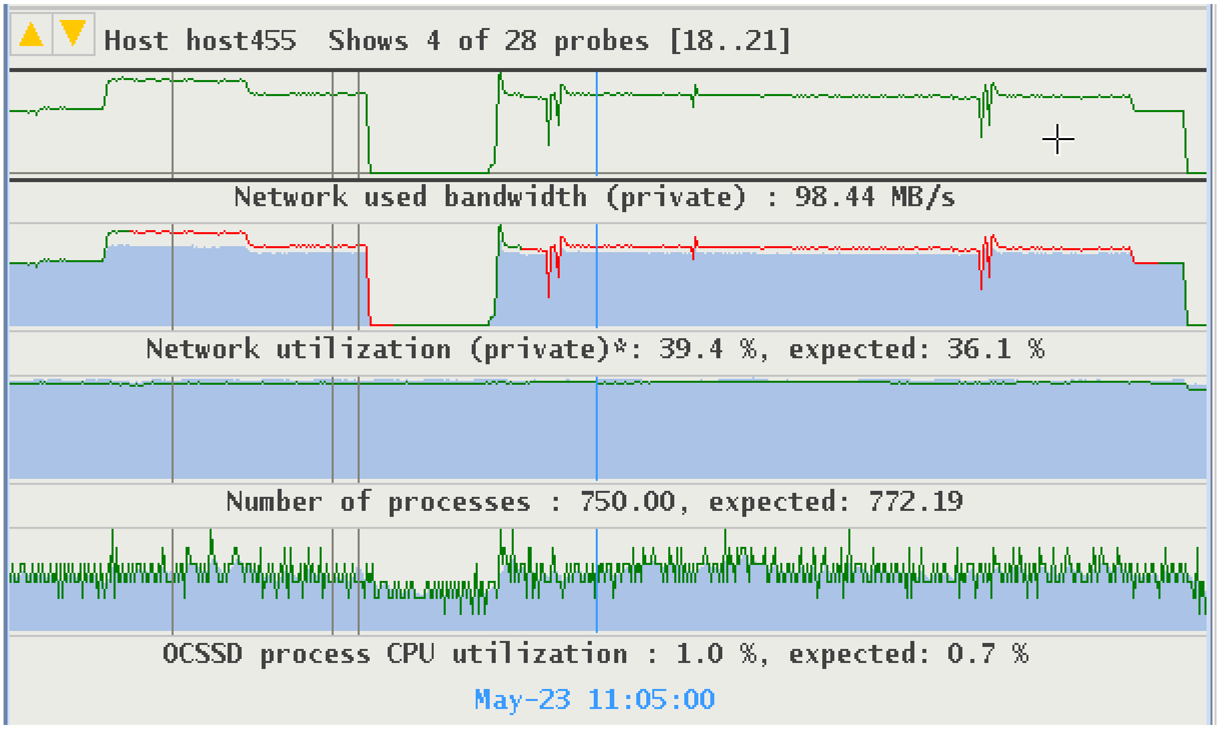
Figure 6-28 Activating Expert Mode


Showing abnormal probes of Host host455, Expert mode.
Host Detail
Instances
Expert
High probes at May-23 11:05:00
10:50
11:00
11:10
11:20
11:3
Host host455
CPU utilization (total)*: 62.3 %, residual: 6.0 %
Open file descriptors*: 37900.00, residual: 662.51
Network traffic received (private)*: 49.70 MB/s, residual: 9.46 MB/s
Network utilization (private)*: 39.4 %, residual: 3.3 %
May-23 11:05:00

Note how the differences in values of "Open file descriptors" become visible. Positive residuals are displayed as "green hills" (observed value is greater than the predicted), and negative residuals are displayed as "blue pools" (observed value less than predicted).

This display will be meaningful only for probes for which CHA provides both expected and observed values. Otherwise, they will appear empty. Consider the following example, in which the metric "Network used bandwidth" does not have expected values.

Figure 6-29   Activating Expert Mode



Host host455 Shows 4 of 28 probes [18..21]

Network used bandwidth (private) : 98.44 MB/s

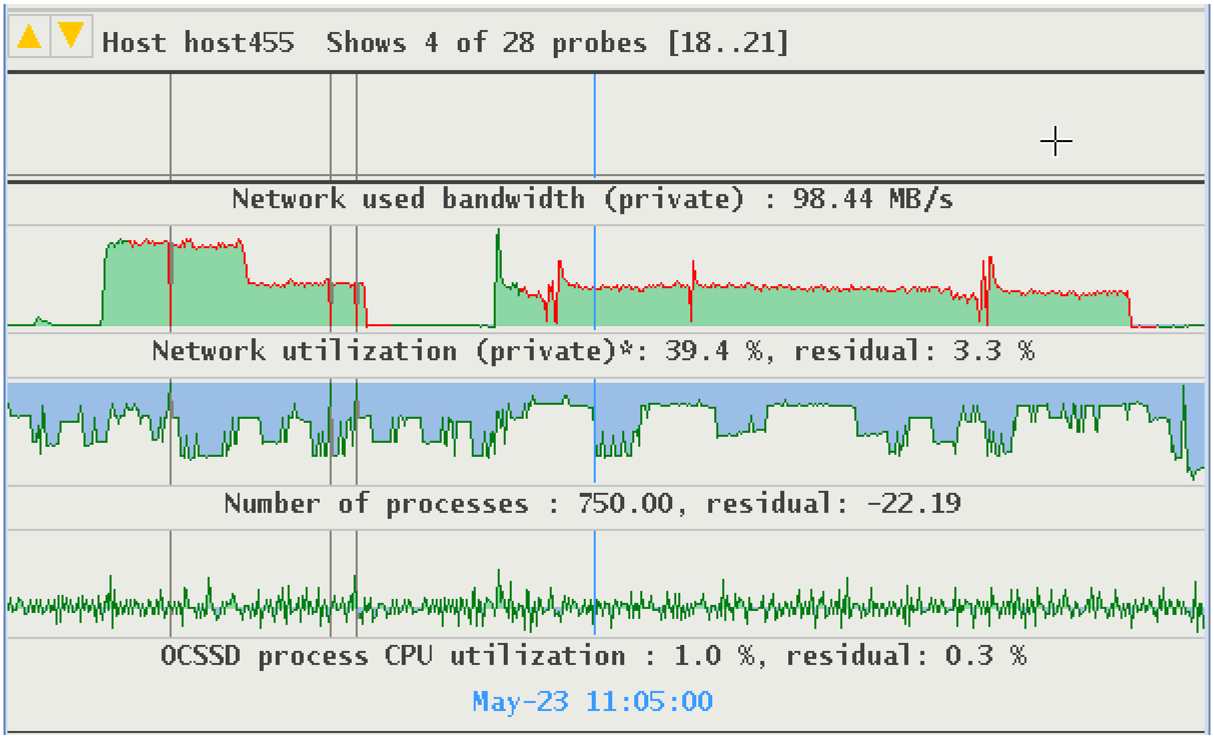
Network utilization (private)*: 39.4 %, expected: 36.1 %

Number of processes : 750.00, expected: 772.19

OCSSD process CPU utilization : 1.0 %, expected: 0.7 %

Display of residuals for this metric is empty. The display for "Network utilization" and "Number of processes" provide good visualization of differences between their expected and observed values.

Figure 6-30   Activating Expert Mode

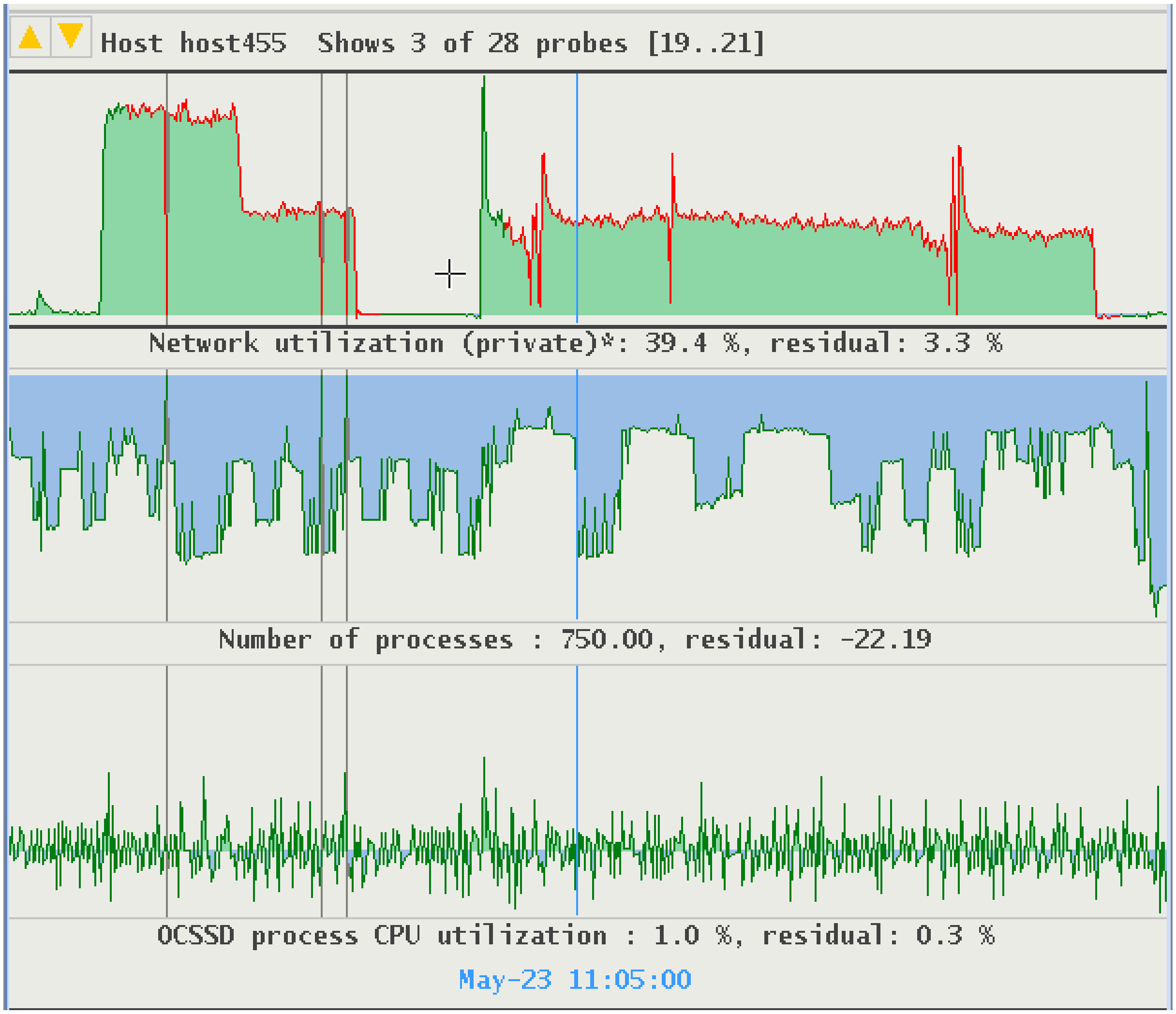

▲ ▼ Host host455 Shows 4 of 28 probes [18..21]
Network used bandwidth (private) : 98.44 MB/s
Network utilization (private)*: 39.4 %, residual: 3.3 %
Number of processes : 750.00, residual: -22.19
OCSSD process CPU utilization : 1.0 %, residual: 0.3 %
May-23 11:05:00

The time series of "OCSSD process CPU utilization" suggest a good similarity between the observed and predicted values.

6.3.2 Resizing Expert Diagrams

Due to auto-scaling, important details in observed and predicted values may not be easily visible. A vertical zoom function is available by placing the cursor over the area of interest and pressing Control+Left mouse button to drag the cursor up or down. The maximum height of each graph is 128 pixels. The example below shows the previous image enlarged to display more detail in graphs.

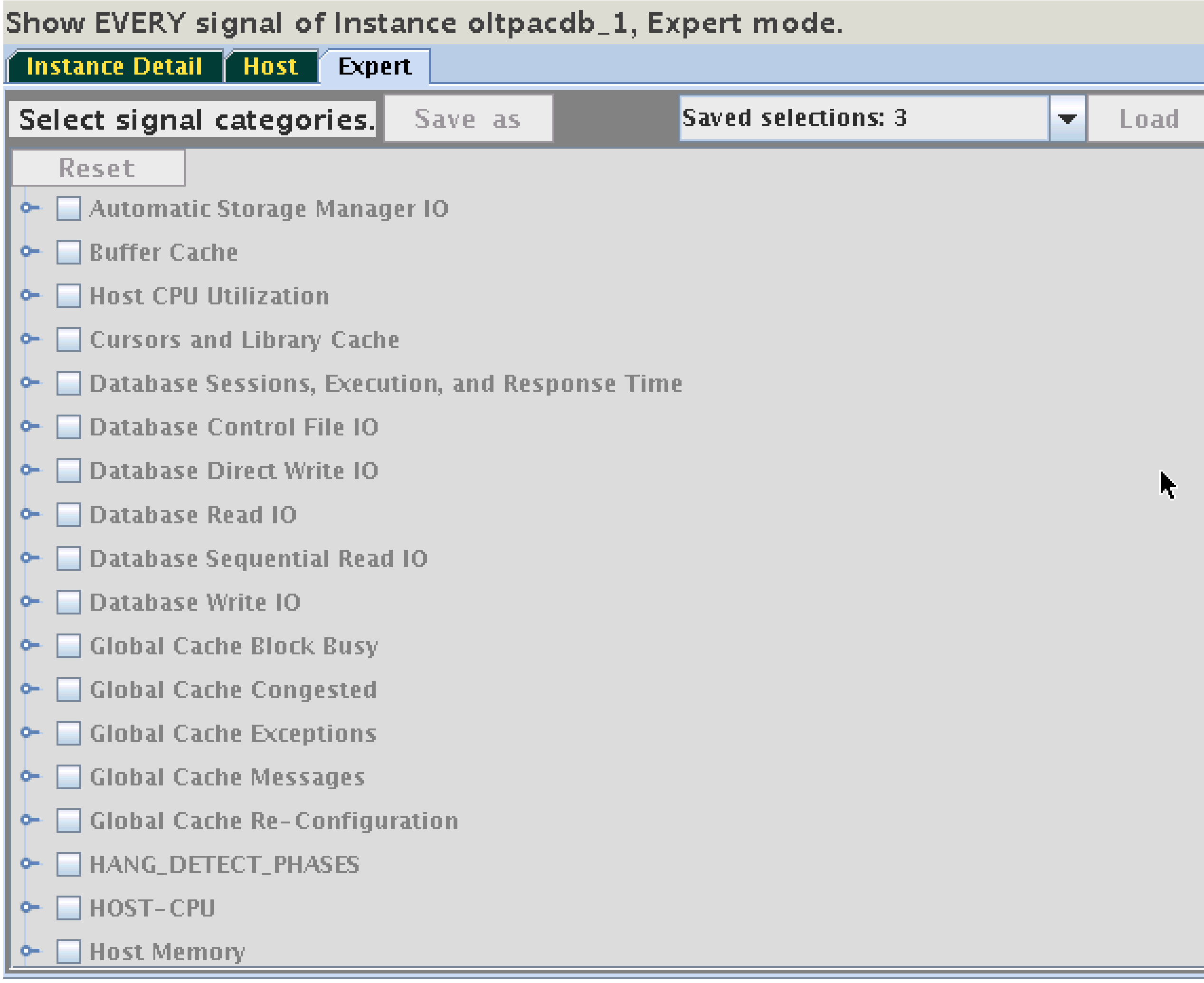
Figure 6-31 Resizing Expert Diagrams


Host host455 Shows 3 of 28 probes [19..21]
Network utilization (private)*: 39.4 %, residual: 3.3 %
Number of processes : 750.00, residual: -22.19
OCSSD process CPU utilization : 1.0 %, residual: 0.3 %
May-23 11:05:00

6.3.3 Selecting Custom Set of Probes

Probes monitored by CHA are grouped into categories. A custom set of probes may be specified based on their categories, or on individual probes from different categories. Click the "Expert" tab, or use the tab and left/right arrow key to navigate to the Expert panel.

Figure 6-32   Selecting Custom Set of Probes

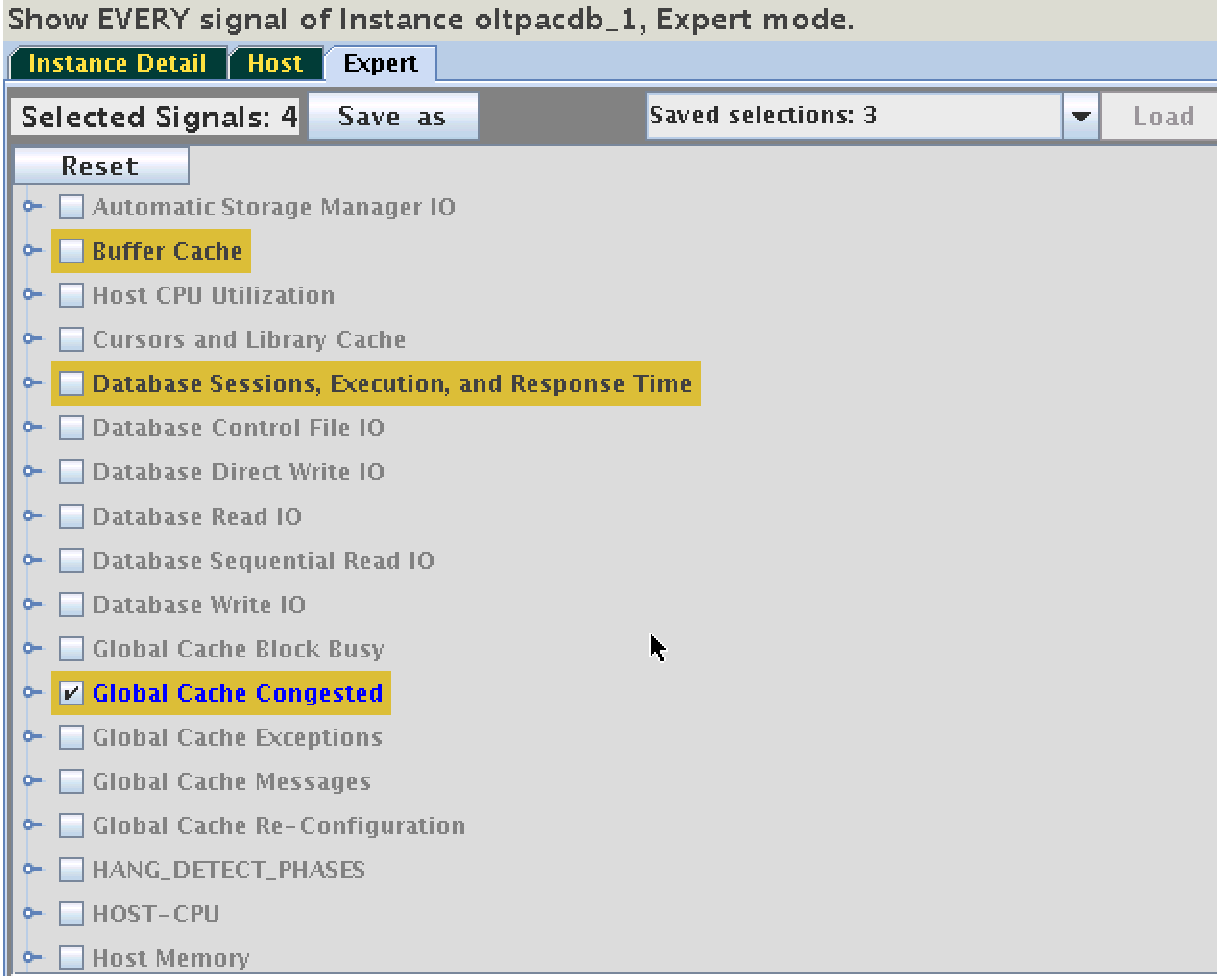


Show EVERY signal of Instance oltpacdb_1, Expert mode.

- □ Automatic Storage Manager IO
- □ Buffer Cache
- □ Host CPU Utilization
- □ Cursors and Library Cache
- □ Database Sessions, Execution, and Response Time
- □ Database Control File IO
- □ Database Direct Write IO
- □ Database Read IO
- □ Database Sequential Read IO
- □ Database Write IO
- □ Global Cache Block Busy
- □ Global Cache Congested
- □ Global Cache Exceptions
- □ Global Cache Messages
- □ Global Cache Re-Configuration
- □ HANG_DETECT_PHASES
- □ HOST-CPU
- □ Host Memory

This panel provides access to a hierarchical tree with probe categories. The number of probe categories may vary between CHA models. To create a custom set of displayed probes, select either a category or expand its tree, and then select individual probes from any category. For example, select the category "Global Cache Congested". Its name is highlighted in yellow and its checkbox is selected. Note, two additional categories became highlighted without their checkboxes being selected. This means that one or more of the probes from "Global Cache Congested" are also their members.

Figure 6-33   Selecting Custom Set of Probes



Show EVERY signal of Instance oltpacdb_1, Expert mode.

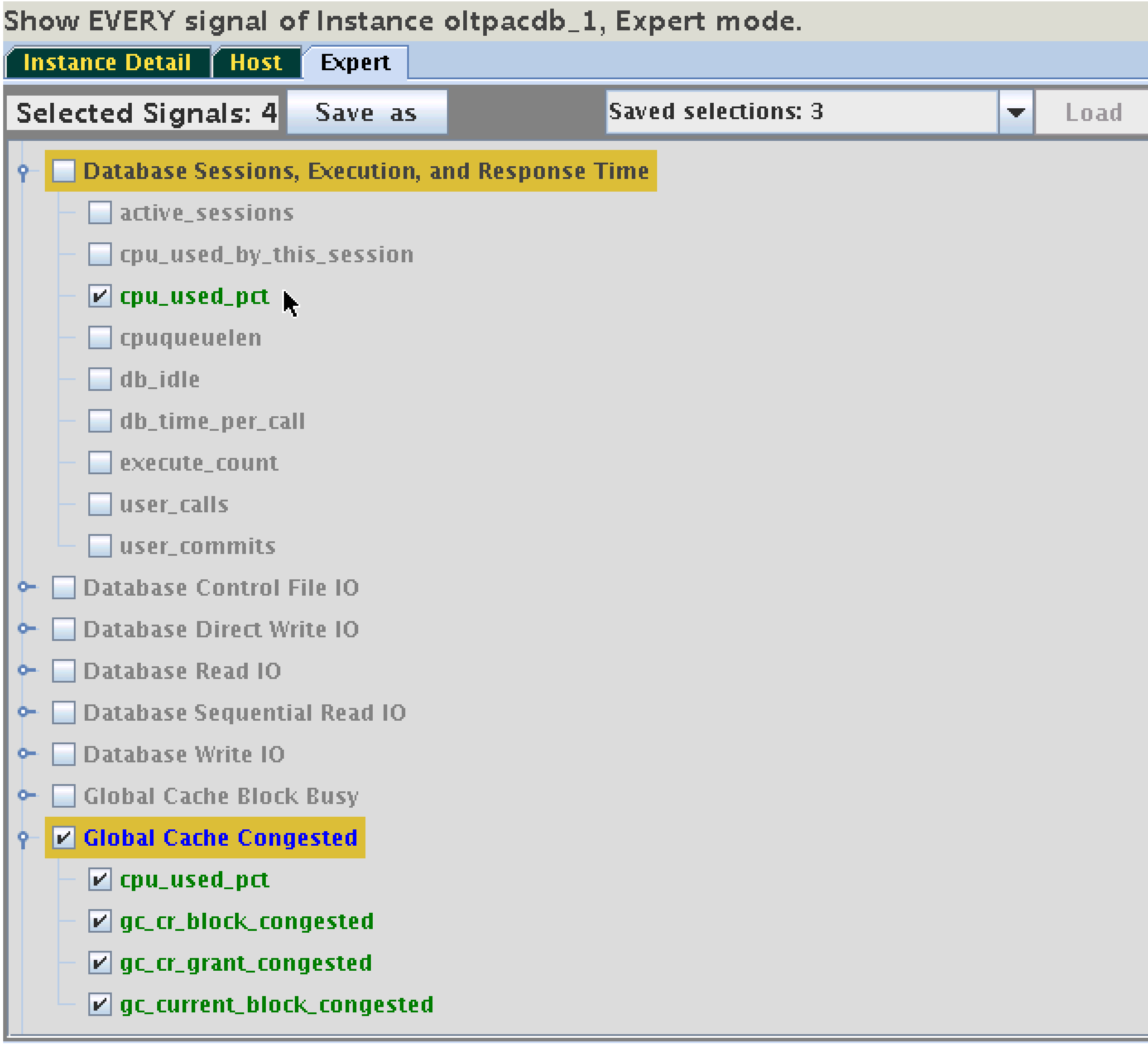
Selected Signals: 4

Saved selections: 3

- □ Automatic Storage Manager IO
- □ Buffer Cache
- □ Host CPU Utilization
- □ Cursors and Library Cache
- □ Database Sessions, Execution, and Response Time
- □ Database Control File IO
- □ Database Direct Write IO
- □ Database Read IO
- □ Database Sequential Read IO
- □ Database Write IO
- □ Global Cache Block Busy
- ☑ Global Cache Congested
- □ Global Cache Exceptions
- □ Global Cache Messages
- □ Global Cache Re-Configuration
- □ HANG_DETECT_PHASES
- □ HOST-CPU
- □ Host Memory

Expand the selected category and one of the other yellow highlighted categories to see which probe they share. In this case, it is the "cpu_used_pct":

Figure 6-34 Selecting Custom Set of Probes



Show EVERY signal of Instance oltpacdb_1, Expert mode.

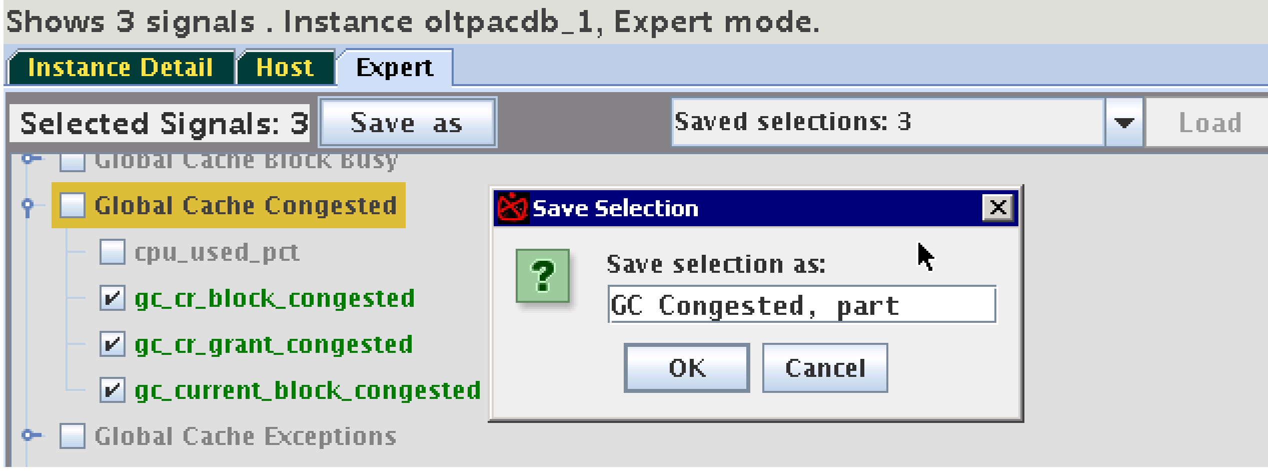
Selected Signals: 4

Saved selections: 3

- ☐ Database Sessions, Execution, and Response Time
  - ☐ active_sessions
  - ☐ cpu_used_by_this_session
  - ☑ cpu_used_pct
  - ☐ cpuqueuelen
  - ☐ db_idle
  - ☐ db_time_per_call
  - ☐ execute_count
  - ☐ user_calls
  - ☐ user_commits
- ☐ Database Control File IO
- ☐ Database Direct Write IO
- ☐ Database Read IO
- ☐ Database Sequential Read IO
- ☐ Database Write IO
- ☐ Global Cache Block Busy
- ☑ Global Cache Congested
  - ☑ cpu_used_pct
  - ☑ gc_cr_block_congested
  - ☑ gc_cr_grant_congested
  - ☑ gc_current_block_congested

By unchecking the probe "cpu_used_pct", only one category will remain highlighted. Switch to the "Instance Detail" tab to see that now only the three signals of the category "Global Cache Congested" are being displayed on the Instance tab. Selections may be stored for reuse. On the Expert tab use the button "Save As" to save the selection under a specified name.

Figure 6-35 Selecting Custom Set of Probes



Shows 3 signals . Instance oltpacdb_1, Expert mode.

Selected Signals: 3

Saved selections: 3

□ Global Cache Block Busy

□ Global Cache Congested

□ cpu_used_pct

☑ gc_cr_block_congested

☑ gc_cr_grant_congested

☑ gc_current_block_congested

□ Global Cache Exceptions

Save selection as: GC Congested, part

These saved selections will be available after a restart of AHF Scope on the same host. Use the drop-down menu "Saved selections" to retrieve any of the saved sets of probes. Press "Load" to activate it, or press "Delete" to remove it from the persistent storage. Note, that selecting of the saved set without a corresponding Loading does not activate it.

6.4 Live and Passive Sessions

AHF Scope maintains two separate sessions in parallel, Live Session (Primary) to receive current metrics in real-time and Past (Replay) Session to display statically a situation encountered at an earlier time.

AHF Scope can be run locally on one of the Oracle RAC cluster nodes and connected to the Grid Infrastructure Management Repository (GIMR,) or by reading exported GIMR data from a file.

> **Note:**
>
> Note, remote GIMR connections are not supported because the SQL connection is not encrypted.

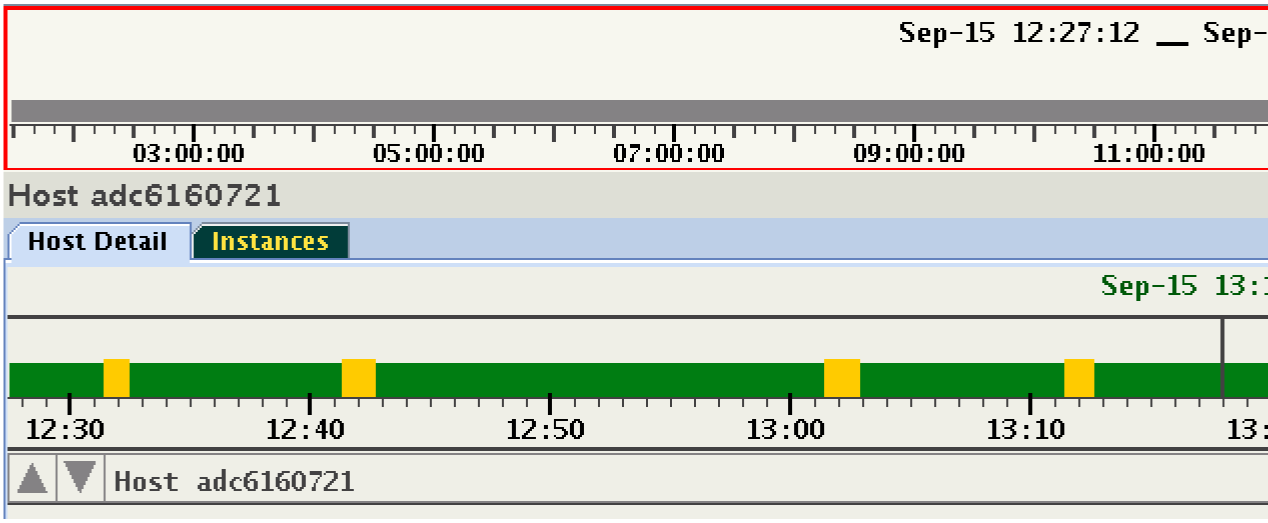
When connected to a GIMR database and actively receiving samples in real-time from a live system, AHF Scope maintains in parallel two separate sessions:

1. **Live Session (Primary):** Receives in real time current metrics.
2. **Past (Replay) Session:** Displays statically a situation encountered at an earlier time.

Access to a replay session is available via the System Timeline (Ticker Tape) only when AHF Scope is connected to a GIMR. When AHF Scope is started with `-f` *`file`* as its feed, Ticker Tape is not active. In such a case, the primary session is passive and AHF Scope does not have any possibility to retrieve data from the past.

Use Ticker Tape to locate the time period of interest. Place the cursor over the Time Selector and press the Shift key. Note that Ticker Tape now displays information about the time range corresponding to the location of the time selector.

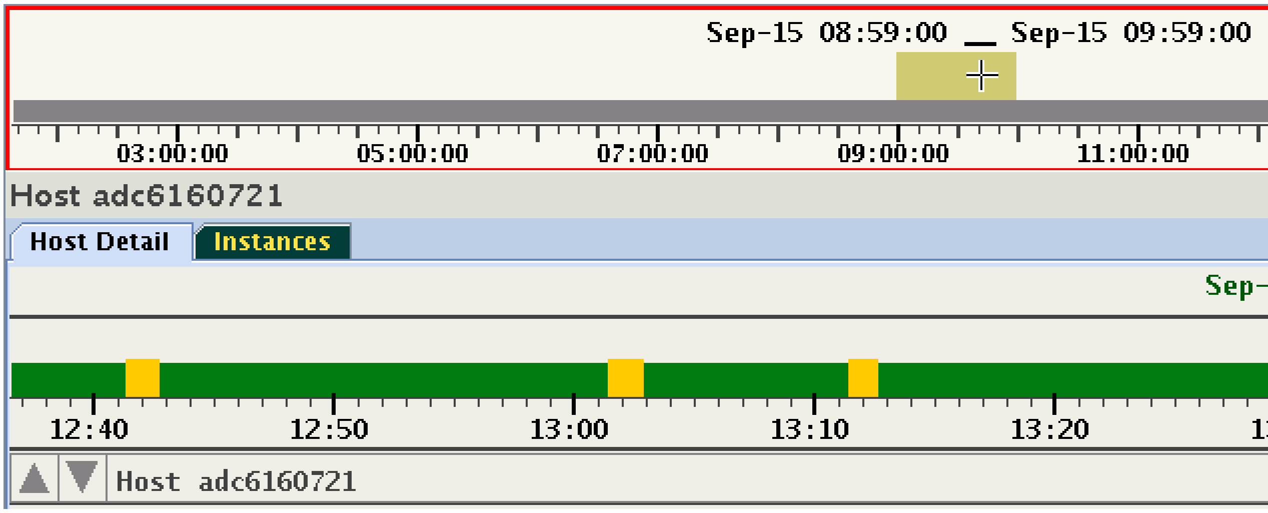
Figure 6-36 Live and Passive Sessions



In this example, the selected time period is the hour from 12:27:12 to 13:27:12. The time selector width (time period) is customizable by using the `-q` *`minutes`* command-line parameter.

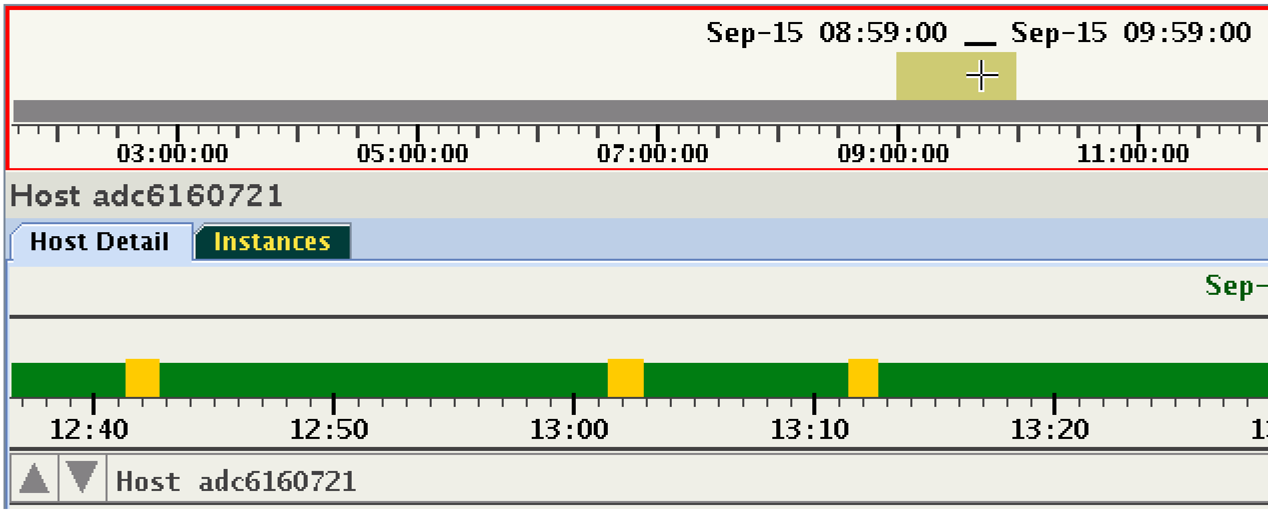
While holding down the Shift key, press the left mouse button, and then slide the time selector to an older time point. Time Selector may also be moved without using a mouse. Press the Shift key and while holding it, press the left or right arrow to shift time selector by 30 minutes. In this example, time selector was moved to approximately. 9:00.

Figure 6-37 Live and Passive Sessions



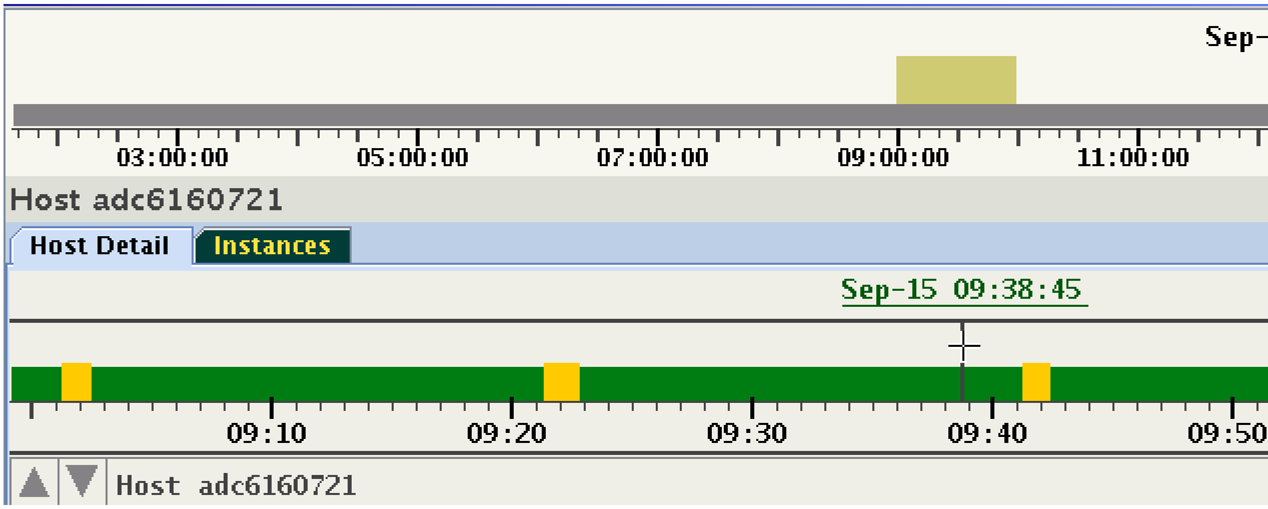
Release the Shift key. AHF Scope will issue a query to GIMR requesting a set of samples for the selected period in time. The time to retrieve this data can be substantial especially when CHA monitors many databases in a large cluster. While the query and the parsing process of the data is in progress, a clock "Wait-Cursor" is displayed. In the background, the current timelines of the live session continue to receive data and advance accordingly.

Figure 6-38 Live and Passive Sessions



Once the query and parsing of the data is finished, AHF Scope displays the data of a "Replay Session". In this example, this session covers one hour, that is approximately 9:00..10:00 o'clock.

Figure 6-39 Live and Passive Sessions



This display never changes. You can investigate the data in the customary way without any time restriction. However, the "Live Session" is still active and in the background the data is constantly being collected. To restore the live session, either slide the time selector to the right end, or with the cursor hovering over System Timeline, press "=". Note that the past session data is discarded from memory once the session is switched to Live.

6.5 ahfscope Console Commands

Use the `ahfscope -i` command option to activate an interactive command-line interface (CLI). Enter a question mark (?) to see the list of available commands.

Syntax

```
cha> ?
    list item
         entities
         inputs
         kinds
              verbose
         metrics
              details
         probes
                 diff
                 nounit
                 noobserved
                 nopredicted
                 missing
                 flagged
                 units
                 diagnose
        trace item
         f: (feed)
         d: (db)
         i: (input)
         p: (probes)
         r: (rootcause)
         t: (topology)
        version
        zoom (in|out)
        quit
```

Parameters

Table 6-1 ahfscope Console Command Parameters

Parameter	Description
`list` *`item`*	• `entities`: List of entities and time ranges of their relations. • `inputs`: Lists input feeds • `kinds`: Kinds of Entities and number of their metrics – `verbose`: Lists metrics with every kind • `metrics`: List of all known metrics and their units of measure. – `details`: Lists metrics with full name and description of value • `probes`: List of all probes (signals) for all entities. – `diff`: Lists probes where number of predicted and observed values differ – `nounit`: Lists probes without unit of measure – `noobserved`: Lists probes without observed values – `nopredicted`: Lists probes without predicted values – `missing`: Lists probes with missing values in some samples – `flagged`: Lists probes flags set • `units`: List units of measure. – `diagnose`: Shows conversion rules and values at conversion thresholds.
`trace` *`item`*	Switch tracing on/off, indicated by '+' or '-'. • `f`: (feed) Live feed activity. • `d`: (db) Toggle `alter session` for trace event 10046 (ORA DB). • `i`: (input) Copy incoming data to the log file. • `p`: (probes) Displays internal or descriptive probe names. • `r`: (rootcause) Prints to console CLOB's containing a root cause of a problem. • `t`: (topology) Displays changes in set of entities (topology).
`version`	Version of the (1) user interface, (2) data stream, and (3) Java Virtual Machine.
`zoom (in|out)`	Sets or resets magnify option.
`quit`	Exits AHF Scope GUI.

For convenience, AHF Scope's CLI provides an abbreviation grammar. For example: Instead of typing `version`, you can simply type `v`:

```
cha> version
   CHA UI version:     V1.00.000
   Data version:       V0.17
   PL/SQL package:     V0.10.11.2
   Java version:       1.8.0_77 on Linux


cha> v
   CHA UI version:     V1.00.000
   Data version:       V0.17
```

```
PL/SQL package:     V0.10.11.2
Java version:       1.8.0_77 on Linux
```

When more than one command starts with the same prefix, they need to be disambiguated. For example, `debug` versus `device` would require typing at least 3 letters to correctly identify the desired command. These commands provide summaries not available in graphical form.

6.6 List of Hot Keys

Hot Keys are keyboard shortcuts that provide an alternate way to do something you would typically do with a mouse.

List of Hot Keys

Table 6-2 List of Hot Keys - on any place

Key	Description
^+ (control +)	Enlarge (Zoom In). On many keyboards '+' might stand over '=', use "shift" to reach '+'
^- (control -)	Shrink (Zoom Out)
w (lower case w)	Toggle theme (Day/Night)

Table 6-3 List of Hot Keys - on a target panel (Host or Instance)

Key	Description
a (lower case a)	Show all probes in high state.
A (upper case A)	Show all existing probes.
c (lower case c)	Show all correlated probes belonging to the same Probe category.
e (lower case e)	Toggle expert mode.
r (lower case r)	Toggle values predicted (expected)/residuals.
p (lower case p)	On state histogram: pin the cursor line at the current position.
f (lower case f)	On state histogram: follow (unpin).
-> (shift right-arrow)	Jump to the next occurrence of the selected problem.
<- (shift left-arrow)	Jump to the previous occurrence of the selected problem.
^q (control q)	Print the values of the focused probe before and after the position marker.
<escape>	Remove time filter, unpin, and deselect a problem

Note:

Set may be filtered in the **Expert** Tab.

Table 6-4 List of Hot Keys - zoom Signal Histograms in Host/Instance panel between 24..128 pixels. The cursor has to be in the histogram area.

Key	Description
control+mouse left-button drag up	Makes the histograms smaller.
control+mouse left-button drag down	Makes the histograms larger.
control+arrow up	Makes the histograms smaller.
control+arrow down	Makes the histograms larger.

Table 6-5 List of Hot Keys - Signal navigation (active when not all signals visible on a panel)

Key	Description
Arrow Up/Down	Navigate between signals, scroll visible signals by one.
Page-Up/Page-Down	Navigate between signals, scroll entire page of signals.

Table 6-6 List of Hot Keys - on the system timeline (Ticker Tape)

Key	Description
= (equal sign)	Jump to the current timestamp from a "Past Session", resume "Live Session".
Shift + Left/Right Cursor	Shift time selector by 30 minutes to the left or right.

Table 6-7 List of Hot Keys - entity navigation on all non-target panels

Key	Description
<Enter>	Selects the focused entity and displays the panel associated with the Entity.

6.7 Set of Persistent Settings

Review the list of persistent settings that you can reuse.

1. Theme dark/light
2. Last time of start
3. Width of the details panel, corresponding to number of minutes on this display
4. Window size and position
5. Last selected set of probes
6. Every set of Named Custom Selections of probes. See *Selecting Custom Set of Probes*.

Related Topics

- Selecting Custom Set of Probes

6.8 Accessibility Aspects

AHF Scope can be used without the help of the mouse.

Every operation can be achieved using the keys, Tab, cursor keys, Enter, and several Hot Keys described in *List of Hot Keys*. Some of the operations are available in combination with Shift and Control keys. No timeout exist on any of these operations, thus they can be used in conjunction with Sticky Keys and Slow Keys. The navigation contains components from standard Java "Swing" augmented by custom implementation of navigation in components designed for the unique, specialized displays in AHF Scope.

A magnification operation allows to enlarge text and components on panels. AHF Scope's displays are always high contrast, without use of images. They do not change with OS High Contrast mode, and AHF Scope's display or mode of operation does not affect the remaining desktop.

To enable accessible technology in Java on Microsoft Windows, follow the instructions outlined in *Enabling and Testing Java Access Bridge on Microsoft Windows*.

AHF Scope can operate with assistive technology software JAWS from Freedom Scientific, V17 and later.

Related Topics

- Enabling and Testing Java Access Bridge on Microsoft Windows
- List of Hot Keys
  Hot Keys are keyboard shortcuts that provide an alternate way to do something you would typically do with a mouse.

6.9 Customizing Java Run Time System

As AHF Scope is written in Java, it is platform independent.

The script `ahfscope` invokes the Java Virtual Machine (JVM) with Oracle classes. Knowledgeable users may consider customizing this script, or use the environment variable `_JAVA_OPTIONS` to determine the way the JVM executes code.

JVM is the run-time process, which interprets Java classes. All contemporary JVM's incorporate some method of on-the-fly translation of bytecode into native code. Dominating in this field is the Hot Spot. Except for beginning invocations of classes, in most cases Java methods run later in native code. Consequently, they perform at speeds comparable to programs written in native languages, such as C.

Furthermore, on many platforms Java supports native 2D and 3D graphics with a hardware acceleration through the use of the Open GL libraries that significantly improves display performance. It is highly recommended that Open GL will be configured for default use with JVM. Information about the Open GL library is available at: *http://www.opengl.org/*. Most manufacturers of rendering hardware, that is graphics cards, provide a version of this library for their video cards. It is important to obtain a current version of this library, besides the current drivers for the graphics card. See the following sites for detailed information about Java rendering using Open GL:

- *https://docs.oracle.com/javase/8/docs/technotes/guides/2d/flags.html#opengl*
- *https://docs.oracle.com/javase/8/docs/technotes/guides/2d/new_features.html*

JVM activation flags for OpenGL are:

- `-Dsun.java2d.opengl=true`: Use the OpenGL pipeline
- `-Dsun.java2d.d3d=true`: Use the Direct3D accelerator for Microsoft Windows

AHF Scope does not render in 3D, but benefits greatly from the accelerated region repaint available through Direct3D.

JVM options may be used with the `java` command, or declared as an environment variable, `_JAVA_OPTIONS`.

Linux Example:

```
_JAVA_OPTIONS="-Dsun.java2d.opengl=True -Dsun.java2d.d3d=true"  export
_JAVA_OPTIONS
```

Note the capitol "T" in the "true": If written with a capital letter, Java will print to the standard output whether the OpenGL pipeline is available or not. The following is an example of a warning that Open GL is not available:

```
Picked up _JAVA_OPTIONS: -Dsun.java2d.opengl=True -Dsun.java2d.d3d=true
Could not enable OpenGL pipeline for default config on screen 0
```

In this case, the system does not have a graphics card supporting OpenGL. The following is an example of a system with a graphics card supporting OpenGL:

```
OpenGL pipeline enabled for default config on screen 0
```

In the case of some graphics cards, OpenGL requires the option: `sun.java2d.opengl.fbobject=false`. See section *3.1.5.5 Diagnosing Rendering and Performance Issues* in the following document: *http://www.oracle.com/technetwork/java/javase/index-142560.html*.

This link is the current and comprehensive description of potential issues with OpenGL and Java 2D drawing package in conjunction with specific hardware/driver versions.

Related Topics

- http://www.opengl.org/
- https://docs.oracle.com/javase/8/docs/technotes/guides/2d/flags.html#opengl
- https://docs.oracle.com/javase/8/docs/technotes/guides/2d/new_features.html

6.10 Setting Proper Character Encoding Page on Microsoft Windows

Specify the encoding to interpret the characters dispalyed on the HTML page correctly.

Should you see strange characters in the text from AHF Scope console, for example:

```
278 waitclass_userio                     Ás/s
```

Verify the code page being active using the `chcp` command. For example, the page 437 (US default) unfortunately does not provide a proper display to the Greek "micro" character. Change the page to page 850 - Multilingual (Latin I) in order to see the "unicode character" Greek 'µ' showing up properly.

```
c:\rac\crf>chcp
Active code page: 437

c:\rac\crf>chcp 850
Active code page: 850

...

278  waitclass_userio                    µs/s
```

6.11 ahfscope

Use the `ahfscope` command to manage AHF Scope.

Syntax

```
ahfscope [flags] [parameters]
-f name
-i
-q value[,value]
    minutes
    clob
    psec
-C
-D item[,item]
    feed
    db
    input
    probes
    rootcause
    topology
    unit
```

Parameters

Table 6-8 ahfscope Command Parameters

Parameter	Description
`-f name`	Specify to read from a file. If you do not specify the file extension, then AHF Scope assumes `.mdb` as the file extension.
`-i`	Specify to run `ahfscope` in interactive mode (recommended). This option permits entering additional commands that are not available from the GUI. `ahfscope -i` When started with this option, a `cha>` command-line prompt appears in the operating system terminal. This can be used to enter terminal commands not available on the graphical panels. These commands are enumerated by entering `help` at the prompt.

Table 6-8 (Cont.) ahfscope Command Parameters

Parameter	Description
`-q` *`value`*`[,`*`value`*`]`	Specify to configure the connection and queries executed in the GIMR. Do not use this option with the `-f` option. Specify a comma-delimited list for optional parameters with no spaces. • **minutes**: Specify to query time period in minutes. **Default:** 60 minutes, **Minimum:** 2 minutes. • **clob**: Specify to use `sql.clob`. • ***psec***: Specify to postpone the query in seconds. **Default:** sampling period. **Minimum:** 1 second Option `-q` *`minutes`* sets the amount of data based upon time for the initial query. Since the sampling rate is 5 seconds, in the default data set with 60 minutes will contain 720 data points. Note that when longer times are selected via the `-q` option, a substantial time might be added to the startup process, especially when the monitored configuration has many nodes and databases. The maximum number of minutes in this option is determined by the width of the screen (number of pixels) divided by the number of samples per minute, which is 12 for the 5 second sample interval. For example, on a standard FHD monitor with 1920 horizontal pixels the number of minutes is limited to 160, or 2 hours and 40 minutes. Option `-q` *`pseconds`* adjusts the delay between the "time in the query" versus "time of the query". The time of the query must trail the time in the query. The smaller the delay, the closer the display is to the real-time. Default delay is one sampling period: 5 seconds. Regardless the delay, a sample always provide 5 seconds of data. For example `-qp10` would cause that a query for 5 seconds of data in the period of 10:20--10:25 would be invoked at 10:35 or later. Use this option when you observe that CHA is too slow and cannot commit transactions on time for AHF Scope. In such a case random gaps in data might be indicated. On a fast system even `-qp1` can be used without any adverse effects. Option `-q clob` directs AHF Scope to use alternative path of retrieving CLOB from the database. In some versions of Oracle Database a direct retrieving of CLOB from SQL query leads to fragmentation in the database. When user enters this option `-qc`, AHF Scope uses a 2-step process to obtain CLOB's, with an explicit disposal command. Elapsed time for every query will increase.
`-C`	Specify to extract the selected data from the `.mdb` file in JSON format. Use this option only with the `-f` option.
`-D` *`item`*`[,`*`item`*`]`	Specify to set the debug mode. Use this option to obtain a complete copy of the data received by AHF Scope stored in a file called `.mdb` file after Management Database. This file can be used as an argument with the `-f` *`file`* option. Specify a comma-delimited list for optional parameters with no spaces. • **feed**: Specify to view timings of all data queries. • **db**: Specify to activate `alter session set event 10046`. • **input**: Specify to copy input data (CLOB) to a log file. • **probes**: Specify to use internal probe names. • **rootcause**: Specify to inform about start and stop of any rootcause • **topology**: Specify to view changes in the set of entities ('topology'). • **unit**: Specify to view warnings about implicit settings for units of measure.

Note:

On a Microsoft Windows system, enclose all comma-separated arguments with double-quotes.
For example: `"-Dprobes,input"`, or shorter `"-Dp,i"`.

AHF Scope Modes

AHF Scope can operate in several modes:

- With a default connection to GIMR database
- Read in a text file with monitoring data (option `-f`).
- Parse text file with data and generate JSON object with information similar to query "diagnosis" (option `-C`).

Default connections initiate a *live session* and provide real-time monitoring. The connection to the GIMR database is established via JDBC using Oracle JDBC thin driver.

Using an MDB file as a parameter (Option `-f`) directs AHF Scope to analyze textual data extracted from a GIMR or data collected during a live session. This data is held in a `*.mdb` file. A `*.mdb` file can be generated from GIMR using command chactl export repository. An example of obtaining one hour worth of data:

```
host:/dir> chactl export repository -format mdb -start '2018-11-22 09:30:00'
-end '2018-11-22 10:30:00'
successfully dumped the CHA statistics to location "/hostname/trc/chad/
cha_dump_20181122_093000_20181122_103000.mdb"
```

Using option `-C` will start AHF Scope without the GUI front end. AHF Scope will only parse the `mdb` file and generate a JSON file, similar to the file generated by `chadiag`. This data can be used by other tools to indicate periods of time in which CHA diagnosed problems.

When AHF Scope is invoked without any command line options, AHF Scope uses JDBC to connect to the GIMR database and operates in a real-time mode as an active monitor. Connection credentials will be obtained from Oracle Wallet or from the manual input in the login console. After the connection is established, AHF Scope retrieves a data set with the most recent N-minutes of data. In a first invocation of AHF Scope the data set contains 60 minutes, unless option `-q` is used. In any subsequent invocation the number of minutes in the data set corresponds to the width of the window selected by the user.

7
Resolve Database Issues

- Resolve Noisy Neighbor Issues
  AHF Balance is a command-line utility that analyzes historical CPU consumption data and Database Resource Manager (DBRM) settings for the set of databases running in a cluster.
- Resolving Database and Database Instance Delays
  Blocker Resolver preserves the database performance by resolving delays and keeping the resources available.
- Resolving ORA-00600 Internal Error Codes
- Resolving ORA-04031: unable to allocate bytes of shared memory Error Codes
- Resolving ORA-07445 exception encountered: core dump
- Resolving ORA-04030 out of process memory when trying to allocate

7.1 Resolve Noisy Neighbor Issues

AHF Balance is a command-line utility that analyzes historical CPU consumption data and Database Resource Manager (DBRM) settings for the set of databases running in a cluster.

It assists in understanding the history of CPU-based noisy neighbor problems and recommends appropriate DBRM settings to minimize the risk of noisy neighbor problems.

AHF Balance queries CPU consumption from Oracle Enterprise Manager's repository database. Before you can generate AHF Balance reports, you need to configure a connection to the Oracle Enterprise Manager repository. For more information, see *ahf configuration*.

- CPU-Based Noisy Neighbor Prevention Strategies
- AHF Balance Reports
- Guided Resolution of Database Performance Problems Caused by Noisy Neighbors
  AHF Balance no-longer requires a GI Home and now works with any Oracle Home.
- Data Source

Related Topics

- ahf configuration
  Use the `ahf configuration` command to change AHF configuration.

7.1.1 CPU-Based Noisy Neighbor Prevention Strategies

- Partitioned – an MAA Best Practice
- Risk Management – supported by AHF Balance
- Terms Associated with AHF Balance

7.1.1.1 Partitioned – an MAA Best Practice

When a cluster is partitioned, each database instance has dedicated CPU capacity. CPU consumption by neighbors cannot interfere with a database instance. CPU resources (up to a configured limit - `CPU_COUNT`) are guaranteed to be available at all times. However, since CPU resources are dedicated to specific database instances, instances cannot take advantage of (borrow) CPU cycles that are not being used by other instances. Typically, when a cluster is partitioned, the degree of database consolidation is limited by the number of physical CPUs on each machine in the cluster, and the peak CPU consumption of each database hosted on the cluster.

A cluster is partitioned when the sum of the `CPU_COUNT` DBRM parameter values for all the database instances running on each machine in the cluster is less than or equal to the number of physical CPUs on the machine. For example, if the machines in a cluster each have 64 CPUs, and each machine is hosting 4 database instances, each with `CPU_COUNT` set to 16, the cluster is partitioned.

If the goal is to partition a cluster, then appropriate `CPU_COUNT` settings can be determined by analyzing historical CPU consumption data. AHF Balance supports this analysis.

7.1.1.2 Risk Management – supported by AHF Balance

When a cluster is hosting more databases than partitioning allows, it is said to be over-provisioned. When a cluster is over-provisioned, it is possible for high CPU consumption by one or more database instances to interfere with the CPU needs of another database instance: that database instance is suffering from noisy neighbors. It is also possible that databases sharing the cluster each need large amounts of CPU at different times, so that at no point in time is any database starved for CPU resources. Since the cluster is not partitioned, this is not guaranteed: the DBRM is not configured to prevent the situation where all the databases need large amounts of CPU simultaneously.

By analyzing historical CPU consumption, AHF Balance can recommend `CPU_COUNT` settings that minimize the amount of time where each database is exposed to high CPU consumption by its neighbors, if the historical record shows that partitioning is not possible.

7.1.1.3 Terms Associated with AHF Balance

- **Limit**: The maximum number of vCPUs a database instance may use simultaneously. The DBRM parameter `CPU_COUNT` implements a limit for the instance.
- **Guarantee**: The number of vCPUs a database instance is guaranteed to be able to use at any time. When a cluster is dedicated to running databases, the DBRM and the operating system cooperate to provide a guarantee.
  If the over-provisioning ratio `R=sum(CPU_COUNT)/physical vCPUs`, then the guarantee for a database instance is its `CPU_COUNT/R`.

  For example, if we had a 64 vCPU machine running 8 database instances, all with `CPU_COUNT` set to 16, then the oversubscription ratio R would be 2, that is, 8 * 16 /

64, and each individual database instance would have a guarantee of 8, that is, 16/2.

- **Not Exposed Hour**: An hour when no database instance's CPU use exceeds its CPU guarantee. When an instance is not exposed, it cannot experience CPU-based noisy neighbor problems regardless of the CPU consumption of the other instances running on the machine.
- **Exposed Hour**: An hour when one or more database instance's CPU use exceeds its CPU guarantee. When an instance is exposed, it may experience noisy neighbor problems depending on the CPU consumption of the other instances running on the machine.
- **Impacted Hour**: An exposed hour, when the host's CPU utilization exceeded 70% during the hour. When an instance is impacted, it is likely to be experiencing noisy neighbor problems because the total CPU consumption of the machine is high.

7.1.2 AHF Balance Reports

The number of entities (clusters, databases, and fleet) being considered in any given report will influence the time to generate the report

Cluster

The Cluster Report provides recommended `CPU_COUNT` settings for all the databases running in a cluster, based on the last month of CPU utilization history for those databases. Tables and graphs in the report show historical exposure and impact for the last month, and what the exposure and impact would have been if the recommended `CPU_COUNT` settings had been in place. This information is provided at both the host level and the database level.

Fleet

The Fleet Report summarizes the Cluster Reports for a fleet of clusters, showing which clusters would benefit most from the recommendations.

Database

The Database Report shows the details of the effects of cluster-wide adoption of recommended `CPU_COUNT` settings on all the instances of an individual database. This report is intended to facilitate a conversation between the owner of a cluster and the database administrator for an individual database. Note that it is not possible to recommend `CPU_COUNT` settings for an individual database. This report shows the effects on an individual database if all the databases running in the cluster adopt the recommendations.

7.1.3 Guided Resolution of Database Performance Problems Caused by Noisy Neighbors

AHF Balance no-longer requires a GI Home and now works with any Oracle Home.

Database CPU use is limited by the database `CPU_COUNT` parameter. When these limits add up to more than the number of CPUs on a machine, noisy-neighbor problems are possible.

AHF Balance analyzes database CPU configuration and historical CPU usage data from Enterprise Manager. The high-level results of this analysis are shown in the Oracle Orachk / Oracle Exachk MAA Score Card.

Further reports can be run to:

- Get an overview of possible noisy neighbors across the fleet.
- See detailed information about a specific database.
- Generate a corrective action plan.

To use AHF Balance:

- Configure AHF Balance to analyze historical CPU usage from Enterprise Manager's repository database:

  ```
  ahf configuration set --type impact --connect-string <EM-DATABASE-
  CONNECT-STRING> --user-name <USER-NAME>
  ```

  > **Note:**
  >
  > Ensure that the connect string does not contain any spaces.

- Run a fleet-wide analysis to create a detailed AHF Balance report to understand noisy neighbors and the improvements possible by changing `CPU_COUNT` settings:

  ```
  ahf analysis create --type impact --scope fleet --name <FLEET_NAME>
  ```

- Run a cluster-level analysis to get a detailed corrective action plan:

  ```
  ahf analysis create --type impact --scope cluster --name
  cluster_name
  ```

For more information, see Data Source.

7.1.4 Data Source

AHF Balance relies on CPU consumption data collected and stored by Enterprise Manager (EM). EM collects hourly CPU consumption for each database instance and each host it is managing. The default retention policy for hourly data collected by EM is 32 days.

Figure 7-1   Status Timeline

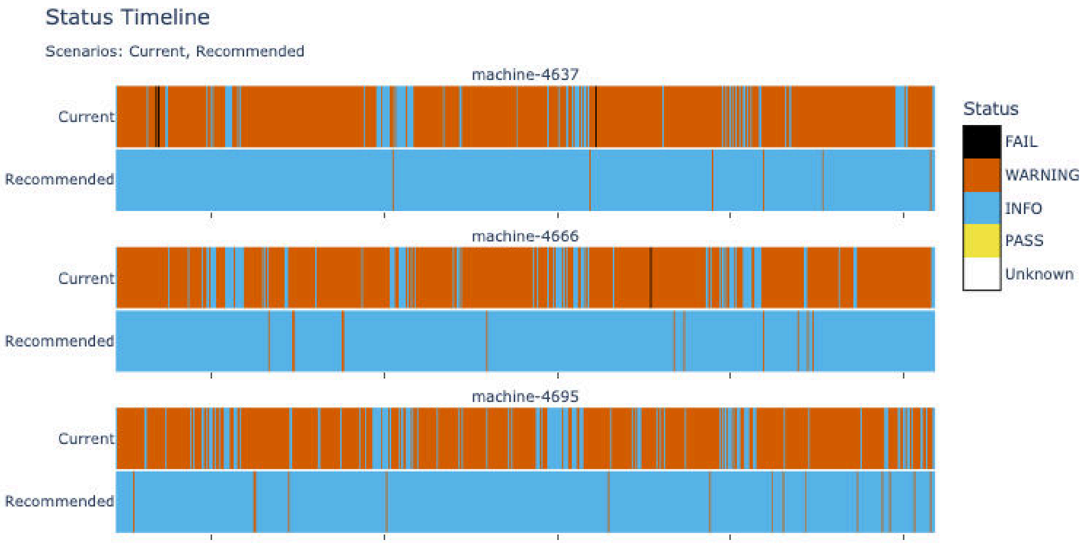
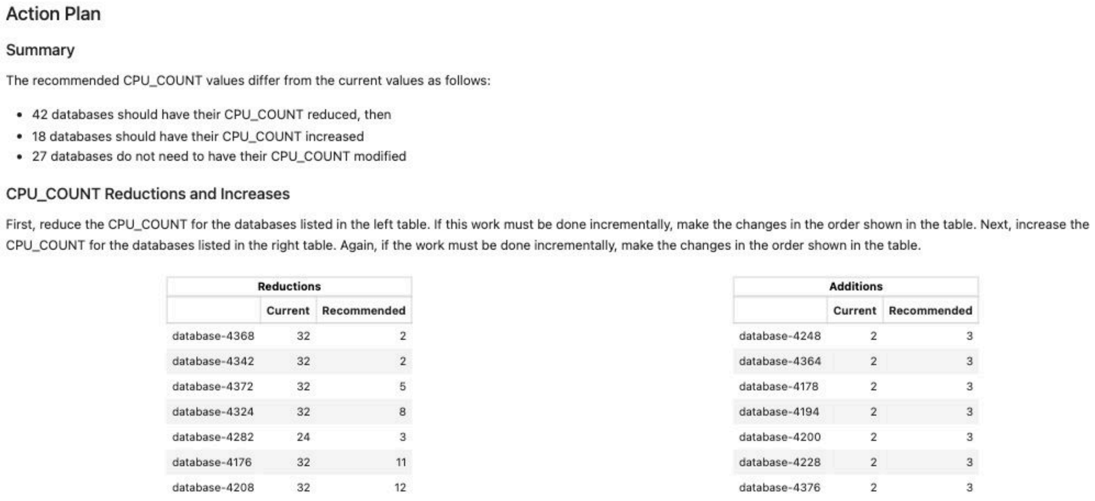


Figure 7-2   Action Plan



Action Plan

Summary

The recommended CPU_COUNT values differ from the current values as follows:

- 42 databases should have their CPU_COUNT reduced, then
- 18 databases should have their CPU_COUNT increased
- 27 databases do not need to have their CPU_COUNT modified

CPU_COUNT Reductions and Increases

First, reduce the CPU_COUNT for the databases listed in the left table. If this work must be done incrementally, make the changes in the order shown in the table. Next, increase the CPU_COUNT for the databases listed in the right table. Again, if the work must be done incrementally, make the changes in the order shown in the table.

Reductions		
	Current	Recommended
database-4368	32	2
database-4342	32	2
database-4372	32	5
database-4324	32	8
database-4282	24	3
database-4176	32	11
database-4208	32	12

Additions		
	Current	Recommended
database-4248	2	3
database-4364	2	3
database-4178	2	3
database-4194	2	3
database-4200	2	3
database-4228	2	3
database-4376	2	3

7.2 Resolving Database and Database Instance Delays

Blocker Resolver preserves the database performance by resolving delays and keeping the resources available.

- Blocker Resolver Architecture
  Blocker Resolver autonomously runs as a `DIA0` task within the database.
- Optional Configuration for Blocker Resolver
  You can adjust the sensitivity, and control the size and number of the log files used by Blocker Resolver.

- Blocker Resolver Diagnostics and Logging
  Blocker Resolver autonomously resolves delays and continuously logs the resolutions in the database alert logs and the diagnostics in the trace files.
- Using the Cluster Resource Activity Log to Monitor Cluster Resource Failures
  The cluster resource activity log provides precise and specific information about a resource failure, separate from diagnostic logs.

7.2.1 Blocker Resolver Architecture

Blocker Resolver autonomously runs as a `DIA0` task within the database.

Blocker Resolver works in the following three phases:

- **Detect:** In this phase, Blocker Resolver collects the data on all the nodes and detects the sessions that are waiting for the resources held by another session.
- **Analyze:** In this phase, Blocker Resolver analyzes the sessions detected in the **Detect** phase to determine if the sessions are part of a potential delay. If the sessions are suspected as delayed, Blocker Resolver then waits for a certain threshold time period to ensure that the sessions are delayed.
- **Verify:** In this phase, after the threshold time period is up, Blocker Resolver verifies that the sessions are delayed and selects a session that's causing the delay.

After selecting the session that's causing the delay, Blocker Resolver applies resolution methods on that session. If the chain of sessions or the delay resolves automatically, then Blocker Resolver does not apply delay resolution methods. However, if the delay does not resolve by itself, then Blocker Resolver resolves the delay by terminating the session that's causing the delay. If terminating the session fails, then Blocker Resolver terminates the process of the session. This entire process is autonomous and does not block resources for a long period and does not affect the performance.

For example, if a high rank session is included in the chain of delayed sessions, then Blocker Resolver expedites the termination of the session that's causing the delay. Termination of the session that's causing the delay prevents the high rank session from waiting too long and helps to maintain performance objective of the high rank session.

7.2.2 Optional Configuration for Blocker Resolver

You can adjust the sensitivity, and control the size and number of the log files used by Blocker Resolver.

> **Note:**
>
> The `DBMS_HANG_MANAGER` package is deprecated in Oracle Database 23c. Use `DBMS_BLOCKER_RESOLVER` instead.
> The `DBMS_HANG_MANAGER` package provides a method of changing some configuration parameters and constraints to address session issues. This package is being replaced with `DBMS_BLOCKER_RESOLVER`. `DBMS_HANG_MANAGER` can be removed in a future release.

Sensitivity

If Blocker Resolver detects a delay, then Blocker Resolver waits for a certain threshold time period to ensure that the sessions are delayed. Change threshold time period by using `DBMS_BLOCKER_RESOLVER` to set the `sensitivity` parameter to either `Normal` or `High`. If the `sensitivity` parameter is set to `Normal`, then Blocker Resolver waits for the default time period. However, if the sensitivity is set to `High`, then the time period is reduced by 50%.

By default, the `sensitivity` parameter is set to `Normal`. To set Blocker Resolver sensitivity, run the following commands in SQL*Plus as `SYS` user:

- To set the `sensitivity` parameter to `Normal`:

  ```
  exec dbms_blocker_resolver.set(dbms_blocker_resolver.sensitivity, 
  dbms_blocker_resolver.sensitivity_normal);
  ```

- To set the `sensitivity` parameter to `High`:

  ```
  exec dbms_blocker_resolver.set(dbms_blocker_resolver.sensitivity, 
  dbms_blocker_resolver.sensitivity_high);
  ```

Size of the Trace Log File

The Blocker Resolver logs detailed diagnostics of the delays in the trace files with `_base_` in the file name. Change the size of the trace files in bytes with the `base_file_size_limit` parameter. Run the following command in SQL*Plus, for example, to set the trace file size limit to 100 MB:

```
exec dbms_blocker_resolver.set(dbms_blocker_resolver.base_file_size_limit, 
104857600);
```

Number of Trace Log Files

The base Blocker Resolver trace files are part of a trace file set. Change the number of trace files in trace file set with the `base_file_set_count` parameter. Run the following command in SQL*Plus, for example, to set the number of trace files in trace file set to 6:

```
exec dbms_blocker_resolver.set(dbms_blocker_resolver.base_file_set_count,6);
```

By default, `base_file_set_count` parameter is set to 5.

7.2.3 Blocker Resolver Diagnostics and Logging

Blocker Resolver autonomously resolves delays and continuously logs the resolutions in the database alert logs and the diagnostics in the trace files.

Blocker Resolver logs the resolutions in the database alert logs as Automatic Diagnostic Repository (ADR) incidents with incident code `ORA-32701`.

You also get detailed diagnostics about the delay detection in the trace files. Trace files and alert logs have file names starting with *`database instance`*`_dia0_`.

- The trace files are stored in the `$ ADR_BASE/diag/rdbms/database name/database instance/incident/incdir_xxxxxx` directory
- The alert logs are stored in the `$ ADR_BASE/diag/rdbms/database name/database instance/trace` directory

Example 7-1 Blocker Resolver Trace File for a Local Instance

This example shows an example of the output you see for Blocker Resolver for the local database instance

```
Trace Log File .../oracle/log/diag/rdbms/hm1/hm11/incident/incdir_111/
hm11_dia0_11111_i111.trc
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit
Production
...
*** 2016-07-16T12:39:02.715475-07:00
HM: Hang Statistics - only statistics with non-zero values are listed

            current number of active sessions 3
              current number of hung sessions 1
  instance health (in terms of hung sessions) 66.67%
       number of cluster-wide active sessions 9
         number of cluster-wide hung sessions 5
   cluster health (in terms of hung sessions) 44.45%

*** 2016-07-16T12:39:02.715681-07:00
Resolvable Hangs in the System
                      Root       Chain Total               Hang
   Hang Hang          Inst Root  #hung #hung  Hang   Hang  Resolution
     ID Type Status   Num  Sess   Sess  Sess  Conf   Span  Action
  ----- ---- --------- ---- ----- ----- ----- ------ ------
-------------------
      1 HANG RSLNPEND    3    44     3     5   HIGH GLOBAL Terminate
Process
  Hang Resolution Reason: Although hangs of this root type are
typically
    self-resolving, the previously ignored hang was automatically
resolved.
```

Example 7-2 Error Message in the Alert Log Indicating a Delayed Session

This example shows an example of a Blocker Resolver alert log on the primary instance

```
2016-07-16T12:39:02.616573-07:00
Errors in file .../oracle/log/diag/rdbms/hm1/hm1/trace/
hm1_dia0_i1111.trc  (incident=1111):
ORA-32701: Possible hangs up to hang ID=1 detected
Incident details in: .../oracle/log/diag/rdbms/hm1/hm1/incident/
incdir_1111/hm1_dia0_11111_i1111.trc
2016-07-16T12:39:02.674061-07:00
DIA0 requesting termination of session sid:44 with serial # 23456
(ospid:34569) on instance 3
     due to a GLOBAL, HIGH confidence hang with ID=1.
     Hang Resolution Reason: Although hangs of this root type are
```

```
typically
    self-resolving, the previously ignored hang was automatically resolved.
DIA0: Examine the alert log on instance 3 for session termination status of
hang with ID=1.
```

Example 7-3 Error Message in the Alert Log Showing a Session Delay Resolved by Blocker Resolver

This example shows an example of a Blocker Resolver alert log on the local instance for resolved delays

```
2016-07-16T12:39:02.707822-07:00
Errors in file .../oracle/log/diag/rdbms/hm1/hm11/trace/hm11_dia0_11111.trc
(incident=169):
ORA-32701: Possible hangs up to hang ID=1 detected
Incident details in: .../oracle/log/diag/rdbms/hm1/hm11/incident/incdir_169/
hm11_dia0_30676_i169.trc
2016-07-16T12:39:05.086593-07:00
DIA0 terminating blocker (ospid: 30872 sid: 44 ser#: 23456) of hang with ID
= 1
     requested by master DIA0 process on instance 1
     Hang Resolution Reason: Although hangs of this root type are typically
    self-resolving, the previously ignored hang was automatically resolved.
     by terminating session sid:44 with serial # 23456 (ospid:34569)
...
DIA0 successfully terminated session sid:44 with serial # 23456
(ospid:34569) with status 0.
```

7.2.4 Using the Cluster Resource Activity Log to Monitor Cluster Resource Failures

The cluster resource activity log provides precise and specific information about a resource failure, separate from diagnostic logs.

If an Oracle Clusterware-managed resource fails, then Oracle Clusterware logs messages about the failure in the **cluster resource activity log**. Failures can occur as a result of a problem with a resource, a hosting node, or the network. The cluster resource activity log provides a unified view of the cause of resource failure.

Writes to the cluster resource activity log are tagged with an activity ID and any related data gets the same parent activity ID, and is nested under the parent data. For example, if Oracle Clusterware is running and you run the `crsctl stop clusterware -all` command, then all activities get activity IDs, and related activities are tagged with the same parent activity ID. On each node, the command creates sub-IDs under the parent IDs, and tags each of the respective activities with their corresponding activity ID. Further, each resource on the individual nodes creates sub-IDs based on the parent ID, creating a hierarchy of activity IDs. The hierarchy of activity IDs enables you to analyze the data to find specific activities.

For example, you may have many resources with complicated dependencies among each other, and with a database service. On Friday, you see that all of the resources are running on one node but when you return on Monday, every resource is on a different node, and you want to know why. Using the `crsctl query calog` command, you can query the cluster resource activity log for all activities involving those resources and the database service. The output provides a complete flow and you can query each sub-ID within the parent service failover ID, and see, specifically, what happened and why.

You can query any number of fields in the cluster resource activity log using filters. For example, you can query all the activities written by specific operating system users such as `root`. The output produced by the `crsctl query calog` command can be displayed in either a tabular format or in XML format.

The cluster resource activity log is an adjunct to current Oracle Clusterware logging and alert log messages.

> **Note:**
>
> Oracle Clusterware does not write messages that contain security-related information, such as log-in credentials, to the cluster activity log.

Use the following commands to manage and view the contents of the cluster resource activity log:

7.3 Resolving ORA-00600 Internal Error Codes

For more information and videos, see https://blogs.oracle.com/database/post/ora-00600.

Follow these step-by-step instructions for everything you need to do to resolve `ORA-00600`.

Understanding ORA-00600

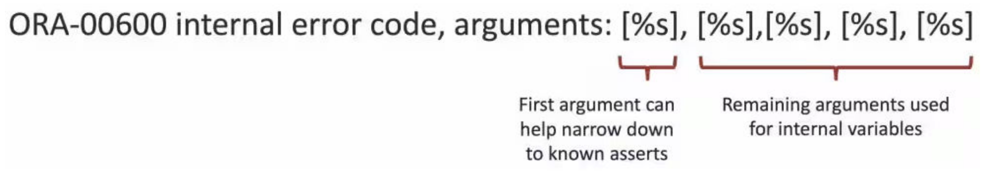
`ORA-00600` is a generic internal error. It indicates the process has encountered a low-level unexpected condition, which typically means you've encountered a bug.

The impact can vary from just being an annoyance that shows up in your logs once in a while, to something major that brings the database down.

When an `ORA-00600` error is logged it includes a list of arguments in square brackets.

- The first argument can be useful to narrow down to known asserts, as it indicates the function logging the error. However, beware if this is a commonly used function there may be multiple different possible causes.
- The remaining arguments are used to show various internal variables for debugging.

Figure 7-3 ORA-00600 Internal Error Code: Arguments

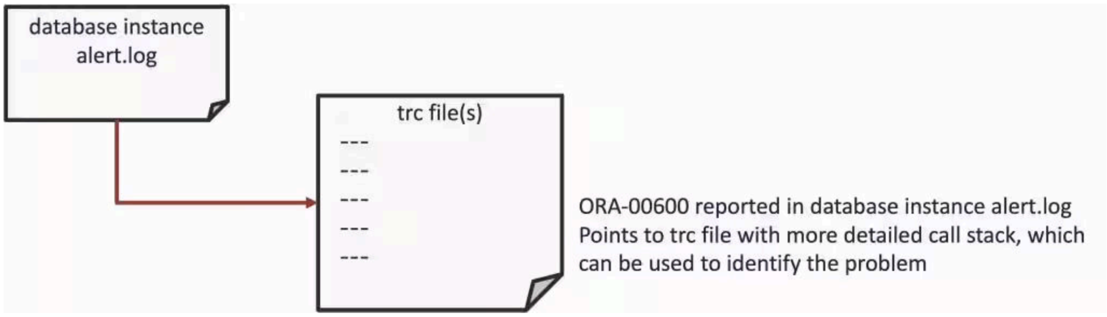


```
ORA-00600 internal error code, arguments: [%s], [%s],[%s], [%s], [%s]
```

First argument can help narrow down to known asserts
Remaining arguments used for internal variables

Whenever an ORA-00600 occurs, it will be logged in the database instance alert.log, which will also point to a trace file. This trace file will contain more detailed call stack information, which may be required to identify the error.

Figure 7-4 Database Instance Alert Log


database instance
alert.log
trc file(s)

ORA-00600 reported in database instance alert.log
Points to trc file with more detailed call stack, which
can be used to identify the problem

Depending on the cause of the ORA-00600, it may be necessary to look at other information to isolate the exact cause.

This can include understanding other configuration details such as:

- Database
- Operating System

ORA-00600 Error Troubleshooting Steps

The basic resolution steps for ORA-00600 are:

- Use AHF to generate an ORA-00600 Service Request Data Collection (SRDC)
- Use ORA-00600 Troubleshooting Tool to find recommendations
- Log a new SR using the diagnostic collection

Use AHF to generate an ORA-00600 Service Request Data Collection (SRDC)

In the first step, use AHF to generate an ORA-00600 diagnostic collection.

1. Log into the machine where the ORA-00600 occurred and as the Oracle user run the command:

```
tfactl diagcollect -srdc ORA-00600
```

   You’ll be prompted to enter the date and time of the ORA-00600 you’re interested in. If you’re not sure, just press return. You'll then be prompted to enter the database name.

   AHF will then check to find all the ORA-00600s that occurred on that database around that time you selected, or if you left the prompts blank it will just find recent ones.

   Next, it will show you a list of everything it found and ask you to choose the specific ORA-00600 you’re interested in.

   For example:

```
$ tfactl diagcollect -srdc ORA-00600
Enter the time of the ORA-00600 [YYYY-MM-DD HH24:MI:SS,<RETURN>=ALL] :
```

```
Enter the Database Name [Required for this SRDC] : cdb19

1. Feb/11/2024 10:15:56 PST: [cdb19] ORA-00600: internal error
code, arguments: [ktsircinfo_num1], [7], [1024], [1921], [], [],
[], [], [], [], [], []
2. Feb/11/2024 06:14:48 PST: [cdb19] ORA-00600: internal error
code, arguments: [ktsircinfo_num1], [7], [1024], [1921], [], [],
[], [], [], [], [], []

Please choose the event : 1-2 [1]
Selected value is : 1 ( Feb/11/2024 10:15:56 )

Components included in this collection: OS DATABASE NOCHMOS ASM
SOSREPORT
Preparing to execute support diagnostic scripts.

Collecting data for local node(s).

TFA is using system timezone for collection, All times shown in PST.
Scanning files from 2024-02-11 09:45:56 PST to 2024-02-11 10:45:56
PST

Collection Id : 20240212103041mymachine

Detailed Logging at : /run/oracle.ahf/data/repository/
srdc_ora600_collection_Mon_Feb_12_10_30_44_PST_2024_node_local/
diagcollect_20240212103041_mymachine.log

Waiting up to 120 seconds for collection to start
2024/02/12 10:30:49 PST : NOTE : Any file or directory name
containing the string .com will be renamed to replace .com with
dotcom
2024/02/12 10:30:49 PST : Collection Name :
tfa_srdc_ora600_Mon_Feb_12_10_30_43_PST_2024.zip
2024/02/12 10:30:50 PST : Scanning of files for Collection in
progress...
2024/02/12 10:30:50 PST : Collecting Additional Diagnostic
Information...
2024/02/12 10:31:10 PST : Getting list of files satisfying time
range [02/11/2024 09:45:56, 02/11/2024 10:45:56]
2024/02/12 10:31:22 PST : Collecting ADR incident files...
2024/02/12 10:31:31 PST : Executing TFA rdahcve with timeout of 600
seconds...
2024/02/12 10:31:32 PST : Executing IPS Incident Package
Collection(s)...
2024/02/12 10:31:34 PST : Generating IPS Pack for 2 incidents on
database cdb19
2024/02/12 10:31:48 PST : Executing SQL Script db_feature_usage.sql
on cdb19 with timeout of 600 seconds...
2024/02/12 10:31:48 PST : Executing Collection for ASM with timeout
of 1800 seconds...
2024/02/12 10:32:13 PST : Executing Collection for AFD with timeout
of 1860 seconds...
2024/02/12 10:32:16 PST : Executing Collection for OS with timeout
of 1920 seconds...
```

```
2024/02/12 10:32:22 PST : Executing Collection for SOSREPORT with timeout
of 1980 seconds...
2024/02/12 10:33:21 PST : Completed Collection of Additional Diagnostic
Information...
2024/02/12 10:33:24 PST : Completed Local Collection
2024/02/12 10:33:24 PST : Not Redacting this Collection on Exadata with
no redaction option passed ..
2024/02/12 10:33:24 PST : Not Redacting this Collection ...
2024/02/12 10:33:24 PST : Collection completed on host: mymachine
2024/02/12 10:33:24 PST : Completed collection of zip files.

.---------------------------------------.
|           Collection Summary          |
+-------------+-----------+------+------+
| Host        | Status    | Size | Time |
+-------------+-----------+------+------+
| mymachine   | Completed | 53MB | 155s |
'-------------+-----------+------+------'

Logs are being collected to: /run/oracle.ahf/data/repository/
srdc_ora600_collection_Mon_Feb_12_10_30_44_PST_2024_node_local
/run/oracle.ahf/data/repository/
srdc_ora600_collection_Mon_Feb_12_10_30_44_PST_2024_node_local/
mymachine.tfa_srdc_ora600_Mon_Feb_12_10_30_43_PST_2024.zip
```

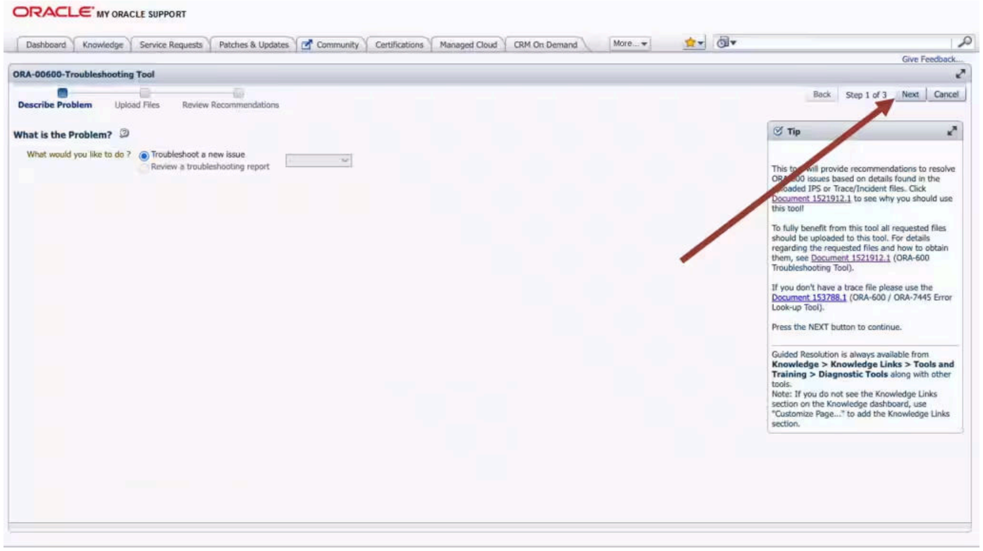
Once it’s finished AHF will package everything for you in a zip file for each machine, as you progress you'll only need the one from the node where the problem occurred.

Now, we can move onto step number two. Use the My Oracle Support ORA-00600 troubleshooting tool to find recommendations.

Use ORA-00600 Troubleshooting Tool to find recommendations

1. Log into My Oracle Support and search for `ORA-00600`, or alternatively go to My Oracle Support ORA-00600 troubleshooting tool to access it directly.
2. When you get to the troubleshooting tool click the **Next** button at the top right.

Figure 7-5   My Oracle Support ORA-00600 Troubleshooting Tool



What is the Problem?

What would you like to do ? ● Troubleshoot a new issue ○ Review a troubleshooting report

This tool will provide recommendations to resolve ORA-600 issues based on details found in the uploaded IPS or Trace/Incident files. Click Document 1521912.1 to see why you should use this tool!

To fully benefit from this tool all requested files should be uploaded to this tool. For details regarding the requested files and how to obtain them, see Document 1521912.1 (ORA-600 Troubleshooting Tool).

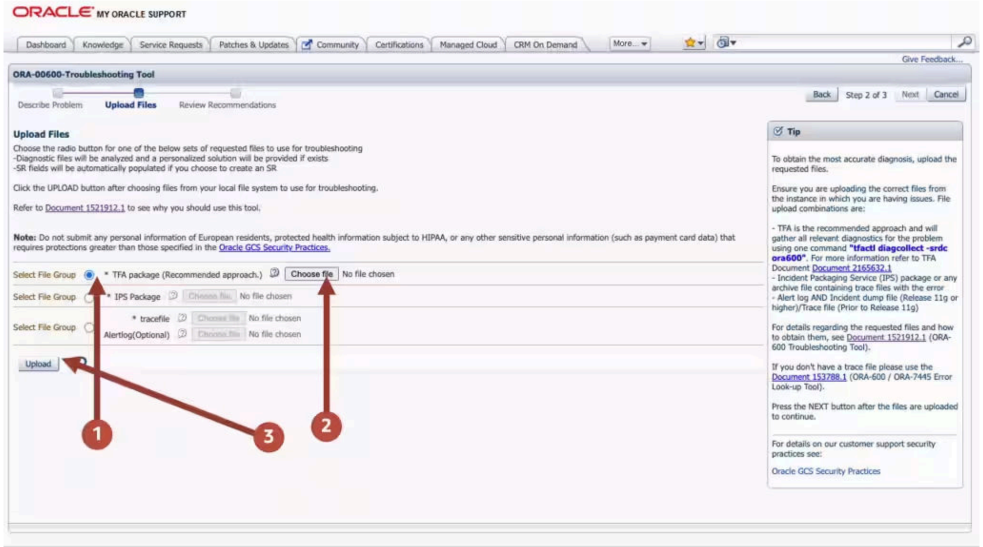
If you don't have a trace file please use the Document 153788.1 (ORA-600 / ORA-7445 Error Look-up Tool).

Press the NEXT button to continue.

Guided Resolution is always available from **Knowledge > Knowledge Links > Tools and Training > Diagnostic Tools** along with other tools.
Note: If you do not see the Knowledge Links section on the Knowledge dashboard, use "Customize Page..." to add the Knowledge Links section.

3. Select the first radio button to choose to upload a TFA package.
4. Then click the **Choose file** button, select the zip file AHF captured for you in step 1.
5. Then press the **Upload** button.

Figure 7-6   Choose Upload



Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521912.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) Choose file No file chosen

Select File Group ○ * IPS Package Choose file No file chosen

Select File Group ○ * tracefile Choose file No file chosen
Alertlog(Optional) Choose file No file chosen

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora600"**. For more information refer to TFA Document Document 2165632.1
- Incident Packaging Service (IPS) package or any archive file containing trace files with the error
- Alert log AND Incident dump file (Release 11g or higher)/Trace file (Prior to Release 11g)

For details regarding the requested files and how to obtain them, see Document 1521912.1 (ORA-600 Troubleshooting Tool).

If you don't have a trace file please use the Document 153788.1 (ORA-600 / ORA-7445 Error Look-up Tool).

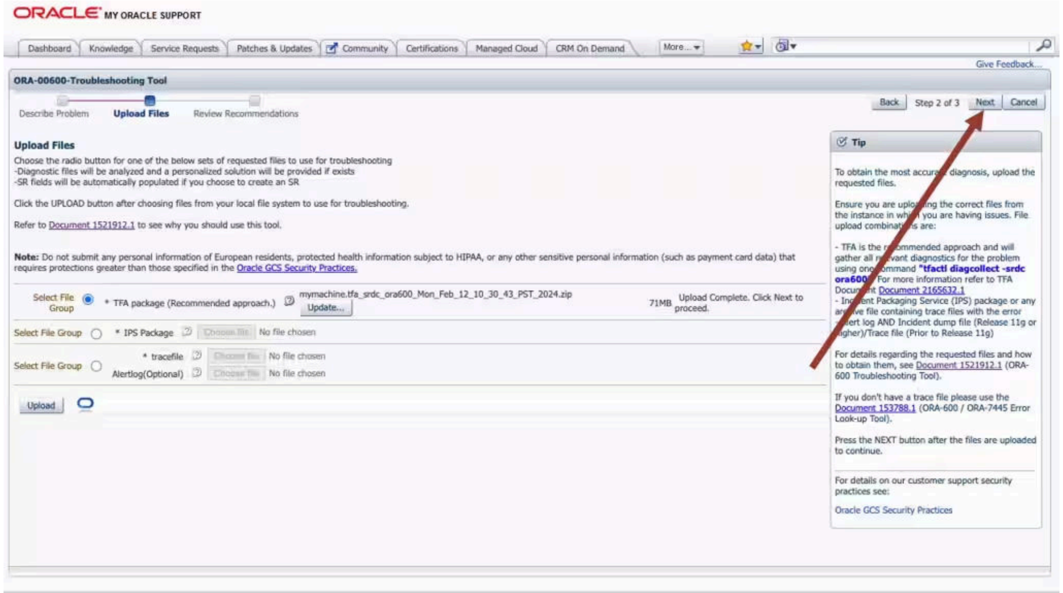
Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

Oracle GCS Security Practices

6. Once this is uploaded click the **Next** button at the top right again.

Figure 7-7   Choose Upload



Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521912.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) mymachine.tfa_srdc_ora600_Mon_Feb_12_10_30_43_PST_2024.zip 71MB Upload Complete. Click Next to proceed.

Select File Group ○ * IPS Package No file chosen

Select File Group ○ * tracefile No file chosen
Alertlog(Optional) No file chosen

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora600"** For more information refer to TFA Document Document 2165632.1
- Incident Packaging Service (IPS) package or any archive file containing trace files with the error
- Alert log AND Incident dump file (Release 11g or higher)/Trace file (Prior to Release 11g)

For details regarding the requested files and how to obtain them, see Document 1521912.1 (ORA-600 Troubleshooting Tool).

If you don't have a trace file please use the Document 153788.1 (ORA-600 / ORA-7445 Error Look-up Tool).

Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

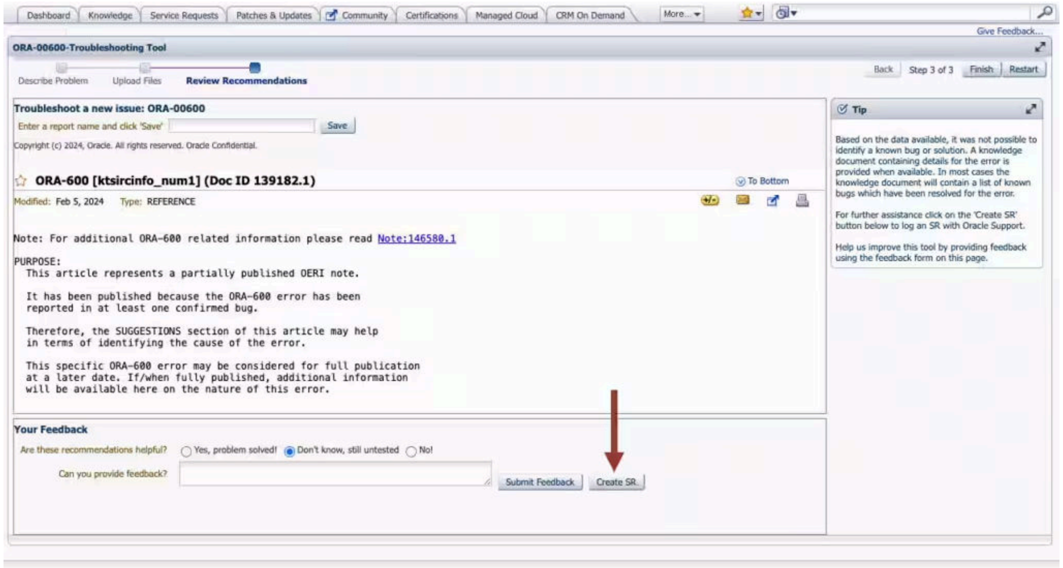
Oracle GCS Security Practices

The troubleshooting tool will then analyze the contents of the diagnostic collection and compare the log entries against its list of known problems. It will then recommend a My Oracle Support (MOS) Knowledge document for you that it thinks is the best fit. This knowledge document will either advise you what to do or show you several bugs where that `ORA-00600` has been reported. You can use this to look up which Database Release Update (RUs) fixed the bug. If you go through the MOS troubleshooting tool and can’t find a solution, or you just need some more help, then you can easily log an SR with Oracle Support.

Log a new SR using the diagnostic collection

1. Press the **Create SR** button at the bottom.

Figure 7-8   Create SR



Troubleshoot a new issue: ORA-00600

Enter a report name and click 'Save'

Copyright (c) 2024, Oracle. All rights reserved. Oracle Confidential.

ORA-600 [ktsircinfo_num1] (Doc ID 139182.1)

Modified: Feb 5, 2024 Type: REFERENCE

```
Note: For additional ORA-600 related information please read Note:146580.1

PURPOSE:
  This article represents a partially published OERI note.

  It has been published because the ORA-600 error has been
  reported in at least one confirmed bug.

  Therefore, the SUGGESTIONS section of this article may help
  in terms of identifying the cause of the error.

  This specific ORA-600 error may be considered for full publication
  at a later date. If/when fully published, additional information
  will be available here on the nature of this error.
```

Your Feedback

Are these recommendations helpful? ○ Yes, problem solved! ● Don't know, still untested ○ No!

Can you provide feedback?

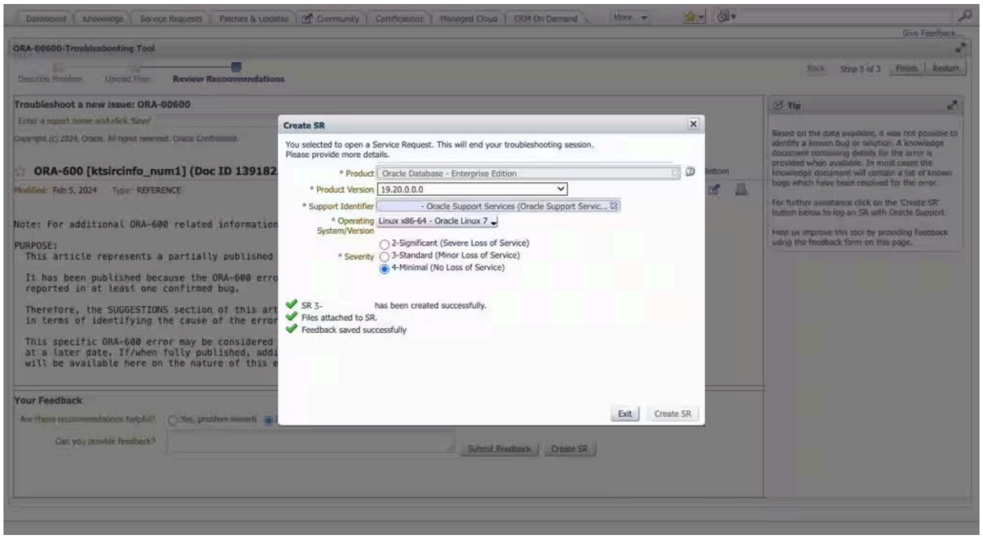
Based on the data available, it was not possible to identify a known bug or solution. A knowledge document containing details for the error is provided when available. In most cases the knowledge document will contain a list of known bugs which have been resolved for the error.

For further assistance click on the 'Create SR' button below to log an SR with Oracle Support.

Help us improve this tool by providing feedback using the feedback form on this page.

2. You'll then be prompted to clarify your:
    - Product
    - Product Version
    - Support Identifier
    - Operating System
    - SR severity
3. Then press the **Create SR** button.
   And, you'll get a new SR number.

Figure 7-9 New SR



Create SR

You selected to open a Service Request. This will end your troubleshooting session.
Please provide more details.

* Product: Oracle Database - Enterprise Edition

* Product Version: 19.20.0.0.0

* Support Identifier: - Oracle Support Services (Oracle Support Servic...

* Operating System/Version: Linux x86-64 - Oracle Linux 7

* Severity:
○ 2-Significant (Severe Loss of Service)
○ 3-Standard (Minor Loss of Service)
● 4-Minimal (No Loss of Service)

✓ SR 3- has been created successfully.
✓ Files attached to SR.
✓ Feedback saved successfully

The AHF diagnostic collection you uploaded originally will be routed onto your SR and Oracle Support will take over.

7.4 Resolving ORA-04031: unable to allocate bytes of shared memory Error Codes

For more information and videos, see https://blogs.oracle.com/database/post/ora-04031.

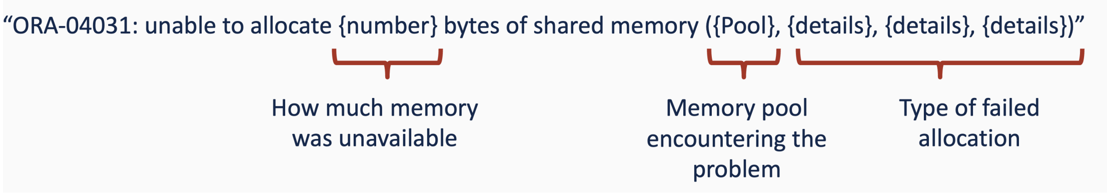
Follow these step-by-step instructions for everything you need to do to resolve `ORA-04031`.

Understanding ORA-04031

The `ORA-4031` error occurs because more shared memory was needed than was available.

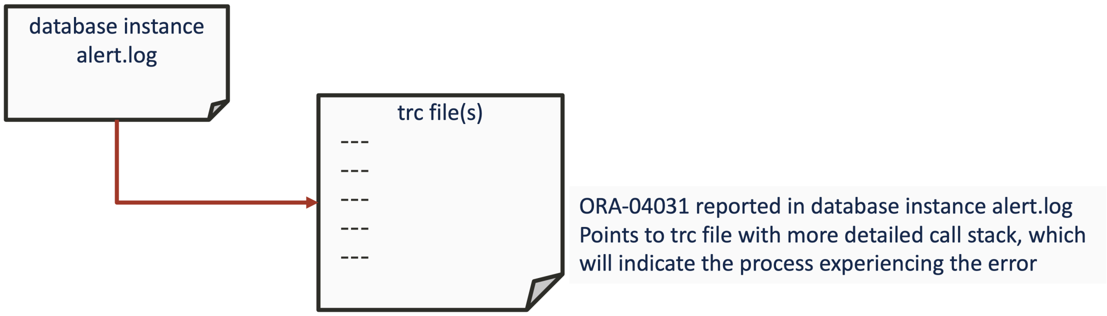
The error message will show how much memory was unavailable, the memory pool encountering the error and details about the type of failed allocation.

Figure 7-10 ORA-04031 Internal Error Code: Arguments


“ORA-04031: unable to allocate {number} bytes of shared memory ({Pool}, {details}, {details}, {details})”
How much memory was unavailable
Memory pool encountering the problem
Type of failed allocation

If the error is raised by a database process, then an entry will be made in the database alert log, which will point to a trace file showing the process experiencing the problem.

Figure 7-11 Database Instance Alert Log


database instance alert.log
trc file(s)

ORA-04031 reported in database instance alert.log
Points to trc file with more detailed call stack, which will indicate the process experiencing the error

However, if the error is encountered by a user process, then nothing will be found in the alert log.

Irrespective of where the error occurs, the process encountering the problem is often the victim of the situation and typically not the cause.

The underlying cause could be one of varying different things such as:

- Initialization parameters for memory not being set high enough.
- Problems with auto tuning.
- Fragmentation in application design.
- Bug or memory leak.

ORA-04031 Error Troubleshooting Steps

The basic resolution steps for `ORA-04031` are:

1. Use AHF to generate and `ORA-04031` Service Request Data Collection (SRDC)
2. Use `ORA-04031` Troubleshooting Tool to find recommendations
3. Log a new SR using the diagnostic collection

Use AHF to generate an ORA-04031 Service Request Data Collection (SRDC)

In the first step, use AHF to generate an `ORA-04031` diagnostic collection.

1. Log into the machine where the `ORA-04031` occurred and as the `Oracle` user run the command:

   ```
   tfactl diagcollect -srdc ORA-04031
   ```

   You’ll be prompted to enter the date and time of the `ORA-04031` you’re interested in, and then the database name

   For example:

   ```
   $ tfactl diagcollect -srdc ora4031
   Enter the time of the ORA-04031 [YYYY-MM-DD
   HH24:MI:SS,<RETURN>=ALL] : 2024-02-11 13:33:58
   Enter the Database Name [Required for this SRDC] : CDB12

   Components included in this collection: OS DATABASE CHMOS SOSREPORT

   Preparing to execute support diagnostic scripts.
    Executing DB Script srdc_db_ora4031.sql on CDB12 with timeout of
   300 seconds...

   Collecting data for all nodes

   TFA is using system timezone for collection, All times shown in PST.
   Scanning files from 2023-10-27 13:03:58 PDT to 2023-10-27 14:03:58
   PDT

   Collection Id : 20240212112211mymachine

   Detailed Logging at : /opt/oracle.ahf/data/repository/
   srdc_ora4031_collection_Mon_Feb_12_11_22_14_PST_2024_node_all/
   diagcollect_20240212112211_mymachine.log

   Waiting up to 120 seconds for collection to start
   2024/02/12 11:22:20 PST : NOTE : Any file or directory name
   containing the string .com will be renamed to replace .com with
   dotcom
   2024/02/12 11:22:20 PST : Collection Name :
   tfa_srdc_ora4031_Mon_Feb_12_11_22_13_PST_2024.zip
   2024/02/12 11:22:20 PST : Collecting diagnostics from hosts :
   [mymachine2, mymachine]
   2024/02/12 11:22:21 PST : Collecting Additional Diagnostic
   Information...
   2024/02/12 11:22:21 PST : Scanning of files for Collection in
   progress...
   2024/02/12 11:22:31 PST : Getting list of files satisfying time
   range [10/27/2023 13:03:58, 10/27/2023 14:03:58]
   2024/02/12 11:22:36 PST : Executing DB Script runawr on cdb12 with
   timeout of 3600 seconds...
   2024/02/12 11:22:42 PST : Executing TFA rdahcve with timeout of 600
   seconds...
   2024/02/12 11:22:51 PST : Collecting ADR incident files...
   2024/02/12 11:24:20 PST : Executing IPS Incident Package
   Collection(s)...
   2024/02/12 11:24:22 PST : Unexpected Error from ADR, please review
   ```

```
the <hostname>_collection.log for details and consult Oracle Support if 
necessary
2024/02/12 11:24:22 PST : Executing SQL Script db_feature_usage.sql on 
cdb12 with timeout of 600 seconds...
2024/02/12 11:24:22 PST : Executing Collection for OS with timeout of 
1800 seconds...
2024/02/12 11:24:29 PST : Executing Collection for SOSREPORT with timeout 
of 1860 seconds...
2024/02/12 11:25:29 PST : Completed Collection of Additional Diagnostic 
Information...
2024/02/12 11:25:32 PST : Completed Local Collection
2024/02/12 11:25:32 PST : Not Redacting this Collection on Exadata with 
no redaction option passed ..
2024/02/12 11:25:32 PST : Not Redacting this Collection ...
2024/02/12 11:25:32 PST : Remote Collection in Progress...
2024/02/12 11:26:13 PST : Collection completed on host: mymachine2
2024/02/12 11:26:13 PST : Collection completed on host: mymachine
2024/02/12 11:26:12 PST : Completed collection of zip files.

.----------------------------------------.
|           Collection Summary           |
+-------------+-----------+------+------+
| Host        | Status    | Size | Time |
+-------------+-----------+------+------+
| mymachine2  | Completed | 14MB | 182s |
| mymachine   | Completed | 27MB | 192s |
'-------------+-----------+------+------'

Logs are being collected to: /opt/oracle.ahf/data/repository/
srdc_ora4031_collection_Mon_Feb_12_11_22_14_PST_2024_node_all
/opt/oracle.ahf/data/repository/
srdc_ora4031_collection_Mon_Feb_12_11_22_14_PST_2024_node_all/
mymachine.tfa_srdc_ora4031_Mon_Feb_12_11_22_13_PST_2024.zip
/opt/oracle.ahf/data/repository/
srdc_ora4031_collection_Mon_Feb_12_11_22_14_PST_2024_node_all/
mymachine2.tfa_srdc_ora4031_Mon_Feb_12_11_22_13_PST_2024.zip
```

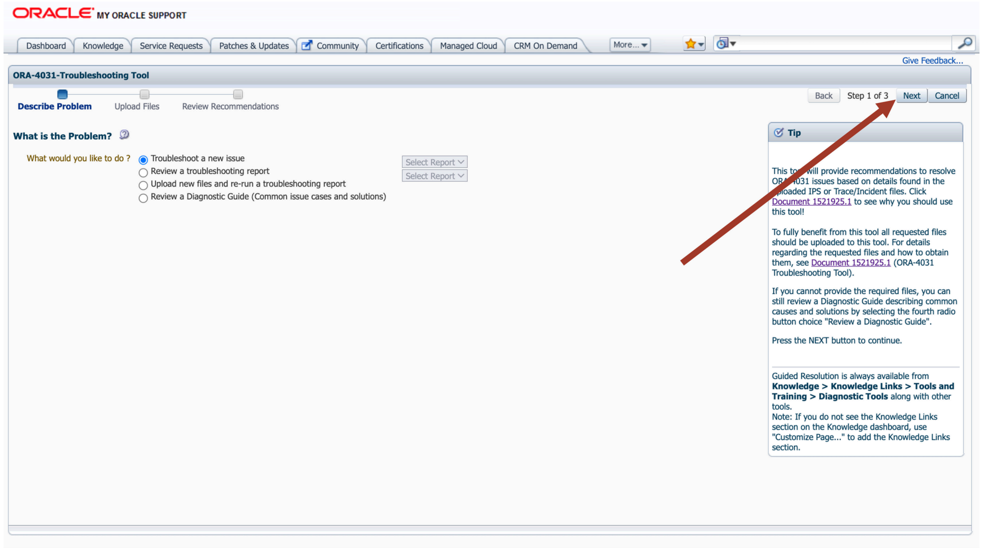
Once it’s finished AHF will package everything for you in a zip file for each machine, as you progress you'll only need the one from the node where the problem occurred.

Now we can move on to step number two. Use the My Oracle Support ORA-04031 troubleshooting tool to find recommendations.

Use ORA-04031 Troubleshooting Tool to find recommendations

1. Log into My Oracle Support and search for `ORA-04031`, or alternatively go to My Oracle Support ORA-04031 troubleshooting tool to access it directly.
2. When you get to the troubleshooting tool click the **Next** button at the top right.

Figure 7-12   My Oracle Support ORA-04031 Troubleshooting Tool



ORA-4031-Troubleshooting Tool

What is the Problem?

What would you like to do ?
● Troubleshoot a new issue
○ Review a troubleshooting report
○ Upload new files and re-run a troubleshooting report
○ Review a Diagnostic Guide (Common issue cases and solutions)

This tool will provide recommendations to resolve ORA-4031 issues based on details found in the uploaded IPS or Trace/Incident files. Click Document 1521925.1 to see why you should use this tool!

To fully benefit from this tool all requested files should be uploaded to this tool. For details regarding the requested files and how to obtain them, see Document 1521925.1 (ORA-4031 Troubleshooting Tool).

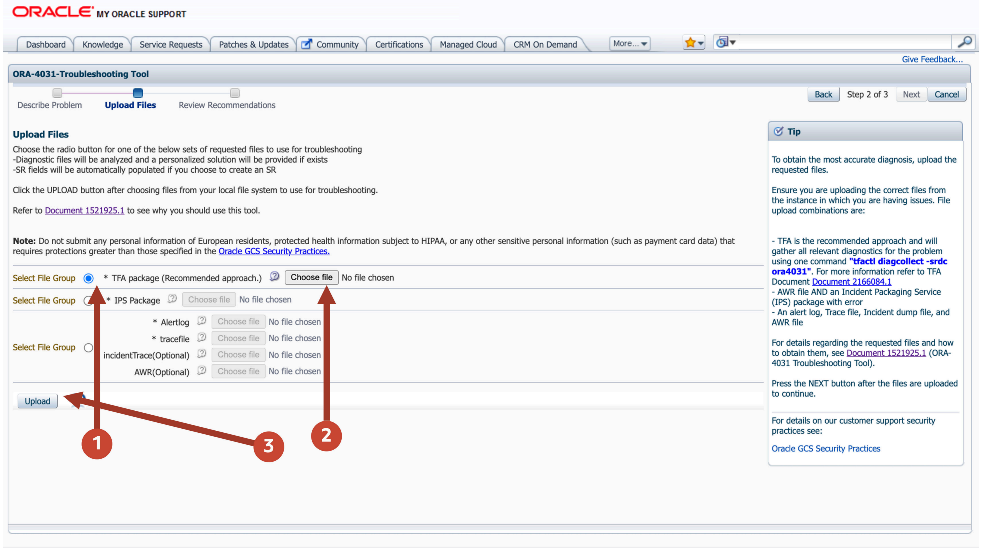
If you cannot provide the required files, you can still review a Diagnostic Guide describing common causes and solutions by selecting the fourth radio button choice "Review a Diagnostic Guide".

Press the NEXT button to continue.

Guided Resolution is always available from **Knowledge > Knowledge Links > Tools and Training > Diagnostic Tools** along with other tools.
Note: If you do not see the Knowledge Links section on the Knowledge dashboard, use "Customize Page..." to add the Knowledge Links section.

3. Select the first radio button to choose to upload a TFA package.
4. Click the **Choose file** button, select the zip from the failing node that AHF captured for you in step 1.
5. Then press the **Upload** button.

Figure 7-13   Choose Upload



ORA-4031-Troubleshooting Tool

Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521925.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) Choose file No file chosen
Select File Group ○ * IPS Package Choose file No file chosen
Select File Group ○ * Alertlog Choose file No file chosen
* tracefile Choose file No file chosen
incidentTrace(Optional) Choose file No file chosen
AWR(Optional) Choose file No file chosen

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora4031"**. For more information refer to TFA Document Document 2166084.1
- AWR file AND an Incident Packaging Service (IPS) package with error
- An alert log, Trace file, Incident dump file, and AWR file

For details regarding the requested files and how to obtain them, see Document 1521925.1 (ORA-4031 Troubleshooting Tool).

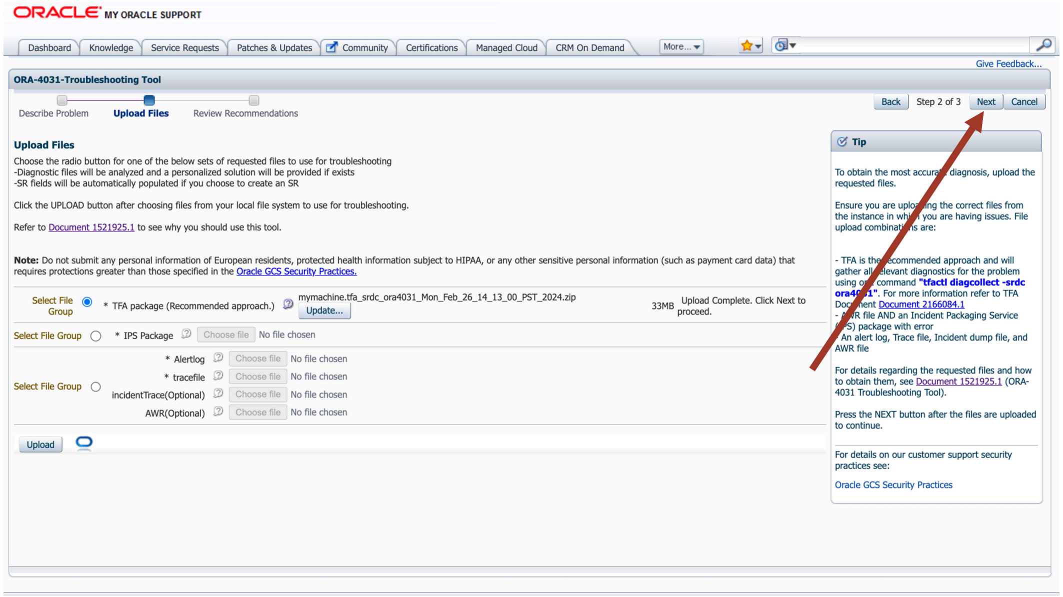
Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

Oracle GCS Security Practices

6. Once this is uploaded click the **Next** button at the top right again.

Figure 7-14 Choose Upload



ORA-4031-Troubleshooting Tool

Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521925.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) mymachine.tfa_srdc_ora4031_Mon_Feb_26_14_13_00_PST_2024.zip 33MB Upload Complete. Click Next to proceed.

Select File Group ○ * IPS Package No file chosen

Select File Group ○
* Alertlog No file chosen
* tracefile No file chosen
incidentTrace(Optional) No file chosen
AWR(Optional) No file chosen

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora4031"**. For more information refer to TFA Document Document 2166084.1
- AWR file AND an Incident Packaging Service (IPS) package with error
- An alert log, Trace file, Incident dump file, and AWR file

For details regarding the requested files and how to obtain them, see Document 1521925.1 (ORA-4031 Troubleshooting Tool).

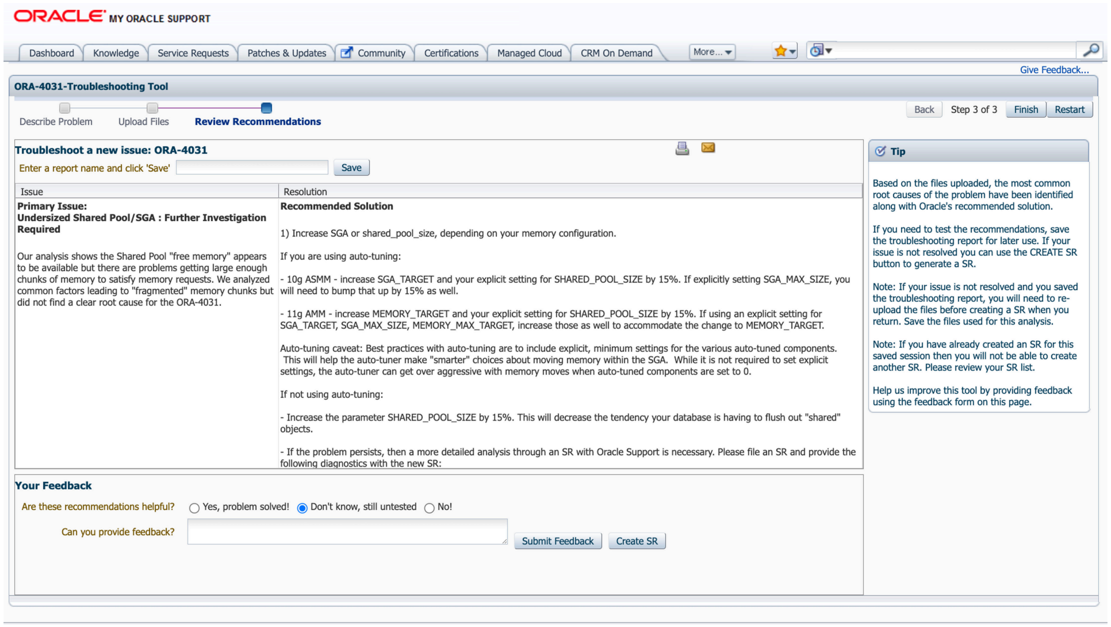
Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

Oracle GCS Security Practices

The troubleshooting tool will then analyze the contents of the diagnostic collection and compare the log entries against it’s list of known problems and recommend a solution.

Figure 7-15 Review Recommendations



ORA-4031-Troubleshooting Tool

Troubleshoot a new issue: ORA-4031

Enter a report name and click 'Save'

Issue	Resolution
Primary Issue: **Undersized Shared Pool/SGA : Further Investigation Required** Our analysis shows the Shared Pool "free memory" appears to be available but there are problems getting large enough chunks of memory to satisfy memory requests. We analyzed common factors leading to "fragmented" memory chunks but did not find a clear root cause for the ORA-4031.	**Recommended Solution** 1) Increase SGA or shared_pool_size, depending on your memory configuration. If you are using auto-tuning: - 10g ASMM - increase SGA_TARGET and your explicit setting for SHARED_POOL_SIZE by 15%. If explicitly setting SGA_MAX_SIZE, you will need to bump that up by 15% as well. - 11g AMM - increase MEMORY_TARGET and your explicit setting for SHARED_POOL_SIZE by 15%. If using an explicit setting for SGA_TARGET, SGA_MAX_SIZE, MEMORY_MAX_TARGET, increase those as well to accommodate the change to MEMORY_TARGET. Auto-tuning caveat: Best practices with auto-tuning are to include explicit, minimum settings for the various auto-tuned components. This will help the auto-tuner make "smarter" choices about moving memory within the SGA. While it is not required to set explicit settings, the auto-tuner can get over aggressive with memory moves when auto-tuned components are set to 0. If not using auto-tuning: - Increase the parameter SHARED_POOL_SIZE by 15%. This will decrease the tendency your database is having to flush out "shared" objects. - If the problem persists, then a more detailed analysis through an SR with Oracle Support is necessary. Please file an SR and provide the following diagnostics with the new SR:

Your Feedback

Are these recommendations helpful? ○ Yes, problem solved! ● Don't know, still untested ○ No!

Can you provide feedback?

Based on the files uploaded, the most common root causes of the problem have been identified along with Oracle's recommended solution.

If you need to test the recommendations, save the troubleshooting report for later use. If your issue is not resolved you can use the CREATE SR button to generate a SR.

Note: If your issue is not resolved and you saved the troubleshooting report, you will need to re-upload the files before creating a SR when you return. Save the files used for this analysis.

Note: If you have already created an SR for this saved session then you will not be able to create another SR. Please review your SR list.

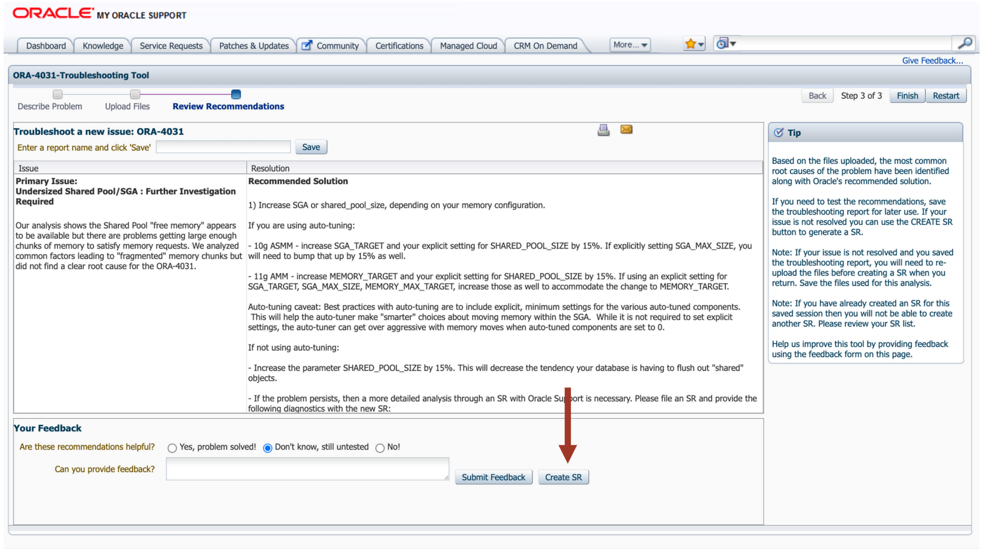
Help us improve this tool by providing feedback using the feedback form on this page.

If you go through the MOS troubleshooting tool and can’t find a solution, or you just need some more help, then you can easily log an SR with Oracle Support.

Log a new SR using the diagnostic collection

1. Press the **Create SR** button at the bottom.

Figure 7-16   Create SR



ORA-4031-Troubleshooting Tool

Troubleshoot a new issue: ORA-4031

Enter a report name and click 'Save'

Issue	Resolution
Primary Issue: **Undersized Shared Pool/SGA : Further Investigation Required** Our analysis shows the Shared Pool "free memory" appears to be available but there are problems getting large enough chunks of memory to satisfy memory requests. We analyzed common factors leading to "fragmented" memory chunks but did not find a clear root cause for the ORA-4031.	**Recommended Solution** 1) Increase SGA or shared_pool_size, depending on your memory configuration. If you are using auto-tuning: - 10g ASMM - increase SGA_TARGET and your explicit setting for SHARED_POOL_SIZE by 15%. If explicitly setting SGA_MAX_SIZE, you will need to bump that up by 15% as well. - 11g AMM - increase MEMORY_TARGET and your explicit setting for SHARED_POOL_SIZE by 15%. If using an explicit setting for SGA_TARGET, SGA_MAX_SIZE, MEMORY_MAX_TARGET, increase those as well to accommodate the change to MEMORY_TARGET. Auto-tuning caveat: Best practices with auto-tuning are to include explicit, minimum settings for the various auto-tuned components. This will help the auto-tuner make "smarter" choices about moving memory within the SGA. While it is not required to set explicit settings, the auto-tuner can get over aggressive with memory moves when auto-tuned components are set to 0. If not using auto-tuning: - Increase the parameter SHARED_POOL_SIZE by 15%. This will decrease the tendency your database is having to flush out "shared" objects. - If the problem persists, then a more detailed analysis through an SR with Oracle Support is necessary. Please file an SR and provide the following diagnostics with the new SR:

Tip

Based on the files uploaded, the most common root causes of the problem have been identified along with Oracle's recommended solution.

If you need to test the recommendations, save the troubleshooting report for later use. If your issue is not resolved you can use the CREATE SR button to generate a SR.

Note: If your issue is not resolved and you saved the troubleshooting report, you will need to re-upload the files before creating a SR when you return. Save the files used for this analysis.

Note: If you have already created an SR for this saved session then you will not be able to create another SR. Please review your SR list.

Help us improve this tool by providing feedback using the feedback form on this page.

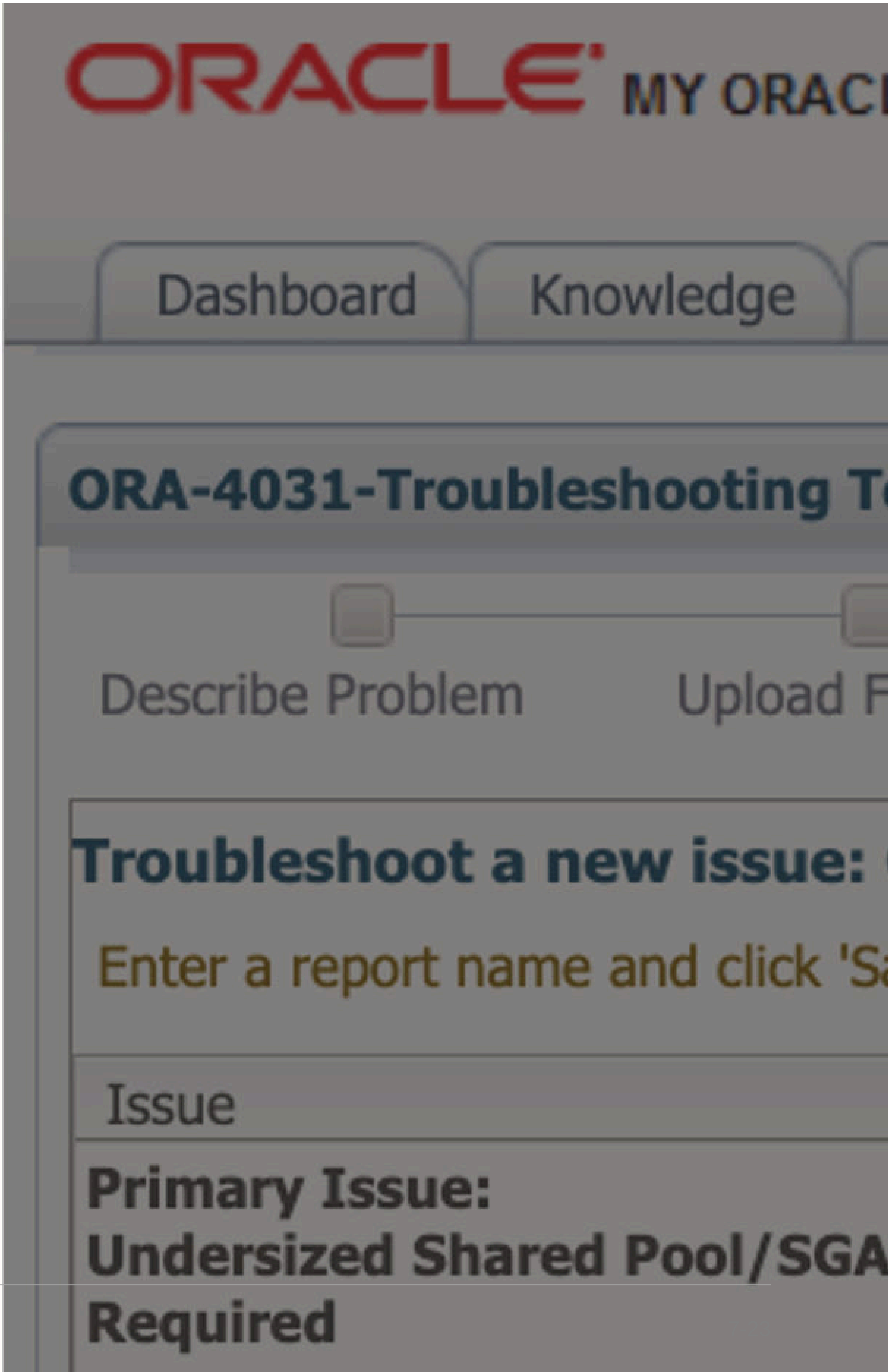
Your Feedback

Are these recommendations helpful? ○ Yes, problem solved! ● Don't know, still untested ○ No!

Can you provide feedback?

2. You'll then be prompted to clarify your:
   - Product
   - Product Version
   - Support Identifier
   - Operating System
   - SR severity
3. Then press the **Create SR** button.
   And, you'll get a new SR number.

Figure 7-17   New SR



ORA-4031-Troubleshooting T

Troubleshoot a new issue: (

Enter a report name and click 'Sa

Issue

Primary Issue:
Undersized Shared Pool/SGA
Required

The AHF diagnostic collection you uploaded originally will be attached your SR and Oracle Support will take over.

7.5 Resolving ORA-07445 exception encountered: core dump

For more information and videos, see https://blogs.oracle.com/database/post/ora-07445.

Follow these step-by-step instructions for everything you need to do to resolve `ORA-07445`.

Understanding ORA-07445

The `ORA-07445 exception encountered: core dump` occurs because an operating system exception occurring which should result in the creation of a core file.

The error message will show the Oracle function that was executing when it encountered the error and other variables such as memory addresses.

Figure 7-18 ORA-07445 Internal Error Code: Arguments

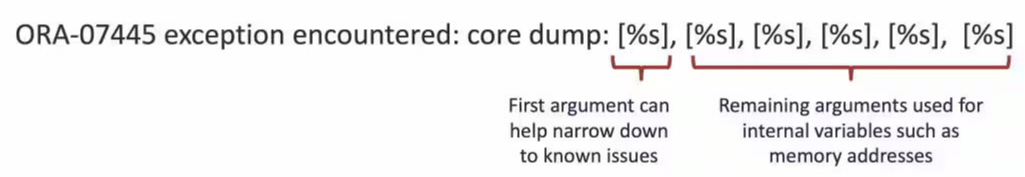
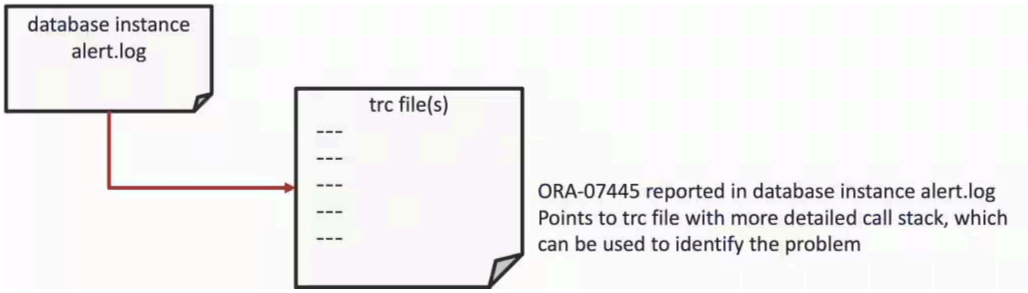

ORA-07445 exception encountered: core dump: [%s], [%s], [%s], [%s], [%s], [%s]
First argument can help narrow down to known issues
Remaining arguments used for internal variables such as memory addresses

Figure 7-19 Database Instance Alert Log


database instance alert.log
trc file(s)

ORA-07445 reported in database instance alert.log
Points to trc file with more detailed call stack, which can be used to identify the problem

This error is usually caused by either:

- Bad data
- Severe misconfiguration
- Bug

The impact can vary from just being an annoyance that shows up in your logs once in a while, to something major that brings the database down.

ORA-07445 Error Troubleshooting Steps

The basic resolution steps for `ORA-07445` are:

- Use AHF to generate an `ORA-07445` Service Request Data Collection (SRDC)
- Use `ORA-07445` Troubleshooting Tool to find recommendations
- Log a new SR using the diagnostic collection

Use AHF to generate an ORA-07445 Service Request Data Collection (SRDC)

In the first step, use AHF to generate an `ORA-07445` diagnostic collection.

1. Log into the machine where the `ORA-07445` occurred and as the `Oracle` user run the command:

   ```
   tfactl diagcollect -srdc ORA-07445
   ```

   You’ll be prompted to enter the date and time of the `ORA-07445` you’re interested in. If you’re not sure, just press return. You'll then be prompted to enter the database name.

   For example:

   ```
   $ tfactl diagcollect -srdc ORA-07445
   Enter the time of the ORA-07445 [YYYY-MM-DD HH24:MI:SS,<RETURN>=ALL] :
   2024-03-11 10:11:22
   Enter the Database Name [Required for this SRDC] : cdb19

   Components included in this collection: OS DATABASE NOCHMOS ASM SOSREPORT

   Preparing to execute support diagnostic scripts.

   Collecting data for local node(s).

   TFA is using system timezone for collection, All times shown in PDT.
   Scanning files from 2024-03-11 09:41:22 PDT to 2024-03-11 10:14:32 PDT

   Collection Id : 20240311101444mymachine1

   Detailed Logging at : /u01/app/grid21/oracle.ahf/data/repository/
   srdc_ora7445_collection_Mon_Mar_11_10_14_47_PDT_2024_node_local/
   diagcollect_20240311101444_mymachine1.log

   Waiting up to 120 seconds for collection to start
   2024/03/11 10:14:52 PDT : NOTE : Any file or directory name containing
   the string .com will be renamed to replace .com with dotcom
   2024/03/11 10:14:52 PDT : Collection Name :
   tfa_srdc_ora7445_Mon_Mar_11_10_14_46_PDT_2024.zip
   2024/03/11 10:14:53 PDT : Collecting Additional Diagnostic Information...
   2024/03/11 10:14:53 PDT : Getting list of files satisfying time range
   [03/11/2024 09:41:22, 03/11/2024 10:14:32]
   2024/03/11 10:15:34 PDT : Executing TFA rdahcve with timeout of 600
   seconds...
   2024/03/11 10:15:36 PDT : Executing IPS Incident Package Collection(s)...
   2024/03/11 10:15:38 PDT : Generating IPS Pack for 1 incidents on database
   ```

```
cdb19
2024/03/11 10:15:46 PDT : Executing SQL Script db_feature_usage.sql
on cdb19 with timeout of 600 seconds...
2024/03/11 10:15:46 PDT : Executing Collection for ASM with timeout
of 1800 seconds...
2024/03/11 10:15:56 PDT : Collecting ADR incident files...
2024/03/11 10:16:07 PDT : Executing Collection for AFD with timeout
of 1860 seconds...
2024/03/11 10:16:11 PDT : Executing Collection for OS with timeout
of 1920 seconds...
2024/03/11 10:16:15 PDT : Executing Collection for SOSREPORT with
timeout of 1980 seconds...
2024/03/11 10:17:54 PDT : Completed Collection of Additional
Diagnostic Information...
2024/03/11 10:17:58 PDT : Completed Local Collection
2024/03/11 10:17:58 PDT : Not Redacting this Collection on Exadata
with no redaction option passed ..
2024/03/11 10:17:58 PDT : Not Redacting this Collection ...
2024/03/11 10:17:58 PDT : Collection completed on host: mymachine1
2024/03/11 10:17:58 PDT : Completed collection of zip files.

.----------------------------------------.
|           Collection Summary           |
+-------------+-----------+------+------+
| Host        | Status    | Size | Time |
+-------------+-----------+------+------+
| mymachine1  | Completed | 44MB | 185s |
'-------------+-----------+------+------'

Logs are being collected to: /u01/app/grid21/oracle.ahf/data/
repository/
srdc_ora7445_collection_Mon_Mar_11_10_14_47_PDT_2024_node_local
/u01/app/grid21/oracle.ahf/data/repository/
srdc_ora7445_collection_Mon_Mar_11_10_14_47_PDT_2024_node_local/
mymachine1.tfa_srdc_ora7445_Mon_Mar_11_10_14_46_PDT_2024.zip
```

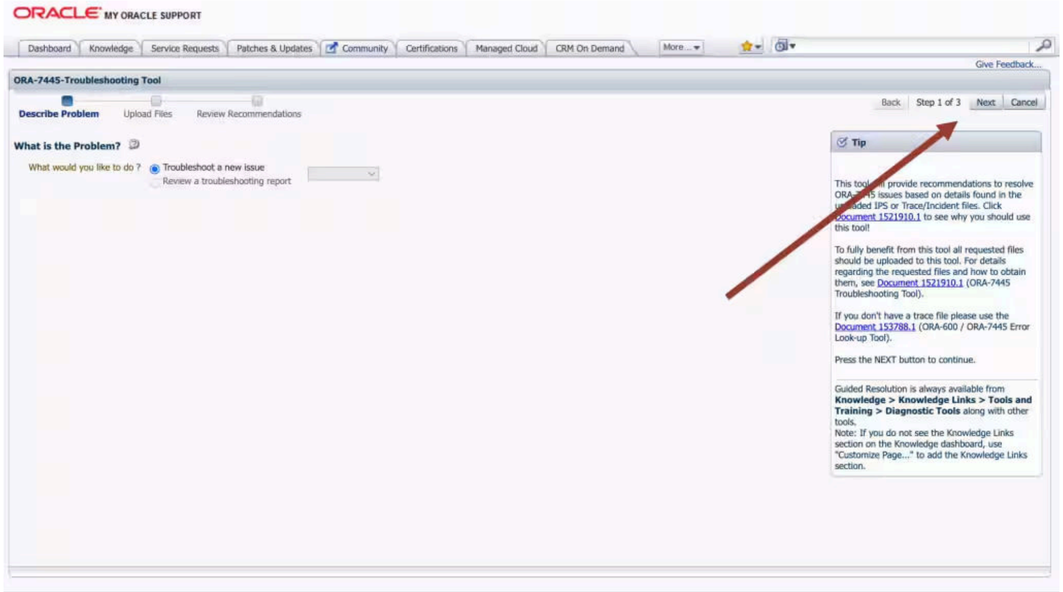
Once it’s finished AHF will package everything for you in a zip file for each machine, as you progress you'll only need the one from the node where the problem occurred.

Now, we can move onto step number two. Use the My Oracle Support ORA-07445 troubleshooting tool to find recommendations.

Use ORA-07445 Troubleshooting Tool to find recommendations

1. Log into My Oracle Support and search for `ORA-07445`, or alternatively go to My Oracle Support ORA-07445 troubleshooting tool to access it directly.
2. When you get to the troubleshooting tool click the **Next** button at the top right.

Figure 7-20   My Oracle Support ORA-07445 Troubleshooting Tool



What is the Problem?

What would you like to do ? ● Troubleshoot a new issue ○ Review a troubleshooting report

This tool will provide recommendations to resolve ORA-7445 issues based on details found in the uploaded IPS or Trace/Incident files. Click Document 1521910.1 to see why you should use this tool!

To fully benefit from this tool all requested files should be uploaded to this tool. For details regarding the requested files and how to obtain them, see Document 1521910.1 (ORA-7445 Troubleshooting Tool).

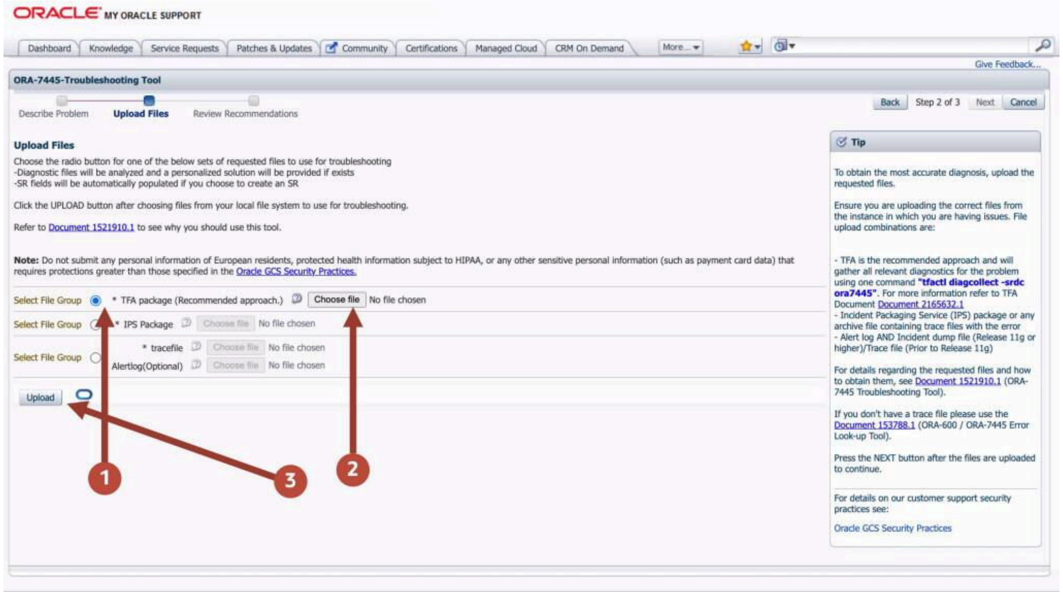
If you don't have a trace file please use the Document 153788.1 (ORA-600 / ORA-7445 Error Look-up Tool).

Press the NEXT button to continue.

Guided Resolution is always available from **Knowledge > Knowledge Links > Tools and Training > Diagnostic Tools** along with other tools.
Note: If you do not see the Knowledge Links section on the Knowledge dashboard, use "Customize Page..." to add the Knowledge Links section.

3. Select the first radio button to choose to upload a TFA package.
4. Then click the **Choose file** button, select the zip file AHF captured for you in step 1.
5. Then press the **Upload** button.

Figure 7-21   Choose Upload



Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521910.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) Choose file No file chosen
Select File Group ○ * IPS Package Choose file No file chosen
Select File Group ○ * tracefile Choose file No file chosen
Alertlog(Optional) Choose file No file chosen

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora7445"**. For more information refer to TFA Document Document 2165632.1
- Incident Packaging Service (IPS) package or any archive file containing trace files with the error
- Alert log AND Incident dump file (Release 11g or higher)/Trace file (Prior to Release 11g)

For details regarding the requested files and how to obtain them, see Document 1521910.1 (ORA-7445 Troubleshooting Tool).

If you don't have a trace file please use the Document 153788.1 (ORA-600 / ORA-7445 Error Look-up Tool).

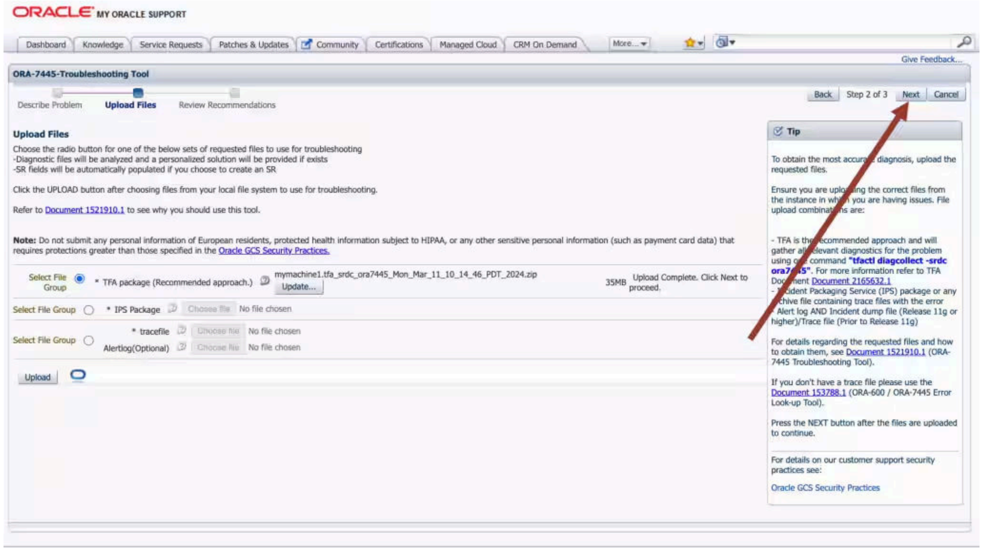
Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

Oracle GCS Security Practices

6. Once this is uploaded click the **Next** button at the top right again.

Figure 7-22   Choose Upload



ORA-7445-Troubleshooting Tool

Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521910.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) mymachine1.tfa_srdc_ora7445_Mon_Mar_11_10_14_46_PDT_2024.zip 35MB Upload Complete. Click Next to proceed.

Select File Group ○ * IPS Package No file chosen

Select File Group ○ * tracefile No file chosen
Alertlog(Optional) No file chosen

Tip

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora7445"**. For more information refer to TFA Document Document 2165632.1
- Incident Packaging Service (IPS) package or any archive file containing trace files with the error
- Alert log AND Incident dump file (Release 11g or higher)/Trace file (Prior to Release 11g)

For details regarding the requested files and how to obtain them, see Document 1521910.1 (ORA-7445 Troubleshooting Tool).

If you don't have a trace file please use the Document 153788.1 (ORA-600 / ORA-7445 Error Look-up Tool).

Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

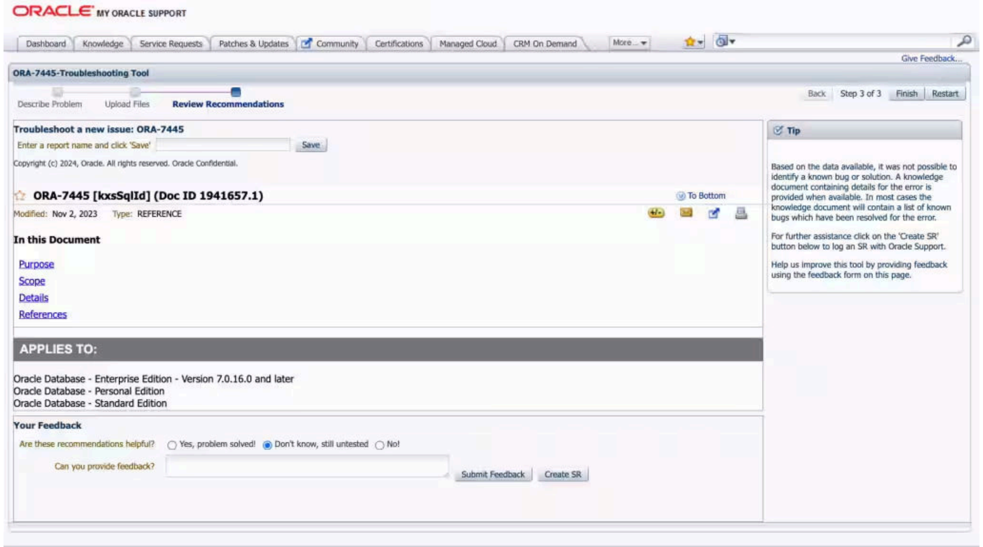
Oracle GCS Security Practices

The troubleshooting tool will then analyze the contents of the diagnostic collection and compare the log entries against its list of known problems. It will then recommend a My Oracle Support (MOS) Knowledge document for you that it thinks is the best fit. This knowledge document will either advise you what to do or show you several bugs where that `ORA-07445` has been reported. You can use this to look up which Database Release Update (RUs) fixed the bug. If you go through the MOS troubleshooting tool and can't find a solution, or you just need some more help, then you can easily log an SR with Oracle Support.

Log a new SR using the diagnostic collection

1. Press the **Create SR** button at the bottom.

Figure 7-23   Create SR



ORA-7445-Troubleshooting Tool

Troubleshoot a new issue: ORA-7445

Enter a report name and click 'Save'

Copyright (c) 2024, Oracle. All rights reserved. Oracle Confidential.

ORA-7445 [kxsSqlId] (Doc ID 1941657.1)

Modified: Nov 2, 2023   Type: REFERENCE

In this Document

Purpose
Scope
Details
References

APPLIES TO:

Oracle Database - Enterprise Edition - Version 7.0.16.0 and later
Oracle Database - Personal Edition
Oracle Database - Standard Edition

Your Feedback

Are these recommendations helpful? ○ Yes, problem solved! ● Don't know, still untested ○ No!

Can you provide feedback?

Tip

Based on the data available, it was not possible to identify a known bug or solution. A knowledge document containing details for the error is provided when available. In most cases the knowledge document will contain a list of known bugs which have been resolved for the error.

For further assistance click on the 'Create SR' button below to log an SR with Oracle Support.

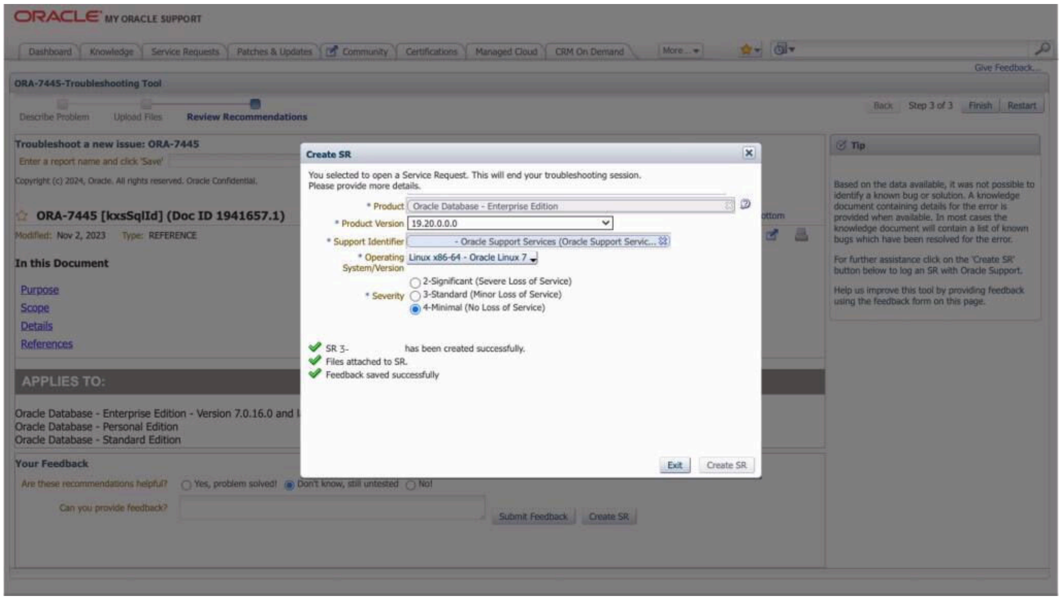
Help us improve this tool by providing feedback using the feedback form on this page.

2. You'll then be prompted to clarify your:

- Product
- Product Version
- Support Identifier
- Operating System
- SR severity

3. Then press the **Create SR** button.
   And, you'll get a new SR number.

Figure 7-24 New SR



Create SR

You selected to open a Service Request. This will end your troubleshooting session.
Please provide more details.

* Product: Oracle Database - Enterprise Edition
* Product Version: 19.20.0.0.0
* Support Identifier: - Oracle Support Services (Oracle Support Servic...
* Operating System/Version: Linux x86-64 - Oracle Linux 7
* Severity: ○ 2-Significant (Severe Loss of Service) ○ 3-Standard (Minor Loss of Service) ● 4-Minimal (No Loss of Service)

✓ SR 3- has been created successfully.
✓ Files attached to SR.
✓ Feedback saved successfully

The AHF diagnostic collection you uploaded originally will be routed onto your SR and Oracle Support will take over.

7.6 Resolving ORA-04030 out of process memory when trying to allocate

For more information and videos, see https://blogs.oracle.com/database/post/ora-04030.

Follow these step-by-step instructions for everything you need to do to resolve `ORA-04030`.

Understanding ORA-04030

The `ORA-04030`: out of process memory when trying to allocate bytes, occurs when an Oracle process runs out of operating system memory.

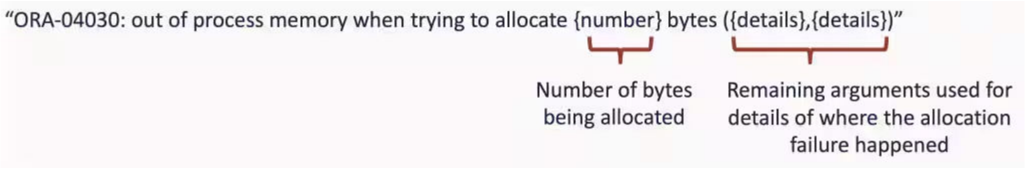
This can be caused by either:

- Exhausting total machine memory. That is, there isn't enough physical RAM on the machine
  (or)

- Exhausting designated space in the Program Global Area, known as the PGA.

The error message will show how much memory the process tried to allocate and provide details of where the allocation failure happened.

Figure 7-25   ORA-04030 Internal Error Code: Arguments

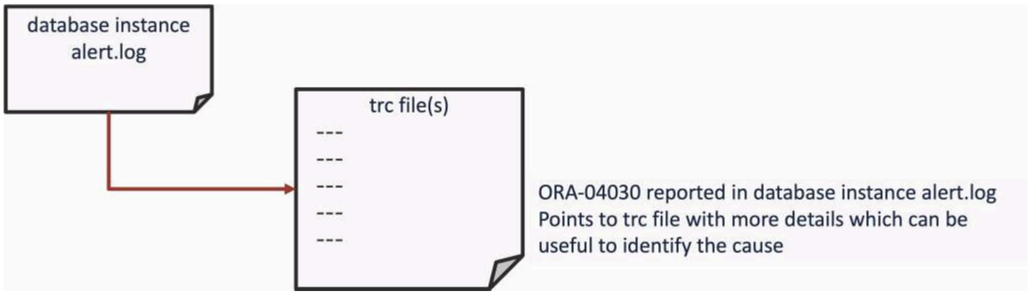


“ORA-04030: out of process memory when trying to allocate {number} bytes ({details},{details})”

Number of bytes being allocated
Remaining arguments used for details of where the allocation failure happened

ORA-04030 can occur in either a client or database process. If raised by a database process then an entry will be made in the database alert log, which will point to a trace file containing more details, which can be useful to identify the cause.

Figure 7-26   Database Instance Alert Log



ORA-04030 reported in database instance alert.log Points to trc file with more details which can be useful to identify the cause

Resolving an ORA-04030 error typically involves addressing the memory limitations that caused it.

This might be:

- Increasing available RAM
- Adjusting PGA size
- Optimizing resource usage
- Reviewing operating system limits
- Identifying and resolving memory leaks

ORA-04030 Error Troubleshooting Steps

The basic resolution steps for ORA-04030 are:

- Use AHF to generate an ORA-04030 Service Request Data Collection (SRDC)
- Use ORA-04030 Troubleshooting Tool to find recommendations
- Log a new SR using the diagnostic collection

Use AHF to generate an ORA-04030 Service Request Data Collection (SRDC)

In the first step, use AHF to generate an `ORA-04030` diagnostic collection.

1. Log into the machine where the `ORA-04030` occurred and as the `Oracle` user run the command:

   ```
   tfactl diagcollect -srdc ORA-04030
   ```

   You'll be prompted to enter the date and time of the `ORA-04030` you're interested in. If you're not sure, just press return. You'll then be prompted to enter the database name.

   For example:

   ```
   $ tfactl diagcollect -srdc ORA-04030
   Enter the time of the ORA-04030 [YYYY-MM-DD HH24:MI:SS,<RETURN>=ALL] :

   Enter the Database Name [Required for this SRDC] :

   Components included in this collection: OS DATABASE CHMOS SOSREPORT

   Preparing to execute support diagnostic scripts.
       Executing DB Script srdc_db_sid_memorysizes_11gplus.sql on CDB12 with
   timeout of 300 seconds...

   Collecting data for all nodes

   TFA is using system timezone for collection, All times shown in PDT.
   Scanning files from 2024-03-25 10:07:36 PDT to 2024-03-25 10:40:07 PDT

   Collection Id : 20240325104016mymachine03

   Detailed Logging at : /opt/oracle.ahf/data/repository/
   srdc_ora4030_collection_Mon_Mar_25_10_40_19_PDT_2024_node_all/
   diagcollect_20240325104016_mymachine03.log

   Waiting up to 120 seconds for collection to start
   2024/03/25 10:40:24 PDT : NOTE : Any file or directory name containing
   the string .com will be renamed to replace .com with dotcom
   2024/03/25 10:40:24 PDT : Collection Name :
   tfa_srdc_ora4030_Mon_Mar_25_10_40_18_PDT_2024.zip
   2024/03/25 10:40:24 PDT : Collecting diagnostics from hosts :
   [mymachine04, mymachine03]
   2024/03/25 10:40:25 PDT : Getting list of files satisfying time range
   [03/25/2024 10:07:36, 03/25/2024 10:40:07]
   2024/03/25 10:40:25 PDT : Collecting Additional Diagnostic Information...
   2024/03/25 10:40:44 PDT : Collecting ADR incident files...
   2024/03/25 10:41:06 PDT : Executing TFA rdahcve with timeout of 600
   seconds...
   2024/03/25 10:41:08 PDT : Executing IPS Incident Package Collection(s)...
   2024/03/25 10:41:10 PDT : Generating IPS Pack for 1 incidents on database
   cdb12
   2024/03/25 10:41:17 PDT : Executing SQL Script db_feature_usage.sql on
   cdb12 with timeout of 600 seconds...
   ```

```
2024/03/25 10:41:17 PDT : Executing Collection for OS with timeout
of 1800 seconds...
2024/03/25 10:41:25 PDT : Executing Collection for SOSREPORT with
timeout of 1860 seconds...
2024/03/25 10:42:30 PDT : Completed Collection of Additional
Diagnostic Information...
2024/03/25 10:42:35 PDT : Completed Local Collection
2024/03/25 10:42:35 PDT : Not Redacting this Collection on Exadata
with no redaction option passed ..
2024/03/25 10:42:35 PDT : Not Redacting this Collection ...
2024/03/25 10:42:35 PDT : Remote Collection in Progress...
2024/03/25 10:42:56 PDT : Collection completed on host: mymachine04
2024/03/25 10:42:56 PDT : Collection completed on host: mymachine03
2024/03/25 10:42:56 PDT : Completed collection of zip files.

.---------------------------------------.
|           Collection Summary          |
+-------------+-----------+------+------+
| Host        | Status    | Size | Time |
+-------------+-----------+------+------+
| mymachine04 | Completed | 21MB | 113s |
| mymachine03 | Completed | 36MB | 131s |
'-------------+-----------+------+------'

Logs are being collected to: /opt/oracle.ahf/data/repository/
srdc_ora4030_collection_Mon_Mar_25_10_40_19_PDT_2024_node_all
/opt/oracle.ahf/data/repository/
srdc_ora4030_collection_Mon_Mar_25_10_40_19_PDT_2024_node_all/
mymachine04.tfa_srdc_ora4030_Mon_Mar_25_10_40_18_PDT_2024.zip
/opt/oracle.ahf/data/repository/
srdc_ora4030_collection_Mon_Mar_25_10_40_19_PDT_2024_node_all/
mymachine03.tfa_srdc_ora4030_Mon_Mar_25_10_40_18_PDT_2024.zip
```

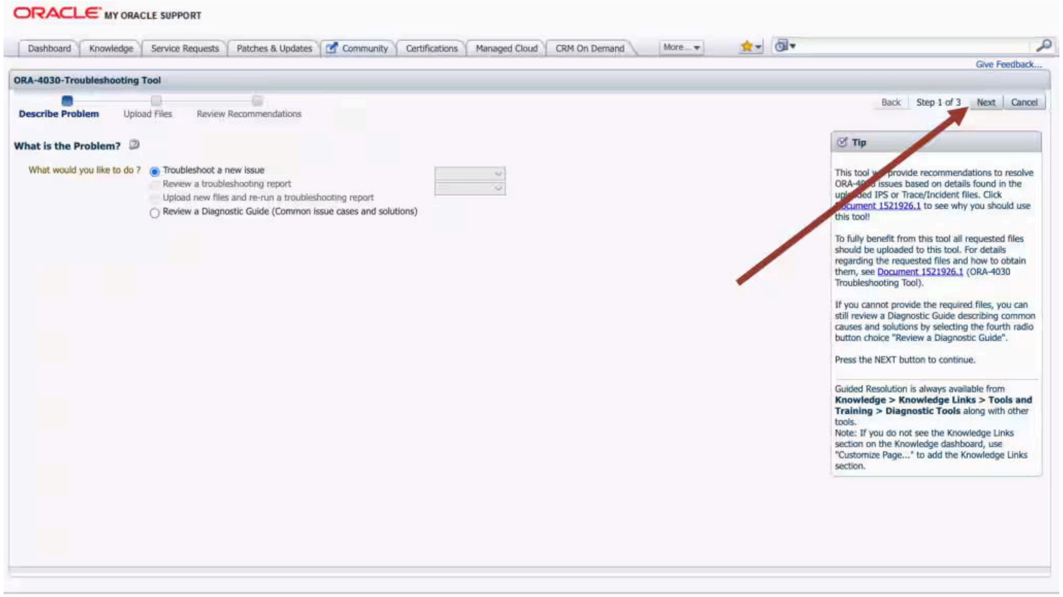
Once it’s finished AHF will package everything for you in a zip file for each machine, as you progress you'll only need the one from the node where the problem occurred.

Now, we can move onto step number two. Use the My Oracle Support ORA-04030 troubleshooting tool to find recommendations.

Use ORA-04030 Troubleshooting Tool to find recommendations

1. Log into My Oracle Support and search for `ORA-04030`, or alternatively go to My Oracle Support ORA-04030 troubleshooting tool to access it directly.
2. When you get to the troubleshooting tool click the **Next** button at the top right.

Figure 7-27   My Oracle Support ORA-04030 Troubleshooting Tool



ORA-4030-Troubleshooting Tool

Describe Problem — Upload Files — Review Recommendations

What is the Problem?

What would you like to do ?
- ● Troubleshoot a new issue
- Review a troubleshooting report
- Upload new files and re-run a troubleshooting report
- ○ Review a Diagnostic Guide (Common issue cases and solutions)

Tip

This tool will provide recommendations to resolve ORA-4030 issues based on details found in the uploaded IPS or Trace/Incident files. Click Document 1521926.1 to see why you should use this tool!

To fully benefit from this tool all requested files should be uploaded to this tool. For details regarding the requested files and how to obtain them, see Document 1521926.1 (ORA-4030 Troubleshooting Tool).

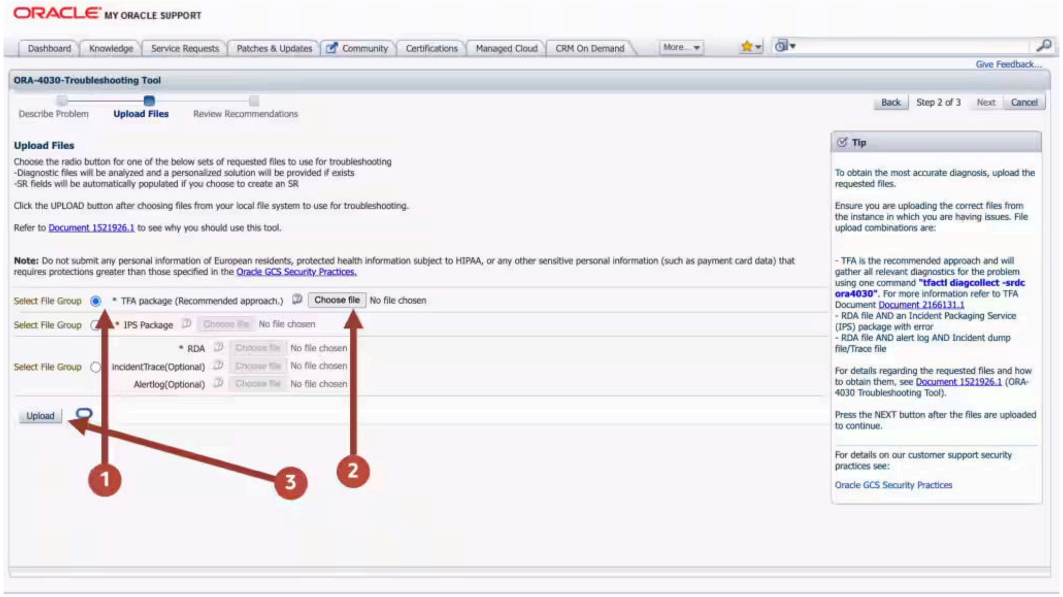
If you cannot provide the required files, you can still review a Diagnostic Guide describing common causes and solutions by selecting the fourth radio button choice "Review a Diagnostic Guide".

Press the NEXT button to continue.

Guided Resolution is always available from **Knowledge > Knowledge Links > Tools and Training > Diagnostic Tools** along with other tools.
Note: If you do not see the Knowledge Links section on the Knowledge dashboard, use "Customize Page..." to add the Knowledge Links section.

3. Select the first radio button to choose to upload a TFA package.
4. Then click the **Choose file** button, select the zip file AHF captured for you in step 1.
5. Then press the **Upload** button.

Figure 7-28   Choose Upload



ORA-4030-Troubleshooting Tool

Describe Problem — Upload Files — Review Recommendations

Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521926.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) Choose file No file chosen
Select File Group ○ * IPS Package Choose file No file chosen
Select File Group ○ * RDA Choose file No file chosen
IncidentTrace(Optional) Choose file No file chosen
Alertlog(Optional) Choose file No file chosen

Tip

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora4030"**. For more information refer to TFA Document Document 2166131.1
- RDA file AND an Incident Packaging Service (IPS) package with error
- RDA file AND alert log AND Incident dump file/Trace file

For details regarding the requested files and how to obtain them, see Document 1521926.1 (ORA-4030 Troubleshooting Tool).

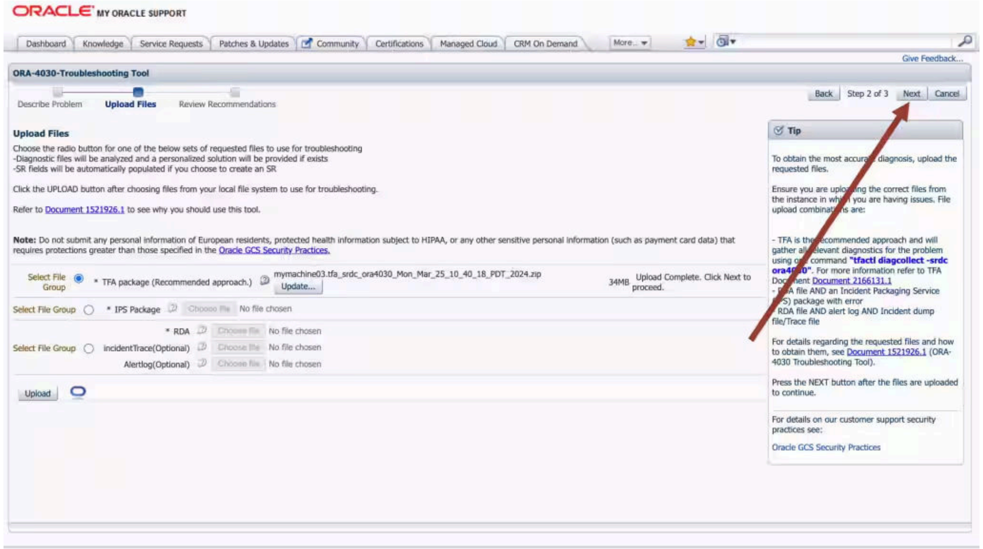
Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

Oracle GCS Security Practices

6. Once this is uploaded click the **Next** button at the top right again.

Figure 7-29   Choose Upload



ORA-4030-Troubleshooting Tool

Upload Files

Choose the radio button for one of the below sets of requested files to use for troubleshooting
-Diagnostic files will be analyzed and a personalized solution will be provided if exists
-SR fields will be automatically populated if you choose to create an SR

Click the UPLOAD button after choosing files from your local file system to use for troubleshooting.

Refer to Document 1521926.1 to see why you should use this tool.

Note: Do not submit any personal information of European residents, protected health information subject to HIPAA, or any other sensitive personal information (such as payment card data) that requires protections greater than those specified in the Oracle GCS Security Practices.

Select File Group ● * TFA package (Recommended approach.) mymachine03.tfa_srdc_ora4030_Mon_Mar_25_10_40_18_PDT_2024.zip 34MB Upload Complete. Click Next to proceed.

Select File Group ○ * IPS Package No file chosen

Select File Group ○ * RDA No file chosen
incidentTrace(Optional) No file chosen
Alertlog(Optional) No file chosen

Tip

To obtain the most accurate diagnosis, upload the requested files.

Ensure you are uploading the correct files from the instance in which you are having issues. File upload combinations are:

- TFA is the recommended approach and will gather all relevant diagnostics for the problem using one command **"tfactl diagcollect -srdc ora4030"**. For more information refer to TFA Document Document 2166131.1
- RDA file AND an Incident Packaging Service (IPS) package with error
- RDA file AND alert log AND Incident dump file/Trace file

For details regarding the requested files and how to obtain them, see Document 1521926.1 (ORA-4030 Troubleshooting Tool).

Press the NEXT button after the files are uploaded to continue.

For details on our customer support security practices see:

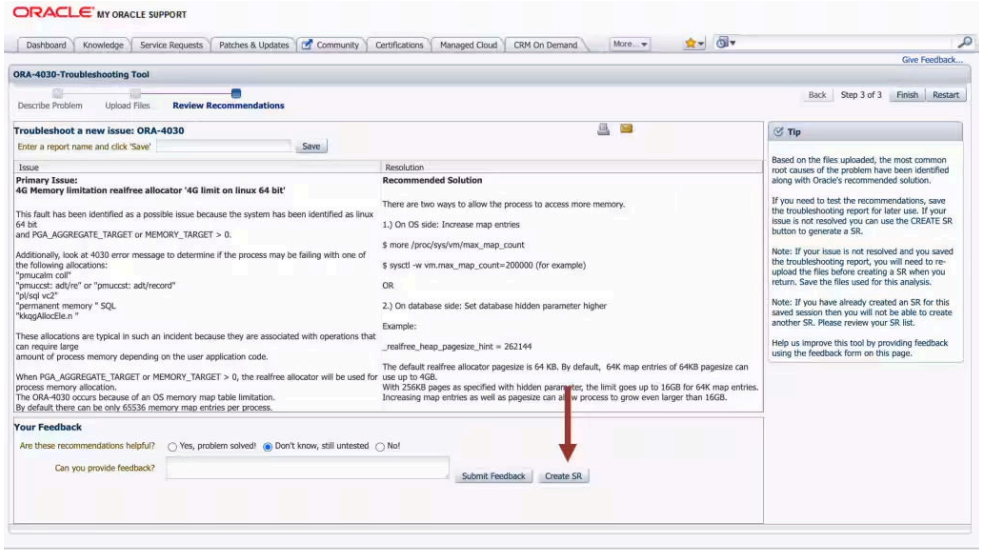
Oracle GCS Security Practices

The troubleshooting tool will then analyze the contents of the diagnostic collection and compare the log entries against its list of known problems. It will then recommend a My Oracle Support (MOS) Knowledge document for you that it thinks is the best fit. This knowledge document will either advise you what to do or show you several bugs where that `ORA-04030` has been reported. You can use this to look up which Database Release Update (RUs) fixed the bug. If you go through the MOS troubleshooting tool and can't find a solution, or you just need some more help, then you can easily log an SR with Oracle Support.

Log a new SR using the diagnostic collection

1. Press the **Create SR** button at the bottom.

Figure 7-30   Create SR



ORA-4030-Troubleshooting Tool

Troubleshoot a new issue: ORA-4030

Enter a report name and click 'Save'

Issue	Resolution

Primary Issue:
4G Memory limitation realfree allocator '4G limit on linux 64 bit'
 	
This fault has been identified as a possible issue because the system has been identified as linux 64 bit
and PGA_AGGREGATE_TARGET or MEMORY_TARGET > 0.
 	
Additionally, look at 4030 error message to determine if the process may be failing with one of the following allocations:
"pmucalm coll"
"pmuccst: adt/re" or "pmuccst: adt/record"
"pl/sql vc2"
"permanent memory " SQL
"kkqgAllocEle.n "
 	
These allocations are typical in such an incident because they are associated with operations that can require large
amount of process memory depending on the user application code.
 	
When PGA_AGGREGATE_TARGET or MEMORY_TARGET > 0, the realfree allocator will be used for process memory allocation.
The ORA-4030 occurs because of an OS memory map table limitation.
By default there can be only 65536 memory map entries per process.
	Recommended Solution
	
	There are two ways to allow the process to access more memory.
	
	1.) On OS side: Increase map entries
	
	$ more /proc/sys/vm/max_map_count
	
	$ sysctl -w vm.max_map_count=200000 (for example)
	
	OR
	
	2.) On database side: Set database hidden parameter higher
	
	Example:
	
	_realfree_heap_pagesize_hint = 262144
	
	The default realfree allocator pagesize is 64 KB. By default, 64K map entries of 64KB pagesize can use up to 4GB.
	With 256KB pages as specified with hidden parameter, the limit goes up to 16GB for 64K map entries.
	Increasing map entries as well as pagesize can allow process to grow even larger than 16GB.

Your Feedback

Are these recommendations helpful? ○ Yes, problem solved! ● Don't know, still untested ○ No!

Can you provide feedback?

Tip

Based on the files uploaded, the most common root causes of the problem have been identified along with Oracle's recommended solution.

If you need to test the recommendations, save the troubleshooting report for later use. If your issue is not resolved you can use the CREATE SR button to generate a SR.

Note: If your issue is not resolved and you saved the troubleshooting report, you will need to re-upload the files before creating a SR when you return. Save the files used for this analysis.

Note: If you have already created an SR for this saved session then you will not be able to create another SR. Please review your SR list.

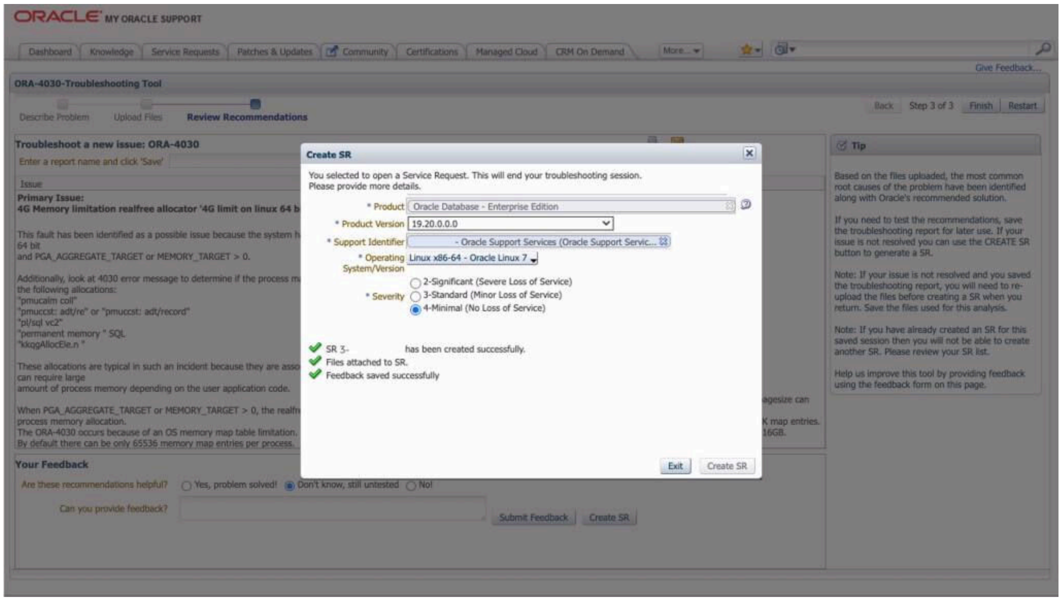
Help us improve this tool by providing feedback using the feedback form on this page.

2. You'll then be prompted to clarify your:

- Product
- Product Version
- Support Identifier
- Operating System
- SR severity

3. Then press the **Create SR** button.
   And, you’ll get a new SR number.

Figure 7-31   New SR



ORA-4030-Troubleshooting Tool

Troubleshoot a new issue: ORA-4030

Enter a report name and click 'Save'

Issue

Primary Issue:
4G Memory limitation realfree allocator '4G limit on linux 64 b

This fault has been identified as a possible issue because the system h
64 bit
and PGA_AGGREGATE_TARGET or MEMORY_TARGET > 0.

Additionally, look at 4030 error message to determine if the process m
the following allocations:
"pmucalm coll"
"pmuccst: adt/re" or "pmuccst: adt/record"
"pl/sql vc2"
"permanent memory " SQL
"kkqgAllocEle.n "

These allocations are typical in such an incident because they are asso
can require large
amount of process memory depending on the user application code.

When PGA_AGGREGATE_TARGET or MEMORY_TARGET > 0, the realfr
process memory allocation.
The ORA-4030 occurs because of an OS memory map table limitation.
By default there can be only 65536 memory map entries per process.

Create SR

You selected to open a Service Request. This will end your troubleshooting session.
Please provide more details.

* Product: Oracle Database - Enterprise Edition
* Product Version: 19.20.0.0.0
* Support Identifier: - Oracle Support Services (Oracle Support Servic...
* Operating System/Version: Linux x86-64 - Oracle Linux 7
* Severity: ○ 2-Significant (Severe Loss of Service) ○ 3-Standard (Minor Loss of Service) ● 4-Minimal (No Loss of Service)

✓ SR 3- has been created successfully.
✓ Files attached to SR.
✓ Feedback saved successfully

Exit | Create SR

Tip

Based on the files uploaded, the most common root causes of the problem have been identified along with Oracle's recommended solution.

If you need to test the recommendations, save the troubleshooting report for later use. If your issue is not resolved you can use the CREATE SR button to generate a SR.

Note: If your issue is not resolved and you saved the troubleshooting report, you will need to re-upload the files before creating a SR when you return. Save the files used for this analysis.

Note: If you have already created an SR for this saved session then you will not be able to create another SR. Please review your SR list.

Help us improve this tool by providing feedback using the feedback form on this page.

Your Feedback

Are these recommendations helpful? ○ Yes, problem solved! ● Don't know, still untested ○ No!

Can you provide feedback?

Submit Feedback | Create SR

The AHF diagnostic collection you uploaded originally will be routed onto your SR and Oracle Support will take over.

8 Troubleshoot

Learn to fix Oracle Trace File Analyzer and Compliance Framework (Oracle ORAchk and Oracle EXAchk) issues.

- Troubleshooting Oracle Trace File Analyzer
  This section helps you diagnose and fix Oracle Trace File Analyzer issues.
- Troubleshooting Compliance Framework (Oracle Orachk and Oracle Exachk)
  Follow the steps explained in this section to troubleshoot and fix Compliance Framework (Oracle Orachk / Oracle Exachk) related issues.

8.1 Troubleshooting Oracle Trace File Analyzer

This section helps you diagnose and fix Oracle Trace File Analyzer issues.

- Cluster Nodes are Not Showing As One Cluster When Viewed by Running the tfactl status Command
- Oracle Trace File Analyzer is Not Starting and the init.tfa script is Missing After Reboot
- Error Message Similar to "Can't locate **** in @inc (@inc contains:....)"
- Non-Release Update Revisions (RURs) Oracle Trace File Analyzer Patching Fails on Remote Nodes
- Non-Root Access is Not Enabled After Installation
- TFA_HOME and Repository Locations are Moved After Patching or Upgrade
- Oracle Trace File Analyzer Fails with TFA-00103 After Applying the July 2015 Release Update Revision (RUR) or Later
- OSWatcher Parameters are Different After a Reboot or Otherwise Unexpectedly Different
- Oracle Trace File Analyzer Installation or Oracle Trace File Analyzer Discovery (tfactl rediscover) Fails on Linux 7
- OSWatcher Analyzer Fails When OSWatcher is Not Running from the TFA_HOME
- Oracle Trace File Analyzer Fails to Start with com.sleepycat.je.EnvironmentLockedException Java Exception
- Oracle Trace File Analyzer Startup Fails When Solution-Soft Time Machine Software is Installed, but Not Running on the System
- Non-privileged User is Not Able to Run tfactl Commands
- Oracle Trace File Analyzer Daemon is Not Starting or Not Running?
- Oracle Trace File Analyzer Is Not Collecting Diagnostic Traces of Components Such As CRS, DB, ASM, and So On
- Oracle Trace File Analyzer Fails to Start

8.1.1 Cluster Nodes are Not Showing As One Cluster When Viewed by Running the tfactl status Command

Cause: Certificates are not synchronized.

Action: Manually synchronize the keys.

Go to any one of the cluster nodes and run the `synctfanodes.sh` script as `root`.

```
# $GIHOME/tfa/nodename/tfa_home/bin/synctfanodes.sh
```

Note:

The script uses SSH and SCP. If passwordless SSH is not set for `root`, then Oracle Trace File Analyzer prompts you 3 times per node for password each time a command is run.

If the Expect utility is available on the node, then Oracle Trace File Analyzer uses Expect thus reducing the number of prompts for password.

8.1.2 Oracle Trace File Analyzer is Not Starting and the init.tfa script is Missing After Reboot

Description: The file system housing `TFA_HOME` with Oracle Trace File Analyzer binaries was not mounted when `init.tfa` was run from `init` or `System D` on Linux 6 and above.

Cause: There are many reasons and not restricted to the following:

- Mounting the file system was disabled for maintenance or patching
- Problems or errors related to the file system
- NFS inaccessible network
- File system with `TFA_HOME` is mounting slowly

Action: Refer to My Oracle Support note 2224163.1 to fix this issue.

Related Topics

- https://support.oracle.com/rs?type=doc&id=2224163.1

8.1.3 Error Message Similar to "Can't locate **** in @inc (@inc contains:....)"

Cause: Using an old version of Perl causes this error.

Action: Oracle Trace File Analyzer requires Perl version 5.10 or above. If you encounter similar errors, then upgrade Perl to version 5.10 or above.

After installing, update the location of Perl in the `tfa_home/tfa_setup.txt` file to point to the new location:

```
PERL=/u01/perl/bin/perl
```

If the problem occurs during installation, then use the `-perlhome` *`dir`* install option.

The directory you specify must contain `/bin/perl`. If you install Perl as `root`, then `root` must own the Perl executable.

```
# which perl
/usr/bin/perl


# ahf_setup
```

8.1.4 Non-Release Update Revisions (RURs) Oracle Trace File Analyzer Patching Fails on Remote Nodes

Cause: Remote nodes fail to upgrade due to a socket issue when upgrading Oracle Trace File Analyzer through Oracle Trace File Analyzer sockets.

Description: After completing the upgrade, crosscheck the report if all nodes are at the same version, build id, and status.

```
.-------------------------------------------------------------.
| Host  | TFA Version | TFA Build ID         | Upgrade Status |
+-------+-------------+----------------------+----------------+
| node1 | 19.3.0.0.0  | 12126020151019114604 | UPGRADED       |
| node2 | 19.3.0.0.0  | 12126020151019114604 | UPGRADED       |
'-------+-------------+----------------------+----------------'
```

If you see any differences as follows, then you must fix the issue.

```
.--------------------------------------------------------------.
| Host  | TFA Version | TFA Build ID          | Upgrade Status |
+-------+-------------+-----------------------+----------------+
| node1 | 19.3.0.0.0  | 12126020151019114604  | UPGRADED       |
| node2 | 19.3.0.0.0  | 12120020140619094932  | NOT UPGRADED   |
'-------+-------------+-----------------------+----------------'
```

Action: Copy the Oracle Trace File Analyzer installer to all nodes that failed to upgrade and run the installer locally on those nodes.

```
ahf_setup
```

After upgrading the binaries, replace the root SSL certificates from the node that initiated upgrade.

Copy the following files from the existing configuration node to the node to be added. Change the permission for those files to `700` for `root` on the machine to be added.

```
TFA_HOME/data/hostname/tfa/server.jks
TFA_HOME/data/hostname/tfa/client.jks
TFA_HOME/data/hostname/tfa/internal/ssl.properties
```

8.1.5 Non-Root Access is Not Enabled After Installation

Description: Non-root access for the Oracle Grid Infrastructure software owner must be activated by default when non-root access is enabled.

Action: To enable non-root access to Oracle Trace File Analyzer, run the `tfactl access add -user` command as `root`.

For example:

```
tfactl access add -user xyx
```

Running command enables the non-root user group *xyz* to access Oracle Trace File Analyzer.

8.1.6 TFA_HOME and Repository Locations are Moved After Patching or Upgrade

Description: Before Oracle Trace File Analyzer version 12.1.2.6.0, when an existing free standing Oracle Trace File Analyzer was installed (MOS version installed outside the `GRID_HOME`) and Oracle Trace File Analyzer is then patched with Oracle Grid Infrastructure as part of Oracle 12.1.0.2, then `TFA_HOME` is moved into the `GRID_HOME` and the repository directory is moved to the Oracle Grid Infrastructure owners `ORACLE_BASE` directory.

If the repository directory is changed to a non-default location, then the change is lost.

- To set the Oracle Trace File Analyzer zip file repository location to the required base directory, run the `tfactl set repositorydir` command.
- To change the maximum size of the Oracle Trace File Analyzer repository, run the `tfactl set reposizeMB` command.

Starting with Oracle Trace File Analyzer version 12.1.2.6.0 and above, if `TFA_HOME` exists outside the `GRID_HOME`, then Oracle Trace File Analyzer installation is moved as part of Release Update Revision (RUR) installation. However, if the Release Update Revision (RUR) has a newer version of Oracle Trace File Analyzer, then Oracle Trace File Analyzer is upgraded in its current location.

If Oracle Trace File Analyzer is installed in the `GRID_HOME` and the `GRID_HOME` is moved as part of any patching, then the existing `TFA_HOME` is migrated to the new `GRID_HOME` and upgraded as required.

8.1.7 Oracle Trace File Analyzer Fails with TFA-00103 After Applying the July 2015 Release Update Revision (RUR) or Later

- Phase 1 of Oracle Trace File Analyzer upgrade
- Phase 2 of Oracle Trace File Analyzer upgrade
- How can I verify that both phases have been completed and that Oracle Trace File Analyzer communication among all the nodes has been established?
- What if I do not upgrade all my nodes at the same time by choice or if some are down for maintenance?
- I know that not all nodes are upgraded at the same time. I do not want to wait 24 hours for Oracle Trace File Analyzer to sync the key files. What do I do?

Phase 1 of Oracle Trace File Analyzer upgrade

Oracle Trace File Analyzer communication model has been changed in versions greater than 12.1.2.4.1. To avoid communication problems, Oracle Trace File Analyzer communication change must be complete across all nodes of the Oracle Trace File Analyzer configuration. Oracle Trace File Analyzer is upgraded on each node locally as part of application of Release Update Revision (RUR). The Release Update Revision (RUR) process applies the new software and restarts Oracle Trace File Analyzer, but does not put in place the new connection model.

Phase 2 of Oracle Trace File Analyzer upgrade

Before automatically implementing the new communication model, Oracle Trace File Analyzer waits for 24 hours to complete the application of Release Update Revision (RUR) on all nodes. Once Oracle Trace File Analyzer is upgraded on all the nodes, phase 2 must occur within 10 minutes. The new Oracle Trace File Analyzer communication model is not implemented (phase 2) until Release Update Revision (RUR) is applied on all nodes (phase 1).

Oracle Trace File Analyzer indicates by displaying the message:

```
TFA-00103 - TFA is not yet secured to run all commands.
```

Once Oracle Trace File Analyzer is upgraded on all nodes in the configuration (phase 1), Oracle Trace File Analyzer:

- Generates new SSL keys
- Sends the keys to the valid nodes in the cluster
- Restart Oracle Trace File Analyzer on each of these nodes (phase 2)

On completion of phase 2, Oracle Trace File Analyzer must process commands normally using the new communication model.

How can I verify that both phases have been completed and that Oracle Trace File Analyzer communication among all the nodes has been established?

First, as `root` run:

```
 tfactl print status
```

```
.------------------------------------------------------------------------
----------.
| Host    | Status   | PID    | Port |   Version   |      Build ID
| Inventory|
+--------+---------+-------+------+-----------+---------------------
+----------+
| sales1 | RUNNING | 4390  | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
| sales2 | RUNNING | 23604 | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
| sales3 | RUNNING | 28653 | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
| sales4 | RUNNING | 5989  | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
'--------+---------+-------+------+-----------+---------------------
+----------'
```

Once all nodes are shown to be at the same version and build ID then within about 10 minutes maximum the synchronization of keys must complete.

Ensure that you run the following command:

```
tfactl print directories
```

Running `tfactl print directories` must return the list of directories registered in Oracle Trace File Analyzer. If the communication is not established among all the nodes, then the command returns the message, `TFA is not yet secured to run all commands`.

The message also indicates that phase 2 has not been completed. To verify on which nodes phase 2 has not yet been completed, on each node, check the existence of the following files. The files must be readable only by `root`, `ownership:group` of `root`. The checksum for each file must match on all nodes.

```
# ls -al /u01/app/12.1.0/grid/tfa/sales1/tfa_home/client.jks

-rwx------   1 root  root   3199 Jun 30 14:12 /u01/app/12.1.0/grid/tfa/
sales1/tfa_home/client.jks

# ls -al /u01/app/12.1.0/grid/tfa/sales1/tfa_home/server.jks

-rwx------   1 root  root   3201 Jun 30 14:12 /u01/app/12.1.0/grid/tfa/
sales1/tfa_home/server.jks

# ls -al /u01/app/12.1.0/grid/tfa/sales1/tfa_home/internal/
ssl.properties

-rwx------   1 root  root   220 Jun 30 14:12 /u01/app/12.1.0/grid/tfa/
sales1/tfa_home/internal/ssl.properties
```

What if I do not upgrade all my nodes at the same time by choice or if some are down for maintenance?

Oracle Trace File Analyzer waits to complete the phase 2 operations until all nodes have completed upgrade or until 24 hours has passed.

After 24 hours, Oracle Trace File Analyzer:

- Generates new keys
- Copies the key to all the nodes that have been upgraded
- Restarts Oracle Trace File Analyzer on those nodes

Any nodes that did not get the keys are outside of the Oracle Trace File Analyzer configuration. After upgrading Oracle Trace File Analyzer, manually synchronize the keys with other nodes.

If the application of Release Update Revision (RUR) on all the nodes is completed within 24 hours, then manually synchronize the keys.

To manually synchronize the keys, go to one node that has completed Phase 2 and run the `synctfanodes.sh` script as `root`.

```
# $GIHOME/tfa/nodename/tfa_home/bin/synctfanodes.sh
```

> **Note:**
>
> The script uses SSH and SCP. If `root` does not have passwordless SSH, then Oracle Trace File Analyzer prompts you 3 time per node for password each time a command is run.
>
> If the Expect utility is available on the node, then Oracle Trace File Analyzer uses Expect thus reducing the number of prompts for password.

The script displays all the nodes in Oracle Trace File Analyzer configuration, including the nodes where Oracle Trace File Analyzer is yet to upgrade.

The script also shows the nodes that are part of the Oracle Grid Infrastructure configuration.

Verify the node list provided and supply a space-separated list of nodes to synchronize. It doesn't hurt to include the nodes that were previously upgraded as the process is idempotent.

For example:

Nodes *sales1*, *sales2*, *sales3*, and *sales4* are all part of Oracle Grid Infrastructure. The nodes were running Oracle Trace File Analyzer 12.1.2.0.0 until the July 2015 Release Update Revision (RUR) was applied.

The Release Update Revision (RUR) was applied initially only to *sales1* and *sales3* due to outage restrictions.

After completion of phase 1 of the Oracle Trace File Analyzer upgrade, run `print status`. Running the command lists all nodes even though different versions of Oracle Trace File Analyzer are running on some of the nodes.

```
-bash-3.2# /u01/app/12.1.0/grid/bin/tfactl print status
.----------------------------------------------------------------------
----------.
| Host   | Status  | PID   | Port |   Version  |       Build ID       |
Inventory |
+--------+---------+------ +------+------------+-----------------------
+----------+
| sales1 | RUNNING | 27270 | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
| sales3 | RUNNING | 19222 | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
| sales2 | RUNNING | 10141 | 5000 | 12.1.2.0.0 | 12120020140619094932
| COMPLETE |
| sales4 | RUNNING | 17725 | 5000 | 12.1.2.0.0 | 12120020140619094932
| COMPLETE |
'--------+---------+-------+------+------------+-----------------------
+----------'
```

Since the new Oracle Trace File Analyzer communication model is not set up among all the nodes, many commands when run as `root` fail with the message:

```
TFA is not yet secured to run all commands.
```

Failed attempts to run `tfactl` commands as a non-root indicates that there is no sufficient permission to use Oracle Trace File Analyzer.

After 24 hours, Oracle Trace File Analyzer completes phase 2 for *sales1* and *sales3*. Oracle Trace File Analyzer communication model is established for *sales1* and *sales3*. You can perform normal Oracle Trace File Analyzer operations on *sales1* and *sales3*. Communication with *sales2* and *sales4* has not yet been established and so running remote commands to them fail.

When running `print status` on *sales1* and *sales3*, we no longer see *sales2* and *sales4*. Only Oracle Trace File Analyzer using the new Oracle Trace File Analyzer communication model communicates.

```
-bash-3.2# /u01/app/12.1.0/grid/bin/tfactl print status

.----------------------------------------------------------------------
----------.
| Host   | Status  | PID   | Port |   Version  |     Build ID         |
Inventory |
+--------+---------+-------+------+------------+-----------------------
+----------+
| sales1 | RUNNING | 4390  | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
| sales3 | RUNNING | 23604 | 5000 | 12.1.2.4.2 | 12124220150629072212
| COMPLETE |
'--------+---------+-------+------+------------+-----------------------
+----------'
```

Running the command `tfactl diagcollect` collects from *sales1* and *sales3* but not from the other nodes.

```
$ tfactl diagcollect
Choose the event you want to perform a diagnostic collection for:
1. Mar/12/2019 16:08:20 [ db.orcl.orcl ]  ORA-04030: out of process memory
when trying to allocate
2. Mar/12/2019 16:08:18 [ db.orcl.orcl ]  ORA-04031: unable to allocate 8
bytes of shared memory
3. Mar/12/2019 16:08:16 [ db.orcl.orcl ]  ORA-00494: enqueue held for too
long more than seconds by osid
4. Mar/12/2019 16:08:14 [ db.orcl.orcl ]  ORA-29709: Communication failure
with Cluster Synchronization
5. Mar/12/2019 16:08:04 [ db.orcl.orcl ]  ORA-29702: error occurred in
Cluster Group Service operation
6. Mar/12/2019 16:07:59 [ db.orcl.orcl ]  ORA-32701: Possible hangs up to
hang ID= detected
7. Mar/12/2019 16:07:51 [ db.orcl.orcl ]  ORA-07445: exception encountered:
core dump [] [] [] [] [] []
8. Mar/12/2019 16:07:49 [ db.orcl.orcl ]  ORA-00700: soft internal error,
arguments: [700], [], [],[]
9. Mar/11/2019 22:02:19 [ db.oradb.oradb ]  DIA0 Critical Database Process
Blocked: Hang ID 1 blocks 5 sessions
10. Default diagnostic collection, for no specific event

Please choose the event : 1-10 [] 10

By default TFA will collect diagnostics for the last 12 hours. This can
result in large collections
For more targeted collections enter the time of the incident, otherwise hit
<RETURN> to collect for the last 12 hours
[YYYY-MM-DD HH24:MI:SS,<RETURN>=Collect for last 12 hours] :

Collecting data for the last 12 hours for all components...
Collecting data for all nodes

Collection Id : 20190312163846node1

Detailed Logging at : /scratch/app/product/18c/tfa/repository/
collection_Tue_Mar_12_16_38_47_PDT_2019_node_all/
diagcollect_20190312163846_node1.log
2019/03/12 16:38:50 PDT : NOTE : Any file or directory name containing the
string .com will be renamed to replace .com with dotcom
2019/03/12 16:38:50 PDT : Collection Name :
tfa_Tue_Mar_12_16_38_47_PDT_2019.zip
2019/03/12 16:38:50 PDT : Collecting diagnostics from hosts : [node1]
2019/03/12 16:38:50 PDT : Scanning of files for Collection in progress...
2019/03/12 16:38:50 PDT : Collecting additional diagnostic information...
2019/03/12 16:38:55 PDT : Getting list of files satisfying time range
[03/12/2019 04:38:50 PDT, 03/12/2019 16:38:55 PDT]
2019/03/12 16:39:02 PDT : Collecting ADR incident files...
2019/03/12 16:39:06 PDT : Completed collection of additional diagnostic
information...
2019/03/12 16:39:07 PDT : Completed Local Collection
.------------------------------------.
```

```
|         Collection Summary         |
+-----------+-----------+------+------+
| Host      | Status    | Size | Time |
+-----------+-----------+------+------+
| node1 | Completed | 21MB |  17s |
'-----------+-----------+------+------'

Logs are being collected to: /scratch/app/product/18c/tfa/repository/
collection_Tue_Mar_12_16_38_47_PDT_2019_node_all
/scratch/app/product/18c/tfa/repository/
collection_Tue_Mar_12_16_38_47_PDT_2019_node_all/
node1.tfa_Tue_Mar_12_16_38_47_PDT_2019.zip
```

While upgrading on the remaining nodes, Oracle Trace File Analyzer cannot see the nodes already upgraded until the configuration is synchronized.

```
bash-3.2# /u01/app/12.1.0/grid/bin/tfactl print status

.----------------------------------------------------------------------
--------.
| Host   | Status   | PID | Port | Version    |     Build ID         |
Inventory|
+--------+---------+-----+------+------------+---------------------
+----------+
| sales3 | RUNNING | 9   | 5000 | 12.1.2.4.2 | 12124220150629072212 |
COMPLETE |
'--------+---------+-----+------+------------+---------------------
+----------'
```

For nodes, on which the application of Release Update Revision (RUR) was not completed within the 24 hour waiting period to become part of Oracle Trace File Analyzer configuration:

1. Run the synchronize script from a node that has the keys already generated
2. Manually copy the SSL configuration to those nodes

In our example from *sales1*:

```
/u01/app/12.1.0/grid/tfa/sales1/tfa_home/bin/synctfanodes.sh
Current Node List in TFA :
sales1
sales2
sales3
sales4

Node List in Cluster :
sales1 sales2 sales3 sales4

Node List to sync TFA Certificates :
1 sales2
2 sales3
3 sales4

Do you want to update this node list? [Y|N] [N]: Y
```

```
Please Enter all the nodes you want to sync...

Enter Node List (seperated by space) : sales2 sales4

Syncing TFA Certificates on sales2 :

TFA_HOME on sales2 : /u01/app/12.1.0/grid/tfa/sales2/tfa_home

Copying TFA Certificates to sales2...
Copying SSL Properties to sales2...
Shutting down TFA on sales2...
Sleeping for 5 seconds...
Starting TFA on sales2...

Syncing TFA Certificates on sales4 :

TFA_HOME on sales4 : /u01/app/12.1.0/grid/tfa/sales4/tfa_home

Copying TFA Certificates to sales4...
Copying SSL Properties to sales4...
Shutting down TFA on sales4...
Sleeping for 5 seconds...
Starting TFA on sales4...

Successfully re-started TFA..

.-----------------------------------------------------------------------------
----.
| Host   | Status  | PID   | Port |   Version  |      Build ID        |
Inventory|
+--------+---------+-------+------+------------+----------------------
+----------+
| sales1 | RUNNING | 4390  | 5000 | 12.1.2.4.2 | 12124220150629072212 |
COMPLETE |
| sales2 | RUNNING | 23604 | 5000 | 12.1.2.4.2 | 12124220150629072212 |
COMPLETE |
| sales3 | RUNNING | 28653 | 5000 | 12.1.2.4.2 | 12124220150629072212 |
COMPLETE |
| sales4 | RUNNING | 5989  | 5000 | 12.1.2.4.2 | 12124220150629072212 |
COMPLETE |
'--------+---------+-------+------+------------+----------------------
+----------'
```

Note:

The node list was changed to only the nodes that needed the keys synchronized, *sales2* and *sales4*.

In this case, it’s fine to synchronize *sales3* as it would have received the same files and restart Oracle Trace File Analyzer.

I know that not all nodes are upgraded at the same time. I do not want to wait 24 hours for Oracle Trace File Analyzer to sync the key files. What do I do?

Use the synchronize script to force Oracle Trace File Analyzer to generate and synchronize certificates. While running, the script prompts if you wish to generate SSL configuration files and then synchronizes them to the remote nodes.

For example:

```
-bash-3.2# /u01/app/12.1.0/grid/tfa/sales1/tfa_home/bin/synctfanodes.sh

Current Node List in TFA :
sales1
sales2
sales3
sales4

TFA has not yet generated any certificates on this Node.

Do you want to generate new certificates to synchronize across the
nodes? [Y|N] [Y]:

Generating new TFA Certificates...

Restarting TFA on sales1...
Shutting down TFA
TFA-00002 : Oracle Trace File Analyzer (TFA) is not running
TFA Stopped Successfully
. . . . .
. . .
Successfully shutdown TFA..
Starting TFA..
Waiting up to 100 seconds for TFA to be started..
. . . . .
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands

Node List in Cluster :
sales1 sales2 sales3 sales4

Node List to sync TFA Certificates :
1 sales2
2 sales3
3 sales4

Do you want to update this node list? [Y|N] [N]:
```

After the key files are generated and synchronized, on each node you must find the files as follows:

```
# ls -al /u01/app/12.1.0/grid/tfa/sales1/tfa_home/client.jks
```

```
-rwx------   1 root     root    3199 Jun 30 14:12 /u01/app/12.1.0/grid/tfa/
sales1/tfa_home/client.jks

# ls -al /u01/app/12.1.0/grid/tfa/sales1/tfa_home/server.jks

-rwx------   1 root     root    3201 Jun 30 14:12 /u01/app/12.1.0/grid/tfa/
sales1/tfa_home/server.jks

# ls -al /u01/app/12.1.0/grid/tfa/sales1/tfa_home/internal/ssl.properties

-rwx------   1 root     root    220 Jun 30 14:12 /u01/app/12.1.0/grid/tfa/
sales1/tfa_home/internal/ssl.properties
```

Readable only by `root`, `ownership:group` of `root`. The checksum for each file must match on all nodes.

8.1.8 OSWatcher Parameters are Different After a Reboot or Otherwise Unexpectedly Different

When Oracle Trace File Analyzer manages OSWatcher, after an installation or a reboot, OSWatcher is started as a non-privileged user such as:

- `grid` on Oracle RAC systems
- `oracle` on non-Oracle RAC systems

Oracle does not recommend stopping and restarting OSWatcher as `root`.

For example:

```
tfactl oswbb stop

tfactl start oswbb 20 72 (interval of 20 seconds and retention of 72 hours)
```

OSWatcher is then run as `root` until it is stopped and re-started as `oracle` or `grid`, or there is a reboot. In either case, the parameters are persisted in a property file. OSWatcher defaults (30,48) are used unless other parameters are specified for interval and retention period. Beginning with Oracle Trace File Analyzer version 12.1.2.5.2, an OSWatcher property file is maintained for each user. Each time OSWatcher is started, the parameters for interval or retention hours are made persistent for that user. In earlier versions, if the OSWatcher startup parameters are different than expected, then it is because OSWatcher was stopped and started as `root` with different parameters. These settings would have persisted across reboots because there was only one properties file.

In 12.1.2.5.2 and above, if there is a reboot, then OSWatcher must always be brought up using the parameters from the properties of `oracle` or `grid`. The OSWatcher startup parameters are different if OSWatcher is stopped and re-started as `root` with different parameters before a reboot. The parameters fetched from the `root` properties must not take effect after a reboot. The parameters must revert to the parameters of `oracle` properties.

The parameters are different and the persistent settings are changed because Oracle Support would have recommended different settings to investigate an issue. In that case, stop, and re-start OSWatcher with the normal parameters as a non-privileged user.

```
tfactl oswbb stop

tfactl start oswbb (in this case the default interval of 30 seconds
and retention of 48 hours would be persisted)
```

> **Note:**
>
> If OSWatcher is installed and running, and not managed by Oracle Trace File Analyzer, then Oracle Trace File Analyzer defers to that installation and parameters. When listing the `oswbb` tool status, the status must be **NOT RUNNING**, that is, not managed by Oracle Trace File Analyzer.

8.1.9 Oracle Trace File Analyzer Installation or Oracle Trace File Analyzer Discovery (tfactl rediscover) Fails on Linux 7

Description: Reported errors are similar to:

```
Can't locate Data/Dumper.pm in @INC (@INC contains: /usr/local/lib64/
perl5
/usr/local/share/perl5 /usr/lib64/perl5/vendor_perl
/usr/share/perl5/vendor_perl /usr/lib64/perl5 /usr/share/perl5 .
/u01/app/12.1.0/grid/tfa/dc75orarac02/tfa_home/bin
/u01/app/12.1.0/grid/tfa/dc75orarac02/tfa_home/bin/common
/u01/app/12.1.0/grid/tfa/dc75orarac02/tfa_home/bin/modules
/u01/app/12.1.0/grid/tfa/dc75orarac02/tfa_home/bin/common/exceptions)
at
/u01/app/12.1.0/grid/tfa/dc75orarac02/tfa_home/bin/common/
tfactlshare.pm line 545.
```

Cause: This error occurs due to Bug 21790910 and Bug 22393355, which are fixed in Oracle Trace File Analyzer version 12.1.2.6.4.

Action: Link the operating system Perl to the version of Perl in the `GRID_HOME`.

8.1.10 OSWatcher Analyzer Fails When OSWatcher is Not Running from the TFA_HOME

Description: Reported errors are similar to:

```
tfactl> oswbb
Error: Cannot find OSWatcher files under
/u01/app/grid/tfa/repository/suptools//oswbb//archive
```

```
OSWatcher analyzer commands are supported only when it is running from
TFA_HOME
```

Cause: Expected behavior when OSWatcher is not running from `TFA_HOME`.

Action:

1. Stop and disable the OSWatcher version running outside of Oracle Trace File Analyzer.
2. Start OSWatcher from within Oracle Trace File Analyzer.

8.1.11 Oracle Trace File Analyzer Fails to Start with com.sleepycat.je.EnvironmentLockedException Java Exception

Description: Reported errors found in the Oracle Trace File Analyzer `syserrorout` log located in `$TFA_BASE//log` are:

```
/u01/app/oracle/tfa//log$ cat syserrorout.08.06.2015-16.19.54

Exception in thread "TFAMain" com.sleepycat.je.EnvironmentLockedException:
(JE 5.0.84)
/u01/app/oracle/tfa//database/BERKELEY_JE_DB The environment cannot be
locked for single writer access.
ENV_LOCKED: The je.lck file could not be locked. Environment is invalid and
must be closed.
at com.sleepycat.je.log.FileManager.(FileManager.java:368)
at com.sleepycat.je.dbi.EnvironmentImpl.(EnvironmentImpl.java:483)
at com.sleepycat.je.dbi.EnvironmentImpl.(EnvironmentImpl.java:409
```

Cause: The root cause is unknown.

Action:

1. Check if there are any processes accessing the BDB.

   ```
   # fuser $GI_BASE/tfa//database/BERKELEY_JE_DB/je.lck
   ```

2. If a process is returned, then kill it.

   ```
   # kill -9
   ```

3. Remove the `$GI_BASE/tfa//database/BERKELEY_JE_DB/je.lck` file.

   ```
   # rm -rf $GI_BASE/tfa//database/BERKELEY_JE_DB/je.lck
   ```

4. Start Oracle Trace File Analyzer.

   ```
   # $TFA_HOME/bin/tfactl start
   ```

8.1.12 Oracle Trace File Analyzer Startup Fails When Solution-Soft Time Machine Software is Installed, but Not Running on the System

Action: Uninstall the Time Machine software.

8.1.13 Non-privileged User is Not Able to Run tfactl Commands

Description:

As root verify that the non-privileged user has Oracle Trace File Analyzer privilege to run the tfactl commands.

```
]# tfactl access lsusers
.---------------------------------.
|  TFA Users in node1            |
+-----------+-----------+---------+
| User Name | User Type | Status  |
+-----------+-----------+---------+
| oracle    | USER      | Allowed |
'-----------+-----------+---------'

.---------------------------------.
|  TFA Users in node2              |
+-----------+-----------+---------+
| User Name | User Type | Status  |
+-----------+-----------+---------+
| oracle    | USER      | Allowed |
'-----------+-----------+---------'
```

If the user is listed and the status is displayed as **Disabled**, then that indicates all non-privileged user access has been disabled.

Action:

If the user, for example, oracle is not listed, then add oracle.

```
tfactl access add -user oracle
```

If none of the above techniques resolve the problem, then run tfactl diagnosetfa -local. Upload the resultant file to Oracle Support.

8.1.14 Oracle Trace File Analyzer Daemon is Not Starting or Not Running?

Description:

```
TFA-00001: Failed to start Oracle Trace File Analyzer (TFA) daemon

TFA-00002: Oracle Trace File Analyzer (TFA) is not running
```

The errors indicate that Java does not start.

Action:

1. Verify that Oracle Trace File Analyzer is not running.

   ```
   ps -ef|grep -i tfa
   ```

   > **Note:**
   >
   > On some operating systems, the `ps` command truncates the output at 80 characters. The `ps` command does not display the process even if it is running.

2. To confirm that the Oracle Trace File Analyzer daemon is not running, run the following command run as `root`.

   ```
   # tfactl print status
   ```

   ```
   TFA-00002 Oracle Trace File Analyzer (TFA) is not running
   ```

3. Try starting the Oracle Trace File Analyzer daemon as `root`.

   ```
   # tfactl start
   Starting TFA..
   Waiting up to 100 seconds for TFA to be started..
   . . . . .
   . . . . .
   . . . . .
   . . . . .
   . . . . .
   . . . . .
   Successfully started TFA Process..
   . . . . .
   TFA Started and listening for commands
   ```

   If Oracle Trace File Analyzer still fails to start, then run `tfactl diagnosetfa -local`. Upload the resultant file to Oracle Support.

8.1.15 Oracle Trace File Analyzer Is Not Collecting Diagnostic Traces of Components Such As CRS, DB, ASM, and So On

Description: When Oracle Trace File Analyzer is unable to collect diagnostic traces of components such as CRS, DB, ASM, and so on, verify that the Grid Infrastructure base and diagnostic directories have been added to AHF by running the `tfactl print directories` command. If they are not added, try adding them using the `tfactl directory add <dir>` command. If the command errors out as, '`<dir> is not a valid directory to add to TFA`', then it indicates that AHF considers the directory in question invalid and, therefore, is not adding it to TFA.

Cause: AHF does not discover and inventory some standard directories where the system files, secured files, data files are placed because AHF considers them as invalid files.

Action: The `root` or `admin` user can add the required sub-directories. It is recommended not to add the entire directory to AHF using the `-force` option in the `tfactl directory add` command, `tfactl directory add <dir> -force`, and rerun diagnostic collection.

8.1.16 Oracle Trace File Analyzer Fails to Start

Description: Oracle Trace File Analyzer fails to start and logs the following exception message in the `tfa_main.trc` file.

```
Exception in isPortAvailable - sdx b.9q23g87y6y: Address already in use: NET_Bind
java.net.BindException: Address already in use: NET_Bind
```

Cause: Oracle Trace File Analyzer is not able to start because the reserved ports, 5000 to 5005 are already used by other processes.

Action: Update the `data_dir/internal/port.txt` file with the port number available, and then run the `tfactl start` command.

8.2 Troubleshooting Compliance Framework (Oracle Orachk and Oracle Exachk)

Follow the steps explained in this section to troubleshoot and fix Compliance Framework (Oracle Orachk / Oracle Exachk) related issues.

- How to Troubleshoot Oracle Orachk and Oracle Exachk Issues
  Follow these steps to fix the Oracle Orachk and Oracle Exachk related issues.
- How to Capture Debug Output
  Follow these procedures to capture debug information.
- Error Messages or Unexpected Output
  Follow these steps to troubleshoot and fix error messages and unexpected output.
- Operating System Is Not Discovered Correctly
  Oracle ORAchk and Oracle EXAchk display this message if the tools are not able to detect the operating system.
- Oracle Clusterware or Oracle Database is not Detected or Connected Issues
  Follow the procedures in this section to troubleshoot and fix Oracle Clusterware or Oracle Database issues.
- Remote Login Problems
  If Oracle Orachk and Oracle Exachk have problem locating and running SSH or SCP, then the tools cannot run any remote checks.
- Permission Problems
  You must have sufficient directory permissions to run Oracle Orachk and Oracle Exachk.
- Slow Performance, Skipped Checks, and Timeouts
  Follow these procedures to fix slow performance and other issues.
- Running Compliance Checks on a Subset of Oracle Home and Oracle Databases
  Use the `-dbconfig` command when Oracle Orachk and Oracle Exachk are not able to discover `ORACLE_HOME`, or the name of the Oracle Database and you have

multiple `ORACLE_HOME`s in a system and each home is running multiple Oracle Databases.

- SSH Connection Timeout
- Oracle Exachk Prompts to Enter Names of RoCE Fabric Switches
- Unable to Implement CA Certificates in Oracle Trace File Analyzer

8.2.1 How to Troubleshoot Oracle Orachk and Oracle Exachk Issues

Follow these steps to fix the Oracle Orachk and Oracle Exachk related issues.

1. Ensure that you are using the correct tool.

   If you have an Oracle Engineered System other than Oracle Database Appliance, then use Oracle Exachk. For all other systems, use Oracle Orachk.

2. Ensure that you are using the latest versions of Oracle Orachk and Oracle Exachk.

   New versions are released every three months.

   a. Check the version using the `-v` option.

   ```
   $ orachk -v
   ```

   ```
   $ exachk -v
   ```

   b. Compare your version with the latest version available here:

      i. For Oracle Orachk, refer to My Oracle Support note 2550798.1.

      ii. For Oracle Exachk, refer to My Oracle Support note 1070954.1.

3. Check the **FAQ** for similar problems in My Oracle Support note 1070954.1.

4. Review files within the `log` directory.

   a. Check applicable `error.log` files for relevant errors.

   This file contains `stderr` output captured during the run, not everything you see in here will mean you have a problem, but if you have a problem this may give more information.

   - *`output_dir`*`/log/orachk _error.log`
   - *`output_dir`*`/log/exachk _error.log`

   b. Check applicable log for other relevant information.

   - *`output_dir`*`/log/orachk.log`
   - *`output_dir`*`/log/exachk.log`

5. Review My Oracle Support notes for similar problems.

6. For Oracle Orachk issues, check My Oracle Support Community (MOSC).

7. If necessary capture debug output, log a new SR and attach the resulting `zip` file.

Related Topics

- Output Files and Directories
  Oracle Orachk and Oracle Exachk create an output directory that contains various files for you to examine.

- How to Capture Debug Output
  Follow these procedures to capture debug information.
- https://support.oracle.com/rs?type=doc&id=2550798.1
- https://support.oracle.com/rs?type=doc&id=1070954.1
- My Oracle Support Community (MOSC)

8.2.2 How to Capture Debug Output

Follow these procedures to capture debug information.

1. Before enabling debug, reproduce the problem with the least run necessary.
   - Debug captures a lot, the resulting `zip` file can be large so try to narrow down the amount of run necessary to reproduce the problem.
     Use relevant command line options to limit the scope of checks.
2. Enable debug.

   If you are running the tool in on-demand mode, then use `-debug` argument.

   If the problem area is known, then debug can be constrained to a particular module by including the `-module` argument too.

   ```
   $ orachk -debug [-module [ setup | discovery | execution |
   output ] ]
   ```

   ```
   $ exachk -debug [-module [ setup | discovery | execution |
   output ] ]
   ```

   When debug is enabled, Oracle Orachk and Oracle Exachk create a new debug log file in:

   - *output_dir*/log/orachk _debug_*date_stamp_time_stamp*.log
   - *output_dir*/log/exachk _debug_*date_stamp_time_stamp*.log

   The *output_dir* directory retains a number of other temporary files used during health checks.

   If you run health checks using the daemon, then restart the daemon with the `-d start -debug` option.

   Running this command generates both debug for daemon and include debug in all client runs:

   ```
   $ orachk -d start -debug
   ```

   ```
   $ exachk -d start -debug
   ```

When debug is run with the daemon, Oracle Orachk and Oracle Exachk create a daemon debug log file in the directory the daemon was started:

```
orachk_daemon_debug.log
```

```
exachk_daemon_debug.log
```

3. Collect the resulting output `zip` file, and the daemon debug log file if applicable.

Related Topics

- Controlling the Scope of Checks
  Use the list of commands to control the scope of checks.

8.2.3 Error Messages or Unexpected Output

Follow these steps to troubleshoot and fix error messages and unexpected output.

- Data Entry Terminal Considerations
- Tool Runs without Producing Files
- Messages similar to “line ****: **** Killed $perl_cmd 2>> $ERRFIL?”
- Messages similar to “RC-001- Unable to read driver files”
- Messages similar to “There are prompts in user profile on [hostname] which will cause issues in [tool] successful execution”
- Problems Related to Remote Login
- Other Error Messages in orachk_error.log or exachk_error.log
- Space available on {node_name} at {path} is {x} MB and required space is 500 MB
- Running Oracle Orachk on Microsoft Windows Throws '{oratab}' is empty Error

8.2.3.1 Data Entry Terminal Considerations

Description:

Use any supported UNIX and Linux terminal type (character mode terminal, ILOM, VNC server) to run Oracle Orachk and Oracle Exachk.

Respond to the prompts during interactive runs, or while configuring the daemon.

Each terminal type has advantages and disadvantages. The effect of a dropped network connection varies based on the terminal type used.

For example, in an interactive run using a character mode terminal, if all the prompts are answered before the network drop, then the running process completes successfully even if the network connection drops. If the network connection drops before all the input prompts are answered, then all the running processes hang. Clean up the hung processes manually when the network connection is restored.

Using a remote connection to a VNC server running on the database where Oracle Orachk and Oracle Exachk are running minimizes the network drop interruptions.

If you use accessibility software or devices that prevent the use of a VNC server, and experience network drops, then contact your system administrator to determine the root cause and adjust the environment as necessary.

For example, if an accessibility aid inserts suspensions and restarts the interactive process running Oracle Orachk and Oracle Exachk lead to an operating system timeout due to terminal inactivity. Lengthen the inactivity timeouts of the environment before running the commands.

The timeout caused by an assistive tool at the operating system level due to terminal inactivity is not specific to Oracle Orachk and Oracle Exachk. The timeout could happen to any process managed by the assistive technology.

8.2.3.2 Tool Runs without Producing Files

Description:

Oracle Orachk and Oracle Exachk create temporary files and directories at runtime, as well as output files for data collection.

If you cancel Oracle Orachk using Ctrl+C or if Oracle Orachk fails due to an error, then Oracle Orachk cleans up the files that Oracle Orachk created while running.

If Oracle Orachk or Oracle Exachk completes health check runs, but did not generate output files, then there is an error probably near the end of the run that caused an ungraceful exit.

Action:

If the problem persists, then run the tool again in debug mode and examine the output. If necessary, contact Oracle Support for assistance.

Related Topics

- How to Capture Debug Output
  Follow these procedures to capture debug information.

8.2.3.3 Messages similar to “line ****: **** Killed $perl_cmd 2>> $ERRFIL?”

Description:

Oracle Orachk and Oracle Exachk have a built-in `watchdog` process that monitors and kills the commands that exceed default timeouts to prevent hangs.

Cause:

Killing a command results in `“line ****: **** Killed $perl_cmd 2>> $ERRFIL?”` error.

Related Topics

- Slow Performance, Skipped Checks, and Timeouts
  Follow these procedures to fix slow performance and other issues.

8.2.3.4 Messages similar to “RC-001- Unable to read driver files”

Description:

There are a number of possible causes related to not having a supported platform or not being able to read or write into temporary, working or installation directories.

Oracle Orachk and Oracle Exachk display the same error message also as, `RC-002- Unable to read driver files`

Action:

1. Verify that you are running on a supported platform.
2. Verify that there is sufficient diskspace available in the temporary or output directory. If necessary increase disk space or direct temporary and output files elsewhere.
3. Verify the hidden subdirectory `.cgrep` exists within the install location. This directory contains various support files some of which are platform-specific.
4. Verify that you are able to write into and read out of the temporary and working directory location.

Related Topics

- Scope and Supported Platforms for Running Oracle Exachk on Oracle Big Data Appliance
  Oracle Exachk for Oracle Big Data Appliance supports all Oracle Big Data Appliance versions later than 2.0.1.
- Output Files and Directories
  Oracle Orachk and Oracle Exachk create an output directory that contains various files for you to examine.
- Permission Problems
  You must have sufficient directory permissions to run Oracle Orachk and Oracle Exachk.

8.2.3.5 Messages similar to “There are prompts in user profile on [hostname] which will cause issues in [tool] successful execution”

Description:

Oracle Orachk and Oracle Exachk exit if the tools detect prompts in the user profile.

Oracle Orachk and Oracle Exachk fetch the user environment files on all nodes. If the user environment files contain prompts, for example, `read -p`, or other commands that pause the running commands, then the commands timeout. The commands timeout because there is no way to respond to the messages when it is being called.

All such commands cannot be detected in the environment. However, the commands that can be detected lead to this message.

Action:

Comment all such prompts from the user profile file (at least temporarily) and test run again.

8.2.3.6 Problems Related to Remote Login

Action:

If you see messages similar to `No such file or directory` or `/usr/bin/scp -q: No such file or directory`, then refer to *Remote Login Problems* to fix the issues.

Related Topics

- Remote Login Problems
  If Oracle Orachk and Oracle Exachk have problem locating and running SSH or SCP, then the tools cannot run any remote checks.

8.2.3.7 Other Error Messages in orachk_error.log or exachk_error.log

Description:

When examining the `orachk_error.log` , some messages are expected and they are not indicative of problems. These errors are redirected and absorbed into the `error.log` to keep them from being reported on the screen.

For example, an error similar to the following is reported numerous times, once for each Oracle software home for each node:

```
/bin/sh: /u01/app/11.2.0/grid/OPatch/opatch: Permission denied
chmod: changing permissions of `/u01/app/oracle_ebs/product/11.2.0.2/
VIS_RAC/.patch_storage': Operation not permitted
OPatch could not open log file, logging will not be possible
Inventory load failed... OPatch cannot load inventory for the given Oracle Home.
```

These types of errors occur in role-separated environments when the tool runs as the Oracle Database software owner uses `Opatch` to list the patch inventories of homes that are owned by Oracle Grid Infrastructure or other Oracle Database home owners. When you run `Opatch` to list the patch inventories for other users, `Opatch` fails because the current user does not have permissions on the other homes. In these cases, the `Opatch` error is ignored and the patch inventories for those homes are gathered by other means. To avoid such errors, Oracle recommends that you run Oracle Orachk and Oracle Exachk as `root` in role-separated environments.

Action:

You do not need to report these types of errors to Oracle Support.

Also, ignore the errors similar to the following:

```
orachk: line [N]: [: : integer expression expected
```

The line number changes over time. However, the error indicates that the tool was expecting an integer return value and no value was found. The value was null that the shell was not able to compare the return values. The error is repeated many times for the same command, once for each node.

8.2.3.8 Space available on {node_name} at {path} is {x} MB and required space is 500 MB

Description:

Oracle Orachk displays an error message when there is no enough space in the location for temporary files and directories.

```
Space available on at /users/oracle is 441 MB and required space is 500 MB
Please make at least mentioned space available at above location and retry to
continue.[y/n][y]?
```

Cause:

Oracle Orachk creates temporary files and directories during execution. The default location for temporary files and directories is the `$HOME` directory of the user who runs the tool.

Action:

To change the location of Oracle Orachk temporary files set the `RAT_TMPDIR` environment variable to the new location before running Oracle Orachk.

Related Topics

- Temporary Files and Directories
  While running compliance checks, Oracle Orachk and Oracle Exachk create temporary directories and files for the purposes of data collection and assessment, and then delete them upon completion of compliance check runs.

8.2.3.9 Running Oracle Orachk on Microsoft Windows Throws '{oratab}' is empty Error

Description:

Running Oracle Orachk commands throws the following error:

```
'{oratab}' is empty.
Verify Oracle database registry entries name in '{regout}' in case Oracle database is
install.
If Oracle database registry entries name does not contains 'ORA'/'OH'
then set registry key patterns using 'RAT_KEY_DB' environment variable.
```

Cause:

1. Oracle Database is not present on the system.
2. The keyword for Oracle Database registry key is different. Generally the registry key contains `ORA` or `OH`, but on some systems it can be different. Set the environment variable `RAT_KEY_DB` to the right Oracle Database registry keyword.
3. The initialization parameter file `initSID.ora` is missing from `$ORACLE_HOME/database`.
   Oracle Orachk looks for the `initSID.ora` file in `$ORACLE_HOME/database` for getting the instance name. If the `initSID.ora` file is not present, then you will encounter the aforementioned error.

Action:

Specify Oracle Database details using the `-dbconfig` option.

```
orachk -dbconfig db_home_path%db_name
```

8.2.4 Operating System Is Not Discovered Correctly

Oracle ORAchk and Oracle EXAchk display this message if the tools are not able to detect the operating system.

Cause:

If Oracle ORAchk and Oracle EXAchk are not able to detect the operating system, then the tools prompt:

- Data needed for the derived platform could not be found
- Improperly detecting an unsupported platform

Action:

Set the `RAT_OS` environment variable to the correct operating system:

```
$ export RAT_OS=platform
```

8.2.5 Oracle Clusterware or Oracle Database is not Detected or Connected Issues

Follow the procedures in this section to troubleshoot and fix Oracle Clusterware or Oracle Database issues.

- Oracle Clusterware Software is Installed, but Cannot be Found
- Oracle Database Software Is Installed, but Cannot Be Found
- Oracle Database Software Is Installed, but Version cannot Be Found
- Oracle ASM Software is Installed, but Cannot be Found
- Oracle Database Discovery Issues on Oracle Real Application Clusters (Oracle RAC) Systems
- Oracle Database Login Problems

8.2.5.1 Oracle Clusterware Software is Installed, but Cannot be Found

Description:

Oracle Orachk discovers the location of the Oracle Clusterware home from the `oraInst.loc` and `oraInventory` files.

Cause:

Oracle Clusterware discovery fails due to:

- Problems discovering the `oraInst.loc` and `oraInventory` files
- Problems with the `oraInst.loc` and `oraInventory` files
- One or more paths in the `oraInst.loc` and `oraInventory` files are incorrect

Action:

1. Ensure that the `oraInst.loc` file is located correctly and is properly formed.
   If the file is not in the default location, then set the `RAT_INV_LOC` environment variable to point to the `oraInventory` directory:

   ```
   $ export RAT_INV_LOC=oraInventory directory
   ```

2. If necessary, set the RAT_CRS_HOME environment variable to point to the location of the Oracle Clusterware home:

```
$ export RAT_CRS_HOME=CRS_HOME
```

8.2.5.2 Oracle Database Software Is Installed, but Cannot Be Found

Description:

Oracle Orachk and Oracle Exachk display this message if the tools cannot find the Oracle Database software installed.

Action:

If the Oracle Database software is installed, but Oracle Orachk and Oracle Exachk cannot find, then set the RAT_ORACLE_HOME environment variable to the applicable ORACLE_HOME directory.

For example, enter the following command, where *your-oracle-home* is the path to the Oracle home on your system:

```
$ export RAT_ORACLE_HOME=your-oracle-home
```

Oracle Orachk and Oracle Exachk perform best practice and recommended patch checks for all the databases running from the home specified in the RAT_ORACLE_HOME environment variable.

8.2.5.3 Oracle Database Software Is Installed, but Version cannot Be Found

Description:

Oracle Orachk and Oracle Exachk display this message if the tools cannot find the version of the Oracle Database software installed.

Action:

If Oracle Orachk and Oracle Exachk cannot find the correct version, then set the RAT_DB environment variable to the applicable version.

For example:

```
$ export RAT_DB=11.2.0.3.0
```

8.2.5.4 Oracle ASM Software is Installed, but Cannot be Found

Description:

Oracle Orachk and Oracle Exachk display this message if the tools cannot find the Oracle ASM software installed.

Action:

If Oracle Orachk and Oracle Exachk cannot find Oracle ASM, then set the `RAT_ASM_HOME` environment variable to the applicable home directory.

```
$ export RAT_ASM_HOME=ASM_HOME
```

8.2.5.5 Oracle Database Discovery Issues on Oracle Real Application Clusters (Oracle RAC) Systems

Description:

On Oracle Real Application Clusters (Oracle RAC) systems, Oracle Orachk discovers the database resources registered in the Oracle Cluster Registry.

The `ORACLE_HOME` for the database resources is derived from the profile of the database resources.

Cause:

If there is a problem with any of the profiles of the database resources, then Oracle Orachk cannot recognize or connect to one or more databases. Use the `-dbnames` option temporarily to fix the problem.

Action:

Specify the names of the database in a comma-delimited list as follows:

```
$ orachk -dbnames ORCL,ORADB
```

Alternatively, use the space-delimited environment variable `RAT_DBNAMES`:

```
$ export RAT_DBNAMES="ORCL ORADB"
```

Use double quotes to specify more than one database.

> **Note:**
>
> Configure the `RAT_DBHOMES` environment variable if you,
>
> - Configure `RAT_DBNAMES` as a subset of databases registered in the Oracle Clusterware
> - Want to check the patch inventories of ALL databases found registered in the Oracle Clusterware for recommended patches
>
> By default, the recommended patch analysis is limited to the homes for the list of databases specified in the `RAT_DBNAMES` environment variable.
>
> To perform the recommended patch analysis for additional database homes, specify space-delimited list of all database names in the `RAT_DBHOMES` environment variable.
>
> For example:
>
> ```
> export RAT_DBNAMES="ORCL ORADB"
> ```
>
> ```
> export RAT_DBHOMES="ORCL ORADB PROD"
> ```
>
> Best practice checks are applied to `ORACL` and `ORADB`.
>
> Recommended patch checks are applied to `ORACL`, `ORADB`, and `PROD`.

Related Topics

- Running Compliance Checks on a Subset of Oracle Home and Oracle Databases
  Use the `-dbconfig` command when Oracle Orachk and Oracle Exachk are not able to discover `ORACLE_HOME`, or the name of the Oracle Database and you have multiple `ORACLE_HOME`s in a system and each home is running multiple Oracle Databases.

8.2.5.6 Oracle Database Login Problems

Oracle Database login problems arise if you run Oracle Orachk and Oracle Exachk without sufficient privileges. If you run Oracle Orachk and Oracle Exachk as a user other than the database software installation owner, `root` or `grid`, and if you experience problems connecting to the database, then perform the following steps:

1. Log in to the system as `grid` (operating system).
2. Run `export ORACLE_HOME=`*`path of Oracle database home`*
3. Run `export ORACLE_SID=`*`database SID`*
4. Run `export PATH=$ORACLE_HOME/bin:$ORACLE_HOME/lib:$PATH`
5. Add alias in the `$ORACLE_HOME/network/admin/tnsnames.ora` file for*`database SID`*.
6. Connect to the database using `$ORACLE_HOME/bin/sqlplus "sys@`*`SID`*` as sysdba"`, and enter the password.
7. Ensure that you have a successful connection.

If this method of connecting to the database does not work, then Oracle Orachk and Oracle Exachk do not connect either.

- If you have multiple homes owned by different users and you are not able to login to the target database as the user running Oracle Orachk independently in SQL*Plus, then Oracle Orachk does not login either.
- If the operating system authentication is not set up, then it should still prompt you for user name and password.

8.2.6 Remote Login Problems

If Oracle Orachk and Oracle Exachk have problem locating and running SSH or SCP, then the tools cannot run any remote checks.

Also, the `root` privileged commands do not work if:

- Passwordless remote `root` login is not permitted over SSH
- Expect utility is not able to pass the `root` password

1. Verify that the SSH and SCP commands can be found.
   - The SSH commands return the error, `No such file or directory`, if SSH is not located where expected.
     Set the `RAT_SSHELL` environment variable pointing to the location of SSH. Note that you cannot export the `RAT_SSHELL` environment variable, set it in the `conf_file`. For more information, see *Running Generic Compliance Framework (Oracle Orachk and Oracle Exachk) Commands*.
   - The SCP commands return the error, `/usr/bin/scp -q: No such file or directory`, if SCP is not located where expected.
     Set the `RAT_SCOPY` environment variable pointing to the location of SCP. Note that you cannot export the `RAT_SCOPY` environment variable, set it in the `conf_file`. For more information, see *Running Generic Compliance Framework (Oracle Orachk and Oracle Exachk) Commands*.
2. Verify that the user you are running as, can run the following command manually from where you are running Oracle Orachk and Oracle Exachk to whichever remote node is failing.

   ```
   $ ssh root@remotehostname "id"
   root@remotehostname's password:
   uid=0(root) gid=0(root)
   groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
   ```

   - If you face any problems running the command, then contact the systems administrators to correct temporarily for running the tool.
   - Oracle Orachk and Oracle Exachk search for the prompts or traps in remote user profiles. If you have prompts in remote profiles, then comment them out at least temporarily and test run again.
   - If you can configure passwordless remote `root` login, then edit the `/etc/ssh/sshd_config` file as follows:

     ```
     n to yes
     ```

Now, run the following command as `root` on all nodes of the cluster:

```
hd restart
```

3. Enable Expect debugging.
   - Oracle Orachk uses the Expect utility when available to answer password prompts to connect to remote nodes for password validation. Also, to run `root` collections without logging the actual connection process by default.
   - Set environment variables to help debug remote target connection issues.
     - **`RAT_EXPECT_DEBUG`**: If this variable is set to `-d` , then the Expect command tracing is activated. The trace information is written to the standard output.
       For example:

       ```
       export RAT_EXPECT_DEBUG=-d
       ```

     - **`RAT_EXPECT_STRACE_DEBUG`**: If this variable is set to `strace`, `strace` calls the Expect command. The trace information is written to the standard output.
       For example:

       ```
       export RAT_EXPECT_STRACE_DEBUG=strace
       ```

   - By varying the combinations of these two variables, you can get three levels of Expect connection trace information.

> **Note:**
>
> Set the `RAT_EXPECT_DEBUG` and `RAT_EXPECT_STRACE_DEBUG` variables only at the direction of Oracle support or development. The `RAT_EXPECT_DEBUG` and `RAT_EXPECT_STRACE_DEBUG` variables are used with other variables and user interface options to restrict the amount of data collected during the tracing. The `script` command is used to capture standard output.

As a temporary workaround while you resolve remote problems, run reports local on each node then merge them together later.

On each node, run:

```
orachk -local
```

```
exachk -local
```

Then merge the collections to obtain a single report:

```
orachk -merge zipfile 1  zip file 2 > zip file 3 > zip file ...
```

```
exachk -merge zipfile 1  zip file 2 > zip file 3 > zip file ...
```

Related Topics

- Running Generic Compliance Framework (Oracle Orachk and Oracle Exachk) Commands
  Review the list of generic Oracle Orachk and Oracle Exachk command options.

8.2.7 Permission Problems

You must have sufficient directory permissions to run Oracle Orachk and Oracle Exachk.

1. Verify that the permissions on the tools scripts `orachk` and `exachk` are set to `755` `(-rwxr-xr-x)`.

   If the permissions are not set, then set the permissions as follows:

   ```
   $ chmod 755 orachk
   ```

   ```
   $ chmod 755 exachk
   ```

2. If you install Oracle Orachk and Oracle Exachk as `root` and run the tools as a different user, then you may not have the necessary directory permissions.

   ```
   [root@randomdb01 exachk]# ls -la
   total 14072
   drwxr-xr-x  3 root root    4096 Jun  7 08:25 .
   drwxrwxrwt 12 root root    4096 Jun  7 09:27 ..
   drwxrwxr-x  2 root root    4096 May 24 16:50 .cgrep
   -rw-rw-r--  1 root root 9099005 May 24 16:50 collections.dat
   -rwxr-xr-x  1 root root  807865 May 24 16:50 exachk
   -rw-r--r--  1 root root 1646483 Jun  7 08:24 exachk.zip
   -rw-r--r--  1 root root    2591 May 24 16:50 readme.txt
   -rw-rw-r--  1 root root 2799973 May 24 16:50 rules.dat
   -rw-r--r--  1 root root     297 May 24 16:50 UserGuide.txt
   ```

- If Oracle Clusterware is installed, then:
  - Install Oracle Exachk in `/opt/oracle.SupportTools/exachk` as the Oracle Grid Infrastructure home owner
  - Install Oracle Orachk in `CRS_HOME/suptools/orachk` as the Oracle Grid Infrastructure home owner
- If Oracle Clusterware is not installed, then:
  - Install Oracle Exachk in `/opt/oracle.SupportTools/exachk` as `root`
  - Install Oracle Orachk (in a convenient location) as `root` (if possible)
    or

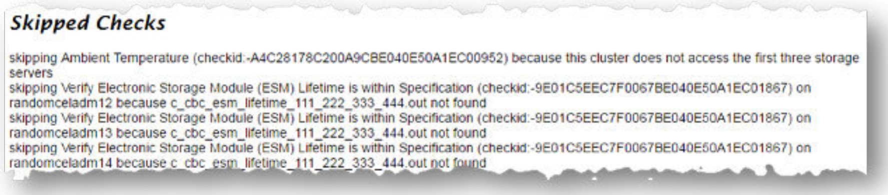
    Install Oracle Orachk (in a convenient location) as Oracle software install user or Oracle Database home owner

8.2.8 Slow Performance, Skipped Checks, and Timeouts

Follow these procedures to fix slow performance and other issues.

When Oracle Orachk and Oracle Exachk run commands, a child process is spawned to run the command and a watchdog daemon monitors the child process. If the child process is slow or hung, then the watchdog kills the child process and the check is registered as skipped:

Figure 8-1 Skipped Checks



Skipped Checks

```
skipping Ambient Temperature (checkid:-A4C28178C200A9CBE040E50A1EC00952) because this cluster does not access the first three storage
servers
skipping Verify Electronic Storage Module (ESM) Lifetime is within Specification (checkid:-9E01C5EEC7F0067BE040E50A1EC01867) on
randomceladm12 because c_cbc_esm_lifetime_111_222_333_444.out not found
skipping Verify Electronic Storage Module (ESM) Lifetime is within Specification (checkid:-9E01C5EEC7F0067BE040E50A1EC01867) on
randomceladm13 because c_cbc_esm_lifetime_111_222_333_444.out not found
skipping Verify Electronic Storage Module (ESM) Lifetime is within Specification (checkid:-9E01C5EEC7F0067BE040E50A1EC01867) on
randomceladm14 because c_cbc_esm_lifetime_111_222_333_444.out not found
```

The `watchdog.log` file also contains entries similar to **killing stuck command**.

Depending on the cause of the problem, you may not see skipped checks.

1. Determine if there is a pattern to what is causing the problem.
   - EBS checks, for example, depend on the amount of data present and may take longer than the default timeout.
   - If there are prompts in the remote profile, then remote checks timeout and be killed and skipped. Oracle Orachk and Oracle Exachk search for prompts or traps in the remote user profiles. If you have prompts in remote profiles, then comment them out at least temporarily, and test run again.
2. Increase the default timeout.
   - You override the default timeouts by setting the environment variables.

Table 8-1 Timeout Controlling

Timeout Controlling	Default Value (seconds)	Environment Variable
Collection of all checks not run by `root` (most). Specify the timeout value for individual checks.	Varies per check.	`RAT_{`*`CHECK-ID`*`}_TIMEOUT`
General timeout for all checks	90	`RAT_TIMEOUT`

Table 8-1 (Cont.) Timeout Controlling

Timeout Controlling	Default Value (seconds)	Environment Variable
SSH login DNS handshake. Specify the time in seconds for checking passwords on the remote nodes.	1	`RAT_PASSWORDCHECK_TIMEOUT`

- The default timeouts are lengthy enough for most cases. If it is not long enough, then it is possible you are experiencing a system performance problem that should be corrected. Many timeouts can be indicative of a non-Oracle Orachk and Oracle Exachk problem in the environment.

3. If you can not increase the timeout, then try excluding problematic checks running separately with a large enough timeout and then merging the reports back together.

4. If the problem does not appear to be down to slow or skipped checks but you have a large cluster, then try increasing the number of slave processes users for parallel database run.

   - Database collections are run in parallel. The default number of slave processes used for parallel database run is calculated automatically. You can change the default number using the options:`-dbparallel` *`slave processes`*, or `-dbparallelmax`
     The higher the parallelism the more resources are consumed. However, the elapsed time is reduced. You can raise or lower the number of parallel slaves beyond the default value. After the entire system is brought up after maintenance, but before the users are permitted on the system, use a higher number of parallel slaves to finish a run as quickly as possible.

     On a busy production system, use a number less than the default value yet more than running in serial mode to get a run more quickly with less impact on the running system.

     Turn off the parallel database run using the `-dbserial` option.

Related Topics

- Using Profiles with Oracle Autonomous Health Framework
  Profiles are logical groupings of related checks. These related checks are grouped by a particular role, a task, or a technology.
- Excluding Individual Checks
  Excluding checks is recommended in situations where you have reviewed all check output and determined a particular check is not relevant for some particular business reason.
- Merging Reports
  Merging reports is useful in role-separated environments where different users are run different subsets of checks and then you want to view everything as a whole.

8.2.9 Running Compliance Checks on a Subset of Oracle Home and Oracle Databases

Use the `-dbconfig` command when Oracle Orachk and Oracle Exachk are not able to discover `ORACLE_HOME`, or the name of the Oracle Database and you have multiple `ORACLE_HOME`s in a system and each home is running multiple Oracle Databases.

Syntax

```
orachk -dbconfig dbhome%dbname(s)[,dbhome%dbname(s)]
```

```
exachk -dbconfig dbhome%dbname(s)[,dbhome%dbname(s)]
```

Specify a comma-delimited list of Oracle Database homes with corresponding Oracle Database names to run health checks only on a subset of Oracle Databases. Oracle Orachk and Oracle Exachk do not prompt you for database selection while running.

Separate the Oracle Database home and the corresponding Oracle Database names with `%`. Specify the list of Oracle Database names associated with a particular Oracle Database home with `:`.

```
orachk -dbconfig dbhome%dbname:dbname:...[,dbhome%dbname:dbname:...]
```

```
exachk -dbconfig dbhome%dbname:dbname:...[,dbhome%dbname:dbname:...]
```

Example 8-1 Limiting Health Checks to a Subset of Oracle Home and Oracle Databases

```
orachk -dbconfig dbhome1%dbname
orachk -dbconfig dbhome1%dbname1:dbname2
orachk -dbconfig dbhome1%dbname1:dbname2,dbhome2%dbname3:dbname4
```

8.2.10 SSH Connection Timeout

Description: SSH connection time out as follows:

```
Select databases from list for checking best practices. For multiple
databases, select 4 for All or comma separated number like 1,2 etc [1-5][4].
Searching out ORACLE_HOME for selected databases.
.   .   .   .   .   .   .   .   .   .
.   .   .   .   .   .   .   .   .   Connection to scag11adm02 closed by remote host.
```

Action: Set `ServerAliveInterval` to *30* in the `/etc/ssh/ssh_config` file on the machine from where Oracle EXAchk run started.

8.2.11 Oracle Exachk Prompts to Enter Names of RoCE Fabric Switches

Description: Oracle Exachk prompts you to enter RoCE switch names each time it's run in an Exadata X8M or higher multi-rack environment.

Action: Add a list of RoCE fabric leaf and spine switches to the `switches.out` file, and then run Oracle Exachk.

For example:

```
# exachk -showdatadir
/u01/app/grid/oracle.ahf/data/scaqan07adm01/exachk/user_root/output
# vi /u01/app/grid/oracle.ahf/data/scaqan07adm01/exachk/user_root/
output/switches.out
<<add switches>>
# cat /u01/app/grid/oracle.ahf/data/scaqan07adm01/exachk/user_root/
output/switches.out
scaqan07sw-rocea0
scaqan07sw-roceb0
```

Even if you have created a file with a list of switches, you can still pass the `-switches` argument to not to read from that file. Specify a comma-delimited list of switch names to run `exachk` on specific switches.

For example:

```
# exachk -switches switch1,switch2,...
```

If you do not provide a list of switches, then `exachk` prompts you to provide it.

```
MyTestPrompt>
MyTestPrompt> exachk
Enter RDMA Network Fabric switch names delimited by comma or skip
switches using -excludeprofile switch option. (eg
switch1,switch2,switch3):
```

To exclude switches from `exachk` running on them, specify a list of comma-delimited list of switches:

```
-excludeprofile -switches switch1,switch2,...
```

8.2.12 Unable to Implement CA Certificates in Oracle Trace File Analyzer

Description: After implementing `TFAMain` starts but ends up in client server SSL socket exceptions errors when running `tfactl` commands.

Cause: Combining both `intermediate.pem` and `server.pem` file into the `caroot.cert.txt` file results in `Empty server certificate chain error`.

Action: Split the `caroot.cert.txt` file into `intermediate.pem` and `server.pem` using the command `openssl x509 -in cerfile.cer -noout -text`, and then follow the keytool steps again.

1.
   ```
   keytool -importkeystore -destkeystore server.p12 -deststoretype pkcs12 -
   srckeystore serverCert.pfx
   ```

2.
   ```
   keytool -v -importkeystore -srckeystore server.p12 -srcstoretype PKCS12 -
   destkeystore server_ac.jks -deststoretype JKS
   ```

3.
   ```
   keytool -v -importkeystore -srckeystore server.p12 -srcstoretype PKCS12 -
   destkeystore client_ac.jks -deststoretype JKS
   ```

4.
   ```
   keytool -list -keystore client_ac.jks
   Enter keystore pswrd:
   Keystore type: jks
   Keystore provider: SUN

   Your keystore contains 1 entry

   1, Nov 30, 2021, PrivateKeyEntry,
   Certificate fingerprint (SHA1):
   59:BA:C8:94:97:48:9C:6C:11:23:36:F9:46:A1:1C:87:67:F7:84:19

   Warning:
   The JKS keystore uses a proprietary format. It is recommended to migrate
   to PKCS12 which is an industry standard format using "keytool -
   importkeystore -srckeystore client_ac.jks -destkeystore client_ac.jks -
   deststoretype pkcs12".
   ```

5.
   ```
   # keytool -list -keystore server_ac.jks
   Enter keystore pswrd:
   Keystore type: jks
   Keystore provider: SUN

   Your keystore contains 1 entry

   1, Nov 30, 2021, PrivateKeyEntry,
   Certificate fingerprint (SHA1):
   59:BA:C8:94:97:48:9C:6C:11:23:36:F9:46:A1:1C:87:67:F7:84:19

   Warning:
   The JKS keystore uses a proprietary format. It is recommended to migrate
   to PKCS12 which is an industry standard format using "keytool -
   importkeystore -srckeystore server_ac.jks -destkeystore server_ac.jks -
   deststoretype pkcs12".
   ```

6.
   ```
   keytool -import -v -alias server-ca -file server.cert.pem -keystore
   client_ac.jks
   ```

7.
   ```
   keytool -import -v -alias client-ca -file server.cert.pem -keystore
   server_ac.jks
   ```

8.
   ```
   keytool -importcert -trustcacerts -alias inter -file
   intermediate.cert.pem -keystore server_ac.jks
   ```

9.
   ```
   keytool -list -keystore server_ac.jks
   Enter keystore pswrd:
   Keystore type: jks
   Keystore provider: SUN

   Your keystore contains 3 entries

   inter, Nov 30, 2021, trustedCertEntry,
   Certificate fingerprint (SHA1):
   F6:E3:AA:60:E0:D0:80:69:12:72:06:E0:FA:62:7A:EB:54:38:11:55
   client-ca, Nov 30, 2021, trustedCertEntry,
   Certificate fingerprint (SHA1):
   59:BA:C8:94:97:48:9C:6C:11:23:36:F9:46:A1:1C:87:67:F7:84:19
   1, Nov 30, 2021, PrivateKeyEntry,
   Certificate fingerprint (SHA1):
   59:BA:C8:94:97:48:9C:6C:11:23:36:F9:46:A1:1C:87:67:F7:84:19

   Warning:
   The JKS keystore uses a proprietary format. It is recommended to
   migrate to PKCS12 which is an industry standard format using
   "keytool -importkeystore -srckeystore server_ac.jks -destkeystore
   server_ac.jks -deststoretype pkcs12"
   ```

10.
    ```
    # keytool -list -keystore client_ac.jks
    Enter keystore pswrd:
    Keystore type: jks
    Keystore provider: SUN

    Your keystore contains 2 entries

    1, Nov 30, 2021, PrivateKeyEntry,
    Certificate fingerprint (SHA1):
    59:BA:C8:94:97:48:9C:6C:11:23:36:F9:46:A1:1C:87:67:F7:84:19
    server-ca, Nov 30, 2021, trustedCertEntry,
    Certificate fingerprint (SHA1):
    59:BA:C8:94:97:48:9C:6C:11:23:36:F9:46:A1:1C:87:67:F7:84:19

    Warning:
    The JKS keystore uses a proprietary format. It is recommended to
    migrate to PKCS12 which is an industry standard format using
    "keytool -importkeystore -srckeystore client_ac.jks -destkeystore
    client_ac.jks -deststoretype pkcs12".
    ```

9
Command Line Reference

9.1 Running the Installer Script

Run the installer script to install Oracle Autonomous Health Framework or to just extract the content of the installer package.

9.1.1 Oracle Autonomous Health Framework Installation Command-Line Options

Understand the options that you can supply to the Oracle Autonomous Health Framework installer script to customize the installation.

The Oracle Autonomous Health Framework installer script:

- Takes you through an interview process if you do not specify any installation parameters.
- Appends `/oracle.ahf` to `-ahf_loc` if it does not already exist.
- Appends `/oracle.ahf/data` to `-data_dir` if it does not already exist.

- Writes the log to the `/tmp/ahf_install_timestamp.log` file, for example, `/tmp/ahf_install_9263_2018_09_25-07_55_52.log`.

Syntax

```
ahf_setup
[-ahf_loc AHF Location]
[-data_dir AHF Repository]
[-nodes node1,node2]
[-extract[orachk|exachk|-notfasetup]]
[-force]
[-local]
[-silent]
[-tmp_loc directory]
[-debug [-level 1-6]]
```

Parameters

Table 9-1   ahf_setup Command Parameters

Parameter	Description
`-ahf_loc`	Specify the installation directory. Ensure that this directory exists before trying this option.
`-data_dir`	Specify the data directory where Oracle Autonomous Health Framework stores all the collections, metadata, and so on. Ensure that this directory exists before trying this option.
`-nodes`	By default, Oracle Autonomous Health Framework is installed on all the cluster nodes. Specify a comma-delimited list of nodes where you want to install AHF.
`-extract`	Extracts the files from the installer. This option is default for non-root users. Specify the `-notfasetup` option just to extract and not to configure Oracle Trace File Analyzer. **Note:** • You cannot use the `-extract` option as `root` to extract Oracle Trace File Analyzer binaries. • For `-extract`, only the install user must run AHF commands for the given installation. Run the `ahf_setup -extract [exachk|orachk]` command to install a local copy of Oracle ORAchk or Oracle EXAchk without installing the rest of AHF.

Table 9-1 (Cont.) ahf_setup Command Parameters

Parameter	Description
`-force`	The `-force` option is applicable only when you specify the compliance type `orachk` or `exachk` with the `–extract` option else the installer script ignores the `–force` option. `-extract orachk|exachk`
`-local`	Installs only on the local node.
`-silent`	Use this option for the Oracle Autonomous Health Framework installer script not to prompt any installation questions. If you use `-silent` option, then ensure that you use `–data_dir` option. The installer script fails if you do not use `-data_dir` option.
`-tmp_loc`	Specify a temporary location for the Oracle Autonomous Health Framework installer script to extract the install archive. Ensure that this directory exists before trying this option. Default: `/tmp`.
`-perlhome`	Specify a custom location for Perl binaries.
`-debug`	Debugs the Oracle Autonomous Health Framework installer script.
`-level`	Specify the Oracle Autonomous Health Framework Install debug level. Default `4` with option `-debug`. • `1` - FATAL • `2` - ERROR • `3` - WARNING • `4` - INFO • `5` - DEBUG • `6` - TRACE

Understanding the Location of the Data Directory

- If you install Oracle Autonomous Health Framework using the `-data_dir` option, then the installer script uses the location that you specify. The installer script will not create the specified data directory so ensure that this directory exists before trying the `-data_dir` option. You can specify a new data directory either under the current Oracle Trace File Analyzer install location or under a different directory.
- If you install Oracle Autonomous Health Framework using the `-silent` option, then ensure that you use the `-data_dir` option, otherwise, the installer script will fail.
- If you install Oracle Autonomous Health Framework without the `-data_dir` option, then the installer script will list all possible options:
  - Oracle Autonomous Health Framework installation location (`-ahf_loc`) if the free space is more than 5 GB

  - Oracle Trace File Analyzer repository if installed outside the Oracle Grid Infrastructure Home
  - Directory one level above the Oracle Grid Infrastructure Base
  - Option to enter a different directory
- If you do not use the `-silent` option and do not specify `-ahf_loc` and `-data_dir`, then the installer script displays the default options for you to confirm.

  For example:

```
# /tmp/ahf_setup -nodes node1

AHF Installation Log : /tmp/
ahf_install_15992_2019_10_10-08_07_38.log

Starting Autonomous Health Framework (AHF) Installation

AHF Version: 193000 Build Date: 201910100757

Default AHF Location : /opt/oracle.ahf

Do you want to update default AHF Location ? Y|[N] :

AHF Location : /opt/oracle.ahf

Choose Data Directory from below options :

1. /u01/app [Free Space : 6742 MB]
2. Enter a different Location

Choose Option [1 - 2] : 1

AHF Data Directory : /u01/app/oracle.ahf/data

Do you want to add AHF Notification Email IDs ? [Y]|N : n

Extracting AHF to /opt/oracle.ahf
```

9.2 AHFCTL Command Reference

Review the list of AHFCTL commands to manage Autonomous Health Framework.

- Running AHFCTL Commands to Manage EMail Configuration for All AHF Tools
- Running AHFCTL Update Commands to Automatically Patch Oracle Autonomous Health Framework
- Running AHFCTL Update Commands to Apply AHF Metadata and Framework Updates
- Running AHFCTL Upgrade Commands to Upgrade Oracle Autonomous Health Framework
  You need `root` access to run `getupgrade`, `setupgrade`, `unsetupgrade`, and `upgrade` commands.

- Running AHFCTL Upload Commands to Upload Diagnostics
  You need `root` access to `ahfctl`, or `sudo` access to run `setupload`, `getupload`, `checkupload`, and `unsetupload` commands.
- Running AHFCTL Commands to Manage the Scheduler for Oracle Autonomous Health Framework Components
  You need `root` access to `ahfctl`, or `sudo` access to run `startahf`, `stopahf`, and `statusahf` commands.
- Running AHFCTL Commands to Manage Cell, Switches, Databases and exacli Passwords
  You need `root` access to `ahfctl`, or `sudo` access to run `checkpassword`, `setpassword`, and `unsetpassword` commands.
- Running AHFCTL Commands to Get the Repository Locations of Oracle Autonomous Health Framework Components
  You need `root` access to `ahfctl`, or `sudo` access to run `showrepo` command.
- Running AHFCTL Commands to Import Oracle Orachk or Oracle Exachk Wallet Details into Oracle Autonomous Health Framework Wallet and Configuration
  You need `root` access to `ahfctl`, or `sudo` access to run `import` command.
- Running AHFCTL Commands to Limit CPU and Memory Usage
  You need `root` access to `ahfctl`, or `sudo` access to run `getresourcelimit`, `setresourcelimit`, `unsetresourcelimit` commands.
- Running AHFCTL Commands to Collect Storage Server Diagnostic Package
  You need `root` access to `ahfctl`, or `sudo` access to run `celldiagcollect` command.
- Running AHFCTL Commands to Manage Service Upload Parameters
  You need `root` access to `ahfctl`, or `sudo` access to run `getserviceupload`, `setserviceupload`, and `unsetserviceupload` commands.
- AHFCTL Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options
  Review the list of commands that you can use to run compliance checks on Oracle Engineered and non-engineered systems.
- Running AHFCTL Commands to Sanitize Sensitive Information and Reverse Map Sanitized Elements
  Use `ahftcl redact` to sanitize sensitive data in regular files, zip files and directories, and `ahfctl rmap` to reverse map the elements sanitized using Oracle Trace File Analyzer and Oracle ORAchk.
- Running AHFCTL Commands to Manage InfiniBand and RoCE Switches
  Use the `ahfctl` commands to manage InfiniBand and RoCE switches.
- Running AHFCTL Commands to Uninstall AHF
  Use the `ahfctl` commands to uninstall AHF.

9.2.1 Running AHFCTL Commands to Manage EMail Configuration for All AHF Tools

- ahfctl setsmtp
  Use the `ahfctl setsmtp` command to set the SMTP mail configuration parameters.
- ahfctl getsmtp
  Use the `ahfctl getsmtp` command to query the SMTP mail configuration parameters.

- ahfctl checksmtp
  Use the `ahfctl checksmtp` command to check the stored SMTP mail configuration parameters.
- ahfctl unsetsmtp
  Use the `ahfctl unsetsmtp` command to unset the SMTP mail configuration parameters that you have set. AHF is installed with default SMTP configurations. You can use the `ahfctl unsetsmtp` command to unset these default parameters as well.
- ahfctl sendmail
  Use the `ahfctl sendmail` command to send a test email to verify SMTP configuration.

9.2.1.5 ahfctl sendmail

Use the `ahfctl sendmail` command to send a test email to verify SMTP configuration.

Syntax

```
ahfctl sendmail
[-h]
[-to TO]
[-cc CC]
[-bcc BCC]
[-subject SUBJECT]
[-body BODY]
[-attachment ATTACHMENT]
```

Parameter	Description
`-to` *`TO`*	Specify the recipient email address.
`-cc` *`CC`*	Specify the email address to send a carbon copy of the email.
`-bcc` *`BCC`*	Specify the email address to send a blind carbon copy of the email
`-subject` *`SUBJECT`*	Specify to add email subject.
`-body` *`BODY`*	Specify to add body of the email.
`-attachment` *`ATTACHMENT`*	Specify to add an attachment.

Example 9-1

- To send an email to recipients with default/set parameters:

  ```
  ahfctl sendmail
  ```

- To send an email with attachment:

```
ahfctl sendmail -to toaddress@company.com -attachment <path_to_file>
```

```
ahfctl sendmail -to $ORACLE_USER@oracle.com -attachment /tmp/
test_email.log
Mail has sent successfully to  oradb@oracle.com
```

9.2.1.1 ahfctl setsmtp

Use the `ahfctl setsmtp` command to set the SMTP mail configuration parameters.

Syntax

```
ahfctl setsmtp
[-h]
[-debug]
[-all]
[-host HOST]
[-user USER]
[-password]
[-from FROM]
[-to TO]
[-port PORT]
[-cc CC]
[-bcc BCC]
[-ssl SSL]
[-auth AUTH]
```

Parameters

Table 9-2 ahfctl setsmtp Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-all`	Specify to set all `smtp` parameters.
`-host` *`HOST`*	Specify the name of the SMTP server, for example, *smtphostname*.
`-user` *`USER`*	Specify the name of the SMTP user, for example, *smtpuser*.
`-password`	Specify the password of the SMTP user.
`-from` *`FROM`*	Specify the email address of the sender.
`-to` *`TO`*	Specify the email address of the recipient.
`-port` *`PORT`*	Specify the port of the SMTP server, for example, *44*.
`-cc` *`CC`*	Specify the CC email address.
`-bcc` *`BCC`*	Specify the BCC email address.
`-ssl` *`SSL`*	Specify `true` to enable SSL and `false` to disable SSL. Default: `false`.
`-auth` *`AUTH`*	Specify `true` to enable SMTP authentication and `false` to disable SMTP authentication. Default: `false`.

Example 9-2 ahfctl setsmtp

To set all the SMTP parameters:

```
ahfctl setsmtp -user smtpuser -from ahfteam@example.com -to
touser@example.com -port 24 -password
```

To set only the `to` email address:

```
ahfctl setsmtp -to toaddress@example.com
```

If you see the `Parameter smtp.to is already set` message, then run the `unsetsmtp` command to clear the existing `smtp.to` configuration followed by the `setsmtp` command to configure `smtp.to` anew.

```
ahfctl setsmtp -to <email@id>
Parameter smtp.to is already set


ahfctl unsetsmtp -to
Unset SMTP parameters completed successfully.


ahfctl setsmtp -to <email>
Set SMTP parameters completed successfully.
```

9.2.1.2 ahfctl getsmtp

Use the `ahfctl getsmtp` command to query the SMTP mail configuration parameters.

Syntax

```
ahfctl getsmtp
[-h]
[-debug]
[-all]
[-host]
[-user]
[-password]
[-from]
[-to]
[-port]
[-cc]
[-bcc]
[-ssl]
[-auth]
```

Parameters

Table 9-3 ahfctl getsmtp Command Parameters

Parameter	Description
`-debug`	Specify to query if debugging is enabled or not
`-all`	Specify to query all `smtp` parameters.
`-host` *`HOST`*	Specify to query the name of the SMTP server.
`-user` *`USER`*	Specify to query the name of the SMTP user,
`-password`	Specify to query the password of the SMTP user.
`-from` *`FROM`*	Specify to query the email address of the sender.
`-to` *`TO`*	Specify to query the email address of the recipient.
`-port` *`PORT`*	Specify to query the port of the SMTP server.
`-cc` *`CC`*	Specify to query the CC email address.
`-bcc` *`BCC`*	Specify to query the BCC email address.
`-ssl` *`SSL`*	Specify to query if SSL is enabled or not.
`-auth` *`AUTH`*	Specify to query if authentication is enabled or not.

Example 9-3 ahfctl getsmtp

To query all of the SMTP parameters:

```
ahfctl getsmtp -all
```

To query the SMTP server configuration for from email address:

```
ahfctl getsmtp -to
```

9.2.1.3 ahfctl checksmtp

Use the `ahfctl checksmtp` command to check the stored SMTP mail configuration parameters.

Syntax

```
ahfctl checksmtp
[-h]
[-debug]
[-to TO]
[-attachment ATTACHMENT]
```

Parameters

Table 9-4   ahfctl checksmtp Command Parameters

Parameter	Description
`-debug`	Specify to check if debugging is enabled or not.
`-to` *`TO`*	Specify to check the email address of the recipient.
`-attachment` *`ATTACHMENT`*	Specify to check the mail attachment, for example, *`ahf_report.log`*.

Example 9-4   ahfctl checksmtp

To check the stored SMTP parameters:

```
ahfctl checksmtp
```

To check the stored SMTP parameters with the specified recipient email address:

```
ahfctl checksmtp -to toaddress@example.com
```

9.2.1.4 ahfctl unsetsmtp

Use the `ahfctl unsetsmtp` command to unset the SMTP mail configuration parameters that you have set. AHF is installed with default SMTP configurations. You can use the `ahfctl unsetsmtp` command to unset these default parameters as well.

Syntax

```
ahfctl unsetsmtp
[-h]
[-debug]
[-all]
[-host]
[-user]
[-password]
[-from]
[-to]
[-port]
[-cc]
[-bcc]
[-ssl]
[-auth]
```

Parameters

Table 9-5   ahfctl unsetsmtp Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.

Table 9-5 (Cont.) ahfctl unsetsmtp Command Parameters

Parameter	Description
`-all`	Specify to unset all `smtp` parameters and the default SMTP mail configuration parameters as well.
`-host`	Specify the name of the SMTP server to unset.
`-user`	Specify the name of the SMTP user to unset.
`-password`	Specify the password of the SMTP user to unset.
`-from`	Specify the email address of the sender to unset.
`-to`	Specify the email address of the recipient to unset.
`-port`	Specify the port of the SMTP server to unset.
`-cc`	Specify the CC email address to unset.
`-bcc`	Specify the BCC email address to unset.
`-ssl`	Specify to unset SSL configuration.
`-auth`	Specify to unset auth configuration.

Example 9-5 ahfctl unsetsmtp

To unset all of the SMTP parameters

```
ahfctl unsetsmtp -all
```

To unset the from parameter:

```
ahfctl unsetsmtp -from
```

9.2.2 Running AHFCTL Update Commands to Automatically Patch Oracle Autonomous Health Framework

You need AHF install user privileges to run the `update`, `setupdate`, `getupdate`, and `unsetupdate` commands.

- ahfctl update
  Use the `ahfctl update` command to apply AHF updates automatically.
- ahfctl setupdate
  Use the `ahfctl setupdate` command to set update parameters.
- ahfctl getupdate
  Use the `ahfctl getupdate` command to get update parameters.
- ahfctl unsetupdate
  Use the `ahfctl unsetupdate` command to unset update parameters.
- How to Apply an Update
  Configure AHF to automatically download new compliance checks and SRDCs from MOS (My Oracle Support) or a REST Endpoint.

2.5.3.1.1 ahfctl update

Use the `ahfctl update` command to apply AHF updates automatically.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl update` command.

> **Caution:**
>
> Make sure to test the metadata on a pre-production system before copying the downloaded file to the production-mounted filesystem.
>
> 1. Configure automatic download on a staging server.
> 2. Test the downloaded metadata on a pre-production system.
> 3. Configure auto-update on all production systems.
> 4. Copy the test metadata zip on production mounted file systems to automatically apply the update.

Syntax

```
ahfctl update
[-h]
[-nomos]
[-debug]
```

Parameters

Table 9-6 ahfctl update Command Parameters

Parameter	Description
`-nomos`	Specify not to configure MOS.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-6 New AHF metadate update is available at software stage location

```
ahfctl update
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220607 from 20220516
Please copy ahf_data_20220607.zip and run the command 'ahfctl
applyupdate -updatefile ahf_data_20220607.zip' on the below mentioned
```

```
nodes
scao05adm08
```

Example 9-7 REST Endpoints parameters are configured and a new AHF metadata update is available at the REST Endpoint

```
ahfctl update
Applying AHF metedata update...
AHF update zip is not available at stage location /opt/rajeev
Upload configuration check for: ahf_update_loc.
Parameters are configured correctly to upload.
ahf_data_20220607.zip successfully downloaded at /opt/rajeev
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220607 from 20220601
Please copy ahf_data_20220607.zip and run the command 'ahfctl applyupdate -
updatefile ahf_data_20220607.zip' on the below mentioned nodes
scao05adm08
```

2.5.3.1.2 ahfctl setupdate

Use the `ahfctl setupdate` command to set update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl setupdate` command.

Syntax

```
ahfctl setupdate
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupdate AUTOUPDATE]
[-servicename SERVICENAME]
[-fstype FSTYPE]
[-frequency FREQUENCY]
```

Parameters

Table 9-7 ahfctl setupdate Command Parameters

Parameter	Description
`-all`	Specify to configure all parameters.
`-swstage` *`SWSTAGE`*	Specify the software stage location, for example, `/opt/oracle.ahf`.
`-autoupdate` *`AUTOUPDATE`*	Specify to enable or disable autoupdate. Default: `on`. Valid values: `on`| `off`.

Table 9-7 (Cont.) ahfctl setupdate Command Parameters

Parameter	Description
`-servicename` *`SERVICENAME`*	Specify the name of the REST download service. Default: `ahf_update_loc`.
`-fstype` *`FSTYPE`*	Specify the stage location file system type, for example, `nfs/acfs/local`.
`-frequency` *`FREQUENCY`*	Specify the autoupdate frequency in days in the range (1,30), for example, 15.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-8 Set update configuration

```
ahfctl setupdate -swstage /opt/oracle.ahf -autoupdate on
```

Example 9-9 Set all update parameters

```
ahfctl setupdate -all
Enter autoupdate flag <on/off> : on
Enter software stage location : /scratch/ahf_stage
Enter auto update frequency : 30
AHF autoupdate parameters successfully updated
Successfully synced AHF configuration
```

Example 9-10 Disable autoupdate

```
ahfctl setupdate -autoupdate off
AHF autoupdate parameters successfully updated
Successfully synced AHF configuration
```

2.5.3.1.3 ahfctl getupdate

Use the `ahfctl getupdate` command to get update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl getupdate` command.

Syntax

```
ahfctl getupdate
[-h]
[-all]
[-debug]
```

Parameters

Table 9-8 ahfctl getupdate Command Parameters

Parameter	Description
`-all`	Specify to get all parameters.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-11 Get all update parameters

```
ahfctl getupdate -all
autoupdate : on
autoupdate.swstage : /opt/oracle.ahf
autoupdate.frequency : 30
autoupdate.servicename : [not set]
autoupdate.fstype : [not set]
```

2.5.3.1.4 ahfctl unsetupdate

Use the `ahfctl unsetupdate` command to unset update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl unsetupdate` command.

Syntax

```
ahfctl setupdate
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupdate AUTOUPDATE]
[-servicename SERVICENAME]
[-fstype FSTYPE]
[-frequency FREQUENCY]
```

Parameters

Table 9-9 ahfctl setupdate Command Parameters

Parameter	Description
`-all`	Specify to unset all parameters.
`-swstage` *`SWSTAGE`*	Specify to unset the software stage location.
`-autoupdate` *`AUTOUPDATE`*	Specify to unset the autoupdate flag.

Table 9-9 (Cont.) ahfctl setupdate Command Parameters

Parameter	Description
`-servicename` *`SERVICENAME`*	Specify to uset the REST download service name.
`-fstype` *`FSTYPE`*	Specify to unset the stage location file system type.
`-frequency` *`FREQUENCY`*	Specify to unser the autoupdate frequency.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-12 Unset a single update parameter

```
ahfctl unsetupdate -swstage
Software stage location successfully removed
Successfully synced AHF configuration
```

Example 9-13 Unset all update configuration

```
ahfctl unsetupdate -all
AHF update parameters successfully removed
Successfully synced AHF configuration
```

2.5.3.1.5 How to Apply an Update

Configure AHF to automatically download new compliance checks and SRDCs from MOS (My Oracle Support) or a REST Endpoint.

1. Configure MOS credentials.

   For example:

   ```
   ahfctl setupload -name mosconf1 -type https
   Enter mosconf1.https.user : john.doe@acme.com
   Enter mosconf1.https.password :
   Enter mosconf1.https.url : https://transport.oracle.com/upload/issue
   ```

2. Configure auto update.

   For example:

   ```
   ahfctl setupdate -autoupdate on -swstage /my/staging/path -
   frequency 1
   ```

3. Apply update when you're ready.

   ```
   ahfctl update
   ```

9.2.2.1 ahfctl update

Use the `ahfctl update` command to apply AHF updates automatically.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl update` command.

> **Caution:**
>
> Make sure to test the metadata on a pre-production system before copying the downloaded file to the production-mounted filesystem.
>
> 1. Configure automatic download on a staging server.
> 2. Test the downloaded metadata on a pre-production system.
> 3. Configure auto-update on all production systems.
> 4. Copy the test metadata zip on production mounted file systems to automatically apply the update.

Syntax

```
ahfctl update
[-h]
[-nomos]
[-debug]
```

Parameters

Table 9-10 ahfctl update Command Parameters

Parameter	Description
`-nomos`	Specify not to configure MOS.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-14 New AHF metadate update is available at software stage location

```
ahfctl update
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220607 from 20220516
Please copy ahf_data_20220607.zip and run the command 'ahfctl applyupdate -
updatefile ahf_data_20220607.zip' on the below mentioned nodes
scao05adm08
```

Example 9-15 REST Endpoints parameters are configured and a new AHF metadata update is available at the REST Endpoint

```
ahfctl update
Applying AHF metedata update...
AHF update zip is not available at stage location /opt/rajeev
Upload configuration check for: ahf_update_loc.
Parameters are configured correctly to upload.
ahf_data_20220607.zip successfully downloaded at /opt/rajeev
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220607 from 20220601
Please copy ahf_data_20220607.zip and run the command 'ahfctl 
applyupdate -updatefile ahf_data_20220607.zip' on the below mentioned 
nodes
scao05adm08
```

9.2.2.2 ahfctl setupdate

Use the `ahfctl setupdate` command to set update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl setupdate` command.

Syntax

```
ahfctl setupdate
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupdate AUTOUPDATE]
[-servicename SERVICENAME]
[-fstype FSTYPE]
[-frequency FREQUENCY]
```

Parameters

Table 9-11 ahfctl setupdate Command Parameters

Parameter	Description
`-all`	Specify to configure all parameters.
`-swstage` *`SWSTAGE`*	Specify the software stage location, for example, `/opt/oracle.ahf`.
`-autoupdate` *`AUTOUPDATE`*	Specify to enable or disable autoupdate. Default: `on`. Valid values: `on|off`.

Table 9-11 (Cont.) ahfctl setupdate Command Parameters

Parameter	Description
`-servicename` *`SERVICENAME`*	Specify the name of the REST download service. Default: `ahf_update_loc`.
`-fstype` *`FSTYPE`*	Specify the stage location file system type, for example, `nfs/acfs/local`.
`-frequency` *`FREQUENCY`*	Specify the autoupdate frequency in days in the range (1,30), for example, 15.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-16 Set update configuration

```
ahfctl setupdate -swstage /opt/oracle.ahf -autoupdate on
```

Example 9-17 Set all update parameters

```
ahfctl setupdate -all
Enter autoupdate flag <on/off> : on
Enter software stage location : /scratch/ahf_stage
Enter auto update frequency : 30
AHF autoupdate parameters successfully updated
Successfully synced AHF configuration
```

Example 9-18 Disable autoupdate

```
ahfctl setupdate -autoupdate off
AHF autoupdate parameters successfully updated
Successfully synced AHF configuration
```

9.2.2.3 ahfctl getupdate

Use the `ahfctl getupdate` command to get update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl getupdate` command.

Syntax

```
ahfctl getupdate
[-h]
[-all]
[-debug]
```

Parameters

Table 9-12 ahfctl getupdate Command Parameters

Parameter	Description
`-all`	Specify to get all parameters.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-19 Get all update parameters

```
ahfctl getupdate -all
autoupdate : on
autoupdate.swstage : /opt/oracle.ahf
autoupdate.frequency : 30
autoupdate.servicename : [not set]
autoupdate.fstype : [not set]
```

9.2.2.4 ahfctl unsetupdate

Use the `ahfctl unsetupdate` command to unset update parameters.

> **Note:**
>
> You need AHF install user privileges to run the `ahfctl unsetupdate` command.

Syntax

```
ahfctl setupdate
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupdate AUTOUPDATE]
[-servicename SERVICENAME]
[-fstype FSTYPE]
[-frequency FREQUENCY]
```

Parameters

Table 9-13 ahfctl setupdate Command Parameters

Parameter	Description
`-all`	Specify to unset all parameters.
`-swstage` *`SWSTAGE`*	Specify to unset the software stage location.
`-autoupdate` *`AUTOUPDATE`*	Specify to unset the autoupdate flag.

Table 9-13 (Cont.) ahfctl setupdate Command Parameters

Parameter	Description
`-servicename` *`SERVICENAME`*	Specify to uset the REST download service name.
`-fstype` *`FSTYPE`*	Specify to unset the stage location file system type.
`-frequency` *`FREQUENCY`*	Specify to unser the autoupdate frequency.
`-debug`	Specify the `-debug` option to enable debugging.

Example 9-20 Unset a single update parameter

```
ahfctl unsetupdate -swstage
Software stage location successfully removed
Successfully synced AHF configuration
```

Example 9-21 Unset all update configuration

```
ahfctl unsetupdate -all
AHF update parameters successfully removed
Successfully synced AHF configuration
```

9.2.2.5 How to Apply an Update

Configure AHF to automatically download new compliance checks and SRDCs from MOS (My Oracle Support) or a REST Endpoint.

1. Configure MOS credentials.

   For example:

   ```
   ahfctl setupload -name mosconf1 -type https
   Enter mosconf1.https.user : john.doe@acme.com
   Enter mosconf1.https.password :
   Enter mosconf1.https.url : https://transport.oracle.com/upload/issue
   ```

2. Configure auto update.

   For example:

   ```
   ahfctl setupdate -autoupdate on -swstage /my/staging/path -frequency 1
   ```

3. Apply update when you're ready.

   ```
   ahfctl update
   ```

9.2.3 Running AHFCTL Update Commands to Apply AHF Metadata and Framework Updates

You need AHF install user privileges to run these commands.

Note:

To configure AHF auto-update refer to:

- ahfctl update
- ahfctl setupdate
- ahfctl getupdate
- ahfctl unsetupdate

- ahfctl applyupdate
  Use the `ahfctl applyupdate` command to update metadata and framework files on the local node from the `zip` file provided.
- ahfctl queryupdate
  Use the `ahfctl queryupdate` command to check if an update was applied. To get a list of all the metadata and framework updates applied, use the `-all` option. To query a metadata or framework update with a specific update ID, use the `-updateid` option.
- ahfctl rollbackupdate
  Use the `ahfctl rollbackupdate` command to rollback the updates with a specific update ID applied to the local node. If you do not specify the update ID, then AHF rolls back to the previous state by default.
- ahfctl deleteupdatebackup
  Use the `ahfctl deleteupdatebackup` command to delete the backup directories used for AHF update.

2.5.3.2.1 ahfctl applyupdate

Use the `ahfctl applyupdate` command to update metadata and framework files on the local node from the `zip` file provided.

Note:

- You need AHF install user privileges to run the `ahfctl applyupdate` command.
- You must apply metadata and framework updates to all cluster nodes.

Syntax

```
ahfctl applyupdate [-h] [-debug] [-updatefile UPDATEFILE]
```

Parameters

Table 9-14 ahfctl applyupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updatefile` *`UPDATEFILE`*	Specify the name of the `zip` file. The existing metadata and framework files will be replaced with the files in the `zip` file. Download the `zip` file from My Oracle Support note 2550798.1.

Example 9-22 ahfctl applyupdate

```
# ahfctl applyupdate -updatefile /tmp/ahf_data_20220203.zip
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220203 from 20211220
```

Related Topics

- https://support.oracle.com/epmos/faces/DocContentDisplay?id=2550798.1

2.5.3.2.2 ahfctl queryupdate

Use the `ahfctl queryupdate` command to check if an update was applied. To get a list of all the metadata and framework updates applied, use the `-all` option. To query a metadata or framework update with a specific update ID, use the `-updateid` option.

> **Note:**
>
> To verify if the metadata and framework updates were applied to all nodes in a cluster, run the `ahfctl queryupdate` command as the AHF install user on each cluster node.

Syntax

```
ahfctl queryupdate [-h] [-debug] [-updateid UPDATEID] [-all] [-json]
```

Parameters

Table 9-15 ahfctl queryupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.

Table 9-15 (Cont.) ahfctl queryupdate Command Parameters

Parameter	Description
`-updateid` *`UPDATEID`*	To query framework update with a specific update ID. Specify `-updateid` *`UPDATEID`* option to query framework updates. **Note:** To query metadata updates, please use the `-all` option.
`-all`	Lists all applied metadata and framework updates.
`-json`	Specify this option to get the output in JSON format.

Example 9-23 ahfctl queryupdate

```
# ahfctl queryupdate -all
AHF Metadata Update: 20220203
Status: Applied
Applied on: Fri Feb 4 00:47:00 2022


# ahfctl queryupdate -all
AHF Framework update: PATCH_22.2.4.1
Status: Applied
Fixes: 34716496
Applied on: Wed Nov 30 15:14:56 2022
```

34716496 is the updateid for AHF framework update applied.

```
ahfctl queryupdate -updateid 34716496
AHF Framework update: PATCH_22.2.4.1
Status: Applied
Fixes: 34716496
Applied on: Wed Nov 30 15:14:56 2022
1:53
AHF framework updated files:
/opt/oracle.ahf/ahf/lib/ahfcomponents.py
/opt/oracle.ahf/ahf/lib/ahfctl.py
/opt/oracle.ahf/exachk/messages/framework_messages.json
/opt/oracle.ahf/exachk/lib/ahf_metadata.py
```

2.5.3.2.3 ahfctl rollbackupdate

Use the `ahfctl rollbackupdate` command to rollback the updates with a specific update ID applied to the local node. If you do not specify the update ID, then AHF rolls back to the previous state by default.

> **Note:**
>
> To rollback the metadata and framework updates applied to all nodes in a cluster, you must run the `ahfctl rollbackupdate` command as the AHF install user on each cluster node.

Syntax

```
ahfctl rollbackupdate [-h] [-debug] [-updateid UPDATEID]
```

Parameters

Table 9-16   ahfctl rollbackupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	Specify update ID, for example, Bug ID, Build ID, that you want to rollback.

Example 9-24   ahfctl rollbackupdate

```
# ahfctl rollbackupdate -updateid 20220203
Data files with timestamp 20220203 identified. Rolling back the files to
Production version 20211220
Rolled back the data files 20220203 to Production version 20211220
```

2.5.3.2.4 ahfctl deleteupdatebackup

Use the `ahfctl deleteupdatebackup` command to delete the backup directories used for AHF update.

> **Note:**
>
> - To delete the backup directories on all nodes in a cluster, you must run the `ahfctl deleteupdatebackup` command as the AHF install user on each cluster node.
> - You must not delete the backup directories randomly. Oracle recommends deleting the backup directories in the same order the updates were applied. If you delete the backup directories associated with a specific timestamp, then you will not be able to roll back to the state before the updates with that specific timestamp were applied.
> - Upgrading AHF using the `ahf_setup` script automatically deletes the backup directories of the previous AHF versions.
> - Oracle recommended to delete the AHF update backup directories only when there's a need to free up space on the system. You cannot delete the AHF update backup directory of the current running timestamp/update because once the backup directory is deleted for the specific timestamp, rolling back the update to specific timestamp/update is not possible.
>   For example: AHF Updates applied in order is: 20230901 -> 20231001 -> 20231101 (Current latest update). You can delete update backups for 20230901 and 20231001 but not the 20231101.

Syntax

```
ahfctl deleteupdatebackup [-h] [-debug] [-updateid UPDATEID] [-silent]
```

Parameters

Table 9-17 ahfctl deleteupdatebackup Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	Deletes the backup directories with the specified timestamp.
`-silent`	Skips user confirmation for delete backup directories.

Example 9-25 ahfctl deletebackup

```
# ahfctl deleteupdatebackup -updateid 20220130
Deleted metadata backup directory for: /opt/oracle.ahf/data/
work/.exachk_patch_directory/.20220130_metadata_bkp
```

9.2.3.1 ahfctl applyupdate

Use the `ahfctl applyupdate` command to update metadata and framework files on the local node from the `zip` file provided.

> **Note:**
>
> - You need AHF install user privileges to run the `ahfctl applyupdate` command.
> - You must apply metadata and framework updates to all cluster nodes.

Syntax

```
ahfctl applyupdate [-h] [-debug] [-updatefile UPDATEFILE]
```

Parameters

Table 9-18 ahfctl applyupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updatefile` *`UPDATEFILE`*	Specify the name of the `zip` file. The existing metadata and framework files will be replaced with the files in the `zip` file. Download the `zip` file from My Oracle Support note 2550798.1.

Example 9-26 ahfctl applyupdate

```
# ahfctl applyupdate -updatefile /tmp/ahf_data_20220203.zip
Updated file /opt/oracle.ahf/exachk/.cgrep/collections.dat
Updated file /opt/oracle.ahf/exachk/rules.dat
Updated file /opt/oracle.ahf/exachk/.cgrep/versions.dat
Updated file /opt/oracle.ahf/exachk/messages/check_messages.json
Data files updated to 20220203 from 20211220
```

Related Topics

- https://support.oracle.com/epmos/faces/DocContentDisplay?id=2550798.1

9.2.3.2 ahfctl queryupdate

Use the `ahfctl queryupdate` command to check if an update was applied. To get a list of all the metadata and framework updates applied, use the `-all` option. To query a metadata or framework update with a specific update ID, use the `-updateid` option.

> **Note:**
>
> To verify if the metadata and framework updates were applied to all nodes in a cluster, run the `ahfctl queryupdate` command as the AHF install user on each cluster node.

Syntax

```
ahfctl queryupdate [-h] [-debug] [-updateid UPDATEID] [-all] [-json]
```

Parameters

Table 9-19 ahfctl queryupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	To query framework update with a specific update ID. Specify `-updateid` *`UPDATEID`* option to query framework updates. **Note:** To query metadata updates, please use the `-all` option.
`-all`	Lists all applied metadata and framework updates.
`-json`	Specify this option to get the output in JSON format.

Example 9-27 ahfctl queryupdate

```
# ahfctl queryupdate -all
AHF Metadata Update: 20220203
Status: Applied
Applied on: Fri Feb 4 00:47:00 2022


# ahfctl queryupdate -all
AHF Framework update: PATCH_22.2.4.1
Status: Applied
Fixes: 34716496
Applied on: Wed Nov 30 15:14:56 2022
```

34716496 is the updateid for AHF framework update applied.

```
ahfctl queryupdate -updateid 34716496
AHF Framework update: PATCH_22.2.4.1
Status: Applied
Fixes: 34716496
Applied on: Wed Nov 30 15:14:56 2022
1:53
AHF framework updated files:
/opt/oracle.ahf/ahf/lib/ahfcomponents.py
/opt/oracle.ahf/ahf/lib/ahfctl.py
/opt/oracle.ahf/exachk/messages/framework_messages.json
/opt/oracle.ahf/exachk/lib/ahf_metadata.py
```

9.2.3.3 ahfctl rollbackupdate

Use the `ahfctl rollbackupdate` command to rollback the updates with a specific update ID applied to the local node. If you do not specify the update ID, then AHF rolls back to the previous state by default.

> **Note:**
>
> To rollback the metadata and framework updates applied to all nodes in a cluster, you must run the `ahfctl rollbackupdate` command as the AHF install user on each cluster node.

Syntax

```
ahfctl rollbackupdate [-h] [-debug] [-updateid UPDATEID]
```

Parameters

Table 9-20 ahfctl rollbackupdate Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	Specify update ID, for example, Bug ID, Build ID, that you want to rollback.

Example 9-28 ahfctl rollbackupdate

```
# ahfctl rollbackupdate -updateid 20220203
Data files with timestamp 20220203 identified. Rolling back the files to
Production version 20211220
Rolled back the data files 20220203 to Production version 20211220
```

9.2.3.4 ahfctl deleteupdatebackup

Use the `ahfctl deleteupdatebackup` command to delete the backup directories used for AHF update.

> **Note:**
>
> - To delete the backup directories on all nodes in a cluster, you must run the `ahfctl deleteupdatebackup` command as the AHF install user on each cluster node.
> - You must not delete the backup directories randomly. Oracle recommends deleting the backup directories in the same order the updates were applied. If you delete the backup directories associated with a specific timestamp, then you will not be able to roll back to the state before the updates with that specific timestamp were applied.
> - Upgrading AHF using the `ahf_setup` script automatically deletes the backup directories of the previous AHF versions.
> - Oracle recommended to delete the AHF update backup directories only when there's a need to free up space on the system. You cannot delete the AHF update backup directory of the current running timestamp/ update because once the backup directory is deleted for the specific timestamp, rolling back the update to specific timestamp/update is not possible.
>   For example: AHF Updates applied in order is: 20230901 -> 20231001 -> 20231101 (Current latest update). You can delete update backups for 20230901 and 20231001 but not the 20231101.

Syntax

```
ahfctl deleteupdatebackup [-h] [-debug] [-updateid UPDATEID] [-silent]
```

Parameters

Table 9-21 ahfctl deleteupdatebackup Command Parameters

Parameter	Description
`-debug`	Specify the `-debug` option to enable debugging.
`-updateid` *`UPDATEID`*	Deletes the backup directories with the specified timestamp.
`-silent`	Skips user confirmation for delete backup directories.

Example 9-29 ahfctl deletebackup

```
# ahfctl deleteupdatebackup -updateid 20220130
Deleted metadata backup directory for: /opt/oracle.ahf/data/
work/.exachk_patch_directory/.20220130_metadata_bkp
```

9.2.4 Running AHFCTL Upgrade Commands to Upgrade Oracle Autonomous Health Framework

You need `root` access to run `getupgrade`, `setupgrade`, `unsetupgrade`, and `upgrade` commands.

- ahfctl getupgrade
  Use the `ahfctl getupgrade` command to fetch upgrade config from the `ahf.properties` file.
- ahfctl setupgrade
  Use the `ahfctl setupgrade` command to set upgrade parameters.
- ahfctl unsetupgrade
  Use the `ahfctl unsetupgrade` command to unset upgrade parameters.
- ahfctl upgrade
  Use the `ahfctl upgrade` command to upgrade AHF to a new version.

9.2.4.1 ahfctl getupgrade

Use the `ahfctl getupgrade` command to fetch upgrade config from the `ahf.properties` file.

Syntax

```
ahfctl getupgrade -all
```

```
ahfctl getupgrade -all -json
```

Parameters

Table 9-22 ahfctl getupgrade Command Parameters

Parameter	Description
`-all`	Fetches upgrade configuration details from the `ahf.properties` file.
`-json`	Optionally, specify this option to get the output in JSON format.

Example 9-30 Print upgrade parameters

```
ahfctl getupgrade -all

autoupgrade : off
autoupgrade.swstage : /scratch/ahf_stage
autoupgrade.frequency : 30
autoupgrade.servicename : [not set]
autoupgrade.fstype : [not set]
autoupgrade.tmp_loc : [not set]
autoupgrade.remove_installer : [not set]
autoupgrade.upgradetime : [not set]


ahfctl getupgrade -all -json
{
    "autoupgrade": "off",
    "autoupgrade.swstage": "/opt/oracle.ahf",
    "autoupgrade.frequency": "30",
    "autoupgrade.servicename": "[not set]",
    "autoupgrade.fstype": "[not set]",
    "autoupgrade.tmp_loc": "[not set]",
    "autoupgrade.remove_installer": "[not set]",
    "autoupgrade.upgradetime": "[not set]"
}
```

9.2.4.2 ahfctl setupgrade

Use the `ahfctl setupgrade` command to set upgrade parameters.

Syntax

```
ahfctl setupgrade
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupgrade AUTOUPGRADE]
[-upgradetime UPGRADETIME]
[-fstype FSTYPE]
[-tmp_loc TMP_LOC]
[-remove_installer REMOVE_INSTALLER]
[-servicename SERVICENAME]
[-frequency FREQUENCY]
[-debug]
[-autoupdate AUTOUPDATE]
```

> **Note:**
>
> If you are not using the default port (443), then you must configure a custom port using the ahfctl setupload command to upgrade AHF successfully.

Parameters

Table 9-23 ahfctl setupgrade Command Parameters

Parameter	Description
`-all`	Sets all the parameters.
`-swstage` *`SWSTAGE`*	Specify the software stage location. For example: `/opt/oracle.ahf`

Table 9-23 (Cont.) ahfctl setupgrade Command Parameters

Parameter	Description
-autoupgrade *AUTOUPGRADE*	Specify to turn on or off autoupgrade. For example: ahfctl setupgrade -autoupgrade <on/off>
-upgradetime *UPGRADETIME*	Specify the upgradetime in the format [H], [HH], or [HH:MM].
-fstype *FSTYPE*	Specify the stage location filesystem type. For example: nfs/acfs/local.
-tmp_loc *TMP_LOC*	Specify the temporary location directory for AHF to extract the install archive. The specified directory must exist. **Default** /tmp
-remove_installer *REMOVE_INSTALLER*	Specify this flag to remove AHF installer zip at stage location after auto upgrade. By default AHF does not remove the AHF installer zip. Valid values: yes|no
-servicename	Specify the name of REST download service. Default: ahf_upgrade_loc
-frequency	Specify the autoupgrade frequency in the range (1,30) days. For example: 15
-debug	Specify the -debug option to enable debugging.
-autoupdate *AUTOUPDATE*	Specify to turn on or off to include or remove autoupdate configurations. Valid values: ON||OFF For example: • ahfctl setupgrade -autoupgrade on -swstage */opt/oracle.ahf* -frequency 1 -autoupdate on • ahfctl setupgrade -autoupgrade on -swstage */opt/oracle.ahf* -frequency 1 -autoupdate off

Example 9-31 Set upgrade configuration

```
ahfctl setupgrade -swstage /scratch/ahf_stage -autoupgrade on -frequency 21
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
```

Example 9-32 Set all upgrade configuration

```
ahfctl setupgrade -all
Enter autoupgrade flag <on/off> : on
Enter software stage location : /scratch/ahf_stage
Enter auto upgrade frequency : 30
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
```

Example 9-33   Turn off autoupgrade

```
ahfctl setupgrade -autoupgrade off
AHF autoupgrade parameters successfully updated
Successfully synced AHF configuration
```

9.2.4.3 ahfctl unsetupgrade

Use the `ahfctl unsetupgrade` command to unset upgrade parameters.

Syntax

```
ahfctl unsetupgrade
[-h]
[-all]
[-swstage SWSTAGE]
[-autoupgrade AUTOUPGRADE]
[-upgradetime UPGRADETIME]
[-fstype FSTYPE]
[-tmp_loc TMP_LOC]
[-remove_installer REMOVE_INSTALLER]
[-servicename SERVICENAME]
[-frequency FREQUENCY]
[-debug]
[-autoupdate AUTOUPDATE]
```

Parameters

Table 9-24   ahfctl unsetupgrade Command Parameters

Parameter	Description
`-all`	Unsets all the parameters.
`-swstage` *`SWSTAGE`*	Specify the software stage location to unset.
`-autoupgrade` *`AUTOUPGRADE`*	Specify to turn on or off autoupgrade.
`-upgradetime` *`UPGRADETIME`*	Specify unset `upgradetime`.
`-fstype` *`FSTYPE`*	Specify to unset stage location filesystem type.
`-tmp_loc` *`TMP_LOC`*	Specify to unset the temporary location directory for AHF to extract the install archive.
`-remove_installer` *`REMOVE_INSTALLER`*	Specify this flag to unset the stage location configured to remove AHF installer zip after auto upgrade.
`-servicename`	Specify the name of REST download service to unset.
`-frequency`	Unsets autoupgrade frequency.
`-debug`	Specify to unset debugging.
`-autoupdate` *`AUTOUPDATE`*	Specify to unset autoupdate configurations. For example: `ahfctl unsetupgrade -autoupdate`

Example 9-34 Set a single upgrade parameter

```
ahfctl unsetupgrade -swstage
Software stage location successfully removed
Successfully synced AHF configuration
```

Example 9-35 Unset all upgrade configuration

```
ahfctl unsetupgrade -all
AHF upgrade parameters successfully removed
Successfully synced AHF configuration
```

Example 9-36 Unset autoupgrade frequency

```
ahfctl unsetupgrade -frequency
Autoupgrade frequency successfully removed
Successfully synced AHF configuration
```

9.2.4.4 ahfctl upgrade

Use the `ahfctl upgrade` command to upgrade AHF to a new version.

Syntax

```
ahfctl upgrade [-nomos]
```

Parameters

Table 9-25 ahfctl upgrade Command Parameters

Parameter	Description
`-nomos`	Specify not to configure MOS.

Example 9-37 New AHF setup is available at software stage location

```
ahfctl upgrade -nomos

AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/ahf_install_211000_8398_2021_03_02-03_56_28.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 21.1.0 Build Date: 202103010521
AHF is already installed at /opt/oracle.ahf
Installed AHF Version: 21.1.0 Build Date: 202102242242
Upgrading /opt/oracle.ahf
Shutting down AHF Services

Starting AHF Services
Oracle Trace File Analyzer (TFA) is already running
No new directories were added to TFA

AHF is successfully upgraded to latest version
```

```
.----------------------------------------------------------------------.
| Host           | TFA Version | TFA Build ID         | Upgrade Status |
+----------------+-------------+----------------------+----------------+
| node1         |  21.1.0.0.0 | 21100020210224224247 | UPGRADED       |
'----------------+-------------+----------------------+----------------'

Moving /tmp/ahf_install_211000_8398_2021_03_02-03_56_28.log to
/u01/app/oracle/oracle.ahf/data/node1/diag/ahf/
```

Example 9-38 New AHF is available at Rest Endpoint

```
ahfctl upgrade

Started downloading...
AHF-LINUX_v20.4.4.zip is successfully downloaded to /opt/oracle.ahf/
download location!
AHF Installer for Platform Linux Architecture x86_64
AHF Installation Log : /tmp/
ahf_install_211000_8398_2021_03_02-03_56_28.log
Starting Autonomous Health Framework (AHF) Installation
AHF Version: 21.1.0 Build Date: 202103010521
AHF is already installed at /opt/oracle.ahf
Installed AHF Version: 21.1.0 Build Date: 202102242242
Upgrading /opt/oracle.ahf
Shutting down AHF Services

Starting AHF Services
Oracle Trace File Analyzer (TFA) is already running
No new directories were added to TFA

AHF is successfully upgraded to latest version
.----------------------------------------------------------------------.
| Host | TFA Version | TFA Build ID | Upgrade Status |
+----------------+-------------+----------------------+----------------+
| node1    | 21.1.0.0.0 | 21100020210224224247 | UPGRADED |
'----------------+-------------+----------------------+----------------'

Moving /tmp/ahf_install_211000_8398_2021_03_02-03_56_28.log to
/u01/app/oracle/oracle.ahf/data/node1/diag/ahf/
```

9.2.5 Running AHFCTL Upload Commands to Upload Diagnostics

You need `root` access to `ahfctl`, or `sudo` access to run `setupload`, `getupload`, `checkupload`, and `unsetupload` commands.

- ahfctl upload
  Use the `ahfctl upload` command to configure upload parameters.
- ahfctl checkupload
  Use the `ahfctl checkupload` command to validate the configured upload parameters.

- ahfctl getupload
  Use the `ahfctl getupload` command to fetch the details of configured upload parameters.
- ahfctl setupload
  Use the `ahfctl setupload` command to set upload parameters.
- ahfctl unsetupload
  Use the `ahfctl unsetupload` command to unset the configured upload parameters.

9.2.5.1 ahfctl upload

Use the `ahfctl upload` command to configure upload parameters.

You can run the `upload` command as `root` or a non-root user.

Syntax

```
ahfctl upload
[-h]
[-debug]
[-name NAME]
[-id ID]
[-file FILE]
[-header HEADER]
[-tls TLS]
[-ciphers CIPHERS]
[-insecure <True/False>]
```

Parameters

Table 9-26 ahfctl upload Command Parameters

Parameter	Description
`debug`	Specify the name of the debug script file.
`name`	Specify the name of your configuration. For example, *sftpconf* to upload a file using SFTP.
`id`	Specify the identifier number, for example, SR number.
`file`	Specify the name of the file to upload, for example, */tmp/generated.zip*.
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`ahfctl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`
`tls`	Specify the version of TLS for curl OSS upload.
ciphers	Specify ciphers for curl OSS upload.
`insecure`	Enables or disables security.

Example 9-39 Upload to MOS using ahfctl upload:

```
ahfctl upload -name mos -id 3-23104325631 -file
/opt/oracle.ahf/data/repository/
auto_srdc_ORA-00600_20200706T18:58:09_myserver
1.zip
```

Example 9-40 Upload to MOS using ahfctl diagcollect:

```
ahfctl diagcollect -upload mos -srdc ORA-00600 -id 3-23104325631
```

or

```
ahfctl diagcollect -srdc ORA-00600 -sr 3-23104325631
```

Ensure that the MOS configuration name is "mos". For more information, see *ahfctl setupload*.

9.2.5.2 ahfctl checkupload

Use the `ahfctl checkupload` command to validate the configured upload parameters.

You can run the `checkupload` command as `root` or a non-root user.

Syntax

```
ahfctl checkupload
[-h][--help]
[-name NAME]
```

Parameters

Table 9-27 ahfctl checkupload Command Parameters

Parameter	Description
name	Specify the name of your configuration. For example, *mosconfig* to upload to My Oracle Support.

9.2.5.3 ahfctl getupload

Use the `ahfctl getupload` command to fetch the details of configured upload parameters.

You can run the `getupload` command as `root` or a non-root user.

Syntax

```
ahfctl getupload
[-h][--help]
[-all]
[-name NAME]
```

```
[-user USER]
[-password]
[-server SERVER]
[-url URL]
[-proxy PROXY]
[-noauth NOAUTH]
[-request REQUEST]
[-https_token HTTPS_TOKEN]
[-header HEADER]
[-secure SECURE]
[-connectstring CONNECTSTRING]
[-uploadtable UPLOADTABLE]
[-port PORTNUMBER]
```

Parameters

Table 9-28 ahfctl getupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`name`	Specify the name of your configuration. For example, *mosconfig*.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`server`	Specify the name of the server to which you have uploaded files. For example, *bugsftp.example.com*.
`url`	Specify the target URL in case of HTTPS type. For example, *https://samplehost.com*.
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`noauth`	Specify `true` and `false`. Default value is `false`. If `noauth` is set to `true`, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/password authentication is required.
`request`	Specify the request type, for example, `POST`.
`https_token`	Specify any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. You can also pass dynamic headers at upload time by passing the –`https_token` *`headers`* command option to `tfactl upload` command. For example: *`-H 'X-TFA-REQUESTID: 1'`*.
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`ahfctl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, the `upload` command will run an unsecure upload.

Table 9-28 (Cont.) ahfctl getupload Command Parameters

Parameter	Description
connectstring	Specify the database connect string to log in to the database where you have uploaded files. For example, (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl))).
uploadtable	Specify the name of the table where you have uploaded files as BLOB type. For example, for uploading Oracle Orachk collections to the Collection Manager it is set to RCA13_DOCS.
port	Specify a custom port number. If you do not specify a port, then 443 is used by default. You can set a port number in the range of 0 - 65353.

```
ahfctl getupload -name ahf_upgrade_loc
Upload configuration get for: ahf_upgrade_loc
type: https
ahf_upgrade_loc.https.user : [not set]
ahf_upgrade_loc.https.password : [not set]
ahf_upgrade_loc.https.url :
https://10.65.16.53/rest/tfa-processor/download?
osName=LINUX&ahfVersion=%2720.2%27
ahf_upgrade_loc.https.storetype : [not set]
ahf_upgrade_loc.https.proxy : [not set]
ahf_upgrade_loc.https.secure : [not set]
ahf_upgrade_loc.https.noauth : [not set]
ahf_upgrade_loc.https.https_token : ******
ahf_upgrade_loc.https.request : [not set]
ahf_upgrade_loc.https.header : Content-Type:application/json
ahf_upgrade_loc.https.useinstanceprincipal : [not set]
ahf_upgrade_loc.https.ociclient : [not set]
ahf_upgrade_loc.https.port : 4545
```

9.2.5.4 ahfctl setupload

Use the ahfctl setupload command to set upload parameters.

AHF 23.8

Starting in AHF 23.8, you will be able to upload AHF Insights report automatically if Object Store is configured as part of AHF. Uploading AHF Insights reports helps Oracle Cloud Operations to identify, investigate, track, and resolve system health issues and divergences in best practice configurations quickly and effectively.

Oracle Autonomous Database on Dedicated Exadata Infrastructure and Oracle SaaS

To set REST endpoints (Object Store's), run:

```
ahfctl setupload -name oss -type https -user <user> -url <object_store> -
password
```

To upload AHF Insights report to Object Store, run:

```
ahf analysis create --type insights
```

.

You can run the `setupload` command as `root` or a non-root user.

Syntax

```
ahfctl setupload
[-h][--help]
[-all]
[-type TYPE]
[-name NAME]
[-user USER]
[-password]
[-server SERVER]
[-url URL]
[-proxy PROXY]
[-noauth NOAUTH]
[-https_token HTTPS_TOKEN]
[-request REQUEST]
[-header HEADER]
[-secure SECURE]
[-connectstring CONNECTSTRING]
[-uploadtable UPLOADTABLE]
[-port PORTNUMBER]
```

Parameters

Table 9-29 ahfctl setupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`type`	Specify the type of an endpoint. For example, `https`, `sftp`, or `sqlnet`.
`name`	Specify a unique descriptive name to your configuration. For example, *mosconfig* to upload to My Oracle Support.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`server`	Specify the name of the server to which you want to upload files. For example, *bugsftp.example.com*.
`url`	Specify the target URL to upload files in case of HTTPS type. For example, *https://samplehost.com*.

Table 9-29 (Cont.) ahfctl setupload Command Parameters

Parameter	Description
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`noauth`	Specify `true` and `false`. Default value is `false`. If `noauth` is set to `true`, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/ password authentication is required.
`request`	Specify the request type, for example, `POST`.
`https_token`	Specify any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. For example, `ahfctl setupload -name config -type https -https_token 'abc:13'`. You can also pass dynamic headers at upload time by passing the `–https_token` *`headers`* command option to `tfactl upload` command. For example: *`-H 'X-TFA-REQUESTID: 1'`*.
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`ahfctl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.
`connectstring`	Specify the database connect string to log in to the database where you want to upload files. For example, `(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl)))`.
`uploadtable`	Specify the name of the table where you want to upload files as `BLOB` type. For example, for uploading Oracle Orachk collections to the Collection Manager, it is set to `RCA13_DOCS`.
`port`	Specify a custom port number. If you do not specify a port, then 443 is used by default. You can set a port number in the range of 0 - 65353.

To setup MOS configuration:

```
ahfctl setupload -name mos -type https -user sample_user@domain.com -
url https://transport.oracle.com/upload/issue
```

To set proxy for MOS configuration:

```
ahfctl setupload -name mos -type https -proxy www-proxy.server.com:80
```

To set a custom port:

```
ahfctl setupload -name my_upload -type https -url 'https://samplehost.com' -
https_token "abc:13" -header Content Type:application/json -port 4545
```

To upload to MOS using `tfactl upload`:

```
tfactl upload -name mos -id 3-23104325631 -file /opt/oracle.ahf/data/
repository/auto_srdc_ORA-00600_20200706T18:58:09_myserver1.zip
```

To upload to MOS using `tfactl diagcollect`:

```
tfactl diagcollect -upload mos -srdc ORA-00600 -id 3-23104325631
```

or

```
tfactl diagcollect -srdc ORA-00600 -sr 3-23104325631
```

> **Note:**
>
> Ensure that the configuration name is `mos`.

9.2.5.5 ahfctl unsetupload

Use the `ahfctl unsetupload` command to unset the configured upload parameters.

You can run the `unsetupload` command as `root` or a non-root user.

Syntax

```
ahfctl unsetupload -name <config_name> {-all | <config_parameter> ...
} [Options]
```

```
Options:
  -h, --help       show this help message and exit
  -debug           Debug Script

Config parameters:
  -user
  -password
  -server
  -url
  -storetype
  -proxy
  -secure
  -connectstring
  -uploadtable
  -noauth
  -https_token
```

```
-request
-header
-port
```

Parameters

Table 9-30   ahfctl unsetupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`name`	Specify the name of your configuration. For example, *mosconfig* to upload to My Oracle Support.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`server`	Specify the name of the server to which you have uploaded the files. For example, *bugsftp.example.com*.
`url`	Specify the target URL to which you have uploaded the files in case of HTTPS type. For example, *https://samplehost.com*.
`-storetype`	Specify the storetype. For example, `casper`.
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.
`connectstring`	Specify the database connect string to log in to the database where you have uploaded files. For example, `(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl)))`.
`uploadtable`	Specify the name of the table where you have uploaded the files as `BLOB` type. For example, for uploading Oracle Orachk collections to the Collection Manager it is set to `RCA13_DOCS`.
`noauth`	Specify `true` and `false`. Default value is `false`. If `noauth` is set to `true`, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/password authentication is required.
`https_token`	Specify any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. You can also pass dynamic headers at upload time by passing the `-https_token` *`headers`* command option to `tfactl upload` command. For example: *`-H 'X-TFA-REQUESTID: 1'`*.
`request`	Specify the request type, for example, `POST`.

Table 9-30 (Cont.) ahfctl unsetupload Command Parameters

Parameter	Description
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`ahfctl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`

```
ahfctl unsetupload -name mos -all
```

```
ahfctl unsetupload -name mos -url -secure
```

9.2.6 Running AHFCTL Commands to Manage the Scheduler for Oracle Autonomous Health Framework Components

You need `root` access to `ahfctl`, or `sudo` access to run `startahf`, `stopahf`, and `statusahf` commands.

- ahfctl startahf
  Use the `ahfctl startahf` command to start the scheduler for Oracle Autonomous Health Framework components.
- ahfctl statusahf
  Use the `ahfctl statusahf` command to check the scheduler status for Oracle Autonomous Health Framework components.
- ahfctl stopahf
  Use the `ahfctl stopahf` command to stop the scheduler for Oracle Autonomous Health Framework components.

9.2.6.1 ahfctl startahf

Use the `ahfctl startahf` command to start the scheduler for Oracle Autonomous Health Framework components.

Syntax

```
ahfctl startahf
[-h]
[-all]
[-tfa tfa_start_args]
[-compliance compliance_autostart_args]
```

Parameters

Table 9-31   ahfctl startahf Command Parameters

Parameter	Description
-all	Starts the Oracle Trace File Analyzer and Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons.
-tfa	Starts the Oracle Trace File Analyzer daemon.
-tfa *tfa_start_args*	Starts the Oracle Trace File Analyzer daemon with the option specified. You can specify all Oracle Trace File Analyzer supported options. For example: ahfctl startahf -tfa "*tfa_start_args*"
-compliance	Starts the Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons.
-compliance *compliance_autostart_args*	Starts the Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons with the option specified. Prepend the argument with a space followed by an hyphen and then wrap it with double quotes. You can specify all Oracle Orachk and Oracle Exachk supported options. For example: ahfctl startahf -compliance " -*compliance_autostart_args*" ahfctl startahf -compliance -cargs " -c X4-2,EXAMAA" ahfctl startahf -compliance -cargs " -debug" ahfctl startahf -compliance -cagrs " -withisa"

Example 9-41   ahfctl startahf

```
ahfctl startahf

Starting TFA..
Waiting up to 100 seconds for TFA to be started..
. . . . .
. . . . .
. . . . .
. . . . .
. . . . .
Successfully started TFA Process..
. . . . .
TFA Started and listening for commands

INFO: Configuring orachk to use TFA scheduler. Process sent to
background. Details for the process can be found at /opt/oracle.ahf/
data/node1/diag/orachk/compliance_start_070324_012319.log
```

9.2.6.2 ahfctl statusahf

Use the `ahfctl statusahf` command to check the scheduler status for Oracle Autonomous Health Framework components.

Syntax

```
ahfctl statusahf [-h]
[-all]
[-tfa]
[-compliance]
```

Parameters

Table 9-32 ahfctl statusahf Command Parameters

Parameter	Description
`-all`	Checks and displays the status of Oracle Trace File Analyzer and Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons.
`-tfa`	Checks and displays the status of Oracle Trace File Analyzer daemon.
`-compliance`	Checks and displays the status of Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons.

Example 9-42 ahfctl statusahf

```
ahfctl statusahf

.----------------------------------------------------------------------------
--------------------.
| Host     | Status of TFA | PID   | Port | Version    | Build
ID              | Inventory Status |
+---------+---------------+-------+------+------------
+-----------------------+------------------+
| node1    | RUNNING       | 29745 | 5000 | 24.3.0.0.0 |
240300020240306182236 | COMPLETE          |
| node2    | RUNNING       | 11544 | 5000 | 24.3.0.0.0 |
240300020240306182236 | COMPLETE          |
'---------+---------------+-------+------+------------
+-----------------------+------------------'



-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
|Parameter                                                               |
Value
                 |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
```

```
|Master
node                                                             |
node2
                     |
|orachk daemon
version                                                   |
2403000
                       |
|Install
location                                                        | /opt/
oracle.ahf/
orachk
       |
|Scheduled orachk collection
location                                    | /opt/oracle.ahf/data/
node2/orachk/user_root/output on Master node node2                    |
|Started
at                                                              | Wed
Mar 06 18:35:16 UTC
2024                                                                   |
|Scheduler
type                                                          | TFA
Scheduler
                   |
|Scheduler
PID                                                           |
29745
                       |
-----------------------------------------------------------------------
+----------------------------------------------------------------------
-------------------------
|Scheduled
runs
|
                         |
-----------------------------------------------------------------------
+----------------------------------------------------------------------
-------------------------
|
Scheduler
|
orachk.autostart_client_oratier1
                       |
-----------------------------------------------------------------------
+----------------------------------------------------------------------
-------------------------
|
AUTORUN_FLAGS
| -usediscovery -profile oratier1 -dball -showpass -tag
autostart_client_oratier1 -readenvconfig|
|
AUTORUN_SCHEDULE
| 3 2 * *
1,2,3,4,5,6
               |
|COLLECTION_RETENTION                                                   |
7
                 |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
|Scheduler                                                              |
orachk.autostart_client
                 |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
|AUTORUN_FLAGS                                                          | -
usediscovery -tag autostart_client -
readenvconfig                                            |
|AUTORUN_SCHEDULE                                                       | 3
3 * *
0
         |
|COLLECTION_RETENTION                                                   |
14
                 |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
|Previous runs
|
                   |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
|No previous runs since last two runs from lucene index are manual runs
|
                   |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
|Next auto run starts on                                                |
Mar 07, 2024 02:03:00
ID:orachk.autostart_client_oratier1                                     |
-----------------------------------------------------------------------
+----------------------------------------------------------------------------
-------------------
```

9.2.6.3 ahfctl stopahf

Use the `ahfctl stopahf` command to stop the scheduler for Oracle Autonomous Health Framework components.

Syntax

```
ahfctl stopahf [-h]
[-all]
```

```
[-tfa]
[-compliance]
```

Parameters

Table 9-33 ahfctl stopahf Command Parameters

Parameter	Description
`-all`	Stops the Oracle Trace File Analyzer and Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons.
`-tfa`	Stops the Oracle Trace File Analyzer daemon.
`-compliance`	Stops the the Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components daemons.

Example 9-43 ahfctl stopahf

```
ahfctl stopahf

Stopping TFA from the Command Line
Stopped OSWatcher
Nothing to do !
Please wait while TFA stops
Please wait while TFA stops
TFA-00002 Oracle Trace File Analyzer (TFA) is not running
TFA-00106 TFA Shutdown/Stopped by user
TFA Stopped Successfully
Telemetry adapter is not running
Successfully stopped TFA..

No active orachk manual runs found
Stopping orachk scheduler ...
Removing orachk cache discovery....
Successfully completed orachk cache discovery removal.

Unable to send message to TFA
Stopped orachk
```

9.2.7 Running AHFCTL Commands to Manage Cell, Switches, Databases and exacli Passwords

You need `root` access to `ahfctl`, or `sudo` access to run `checkpassword`, `setpassword`, and `unsetpassword` commands.

- ahfctl checkpassword
  Use the `ahfctl checkpassword` command to check cell, switches, databases and `exacli` passwords.
- ahfctl setpassword
  Use the `ahfctl setpassword` command to set cell, switches, databases and `exacli` passwords.

- ahfctl unsetpassword
  Use the `ahfctl unsetpassword` command to unset cell, switches, databases and `exacli` passwords.

9.2.7.1 ahfctl checkpassword

Use the `ahfctl checkpassword` command to check cell, switches, databases and `exacli` passwords.

Syntax

```
ahfctl checkpassword
[-nodes nodes]
[-dbs databases]
[-user user]
[-exacli]
```

Parameters

Table 9-34   ahfctl checkpassword Command Parameters

Parameter	Description
`-nodes nodes`	Specify a comma-delimited list of nodes.
`-dbs databases`	Specify a comma-delimited list of Oracle Databases.
`-user user`	Specify a user name for whom you want check the password.
`-exacli`	Specify to check `exacli` user of a cell.

9.2.7.2 ahfctl setpassword

Use the `ahfctl setpassword` command to set cell, switches, databases and `exacli` passwords.

Syntax

```
ahfctl setpassword
[-nodes nodes]
[-dbs databases]
[-user user]
[-exacli]
```

Parameters

Table 9-35   ahfctl setpassword Command Parameters

Parameter	Description
`-nodes nodes`	Specify a comma-delimited list of nodes.
`-dbs databases`	Specify a comma-delimited list of Oracle Databases.
`-user user`	Specify a user name for whom you want to set password.

Table 9-35 (Cont.) ahfctl setpassword Command Parameters

Parameter	Description
`-exacli`	Specify to set `exacli` user of a cell.

9.2.7.3 ahfctl unsetpassword

Use the `ahfctl unsetpassword` command to unset cell, switches, databases and `exacli` passwords.

Syntax

```
ahfctl unsetpassword
[-nodes nodes]
[-dbs databases]
[-user user]
[-exacli]
```

Parameters

Table 9-36 ahfctl setpassword Command Parameters

Parameter	Description
`-nodes` *`nodes`*	Specify a comma-delimited list of nodes.
`-dbs` *`databases`*	Specify a comma-delimited list of Oracle Databases.
`-user` *`user`*	Specify a user name for whom you want to unset the password.
`-exacli`	Specify to unset `exacli` user of a cell.

9.2.8 Running AHFCTL Commands to Get the Repository Locations of Oracle Autonomous Health Framework Components

You need `root` access to `ahfctl`, or `sudo` access to run `showrepo` command.

- ahfctl showrepo
  Use the `ahfctl showrepo` command to get the repository locations of Oracle Autonomous Health Framework components.

9.2.8.1 ahfctl showrepo

Use the `ahfctl showrepo` command to get the repository locations of Oracle Autonomous Health Framework components.

Syntax

```
ahfctl showrepo
[-h]
[-all]
```

```
[-tfa]
[-compliance]
```

Parameters

Table 9-37   ahfctl showrepo Command Parameters

Parameter	Description
`-all`	Displays the repository locations of Oracle Autonomous Health Framework components.
`-tfa`	Displays the repository locations of Oracle Trace File Analyzer.
`-compliance`	Displays the repository locations of Oracle Autonomous Health Framework compliance (Oracle Orachk and Oracle Exachk) components.

Example 9-44   ahfctl showrepo

```
ahfctl showrepo

.-------------------------------------------------------.
|                         node1                         |
+----------------------+--------------------------------+
| Repository Parameter | Value                          |
+----------------------+--------------------------------+
| Location             | /opt/oracle.ahf/data/repository |
| Maximum Size (MB)    | 10240                          |
| Current Size (MB)    | 250                            |
| Free Size (MB)       | 9990                           |
| Status               | OPEN                           |
'----------------------+--------------------------------'

.-------------------------------------------------------.
|                         node2                         |
+----------------------+--------------------------------+
| Repository Parameter | Value                          |
+----------------------+--------------------------------+
| Location             | /opt/oracle.ahf/data/repository |
| Maximum Size (MB)    | 10240                          |
| Current Size (MB)    | 117                            |
| Free Size (MB)       | 10123                          |
| Status               | OPEN                           |
'----------------------+--------------------------------'
```

9.2.9 Running AHFCTL Commands to Import Oracle Orachk or Oracle Exachk Wallet Details into Oracle Autonomous Health Framework Wallet and Configuration

You need `root` access to `ahfctl`, or `sudo` access to run `import` command.

- ahfctl import
  Use the `ahfctl import` command to import Oracle Orachk or Oracle Exachk wallet (version less than or equal to 19.2.0) details into Oracle Autonomous Health Framework wallet and configuration.

9.2.9.1 ahfctl import

Use the `ahfctl import` command to import Oracle Orachk or Oracle Exachk wallet (version less than or equal to 19.2.0) details into Oracle Autonomous Health Framework wallet and configuration.

Syntax

```
ahfctl import [-h] [-type {wallet}] [-loc location]
```

Parameters

Table 9-38 ahfctl import Command Parameters

Parameter	Description
`-type {wallet}`	Specify to import Oracle Orachk or Oracle Exachk wallet (version less than or equal to 19.2.0) details into Oracle Autonomous Health Framework wallet and configuration.
`-loc` *`location`*	Specify the location of Oracle Orachk or Oracle Exachk wallet that you want to import into Oracle Autonomous Health Framework wallet and configuration.

9.2.10 Running AHFCTL Commands to Limit CPU and Memory Usage

You need `root` access to `ahfctl`, or `sudo` access to run `getresourcelimit`, `setresourcelimit`, `unsetresourcelimit` commands.

> **Note:**
>
> The following commands are enabled only on Linux 64.

- ahfctl getresourcelimit
  Use the `ahfctl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.
- ahfctl setresourcelimit
  Use the `ahfctl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.
- ahfctl unsetresourcelimit
  Use the `ahfctl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.
- ahfctl printresourcestats
  Use the `ahfctl printresourcestats` command to view statistics of the specified resource.

9.2.10.1 ahfctl getresourcelimit

Use the `ahfctl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.

Syntax

```
ahfctl getresourcelimit
[-tool tool_name]
[-resource resource_type]
```

Parameters

Table 9-39 ahfctl getresourcelimit Command Parameters

Parameter	Description
`tool`	Currently, you can only specify `tfa`.
`resource`	You can specify either CPU or memory.

Example 9-45 getresourcelimit Example

```
# ahfctl getresourcelimit
Tool TFA: Resource CPU: Limit value: 1
```

9.2.10.2 ahfctl setresourcelimit

Use the `ahfctl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.

> **Note:**
>
> This feature is available only on Linux and only when Autonomous Health Framework is installed using a full installation by the `root` user.

Syntax

```
ahfctl setresourcelimit [-h]
[-tool {tfa}]
[-resource {cpu,kmem,swmem}]
[-value VALUE]
[-debug]
[-force]
```

Parameters

Table 9-40 ahfctl setresourcelimit Command Parameters

Parameter	Description
`value`	Set the limit to a minimum of 50% of a single CPU, and a maximum of 4 or 75% of the available CPUs, whichever is lower. By default, the CPU limit is set to the maximum. To limit TFA to a maximum of 50% of a single CPU: `ahfctl setresourcelimit -value 0.5` You can limit memory usage either at the system level using `ahfctl setresourcelimit -resource kmem` or combined system and swap memory using `ahfctl setresourcelimit -resource swmem`. Set the kernel memory to a minimum of 500 MB, and a maximum of 2048 MB or 20% of the available memory, whichever is lower. By default, the kernel memory (kmem) limit is not set. Set the system and swap memory to a minimum of 1024 MB, and a maximum of 8192 MB or 50% of the available memory, whichever is lower. By default, the system and swap memory (swmem) limit is not set.
`tool`	Currently, you can only specify `tfa`. Default: *`tfa`*
`resource`	You can specify either CPU or memory.
`value`	Specify to limit the value. • **CPU:** Float number (rounded to 2 decimals) indicating the number of CPU that can be used. – **Range of values:** 0.5 <= value <= max_value, `max_value` is the minimum of (4, total number of CPUs * 0.75) – **Default:** `max_value` • **Kernel Memory (kmem):** Integer number (in MB) indicating the kernel memory that can be used. – **Range of values:** 1600 <= value <= max_value, max_value is the minimum of (20480, total system memory * 0.75) – **Default:** `max_value` • **Memory+swap (swmem):** Integer number (in MB) indicating the memory+swap that can be used. – **Range of values:** 1600 <= value <= max_value, max_value is the minimum of (20480, total system memory * 0.75) – **Default:** `max_value`
`debug`	Specify to enable debugging.
`force`	Specify to set the resource value beyond the `max_value`.

Example 9-46 setresourcelimit Examples

On a server with 10 CPUs, the default limit will be 4 CPUs:

```
# ahfctl setresourcelimit
Tool TFA: Resource CPU: Limit value: 4
```

On a server with 4 CPUs, the default limit will be 3 CPUs (75% of available CPUs):

```
ahfctl setresourcelimit
Tool TFA: Resource CPU: Limit value: 3


# ahfctl setresourcelimit -value 2
Tool TFA: Resource CPU: Limit value: 2
```

To limit the memory usage to only 500 MB of system memory run:

```
ahfctl setresourcelimit -resource kmem -value 500
```

To limit the combined total of system memory and the swap memory to 1 GB run:

```
ahfctl setresourcelimit -resource swmem -value 1024
```

9.2.10.3 ahfctl unsetresourcelimit

Use the `ahfctl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.

Syntax

```
ahfctl unsetresourcelimit
[-tool tool_name]
[-resource resource_type]
```

Parameters

Table 9-41 ahfctl unsetresourcelimit Command Parameters

Parameter	Description
`tool`	Currently, you can only specify `tfa`.
`resource`	You can specify either CPU or memory.

Example 9-47 unsetresourcelimit Example

```
# ahfctl unsetresourcelimit -tool tfa -resource cpu
```

9.2.10.4 ahfctl printresourcestats

Use the `ahfctl printresourcestats` command to view statistics of the specified resource.

> **Note:**
>
> You can run `ahfctl printresourcestats` only if you have run the corresponding `setresourcelimit` command. The resource is managed by Oracle Trace File Analyzer `cgroups`.

Syntax

```
ahfctl printresourcestats
[-tool tool_name]
[-resource resource_type]
```

Parameters

Table 9-42 ahfctl printresourcestats Command Parameters

Parameter	Description
`tool`	Currently, you can only specify `tfa`.
`resource`	You can specify either CPU or memory.

9.2.11 Running AHFCTL Commands to Collect Storage Server Diagnostic Package

You need `root` access to `ahfctl`, or `sudo` access to run `celldiagcollect` command.

- ahfctl celldiagcollect
  Use the `ahfctl celldiagcollect` command to collect storage server diagnostic package.

9.2.11.1 ahfctl celldiagcollect

Use the `ahfctl celldiagcollect` command to collect storage server diagnostic package.

Syntax

```
ahfctl celldiagcollect
[-from time]
[-duration duration]
[-timeframe timeframe]
[-diagpath path]
```

```
[-packpollingtimeout timeout]
[-rpackpollingtimeout timeout]
```

Parameters

Table 9-43 ahfctl celldiagcollect Command Parameters

Parameter	Description
`-from` *`time`*	Specify when to start collecting the logs and traces for storage server diagnostic package. The format of cell diagpack start time are: `Mon/dd/yyyy hh:mm:ss` or `yyyy-MM-dd hh:mm:ss` or `yyyy-MM-ddThh:mm:ss` or `yyyy-MM-dd` or `now`. For example: `ahfctl celldiagcollect -from 2015-07-07T09:00:00`
`-duration` *`duration`*	Specify the number of hours of logs and traces to include in the storage server diagnostic package. Valid values are from 1 (default) to 6. For example: `ahfctl celldiagcollect -duration 2`
`-timeframe` *`timeframe`*	AHF picks storage server diagnostic package if start time is within `timeframe`. Specify `timeframe` in seconds. For example: `ahfctl celldiagcollect -timeframe 60`
`-diagpath` *`path`*	Specify the path where AHF copies the storage server diagnostic package. For example: `ahfctl celldiagcollect -diagpath /opt`
`-packpollingtimeout` *`timeout`*	Specify the amount of time for which AHF waits for submitted storage server diagnostic package generation to finish. Specify `timeout` in seconds. For example: `ahfctl celldiagcollect -packpollingtimeout 2000`

Table 9-43 (Cont.) ahfctl celldiagcollect Command Parameters

Parameter	Description
`-rpackpollingtimeout` *`timeout`*	Specify the amount of time for which AHF waits for previously submitted (within the timeframe) storage server diagnostic package generation to finish. Specify `timeout` in seconds. For example: `ahfctl celldiagcollect -rpackpollingtimeout 1000`

9.2.12 Running AHFCTL Commands to Manage Service Upload Parameters

You need `root` access to `ahfctl`, or `sudo` access to run `getserviceupload`, `setserviceupload`, and `unsetserviceupload` commands.

> **Note:**
>
> The `ahfctl getserviceupload`, `ahfctl setserviceupload`, and `ahfctl unsetserviceupload` commands have been deprecated and removed in 23.3. Oracle recommends using the following commands instead.
>
> - `ahfctl getupload` replaces `ahfctl getserviceupload`
> - `ahfctl setupload` replaces `ahfctl setserviceupload`
> - `ahfctl unsetupload` replaces `ahfctl unsetserviceupload`

- ahfctl getserviceupload
  Use the `ahfctl getserviceupload` command to get service upload parameters.
- ahfctl setserviceupload
  Use the `ahfctl setserviceupload` command to set service upload parameters.
- ahfctl unsetserviceupload
  Use the `ahfctl unsetserviceupload` command to unset service upload parameters.

9.2.12.1 ahfctl getserviceupload

Use the `ahfctl getserviceupload` command to get service upload parameters.

You can run the `getserviceupload` command as `root` or a non-root user.

Syntax

```
ahfctl getserviceupload
[-h][--help]
```

```
[-all]
[-user USER]
[-password]
[-url URL]
[-proxy PROXY]
[-storetype STORETYPE]
[-secure SECURE]
```

Parameters

Table 9-44 ahfctl getserviceupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`url`	Specify the target URL to upload files in case of HTTPS type. For example, *https://samplehost.com*.
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`storetype`	Specify the Keystore format, for example, JKS and PKCS12.
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.

9.2.12.2 ahfctl setserviceupload

Use the `ahfctl setserviceupload` command to set service upload parameters.

You can run the `setserviceupload` command as `root` or a non-root user.

Syntax

```
ahfctl setserviceupload
[-h][--help]
[-all]
[-user USER]
[-password]
[-url URL]
[-proxy PROXY]
[-storetype STORETYPE]
[-secure SECURE]
```

Parameters

Table 9-45 ahfctl setserviceupload Command Parameters

Parameter	Description
all	All of the parameters.
user	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
password	Specify the password of the user.
url	Specify the target URL to upload files in case of HTTPS type. For example, *https://samplehost.com*.
proxy	Specify the URL of the proxy server. For example, *www.example.com:80*.
storetype	Specify the Keystore format, for example, JKS and PKCS12.
secure	Specify true or false. Default value is true. Specifying the secure value checks for certificates. If secure is set to false, then the upload command will run an unsecure upload.

9.2.12.3 ahfctl unsetserviceupload

Use the ahfctl unsetserviceupload command to unset service upload parameters.

You can run the unsetserviceupload command as root or a non-root user.

Syntax

```
ahfctl unsetserviceupload
[-h][--help]
[-all]
[-user USER]
[-password]
[-url URL]
[-proxy PROXY]
[-storetype STORETYPE]
[-secure SECURE]
```

Parameters

Table 9-46 ahfctl unsetserviceupload Command Parameters

Parameter	Description
all	All of the parameters.
user	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
password	Specify the password of the user.
url	Specify the target URL to upload files in case of HTTPS type. For example, *https://samplehost.com*.

Table 9-46 (Cont.) ahfctl unsetserviceupload Command Parameters

Parameter	Description
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`storetype`	Specify the Keystore format, for example, JKS and PKCS12.
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.

9.2.13 AHFCTL Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options

Review the list of commands that you can use to run compliance checks on Oracle Engineered and non-engineered systems.

- ahfctl compliance

9.2.13.1 ahfctl compliance

> **Note:**
>
> The `-setserviceupload`, `-unsetserviceupload`, `-getserviceupload`, `-checkserviceupload`, `-setdbupload`, `-unsetdbupload`, `-getdbupload`, `-checkdbupload`, and `-sanitize` parameters have been deprecated and removed in 23.3. Oracle recommends using the following commands instead.
>
> - `ahfctl setupload` replaces `-setserviceupload` and `-setdbupload`
> - `ahfctl unsetupload` replaces `-unsetserviceupload` and `-unsetdbupload`
> - `ahfctl getupload` replaces `-getserviceupload` and `-getdbupload`
> - `ahfctl checkupload` replaces `-checkserviceupload` and `-checkdbupload`
> - `ahfctl redact` replaces `-sanitize`

Syntax

```
ahfctl compliance -h
[-a]
[-acchk]
[-appjar]
[-applypatch]
[-apptrc]
[-asmhome]
[-asynch]
[-attachment]
```

```
[-autorun_id]
[-autoselect]
[-autostart]
[-autostart reset]
[-autostatus]
[-autostop]
[-autostop unset]
[-b]
[-baseline]
[-basic]
[-cellparallel]
[-cellparallelmax]
[-cells]
[-cellserial]
[-celltmpdir]
[-check]
[-checkdiscovery]
[-checkfaileduploads]
[-checkservicefaileduploads]
[-ciphers]
[-classicjson]
[-cleanup]
[-clusternodes]
[-cmupgrade]
[-configdir]
[-createprofile]
[-credfile]
[-cvuhome]
[-cvuonly]
[-db_config_name]
[-dball]
[-dbconfig]
[-dbnames]
[-dbnone]
[-dbparallel]
[-dbparallelmax]
[-dbserial]
[-debug]
[-decode]
[-decodezip]
[-deleteprofile]
[-diagpath]
[-diff]
[-disabledbupload]
[-disableserviceupload]
[-discovery]
[-discoverydir]
[-download]
[-downloadchecks]
[-duration]
[-ebs32bit]
[-ecra]
[-email_debuglevel]
[-enabledbupload]
[-enableserviceupload]
```

```
[-encode]
[-encodezip]
[-env]
[-escs_mgmt_proxy]
[-escs_user]
[-event]
[-excludecheck]
[-excludecvu]
[-excludedbnames]
[-excludediscovery]
[-excludemaa]
[-excludeprofile]
[-extzfsnodes]
[-f]
[-failedchecks]
[-fileattr]
[-fileattronly]
[-force]
[-from]
[-get]
[-getcheckxml]
[-getfromwallet]
[-getoutputdir]
[-h]
[-hardwaretype]
[-header]
[-help]
[-ibswitches]
[-ibtmpdir]
[-id]
[-identifier]
[-identitydir]
[-includecvu]
[-includedir]
[-includeprofile]
[-insecure]
[-javahome]
[-jdbcver]
[-json]
[-key]
[-localonly]
[-localuser]
[-lockcells]
[-logconf]
[-loglevel]
[-m]
[-merge]
[-modifyprofile]
[-module]
[-monthlyschedule]
[-mos_config_name]
[-mserver_conf]
[-nocleanup]
[-nocvu]
[-nodaemon]
```

```
[-nodeparallel]
[-nodeparallelmax]
[-nodeserial]
[-nopass]
[-noproxy]
[-nordbms]
[-noreport]
[-noscore]
[-noupgrade]
[-o]
[-orainst]
[-ordscheck]
[-ordsrmsetup]
[-ordssetup]
[-oss_config_name]
[-outfile]
[-output]
[-p]
[-packpollingtimeout]
[-perf_path]
[-postupgrade]
[-preupgrade]
[-probe]
[-profile]
[-purge_size]
[-querypatch]
[-r]
[-readenvconfig]
[-rediscovery]
[-remotedestdir]
[-remotehost]
[-remoteuser]
[-repair]
[-rmap]
[-rmdiscovery]
[-rollbackpatch]
[-rpackpollingtimeout]
[-runasroot]
[-s]
[-sendemail]
[-set]
[-setasm]
[-setcrs]
[-setemagent]
[-setinvloc]
[-setinwallet]
[-setjava]
[-setjdbcver]
[-setwls]
[-short]
[-show_critical]
[-showahfhome]
[-showdatadir]
[-showpass]
[-showrepair]
```

```
[-silentforce]
[-skip_security]
[-skip_usr_def_checks]
[-switches]
[-switchparallel]
[-switchparallelmax]
[-switchserial]
[-syslog]
[-systemtype]
[-t]
[-tag]
[-targetversion]
[-testemail]
[-tfa_version]
[-timeframe]
[-tls]
[-tmpdir]
[-torswitches]
[-trace]
[-u]
[-universal]
[-unlockcells]
[-unset]
[-unsetinwallet]
[-updatezip]
[-upgrade]
[-uploadfailed]
[-uploadservicefailed]
[-usediscovery]
[-username]
[-usesocket]
[-usessh]
[-v]
[-wallet_loc]
[-withdebugger]
[-withrepairdata]
[-zfsnodes]
[-zfssa]
[-zipfile]
```

Parameters

Table 9-47   ahfctl compliance Command Parameters

Parameter	Description
`-a`	Runs all checks, including the best practice checks and the recommended patch check. If you do not specify any options, then the tools run all checks by default.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-acchk`	Runs application continuity checks. Set the following environment variable before using the `-acchk` option: • `RAT_AC_ASMJAR`=path to asm-all-5.0.3.jar • `RAT_JAVA_HOME`=path to jdk8 • `RAT_AC_JDBCVER`=Version of the JDBC like 12 or 12.0.1 or 18 or 18.2 or 19 or 19.1 • `RAT_AC_JARDIR`=Directory where jar files are present for concrete class • `RAT_AC_TRCDIR`=Directory where trace files are present for Database coverage tests If the above environment variables are set, `orachk` can be run without any parameter to run `acchk`. Passing values in command line instead of environment variables. `ahfctl compliance -acchk` `-javahome` *`path to jdk8`* `-asmhome` *`path to asm-all-5.0.3.jar`* `-jdbcver` *`jdbc version`* `-appjar` *`directory where jar files are present for concrete class`* `-apptrc` *`directory where database trace files are present to measure database coverage`* Optional variable `RAT_ACTRACEFILE_WINDOW` variable can be set to *number of days*. Based on this value, files older than the `RAT_ACTRACEFILE_WINDOW` days are ignored. **Note:** `-acchk` can be run either for both database coverage and concrete classes or can be run only for database coverage or concrete class separately.
`-appjar`	Specify the directory where `jar` files are present.
`-applypatch`	Applies a new `orachk` patch for the specified bug ID when `orachk_`*`bug_id`*`.zip` is provided. Applies a new `orachk` data patch for the specified data timestamp when `orachk_data_`*`timestamp`*`.zip` is provided.
`-apptrc`	Use `-apptrc` with `-acchk`. Used to specify the directory where trace files are present.
`-asmhome` *`path to asm jar`*	Specify to set asm home for `acchk`.
`-asynch`	Used to send remote `orachk` run in background. Used `-asynch` in combination with command `-remotehost`.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-attachment` *`filename`*	When specified with `-testemail`, sends a test email with attachment to validate email configuration. Attachment should be present on the local node.
`-autorun_id`	Exits `orachk` if an `autorun` with same ID is already running.
`-identitydir` *`directory`* `[-universal|-autoselect]`	Used to specify identity files directory where identity files to all remote host are present. `-universal`: Same identity file is applicable to all of the remote hosts. `-autoselect`: Automatically selects the identity files for multiple remote hosts. Identity file name must follow the naming convention as follows: • `id_ENCRYPTION.HOSTNAME.USER` • `id_ENCRYPTION.*.*` (with -universal) • `id_ENCRYPTION.TAG.USER` (with -autoselect) For example: `id_dsa.myhost67.root` RSA is the default SSH encryption. For DSA SSH encryption, set `RAT_SSH_ENCR="dsa"`.
`-autostart`	Autostart will automatically set and run the `orachk` daemon.
`-autostart reset`	Starts and loads the default schedulers.
`-autostatus`	Checks the status of the scheduler.
`-autostop`	Use `-autostop` to remove `autostart`. It will stop the daemon and remove auto schedule entries from the wallet.
`-autostop unset`	Removes all default unmodified schedulers.
`-b`	Runs only the best practice checks.
`-baseline`	Use `-baseline` option with `-fileattr` to specify the baseline snapshot path.
`-basic`	Use `-basic` encrypt/decrypt using utf-8 character encoding.
`-cellparallel` *`n`*	Runs `orachk` on cells in parallel. *n*: Specify the number of child processes to run on cells. Default is 25% of CPUs.
`-cellparallelmax`	Runs `orachk` on cells in parallel. Number of child processes will be equal to the minimum number of CPUs and number of cells.
`-cells`	Specify a comma-delimited storage server names or file containing storage server names separated by newline to run `orachk` only on the selected storage servers.
`-cellserial`	Runs `orachk` in serial on storage servers.
`-celltmpdir` *`path`*	Sets `RAT_CELL_TMPDIR` internally. Creates `orachk` files on storage servers to non-default location.
`-check`	Runs a specific set of checks. Specify check IDs at the command prompt.
`-checkdiscovery`	Checks if `orachk` cache discovery exist or not.
`-checkfaileduploads`	Prints a list of collections for which upload failed.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-checkservicefailedupl oads`	Prints a list of collections for which service upload failed.
`-ciphers` *`list of ciphers`*	Specify ciphers for curl OSS upload.
`-classicjson`	Generates valid JSON files with results, exceptions, and recommendations.
`-cleanup`	Cleans up the temporary directory.
`-clusternodes`	Specify a comma-delimited list of node names or file containing node names separated by newline to run only on a subset of nodes.
`-cmupgrade`	Upgrades the Collection Manager if a new version of Collection Manager is available and database upload parameters are set in the `orachk` wallet.
`-configdir` *`dir`*	Use to configure ORDS.
`-createprofile`	Creates a custom profile. Specify a custom profile name followed by a list of comma-delimited check IDs to populate.
`-credfile` *`credential file`*	Use to specify a credential file. You need this credential file to run in non-interactive mode.
`-cvuhome`	You can specify a different Cluster Verification Utility (CVU) home with this parameter. When not specified, CVU from GRID home is run.
`-cvuonly`	Runs only Cluster Verification Utility (CVU) related checks.
`-db_config_name` *`db name`*	Use to set the name of database upload configuration.
`-dball`	Runs the database checks on all databases discovered on the system. Does not prompt for database selection.
`-dbconfig`	Specify a comma-delimited list of database homes with corresponding names to run only on a subset of databases. Does not prompt for database selection. Database home and corresponding names are separated by '%' while dbnames corresponding to home are separated by ':'.
`-dbnames` *`db_names`*	Specify a comma-delimited list of database names to run only on a subset of databases.
`-dbnone`	Skips all the database checks. Does not prompt for database selection.
`-dbparallel` *`n`*	Runs `SQL`, `SQL_COLLECT`, and operating system checks in parallel. *n*: Specify the number of child processes. Default is 25% of CPUs.
`-dbparallelmax`	Runs `SQL`, `SQL_COLLECT`, and operating system checks in parallel. Number of child processes will be equal to the minimum number of CPUs and number of databases.
`-dbserial`	Runs `SQL`, `SQL_COLLECT`, and operating system checks in serial.
`-debug [-module]`	Runs `orachk` in debug mode and generates debug log.
`-decodezip` *`zipfilename`*	Use to decrypt the encrypted collection.
`-deleteprofile`	Deletes the specified custom created profile.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-diagpath` *`path`*	Specify the path where storage server diagnostic package will be copied.
`-diff`	Reports the difference between the two HTML reports. For example: `-diff` *`old_report new_report`* `[-outfile` *`output_HTML`*`] [-force]` Specify a directory name, or a ZIP file, or an HTML report file as *old_report* and *new_report*.
`-disabledbupload`	Disables database upload if database upload parameters are set in the wallet. Default behavior of database upload is enabled.
`-disableserviceupload`	Disables service upload if service upload parameters are set in the wallet. Default behavior of service upload is enabled.
`-discovery`	Cache discovery data, which can use for future `orachk` runs.
`-discoverydir` *`location`*	Specify `orachk` cache discovery location.
`-download`	Downloads the `orachk.zip` file from the Oracle website.
`-downloadchecks`	Downloads the `user_defined_checks.xml` file from Oracle Trace File Analyzer.
`-duration` *`duration`*	The duration parameter specifies the number of hours of logs and traces to include in the storage server diagnostic package. Valid values are from 1 (default) to 6.
`-ebs32bit`	Runs `orachk` for EBS 32-bit database on Linux.
`-ecra`	Use to specify that `orachk` is running from ECRA.
`-email_debuglevel [1|2]`	When specified, displays debug messages for email connection and for all messages sent to and received from the server.
`-enabledbupload`	Enables database upload if database upload parameters are set in the wallet. Default behavior of database upload is enabled.
`-enableserviceupload`	Enables service upload if service upload parameters are set in the wallet. Default behavior of service upload is enabled.
`-encodezip` *`zipfilename`*	Encrypts the collection.
`-env` *`env type`*	Sets the environment type. Specify `NORMAL`/`AHF`/`ATP` values as `env` type.
`-escs_mgmt_proxy`	Use to specify that `orachk` is running from Exascale service management proxy.
`-escs_user`	The `-escs_user` option is applicable to Exascale. Specify a user to run checks with user for which `sudo` has been configured on cells and has the ability to SSH to cells.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-event [filename:pattern:task[,filename:pattern:task]]|1`	Applicable to daemon mode. Sets `RAT_SYS_EVENTS` internally. Watches specified files for specified patterns to initiate `orachk` run per specified task. `1` : Watches default files for default pattern to initiate `orachk` run per corresponding default task. `filename:pattern,task`: Watches filename for pattern to initiate `orachk` run per specified task.
`-excludecheck`	Excludes specific set of checks, enter check IDs at the command prompt.
`-excludecvu`	When specified, excludes Cluster Verification Utility (CVU) related checks.
`-excludedbnames` *`db_names`*	Specify a comma-delimited list of database names to exclude.
`-excludediscovery`	Excludes the discovered directories. Use with `-fileattr [start|check]` option.
`-excludemaa`	Excludes Maximum Available Architecture.
`-excludeprofile` *`profile1,profile2,...`*	Excludes specified profiles.
`-extzfsnodes`	Specify a comma-delimited external ZFS storage appliance names to run `orachk` only on the selected external storage appliances.
`-failedchecks`	Use to run `FAIL`, or `INFO`, or `WARNING` checks from a previous run. Specify an HTML file, or collections, or an output directory containing the HTML file.
`-fileattr`	Checks file attribute changes. **Options:** • `start`: Takes file attributes snapshot of discovered directories. • `check`: Takes a recent snapshot of discovered directories and compares with the previous snapshot. • `remove`: Removes file attribute snapshots and related files. • `-includedir`: Includes directories specified at the command-line to check file attributes. • `-excludediscovery`: Excludes the discovered directories. • `-baseline` *`baseline snapshot path`* • `-fileattronly`: Performs file attributes check only and exits `orachk`.
`-fileattronly`	Performs file attributes check and exits `orachk`. Use with `-fileattr` option.
`-force`	Use `-force` with either `-diff` or `-merge`. With `-diff`, the `-force` option is used to compare different profiles collections or profile with non-profile collection. With `-merge`, the `-force` option is used to merge collections from `dom0` and `domu`, or global and local zones.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-from` *`time`*	Specify when to start collecting the logs and traces for storage server diagnostic package. The format of cell diagpack start time is as follows: • `Mon/dd/yyyy hh:mm:ss` • `yyyy-MM-dd hh:mm:ss` • `yyyy-MM-ddThh:mm:ss` • `yyyy-MM-dd` • `now`
`-get` *`parameter`* `or all [-id` *`ID`*`]`	Displays the value of the specified daemon parameter or all the parameters. Use with `-id` *`ID`* to get values for specified autorun schedule ID. Supported parameters are: • `autorun_schedule` • `autorun_flags` • `notification_email` • `collection_retention`
`-getcheckxml`	Gets user-defined checks for execution. User-defined checks are written in XML format.
`-getfromwallet`	Gets an entry for a key in the wallet.
`-getoutputdir`	Prints the output directory.
`-hardwaretype generation-socket`	Specify hardware generation and socket for a system so that `orachk` can run a correct set of checks. Socket is mandatory only for Exadata.
`-header` *`header`*	Stores the *`executionId`* in the `ahf.properties` file.
`-ibswitches`	Specify a comma-delimited InfiniBand switch names to run `orachk` only on the selected InfiniBand switches.
`-ibtmpdir` *`path`*	Sets `RAT_IB_TMPDIR` internally. Creates `orachk` files on the switches to a non-default location.
`-identifier` *`SR or BUG Number`*	Specify an SR or a BUG number.
`-identitydir` *`directory`* `[-universal|-autoselect]`	Specify identity files directory where identity files to all remote host are present. **Options:** • `-universal`: Same identity file is applicable to all of the remote hosts. • `-autoselect`: Automatically selects the identity files for multiple remote hosts.
`-includecvu`	Includes Cluster Verification Utility (CVU) related check.
`-includedir`	Includes the directories specified at the command-line to check file attributes. Use with `-fileattr` option.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-includeprofile`	Specify a comma-delimited list of profiles to the existing checks list. `ahfctl compliance -includeprofile` *`profile1`*`,` *`profile2`*`...` **Note:** You cannot: • use `-includeprofile` and `-profile` options together • use `-includeprofile` and `-excludeprofile` options together
`-insecure <True/False>`	Enables or disables security.
`-javahome`	Use `-javahome` option with `-acchk`. `-javahome` option is used to specify the `JAVA_HOME` directory for a JDK8 installation.
`-jdbcver` *`jdbc version`*	Use to specify JDBC version for `acchk`.
`-json`	Use to generate valid JSON files.
`-key` *`key`*	When specified, use this key for encryption or decryption.
`-localonly`	Runs checks only on the local node.
`-localuser`	The `-localuser` option allows the user to run `root` checks with user for which `sudo` has been configured and has ability to SSH on the remote node.
`-lockcells all | -cells [`*`cell names or cell IPs separated by comma`*`][file` *`containing cell names or IPs separated by newline`*`]`	Locks the storage cells. Applicable only to Exadata and SuperCluster.
`-logconf` *`filename`*	Specify the file containing logging configuration.
`-loglevel DEBUG|INFO|WARNING|ERROR|CRITICAL|NOTSET`	Sets the logging level.
`-m`	Excludes checks for Maximum Availability Architecture (MAA) scorecards.
`-merge [-force]`	Merges reports by providing a comma-delimited list of directories or zip files. **Option:** • `-force`: Merges collections from `dom0` and `domu` or global and local zones.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-modifyprofile`	Modifies a custom profile. Specify the profile name followed by a comma-delimited check IDs. If the checks are present in the profile, they will be removed. If not, check would be added.
`-debug [-module]`	Runs `orachk` in debug mode and generates debug log for the specified region. Valid modules are: • `setup` • `discovery` • `execution` • `output`
`-mos_config_name` *`mos config name`*	Specify the name of MOS upload configuration.
`-mserver_conf hostname[port,debuglevel]`	Email server configuration details. **Options:** • *hostname*: SMTP host server name or IP address. • *port*: SMTP host server port. • *debuglevel*: It can either be 0 or 1. Displays email verbose output
`-nocleanup`	Specify not to clean the temporary directory.
`-nocvu`	Excludes Cluster Verification Utility (CVU) related checks.
`-nodaemon`	Does not send commands to the daemon, usage is interactive.
`-nodeparallel` *`n`*	Run `orachk` on remote nodes in parallel. *n*: Specify the number of child processes to run on the remote node. Default is 25% of CPUs.
`-nodeparallelmax`	Runs `orachk` on remote nodes in parallel. Number of child processes will be equal to the minimum number of CPUs and the number of remote nodes.
`-nodeserial`	Runs `orachk` in serial on compute nodes.
`-nopass`	Skips PASSed checks to print in `orachk` report and uploads to the database.
`-noproxy <True/False>`	Use to disable or enable proxy.
`-nordbms`	If CRS is installed, but Oracle Database is not installed and still the user wants to run `orachk` then user can specify this option.
`-noreport`	Specify not to generate HTML report.
`-noscore`	Specify not to print healthscore in the `orachk` HTML report.
`-noupgrade`	Specify `-noupgrade` option if you do not want to be prompted for an upgrade even if a later version is available under the location specified by `RAT_UPGRADE_LOC`.
`-ordscheck`	Lets you know if ORDS is setup or not. If ORDS is setup, then it prints the URL to be used to submit runs using REST APIs.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-ordsrmsetup`	Removes ORDS setup. It stops the daemon running and deletes the ORDS user's home directory if no collections are found . If collections from previous runs are found, then it prompts the user before a decision is made to remove the setup or not.
`-ordssetup [dir where ords.war is present [-configdir` *dir used for configuring ORDS*`]] [-ordshomedir` *Any directory which has write permission*`]`	Sets up ORDS on a system. **Options** • `-configdir` is optional. If `-configdir` is not specified, then the `dir` where `ords.war` is present is considered as `configdir`. • `-ordshomedir` is optional. This directory needs to be specified if `root` does not have privilege to run `useradd` to create the default home directory. When `-ordshomedir` is specified, then user home will be the path passed along with the `-ordshomedir`.
`-oss_config_name` *ossconfigname*	Specify the name of OSS upload configuration.
`-outfile`	Use `-outfile` option with `-diff`. Used to manually provide a name for the output file.
`-output` *path*	Sets `RAT_OUTPUT` internally. Creates an `orachk` collection zip file and output directory to non-default (current) location.
`-p`	Runs patch checks only.
`-packpollingtimeout` *timeout(in secs)*	Specify the amount of time for which `orachk` will wait for submitted storage server diagnostic package generation to finish.
`-postupgrade`	Runs post-upgrade best practice checks for 11.2.0.4 databases and above.
`-preupgrade`	Runs pre-upgrade best practice checks for 11.2.0.4 databases and above .
`-probe`	Generates probe XML for Enterprise Manager.
`-profile` *profile1, profile2,...*	Specify a comma-delimited list of profiles to run only the checks in the specified profiles.
`-purge_size`	Specify to purge compliance data larger than a certain size.
`-querypatch`	Lists the details of all of the installed `orachk` patches, or for the specified bug ID, or data timestamp.
`-readenvconfig`	Reads configuration file. This file contains parameters previously which were set using `RAT` environment variables.
`-rediscovery`	Refreshes cache discovery data, which can be used for future `orachk` runs.
`-remotedestdir`	Specify the remote destination directory so that `orachk` run can take place from that location.
`-remotehost`	Use to launch `orachk` on a remote system. Once the run on remote system is over, `orachk` brings back collection zip into local host. This feature requires identity file to make connection to remote system
`-remoteuser`	Specify the remote user to run `orachk`. `-remoteuser` is used in combination with `-remotehost`.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description

`-repair` *`file`*`|`
`checkids``|all`
	Repairs checks.
	Options:
	- *`file`*: File containing check ids that need to be repaired.
	- *checkids*: Comma-delimited check IDs that need to be repaired.
	- `all`: Repairs all checks.

`-rmap`	Prints reverse map for sanitized elements.
`-rmdiscovery`	Removes cache discovery data.
`-rollbackpatch`	Rolls back the applied patch `orachk_`*`bug_id`*`.zip` to it is previous state at which the patch was applied. Rolls back the applied data patch `orachk_data_`*`timestamp`*`.zip` to the released production version.
`-rpackpollingtimeout` *`timeout(in secs)`*	Specify the amount of time for which `orachk` will wait for previously submitted (within the timeframe) storage server diagnostic package generation to finish.
`-runasroot`	Runs as `root` user by a promoted user. User can be promoted by running `ahfctl access promote -user` *`username`* as `root` user.
`-sendemail "notification_email=emailaddress[,emailaddress]"`	Emails `orachk` run report.
`-set` *`parameter`* `or all [-id` *`ID`*`]`	Sets parameter(s) for autorun. Configures the `orachk` daemon parameter like `param1=`*`value1`*`;param2=`*`value2`*`....` If `-id` *`ID`* is specified, then it will configure `orachk` daemon parameter(s) for specified autorun schedule ID.
`-setasm` *`path to asm home`*	Sets ASM HOME.
`-setcrs` *`crs home`*	Sets `crs` home.
`-setemagent` *`path to em agent home`*	Sets EM Agent home.
`-setinvloc` *`path to inventory location`*	Sets inventory location.
`-setinwallet` *`wallet_key1,wallet_key2,...`*	Sets an entry for the key:value pair in the wallet.
`-setjava` *`path to java home`*	Sets Java home.
`-setjdbcver` *`jdbc version`*	Sets JDBC version.
`-setwls` *`path to wls home`*	Sets Weblogic server home.
`-short`	Prints short version.
`-show_critical`	Shows critical checks in the `orachk` report by default.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-showahfhome`	Shows AHF home directory.
`-showdatadir`	Shows `orachk` data directory.
`-showpass`	Shows PASSed checks in the `orachk` report by default.
`-showrepair` *`checkid`*	Displays check repair command. *checkid* : Shows repair command for the given check ID.
`-silentforce`	Runs `orachk` in non-interactive mode. Run will not prompt for inputs and hence consider default values.
`-skip_security`	Skips security validation.
`-skip_usr_def_checks`	Does not run the checks specified in the user-defined XML file.
`-switches` *`switch1, switch2,....`*	Specify a comma-delimited switch names to run `orachk` on switches.
`-switchparallel` *`n`*	Runs `orachk` on switches in parallel. *n*: Specify the number of child processes to run on switches. Default is 25% of CPUs.
`-switchparallelmax`	Runs `orachk` on switches in parallel. Number of child processes will be equal to the minimum number of CPUs and number of switches.
`-switchserial`	Runs `orachk` in serial on switches.
`-syslog`	Sets `RAT_SEND_TO_RSYSLOG` internally. `orachk` will write the JSON results to syslog.
`-tag` *`tagname`*	Appends *tagname* to the report name. *Tagname* must contain only alphanumeric characters.
`-targetversion`	Use `-targetversion` with `-preupgrade` in order to specify the target version of the database. Specify a valid database target version and re-run again.
`-testemail "notification_email=emailaddress[,emailaddress]"`	Sends a test email to validate email configuration.
`-timeframe` *`timeframe (in secs)`*	`orachk` will pick storage server diagnostic package if start time is within the timeframe.
`-tls` *`tlsversion`*	Specify the version of TLS for curl OSS upload.
`-tmpdir` *`path`*	Sets `RAT_TMPDIR` internally. Creates `orachk` temporary files to non-default (current user home) location.
`-torswitches`	Specify a comma-delimited Top of Rack switch names to run `orachk` only on the selected Top of Rack switches.
`-identitydir` *`directory`* `[-universal|-autoselect]`	Specify identity files directory where identity files to all remote host are present. **Options:** • `-universal`: Same identity file is applicable to all of the remote hosts. • `-autoselect`: Automatically selects the identity files for multiple remote hosts.

Table 9-47 (Cont.) ahfctl compliance Command Parameters

Parameter	Description
`-unlockcells all | -cells [`*`cell names or cell IPs separated by comma`*`][`*`file containing cell names or IPs separated by newline`*`]`	Unlocks the storage cells. Applicable only for Exadata and SuperCluster. **Options:** • `all`: Unlocks all of the available cells. • `-cells`: Comma-delimited list of cell names or cell IP addresses.
`-unset` *`parameter`* `or all [-id` *`ID`*`]`	Unsets set parameter(s). If `-id` *`ID`* is specified, it will unset the parameter for specified autorun schedule ID.
`-unsetinwallet`	Deletes an entry for the key:value pair in the wallet.
`-updatezip`	Updates `orachk.zip` wallet with the wallet of unzipped toolkit.
`-upgrade`	Force upgrades the version of `orachk` being run if a newer version is available under the location specified by `RAT_UPGRADE_LOC`.
`-uploadfailed all | [`*`comma-delimited list of collections`*`]`	Uploads collections to the database.
`-uploadservicefailed all | [`*`comma-delimited list of collections`*`]`	Uploads collections to the service.
`-usediscovery`	Specify to use cache discovery data for the `orachk` run.
`-username` *`username`*	Specify a user name. User name is required for retrieving URL.
`-usesocket`	Specify to use Oracle Trace File Analyzer socket to run.
`-usessh`	In full AHF installation, `orachk` uses socket connection to communicate with remote compute nodes. `usessh` will force `orachk` to use SSH protocol to communicate with remote compute nodes.
`-v`	Displays version.
`-wallet_loc`	Specify the custom location of the wallet. Setting this would override the default location of the wallet.
`-zfsnodes`	Specify a comma-delimited list of ZFS storage appliance names to run `orachk` only on the selected storage appliances.
`-zfssa`	Specify a comma-delimited list of ZFS storage appliance names to run `orachk`.
`-zipfile` *`zipfile for MOS upload`*	Sets zip for MOS upload.

Related Topics

- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

9.2.14 Running AHFCTL Commands to Sanitize Sensitive Information and Reverse Map Sanitized Elements

Use `ahftcl redact` to sanitize sensitive data in regular files, zip files and directories, and `ahfctl rmap` to reverse map the elements sanitized using Oracle Trace File Analyzer and Oracle ORAchk.

- ahftcl redact
  Use the `ahftcl redact` command to sanitize sensitive data in regular files, zip files and directories.
- ahftcl rmap
  Use the `ahfctl rmap` command to reverse map the elements sanitized using Oracle Trace File Analyzer and Oracle Orachk.

9.2.14.1 ahftcl redact

Use the `ahftcl redact` command to sanitize sensitive data in regular files, zip files and directories.

Syntax

> **Note:**
>
> The `ahftcl redact` command is not supported on Microsoft Windows.

```
ahfctl redact
[-h]
[-i I]
[-o O]
[-m {mask,sanitize}] [-l {system,database,userdata,all}
[{system,database,userdata,all} ...]]
```

Usage

```
ahfctl redact -i file_name -o out_dir -m mask
```

```
ahfctl redact -i dir_name -m sanitize -l system database
```

Parameters

Table 9-48 ahfctl redact Command Parameters

Parameter	Description
`-i I`	Redacts the specified file or directory. Specify a regular file, zip file, or directory. Works with targets in the working directory or full path to the target.

Table 9-48 (Cont.) ahfctl redact Command Parameters

Parameter	Description
`-o O`	Full path to output directory (If not specified, then defaults to in-place redaction)
`-m {mask,sanitize}`	Specify a redaction mode. Redaction modes: - `mask`: Replaces the entity instance with asterisk, for example, `'hrdb'` with `'****'` - `sanitize`: (Default) Replaces the entity instance with substitution map value, for example, `'PDB1'` with `'2zq2'`.
`-l {system, database, userdata, all} [{system, database, userdata, all} ...]`	Redact only the subset of entities based on the level specified. - `system`: hostname, IP address, port, username - `database`: dbname, tbsname, svcname, sqlstmt - `userdata`: userdata in block and redo dumps - `all`: (Default) All levels

Example 9-48 Redacting a regular file

```
ahfctl redact -i stbm000004-vm15.tfa_Thu_Jul_22_13_24_56_UTC_2021.zip.txt -m
mask

AHF is redacting

/opt/oracle.ahf/data/repository/testcollection/stbm000004-
vm15.tfa_Thu_Jul_22_13_24_56_UTC_2021.zip.txt

Successfully redacted file

/opt/oracle.ahf/data/repository/testcollection/owlo000004-
vm15.tfa_Thu_Jul_56_53_62_13_UTC_2021.zip.txt
```

Example 9-49 Redacting a zip file

```
ahfctl redact -i testzip.zip -o dirtest -l system database

AHF is redacting /opt/oracle.ahf/data/repository/testcollection/testzip.zip

Successfully redacted zip

/opt/oracle.ahf/data/repository/testcollection/dirtest/redacted_testzip.zip
```

Example 9-50 Redacting a directory

```
ahfctl redact -i test -m mask -l system userdata

AHF is redacting /opt/oracle.ahf/data/repository/testcollection/test

Successfully redacted dir /opt/oracle.ahf/data/repository/testcollection/test
```

9.2.14.2 ahfctl rmap

Use the `ahfctl rmap` command to reverse map the elements sanitized using Oracle Trace File Analyzer and Oracle Orachk.

Syntax

> **Note:**
>
> The `ahfctl rmap` command is not supported on Microsoft Windows.

```
ahfctl rmap
[-h]
[-l L [L ...]]
[-all]
```

Usage

```
ahfctl rmap -all


ahfctl rmap -l string1 string2 string3
```

Parameters

Table 9-49   ahfctl rmap Command Parameters

Parameter	Description
`-l L [L ...]`	List of substituted strings, for example, string1 string2 string3...
`-all`	(Default) Prints all original strings from the substituted stored strings.

Example 9-51   ahfctl rmap

```
ahfctl rmap -l yudaqpec dwootq 49_57_77_95
_______________________________________________________________________
_________
|  Entity Type   |   Substituted Entity Name    |      Original Entity
Name     |
_______________________________________________________________________
_________
|    username    |           yudaqpec           |
barumuga           |
|    username    |            dwootq            |
emcadm            |
|      IPV4      |         49_57_77_95          |
16_11_47_46          |
```

____
___

9.2.15 Running AHFCTL Commands to Manage InfiniBand and RoCE Switches

Use the `ahfctl` commands to manage InfiniBand and RoCE switches.

> **Note:**
>
> Only the AHF install user with the `root` user privileges can manage switch configurations.

- ahfctl switch
  Use the `ahfctl switch` command to manage manage InfiniBand and RoCE switches.

9.2.15.1 ahfctl switch

Use the `ahfctl switch` command to manage manage InfiniBand and RoCE switches.

Syntax

```
ahfctl switch
[-h]
[-configure]
[-switches SWITCHES]
[-status]
[-json]
[-deconfigure]
[-debug]
```

Parameters

Table 9-50 ahfctl switch Command Parameters

Parameter	Description
`-configure`	Specify to configure InfiniBand and RoCE switches.
`-switches` *`SWITCHES`*	Specify a comma-delimited list of switches to configure. For example: *switch1*,*switch2*,*switch3*
`-status`	Specify to get configuration details of InfiniBand and RoCE switches.
`-json`	Specify to get configuration details of InfiniBand and RoCE switches in JSON format.
`-deconfigure`	Specify to remove configuration details of InfiniBand and RoCE switches from AHF.
`-debug`	Specify to run the debug script.

Example 9-52 ahfctl switch examples

- To configure InfiniBand and RoCE switches:

  ```
  ahfctl switch -configure
  ```

- To store configuration details of the switches specified:

  ```
  ahfctl switch -configure -switches sw1,sw2,sw3
  ```

- To get configuration details of a switch:

  ```
  ahfctl switch -status
  ```

- To get configuration details of a switch in JSON format:

  ```
  ahfctl switch -status -json
  ```

- To remove configuration details of a switch from AHF:

  ```
  ahfctl switch -deconfigure
  ```

If security policies do not permit connection to an InfiniBand switch as the default user root, then specify a different user by setting the `RAT_IBSWITCH_USER` environment variable:

```
export RAT_IBSWITCH_USER=user
```

If security policies do not permit connection to a RoCE switch as the default user admin, then specify a different user by setting the `RAT_IBSWITCH_USER` environment variable:

```
export RAT_IBSWITCH_USER=user
```

> **Note:**
>
> AHF does not discover RoCE switches automatically. You must provide a list of available switches using the `RAT_SWITCHES` environment variable or while running the `ahfctl switch -configure` command.

```
export RAT_SWITCHES="scaqap06sw-roceb1,scaqap06sw-rocea1"
```

```
ahfctl switch -configure -switches sw1,sw2,sw3
```

You can also configure RoCE switches by running the `ahfctl switch -configure` command without specifying a comma-delimited list of RoCE switches. When you run the `ahfctl switch -configure` command, AHF will prompt you to enter a comma-delimited list switch names.

9.2.16 Running AHFCTL Commands to Uninstall AHF

Use the `ahfctl` commands to uninstall AHF.

- ahfctl uninstall
  Use the `ahfctl uninstall` command to uninstall Oracle Autonomous Health Framework.

9.2.16.1 ahfctl uninstall

Use the `ahfctl uninstall` command to uninstall Oracle Autonomous Health Framework.

Running the command:

- Stops Oracle Orachk
- Stops Oracle Trace File Analyzer
- Deletes the Oracle Autonomous Health Framework installation directory

Syntax

```
ahfctl uninstall
[-local]
[-silent]
[-deleterepo]
```

Parameters

Table 9-51 ahfctl uninstall Command Parameters

Parameter	Description
`-local`	Uninstalls Oracle Autonomous Health Framework only on the local node. **Note:** If you do not specify the `-local` option, then the uninstaller script uninstalls Oracle Autonomous Health Framework from all of the configured nodes.
`-silent`	Specify to not ask any uninstall questions.
`-deleterepo`	Deletes the Oracle Autonomous Health Framework repository.

9.3 TFACTL Command Reference

Review the list of TFACTL commands to manage Autonomous Health Framework.

- Running Oracle Trace File Analyzer Administration Commands
  You need `root` access to `tfactl`, or `sudo` access to run all administration commands.

- Running Oracle Trace File Analyzer Summary and Analysis Commands
  Use these commands to view the summary of deployment and status of Oracle Trace File Analyzer, and changes and events detected by Oracle Trace File Analyzer.
- Running Oracle Trace File Analyzer Diagnostic Collection Commands
  Run the diagnostic collection commands to collect diagnostic data.

9.3.1 Running Oracle Trace File Analyzer Administration Commands

You need `root` access to `tfactl`, or `sudo` access to run all administration commands.

Table 9-52 Basic tfactl commands

Command	Description
`tfactl start`	Starts the Oracle Trace File Analyzer daemon on the local node.
`tfactl stop`	Stops the Oracle Trace File Analyzer daemon on the local node.
`tfactl enable`	Enables automatic restart of the Oracle Trace File Analyzer daemon after a failure or system reboot.
`tfactl disable`	Stops any running Oracle Trace File Analyzer daemon and disables automatic restart.
`tfactl uninstall`	Removes Oracle Trace File Analyzer from the local node.
`tfactl syncnodes`	Generates and copies Oracle Trace File Analyzer certificates from one Oracle Trace File Analyzer node to other nodes.
`tfactl restrictprotocol`	Restricts the use of certain protocols.
`tfactl status`	Checks the status of an Oracle Trace File Analyzer process. The output is same as `tfactl print status`.

- tfactl access
  Use the `tfactl access` command to enable non-root users to have controlled access to Oracle Trace File Analyzer, and to run diagnostic collections.
- tfactl availability
  Use the `tfactl availability` command to enable or disable resources for Availability Score, and to search a specific data type in the telemetry cache.
- tfactl blackout
  Use the `tfactl blackout` command to suppress diagnostic collections at a more granular level. By default, blackout will be in effect for 24 hours.
- tfactl cell
  Use the `tfactl cell` command to print or modify various storage cell configuration.
- tfactl checkupload
  Use the `tfactl checkupload` command to validate the configured upload parameters.

- tfactl dbcheck
  Use the `tfactl dbcheck` command to collect diagnostic data from the Oracle Exadata machine to identify issues with operating system, file system, memory, and I/O system.
- tfactl diagnosetfa
  Use the `tfactl diagnosetfa` command to collect Oracle Trace File Analyzer diagnostic data from the local node to identify issues with Oracle Trace File Analyzer.
- tfactl disable
  Use the `tfactl disable` command to prevent the Oracle Trace File Analyzer daemon from restarting.
- tfactl enable
  Use the `tfactl enable` command to enable automatic restart of the Oracle Trace File Analyzer daemon after a failure or system reboot.
- tfactl get
  Use the `tfactl get` command to view the details of various Oracle Trace File Analyzer configuration settings.
- tfactl floodcontrol
  Use the `tfactl floodcontrol` command to limit or stop Oracle Trace File Analyzer collecting the same events in a given frame of time.
- tfactl getresourcelimit
  Use the `tfactl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.
- tfactl getupload
  Use the `tfactl getupload` command to fetch the details of configured upload parameters.
- tfactl host
  Use the `tfactl host` command to add hosts to, or remove hosts from the Oracle Trace File Analyzer configuration.
- tfactl insight
  Use the `tfactl insight` command to generate AHF Insights report from across nodes in the AHF cluster.
- tfactl index
  Use the `tfactl index` command to index events.
- tfactl print
  Use the `tfactl print` command to print information from the Berkeley DB (BDB).
- tfactl print inventory
  Use the `tfactl print inventory` command delete file metadata.
- tfactl print syncstatus
  Use the `tfactl print syncstatus` command to get the sync status of TFA on all cluster nodes.
- tfactl purgeindex
  Use the `tfactl purgeindex` command to index events.
- tfactl purgeinventory
  Use the `tfactl purgeinventory` command delete file metadata.
- tfactl queryindex
  Use the `tfactl queryindex` command to view stored events.

- tfactl rediscover
  Use the `tfactl rediscover` command to discover new components and update inventory.
- tfactl refreshconfig
  Use the `tfactl refreshconfig` command to refresh and list Oracle Trace File Analyzer cron jobs.
- tfactl refreshconfig modifycron
  Use the `tfactl refreshconfig modifycron` command to modify the Oracle Trace File Analyzer cron entry.
- tfactl restrictprotocol
  Use the `tfactl restrictprotocol` command to restrict certain protocols.
- tfactl sendmail
  Use the `tfactl sendmail` command to send a test email to verify SMTP configuration.
- tfactl set
  Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.
- tfactl setresourcelimit
  Use the `tfactl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.
- tfactl setupload
  Use the `tfactl setupload` command to set upload parameters.
- tfactl showrepo
  Use the `tfactl showrepo` command to get the repository locations of Oracle Autonomous Health Framework components.
- tfactl start
  Use the `tfactl start` command to start the Oracle Trace File Analyzer daemon on the local node, and also to start the desired support tool.
- tfactl startahf
  Use the `tfactl startahf` command to start the scheduler for Oracle Autonomous Health Framework components.
- tfactl status
  Use the `tfactl status` command to check the run status of Oracle Trace File Analyzer.
- tfactl statusahf
  Use the `tfactl statusahf` command to check the shceduler status for Oracle Autonomous Health Framework components.
- tfactl stop
  Use the `tfactl stop` command to stop the Oracle Trace File Analyzer daemon on the local node, and also to stop the desired support tool.
- tfactl stopahf
  Use the `tfactl stopahf` command to stop the scheduler for Oracle Autonomous Health Framework components.
- tfactl syncnodes
  Use the `tfactl syncnodes` command to generate and copy Oracle Trace File Analyzer certificates to other Oracle Trace File Analyzer nodes.

- tfactl uninstall
  Use the `tfactl uninstall` command to uninstall Oracle Autonomous Health Framework.
- tfactl upload
  Use the `tfactl upload` command to upload collections or files on demand.
- tfactl unsetresourcelimit
  Use the `tfactl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.
- tfactl unsetupload
  Use the `tfactl unsetupload` command to unset the configured upload parameters.
- tfactl version
  Use the `tfactl version` command to check the version of Oracle Autonomous Health Framework components.

9.3.1.15 tfactl insight

Use the `tfactl insight` command to generate AHF Insights report from across nodes in the AHF cluster.

AHF 23.8

Starting in AHF 23.8, you will be able to upload to pre-authenticated (PAR) URL. Uploading AHF Insights reports helps Oracle Cloud Operations to identify, investigate, track, and resolve system health issues and divergences in best practice configurations quickly and effectively.

Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D) and Oracle Base Database Service

To upload AHF Insights report to PAR location, run:

```
tfactl diagcollect -insight -last 1h -par <par_url>
```

```
tfactl insight -last 1h -par <par_url>
```

Syntax

```
tfactl insight
[-h]
[-node NODE]
[-last LAST | -for FOR | -from [FROM]]
[-to [TO]]
[-refresh]
[-keepinput]
[-par PAR]
[-request_from REQUEST_FROM]
[-onlyinsightsupload]
[-status]
```

Parameters

Prefix each option with a minus sign (-).

Option	Description
`-node all|local|` *`n1,n2,...`*	Specify a comma-delimited list of nodes from which to collect diagnostic information. Default is `all`.

`[-last <`*`n`*`><`*`m`*`|`*`h`*`|`*`d`*`>| | -from `*`time`*` -to `*`time`*` | -for `*`time`*`]`	• Specify the `-last` parameter to collect files that have relevant data for the past specific number of minutes (*m*), number of hours (*h*), or days (*d*). By default, using the command with this parameter also trims files that are large and shows files only from the specified interval.
	• Specify the `-from` and `-to` parameters (you must use these two parameters together) to collect files that have relevant data during a specific time interval, and trim data before this time where files are large.
	Supported time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`
	• Specify the `-for` parameter to collect files that have relevant data for the time given. The files `tfactl` collects will have timestamps in between which the time you specify after `-for` is included. No data trimming is done for this option.
	Supported time formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`
	`date`
	Note:
	If you specify both date and time, then you must enclose both the values in double quotation marks (""). If you specify only the date or the time, then you do not have to enclose the single value in quotation marks.

`-refresh`	Provide fresh data from AHF Insight sources.
`-keepinput`	Specifies not to remove the `input_collection` directory.
`-par `*`PAR`*	Uploads collection to a pre-authenticated URL.
`-request_from `*`REQUEST_FROM`*	Specifies the requestor of the collection.
`-onlyinsightsupload`	Specifies only to upload insights `zip` to Object Store or a pre-authenticated URL.
`-status`	Checks the status of AHF Insights.

9.3.1.1 tfactl access

Use the `tfactl access` command to enable non-root users to have controlled access to Oracle Trace File Analyzer, and to run diagnostic collections.

Non-root users can run a subset of `tfactl` commands. Running a subset of commands enables non-root users to have controlled access to Oracle Trace File Analyzer, and to run diagnostic collections. However, `root` access is still required to install and administer Oracle Trace File Analyzer. Control non-root users using the `tfactl access` command. Add or remove non-root users depending upon your business requirements.

> **Note:**
>
> By default, all Oracle home owners, OS DBA groups, and ASM groups are added to the Oracle Trace File Analyzer Access Manager list while installing or upgrading Oracle Trace File Analyzer.

AHF introduces two roles, **platinum** and **privileged-compliance-check** in release 22.3.

1. **platinum** can perform the following actions:
   - Run the `diagnosetfa` command to collect Oracle Trace File Analyzer diagnostic data from the local node to identify issues with Oracle Trace File Analyzer
   - Set `auto-upgrade`
   - Run compliance-checks as `root`
   - Update AHF metadata
   - Change AHF configuration parameters
   - Run default commands of a non-root TFA user
2. **privileged-compliance-checks** can perform the following actions:
   - Run compliance-checks as `root`
   - Run default commands of a non-root TFA user

- When AHF is upgraded, following operation will be performed for `orarom` user:
  - If the `orarom` user is already promoted, it will be added to the `platinum` role.
  - If the `orarom` user has not already been promoted, it will not be added to the `platinum` role
- After upgrade, to add any user to the `platinum` role, use the below commands:
  - To add a role for an existing TFA user:

    ```
    tfactl access grant -user <user_name> -role platinum
    ```

  - To remove a role for a user:

    ```
    tfactl access revoke -user <user_name> -role platinum
    ```

- A user who has been assigned a role is role-managed. It is not possible for the user to revert to the old promotion system.
- A user can have multiple roles.
- To find the current role of any user, run the `tfactl access lsusers` command.

```
tfactl access lsusers
.-------------------------------------------------------------------
------.
|            TFA Users in
Node1                                           |
+-----------+---------+----------
+----------------------------------------+
| User Name | Status  | Promoted |
Roles                                  |
+-----------+---------+----------
+----------------------------------------+
| dbusr     | Allowed | false    |
n/a                                    |
| giusr     | Allowed | true     |
n/a                                    |
| grid      | Allowed | n/a      | privileged-compliance-
checks           |
| orarom    | Allowed | n/a      |
platinum                               |
| oracle    | Allowed | n/a      | platinum, privileged-compliance-
checks |
'-----------+---------+----------
+----------------------------------------'
```

In this example:

- `dbusr` has the basic set of privileges
- `giusr` and `grid` have the ability to run compliance checks as `root` in addition to basic privileges
- `orarom` user has the privileges of `platinum` user in addition to basic privileges
- `orarom` user has the privileges of `platinum` and privileged-compliance-checks user in addition to basic privileges

Syntax

```
tfactl access <command> [options]
commands:lsusers|add|remove|block|unblock|promote|demote|grant|revoke|
reset|removeall
options: -user|-role|-json|-local
```

```
tfactl access lsusers
```

```
tfactl access lsusers [ -json ]
```

```
tfactl access lsusers [ -local ]
```

```
tfactl access add -user user_name
```

```
tfactl access add -user user_name -role role_name
```

```
tfactl access add -user user_name -role role_name [ -local ]
```

```
tfactl access remove -user user_name [ -local ]
```

```
tfactl access block -user user_name [ -local ]
```

```
tfactl access unblock -user user_name [ -local ]
```

```
tfactl access promote [ -local ]
```

```
tfactl access demote [ -local ]
```

```
tfactl access grant -user user_name -role role_name [ -local ]
```

```
tfactl access revoke -user user_name -role role_name [ -local ]
```

```
tfactl access reset
```

```
tfactl access removeall
```

Parameters

Table 9-53   tfactl access Command Parameters

Parameter	Description
`lsusers`	Lists all the Oracle Trace File Analyzer users.
`add`	Adds a user to the Oracle Trace File Analyzer access list.
`remove`	Removes a user from the Oracle Trace File Analyzer access list.
`block`	Blocks Oracle Trace File Analyzer access for non-root user. Use this command to block a specific user's access to Oracle Trace File Analyzer.
`unblock`	Enables Oracle Trace File Analyzer access for non-root users who were blocked earlier. Use this command to unblock a user that was blocked earlier by running the command `tfactl access block`.
`promote`	Promotes Oracle Trace File Analyzer access for non-root users. Use the `-local` flag to change settings only on the local node.
`demote`	Demotes Oracle Trace File Analyzer access for non-root users. However, the list of users who were granted access to Oracle Trace File Analyzer is stored, if the access to non-root users is promoted later. Use the `-local` flag to change settings only on the local node.
`grant`	Grants a role to a non-root user.
`revoke`	Revokes the role granted to a non-root user.
`reset`	Resets to the default access list that includes all Oracle Home owners and DBA groups.
`removeall`	Removes all Oracle Trace File Analyzer users. Remove all users from the Oracle Trace File Analyzer access list including the default users.

Example 9-53   tfactl access

To list all the Oracle Trace File Analyzer users:

```
tfactl access lsusers
.----------------------------------------------------------------------
---.
|            TFA Users in
Node1                                            |
+-----------+---------+----------
+-----------------------------------------+
| User Name | Status  | Promoted |
Roles                                  |
+-----------+---------+----------
+-----------------------------------------+
| dbusr     | Allowed | false    |
n/a                                    |
| giusr     | Allowed | true     |
n/a                                    |
| grid      | Allowed | n/a      | privileged-compliance-checks           |
| orarom    | Allowed | n/a      | platinum                               |
| oracle    | Allowed | n/a      | platinum, privileged-compliance-checks |
'-----------+---------+----------+----------------------------------------'
```

```
tfactl access lsusers -json

testuser: {
  "node1": [
    {
      "Promoted": "n/a",
      "Roles": "platinum",
      "Status": "Allowed",
      "User Name": "dbusr"
    },
    {
      "Promoted": "false",
      "Roles": "n/a",
      "Status": "Allowed",
      "User Name": "giusr"
    }
  ],
  "node2": [
    {
      "Promoted": "n/a",
      "Roles": "platinum",
      "Status": "Allowed",
      "User Name": "dbusr"
    },
    {
      "Promoted": "false",
      "Roles": "n/a",
      "Status": "Allowed",
      "User Name": "giusr"
    }
  ]
}
```

To add a user, for example, *abc* to the Oracle Trace File Analyzer access list and enable access to Oracle Trace File Analyzer across cluster:

```
tfactl access add -user abc
```

To add a user, for example, *abc*, assign a role, and enable access to Oracle Trace File Analyzer across cluster nodes:

```
tfactl access add -user abc -role platinum
```

To remove a user, for example, *abc* from the Oracle Trace File Analyzer access list:

```
tfactl access remove -user abc
```

To block a user, for example, *xyz* from accessing Oracle Trace File Analyzer:

```
tfactl access block -user xyz
```

To grant a role to non-root user:

```
tfactl access grant -user xyz -role platinum
```

To revoke a role granted to a non-root user:

```
tfactl access revoke -user xyz -role platinum
```

To remove all Oracle Trace File Analyzer users:

```
tfactl access removeall
```

9.3.1.2 tfactl availability

Use the `tfactl availability` command to enable or disable resources for Availability Score, and to search a specific data type in the telemetry cache.

Syntax

```
tfactl availability enable|disable|dumpcache
```

```
tfactl availability enable -key key -value value | -list
```

```
tfactl availability disable -key key -value value [-for nd|D|h|H|m|M]
| -list [-for nd|D|h|H|m|M]
```

```
tfactl availability dumpcache [-data_type data_type]
```

Parameters

Table 9-54 tfactl availability enable Command Parameters

Parameter	Description
`-type` *`resource_type`*	Specify the resource type that you want to enable.
`-key` *`key`*	Specify the key of the resource that you want to enable.
`-list`	Displays the list of resources that are available for enabling.

Parameters

Table 9-55 tfactl availability disable Command Parameters

Parameter	Description
`-type` *resource_type*	Specify the resource type that you want to enable.
`-key` *key*	Specify the key of the resource that you want to enable.
`[-for nd|`*D*`|`*h*`|`*H*`|`*m*`|`*M*`]	-list [-for nd|`*D*`|`*h*`|`*H*`|`*m*`|`*M*`]`	Specify the days, hours, or minutes to determine how long the resource will be disabled. Default is 7 days.
`-list`	Displays the list of resources that are available for disabling..

Parameters

Table 9-56 tfactl availability dumpcache Command Parameters

Parameter	Description
`-data_type` *data_type*	Specify the data type that you want to search in the telemetry cache.

Example 9-54 tfactl availability enable

```
tfactl availability enable -list


tfactl availability enable -type server_disk -key filesystem -value "/dev/
xvdad1"


tfactl availability enable -type server_network -key interface -value eth1
```

Example 9-55 tfactl availability disable

```
tfactl availability disable -list
```

```
tfactl availability disable -list -for 3d
```

```
tfactl availability disable -list -for 15h
```

```
tfactl availability disable -type server_disk -key filesystem -value
"/dev/xvdad1"
```

```
tfactl availability disable -type server_network -key interface -value
eth1
```

```
tfactl availability disable -type server_disk -key filesystem -value
"/dev/xvdad1" -for 3d
```

```
tfactl availability disable -type server_network -key interface -value
eth1 -for 12h
```

Example 9-56 tfactl availability dumpcache

```
tfactl availability dumpcache
```

```
tfactl availability dumpcache -data_type pdb
```

```
tfactl availability dumpcache -data_type db_tablespace
```

```
tfactl availability dumpcache -data_type db_backup
```

```
tfactl availability dumpcache -data_type cstate
```

9.3.1.3 tfactl blackout

Use the `tfactl blackout` command to suppress diagnostic collections at a more granular level. By default, blackout will be in effect for 24 hours.

Syntax

```
tfactl blackout add|remove|print
-targettype host|crs|asm|asmdg|database|dbbackup|db_dataguard|
db_tablespace|pdb_tablespace|pdb|listener|service|os
-target all|name
```

```
[-container name]
[-pdb pdb_name]
-event all|"event_str1,event_str2"|availability
[-timeout nm|nh|nd|none]
[-c|-local|-nodes "node1,node2"]
[-reason "reason for blackout"]
[-docollection]
```

Parameters

Table 9-57 tfactl blackout Command Parameters

Parameter	Description
`add|remove|print|`	Adds, removes, or prints blackout conditions.
`-targettype type` **Target type:** `host|crs|asm|asmdg|database|dbbackup|db_dataguard|db_tablespace|pdb_tablespace|pdb|listener|service|os`	Limits blackout only to the specified target type. `host`: The whole node is under blackout. If there is host blackout, then every blackout element that's shown true in the Telemetry JSON will have the reason for the blackout. `crs`: Blackout the availability of the Oracle Clusterware resource or events in the Oracle Clusterware logs. `asm`: Blackout the availability of Oracle Automatic Storage Management (Oracle ASM) on this machine or events in the Oracle ASM alert logs. `asmdg`: Blackout an Oracle ASM disk group. `database`: Blackout the availability of an Oracle Database, Oracle Database backup, tablespace, and so on, or events in the Oracle Database alert logs. `dbbackup`: Blackout Oracle Database backup events (such as CDB or archive backups). `db_dataguard`: Blackout Oracle Data Guard events. `db_tablespace`: Blackout Oracle Database tablespace events (container database). `pdb_tablespace`: Blackout Oracle Pluggable Database tablespace events (Pluggable database). `pdb`: Blackout Oracle Pluggable Database events. `listener`: Blackout the availability of a listener. `service`: Blackout the availability of a service. `os`: Blackout one or more operating system records.
`-target all|name`	Specify the target for blackout. You can specify a comma-delimited list of targets. By default, the target is set to `all`.
`-container name`	Specify the database container name (`db_unique_name`) where the blackout will take effect (for PDB, DB_TABLESPACE, and PDB_TABLESPACE).
`-pdb pdb_name`	Specify the PDB where the blackout will take effect (for PDB_TABLESPACE only).

Table 9-57 (Cont.) tfactl blackout Command Parameters

Parameter	Description
`-events all|"`*`str1`*`,`*`str2`*`"`	Limits blackout only to the availability events, or event strings, which should not trigger auto collections, or be marked as blacked out in telemetry JSON. `all`: Blackout everything for the target specified. *string*: Blackout for incidents where any part of the line contains the strings specified. Specify a comma-delimited list of strings.
`-timeout `*`nh`*`|`*`nd`*`|none`	Specify the duration for blackout in number of hours or days before timing out. By default, the timeout is set to 24 hours (24h).
`-c|-local`	Specify if blackout should be set to cluster-wide or local. By default, blackout is set to `local`.
`-reason `*`comment`*	Specify a descriptive reason for the blackout.
`-docollection`	Use this option to do an automatic diagnostic collection even if a blackout is set for this target.

Example 9-57 tfactl blackout

- To blackout **event:** ORA-00600 on **targettype:** database, **target:** mydb

  ```
  tfactl blackout add -targettype database -target mydb -event 
  "ORA-00600"
  ```

- To blackout **event:** ORA-04031 on **targettype:** database, **target:** all

  ```
  tfactl blackout add -targettype database -target all -event 
  "ORA-04031" -timeout 1h
  ```

- To blackout **db backup events** on **targettype:** dbbackup, **target:** mydb

  ```
  tfactl blackout add -targettype dbbackup -target mydb
  ```

- To blackout **db dataguard events** on **targettype:** db_dataguard, **target:** mydb

  ```
  tfactl blackout add -targettype db_dataguard -target mydb -timeout 
  30m
  ```

- To blackout **db tablespace events** on **targettype:** db_tablespace, **target:** system, **container:** mydb

  ```
  tfactl blackout add -targettype db_tablespace -target system -
  container mydb -timeout 30m
  ```

- To blackout **ALL events** on **targettype:** host, **target:** all

  ```
  tfactl blackout add -targettype host -event all -target all -
  timeout 1h -reason "Disabling all events during patching"
  ```

- To print blackout details

```
tfactl blackout print
.-------------------------------------------------------------------------
--------------------------------------------------------------------------
----------------------------.
|

myhostname
                     |
+---------------+--------------------+-----------
+------------------------------+------------------------------+--------
+---------------+--------------------------------------+
| Target Type   | Target              | Events    | Start
Time                    | End Time                     | Status | Do
Collection | Reason                               |
+---------------+--------------------+-----------
+------------------------------+------------------------------+--------
+---------------+--------------------------------------+
| HOST          | ALL                 | ALL       | Thu Mar 24 16:48:39
UTC 2022 | Thu Mar 24 17:48:39 UTC 2022 | ACTIVE | false         |
Disabling all events during patching |
| DATABASE      | MYDB                | ORA-00600 | Thu Mar 24 16:39:03
UTC 2022 | Fri Mar 25 16:39:03 UTC 2022 | ACTIVE | false         |
NA                                   |
| DATABASE      | ALL                 | ORA-04031 | Thu Mar 24 16:39:54
UTC 2022 | Thu Mar 24 17:39:54 UTC 2022 | ACTIVE | false         |
NA                                   |
| DB_DATAGUARD  | MYDB                | ALL       | Thu Mar 24 16:41:38
UTC 2022 | Thu Mar 24 17:11:38 UTC 2022 | ACTIVE | false         |
NA                                   |
| DBBACKUP      | MYDB                | ALL       | Thu Mar 24 16:40:47
UTC 2022 | Fri Mar 25 16:40:47 UTC 2022 | ACTIVE | false         |
NA                                   |
| DB_TABLESPACE | SYSTEM_CDBNAME_MYDB | ALL       | Thu Mar 24 16:45:56
UTC 2022 | Thu Mar 24 17:15:56 UTC 2022 | ACTIVE | false         |
NA                                   |
'---------------+--------------------+-----------
+------------------------------+------------------------------+--------
+---------------+--------------------------------------'
```

- To remove blackout for **event:** ORA-00600 on **targettype:** database, **target:** mydb

```
tfactl blackout remove -targettype database -event "ORA-00600" -target
mydb
```

- To remove blackout for **db backup events** on **targettype:** dbbackup, **target:** mydb

```
tfactl blackout remove -targettype dbbackup -target mydb
```

- To remove blackout for **db tablespace events** on **targettype:** db_tablespace, **target:** system, **container:** mydb

  ```
  tfactl blackout remove -targettype db_tablespace -target system -
  container mydb
  ```

- To remove blackout for **host events** on **targettype:** all, **target:** all

  ```
  tfactl blackout remove -targettype host -event all -target all
  ```

9.3.1.4 tfactl cell

Use the `tfactl cell` command to print or modify various storage cell configuration.

Syntax

```
tfactl cell -h
```

```
tfactl cell status
```

```
tfactl cell config
```

```
tfactl cell configure
```

```
tfactl cell deconfigure
```

Parameters

Table 9-58 tfactl cell Command Parameters

Parameter	Description
`status`	Prints the current status of storage cells.
`config`	Prints the current configuration of storage cells.
`configure`	Configures storage cells. Used the `configure` option to configure cell collections where this was not completed at installation time, was not completed due to upgrade or following a previous deconfigure.
`deconfigure`	Removes all of the storage cell configuration.

Example 9-58 tfactl cell status

```
# tfactl cell status
.----------------------------------------------------------.
| | EXADATA CELL | CURRENT STATUS |
+---+----------------------+---------------------------+
| 1 | cel01 | ONLINE |
```

```
| 2 | cel02 | ONLINE |
'----+------------------------+---------------------------
```

Example 9-59   tfactl cell config

```
# tfactl cell config
-------- ------------------------.
| Storage Cell Configuration |
+---------------------------------------------+--------------------------
--------------------------------+
| Configuration Parameter | Value |
+---------------------------------------------+---------------------------
--------------------------------+
| Exadata Support | YES |
| Configured Storage Cells | YES |
| Oracle Wallet Used | YES |
| Oracle Wallet Location | /u01/app/tfa/db01/tfa_home/internal/tfawallet |
| Oracle Wallet Password is with TFA | YES |
| Oracle Wallet Password Storage Status | Stored |
'---------------------------------------
+-------------------------------------
```

Example 9-60   tfactl cell deconfigure

```
# tfactl cell deconfigure
Removing Storage Cell Configuration...
Successfully removed Storage Cell Configuration.
```

9.3.1.5 tfactl checkupload

Use the `tfactl checkupload` command to validate the configured upload parameters.

> **Note:**
>
> The `tfactl checkupload` command has been deprecated in 21.1. Oracle recommends using `ahfctl checkupload` instead.

You can run the `checkupload` command as `root` or a non-root user.

Syntax

```
tfactl checkupload
[-h][--help]
[-name NAME]
```

Parameters

Table 9-59   tfactl checkupload Command Parameters

Parameter	Description
`name`	Specify the name of your configuration. For example, *mosconfig* to upload to My Oracle Support.

9.3.1.6 tfactl dbcheck

Use the `tfactl dbcheck` command to collect diagnostic data from the Oracle Exadata machine to identify issues with operating system, file system, memory, and I/O system.

Syntax

> **Note:**
>
> You can run `dbcheck` command only on Oracle Exadata machines running Oracle Linux operating system.

```
tfactl dbcheck
```

```
Checking Filesystems ...
OS: devtmpfs Checking filesystem /dev : 0%
used                                 ok
OS: tmpfs Checking filesystem /dev/shm : 1%
used                                ok
OS: tmpfs Checking filesystem /run : 1%
used                                    ok
OS: tmpfs Checking filesystem /sys/fs/cgroup : 0%
used                          ok
OS: /dev/mapper/VGExaDb-LVDbSys1 Checking filesystem / : 81%
used               ok
OS: /dev/sda1 Checking filesystem /boot : 14%
used                              ok
OS: /dev/mapper/VGExaDb-LVDbOra1 Checking filesystem /u01 : 97%
used            fail
OS: tmpfs Checking filesystem /run/user/0 : 0%
used                             ok

Check Kernel Setting in sysctl.ctl:
OS: [fs.aio-max-nr] equals to
3145728                                           ok
OS: [kernel.msgmax] equals to
8192                                              ok
OS: [kernel.msgmnb] equals to
65536                                             ok
OS: [kernel.msgmni] equals to
2878                                              ok
```

```
OS: [kernel.sem] [1024 60000 1024 256 <> (expected) 250 32000 100 
142]          fail
OS: [kernel.shmall] [56014625 <> (expected) 
1073741824]                         fail
OS: [kernel.shmmax] [229435904614 <> (expected) 
4398046511104]                  fail
OS: [kernel.shmmni] equals to 
4096                                              ok
OS: [kernel.randomize_va_space] equals to 
2                                     ok
OS: [vm.hugetlb_shm_group] [ <> (expected) 
1001]                                fail
OS: [vm.min_free_kbytes] [2097152 <> (expected) 
524288]                         fail
OS: [vm.nr_hugepages] [26265 <> (expected) 
11264]                               fail

Check Kernel Setting in effect:
OS: [fs.aio-max-nr] equals to 
3145728                                           ok
OS: [kernel.msgmax] equals to 
8192                                              ok
OS: [kernel.msgmnb] equals to 
65536                                             ok
OS: [kernel.msgmni] equals to 
2878                                              ok
OS: [kernel.sem] [1024  60000   1024    256 <> (expected) 250 32000 100 
142]    fail
OS: [kernel.shmall] [56014625 <> (expected) 
1073741824]                         fail
OS: [kernel.shmmax] [229435904614 <> (expected) 
4398046511104]                  fail
OS: [kernel.shmmni] equals to 
4096                                              ok
OS: [kernel.randomize_va_space] equals to 
2                                     ok
OS: [vm.hugetlb_shm_group] [0 <> (expected) 
1001]                               fail
OS: [vm.min_free_kbytes] [2097152 <> (expected) 
524288]                         fail
OS: [vm.nr_hugepages] [26265 <> (expected) 
11264]                               fail
```

9.3.1.7 tfactl diagnosetfa

Use the `tfactl diagnosetfa` command to collect Oracle Trace File Analyzer diagnostic data from the local node to identify issues with Oracle Trace File Analyzer.

Syntax

```
tfactl diagnosetfa [-repo repository] [-tag tag_name] [-local]
```

Parameters

Table 9-60 tfactl diagnosetfa Command Parameters

Parameter	Description
`-repo` *`repository`*	Specify the repository directory for the Oracle Trace File Analyzer diagnostic collections.
`-tag` *`tag_name`*	Oracle Trace File Analyzer collects the files into `tag_name` directory.
`-local`	Runs Oracle Trace File Analyzer diagnostics only on the local node.

9.3.1.8 tfactl disable

Use the `tfactl disable` command to prevent the Oracle Trace File Analyzer daemon from restarting.

Syntax

```
tfactl disable
```

9.3.1.9 tfactl enable

Use the `tfactl enable` command to enable automatic restart of the Oracle Trace File Analyzer daemon after a failure or system reboot.

Syntax

```
tfactl enable
```

9.3.1.10 tfactl get

Use the `tfactl get` command to view the details of various Oracle Trace File Analyzer configuration settings.

Syntax

```
tfactl get
| smartprobclassifier
| autodiagcollect
| autoInsights
| cron
| trimfiles
| tracelevel=COLLECT|SCAN|INVENTORY|OTHER|ISA|HANDLER|MAIN|CLIENT|
CONSOLE: FATAL|ERROR|WARNING|INFO|DEBUG|TRACE
| reposizeMB
| repositorydir
| logsize
| logcount
| maxcorefilesize
| maxcompliancesize
| maxcomplianceruns
| maxcorecollectionsize
| maxfilecollectionsize
| autopurge
| autosynccertificates
| publicip
| redact
| minSpaceForRTScan
| rtscan
| diskUsageMon
| diskUsageMonInterval
| manageLogsAutoPurge
| manageLogsAutoPurgeInterval
| manageLogsAutoPurgePolicyAge
| minfileagetopurge
| tfaIpsPoolSize
| tfaDbUtlPurgeAge
| tfaDbUtlPurgeMode
| tfaDbUtlPurgeThreadDelay
| tfaDbUtlCrsProfileDelay
| indexRecoveryMode
| collection.isa
| discovery
| inventory
| unreachableNodeSleepTime
| unreachableNodeTimeOut
| ipsAlertlogTrimsizeMB
| clustereventmonitor
| rediscoveryInterval]
[-node]
[-match pattern ]
[ scandiskmon ]
```

Example 9-61 tfactl get collect -match

```
tfactl get collect -match
.--------------------------------------------------------------------------.
|                                testserver                                |
+------------------------------------------------------------------+-------+
| Configuration Parameter                                          | Value |
+------------------------------------------------------------------+-------+
| collectAllDirsByFile                                             | ON    |
| Auto Diagcollection ( autodiagcollect )                          | ON    |
| ISA Data Gathering ( collection.isa )                            | ON    |
| collectTrm                                                       | OFF   |
| Generation of Mini Collections ( minicollection )                | ON    |
| chaautocollect                                                   | ON    |
| Max File Collection Size (MB) ( maxFileCollectionSize )          | 5120  |
| Max Collection Size of Core Files (MB) ( maxCoreCollectionSize ) | 500   |
| minTimeForAutoDiagCollection                                     | 12    |
'------------------------------------------------------------------+-------'
```

Example 9-62 tfactl get maxcorefilesize

```
tfactl get maxcorefilesize
.--------------------------------------------------------.
|                        testserver                      |
+------------------------------------------------+-------+
| Configuration Parameter                        | Value |
+------------------------------------------------+-------+
| Max Size of Core File (MB) ( maxCoreFileSize ) | 50    |
'------------------------------------------------+-------'
```

Example 9-63 tfactl get maxcorecollectionsize

```
tfactl get maxcorecollectionsize
.----------------------------------------------------------------------
----.
|
testserver                               |
+------------------------------------------------------------------
+-------+
| Configuration Parameter                                          |
Value |
+------------------------------------------------------------------
+-------+
| Max Collection Size of Core Files (MB) ( maxCoreCollectionSize ) |
500   |
'------------------------------------------------------------------
+-------'
```

Example 9-64 tfactl get clustereventmonitor

```
tfactl get clustereventmonitor
.-------------------------------------------------------.
|                      testserver                       |
+-----------------------------------------------+-------+
| Configuration Parameter                       | Value |
+-----------------------------------------------+-------+
| Cluster Event Monitor ( clustereventmonitor ) | ON    |
'-----------------------------------------------+-------'
```

Example 9-65 tfactl get diskUsageMon

```
tfactl get diskUsageMon
.---------------------------------------------.
|                testserver                   |
+-------------------------------------+-------+
| Configuration Parameter             | Value |
+-------------------------------------+-------+
| Disk Usage Monitor ( diskUsageMon ) | ON    |
'-------------------------------------+-------'
```

Example 9-66   tfactl get diskUsageMonInterval

```
tfactl get diskUsageMonInterval
.-----------------------------------------------------------------------------
---------------------.
|
testserver                                             |
+-----------------------------------------------------------------------------
-------------+-------+
| Configuration
Parameter                                                                  |
Value |
+-----------------------------------------------------------------------------
-------------+-------+
| Time interval between consecutive Disk Usage Snapshot(minutes)
( diskUsageMonInterval ) | 5      |
'-----------------------------------------------------------------------------
-------------+-------'
```

Example 9-67   tfactl get diskUsage.snapshot.save

```
tfactl get diskUsage.snapshot.save
.---------------------------------------------------------------.
|                         testserver                            |
+-------------------------------------------------------+-------+
| Configuration Parameter                               | Value |
+-------------------------------------------------------+-------+
| Save Disk Usage Snapshots ( diskUsage.snapshot.save ) | ON    |
'-------------------------------------------------------+-------'
```

Example 9-68   tfactl get diskUsage.snapshot.interval

```
tfactl get diskUsage.snapshot.interval
.-----------------------------------------------------------------------------
------------------------------------.
|
testserver                                                     |
+-----------------------------------------------------------------------------
----------------------------+-------+
| Configuration
Parameter
            | Value |
+-----------------------------------------------------------------------------
----------------------------+-------+
| Time interval between consecutive Disk Usage Snapshot(minutes) reports
( diskUsage.snapshot.interval ) | 30    |
'-----------------------------------------------------------------------------
----------------------------+-------'
```

Example 9-69   tfactl get diskUsage.snapshot.purgeInterval

```
tfactl get diskUsage.snapshot.purgeInterval
.-----------------------------------------------------------------------------
```

```
------------------------------------------.
|
testserver                                                       |
+----------------------------------------------------------------------
----------------------------------------+-------+
| Configuration
Parameter
                        | Value |
+----------------------------------------------------------------------
----------------------------------------+-------+
| Time interval between consecutive Disk Usage Snapshot Auto
Purge(Hours) ( diskUsage.snapshot.purgeInterval ) | 70    |
'----------------------------------------------------------------------
----------------------------------------+-------'
```

Example 9-70   tfactl get scandiskmon

```
tfactl get scandiskmon
.---------------------------------.
|         testserver              |
+-------------------------+-------+
| Configuration Parameter | Value |
+-------------------------+-------+
| scandiskmon             | ON    |
'-------------------------+-------'
```

9.3.1.11 tfactl floodcontrol

Use the `tfactl floodcontrol` command to limit or stop Oracle Trace File Analyzer collecting the same events in a given frame of time.

Syntax

```
tfactl floodcontrol
[-h][--help]
print|update|clear
[-event name]
[-limit n]
[-limittime n]
[-pausetime n]
```

Parameters

Table 9-61   tfactl floodcontrol Command Parameters

Parameter	Description
`print|update|clear`	Print, update, or clear flood control details.
`event` *`name`*	Flood control event name.
`limit` *`n`*	Flood control limit count.
`limittime` *`n`*	Flood control initital limit time in minutes.

Table 9-61 (Cont.) tfactl floodcontrol Command Parameters

Parameter	Description
`pausetime n`	Flood control pause time in minutes.

9.3.1.12 tfactl getresourcelimit

Use the `tfactl getresourcelimit` command to fetch details of Oracle Trace File Analyzer CPU and memory usage limitations.

> **Note:**
>
> The `tfactl getresourcelimit` command has been deprecated in 21.1. Oracle recommends using `ahfctl getresourcelimit` instead.

Syntax

```
tfactl getresourcelimit
[-tool tool_name]
[-resource resource_type]
```

Parameters

Table 9-62 tfactl getresourcelimit Command Parameters

Parameter	Description
`tool`	Currently, you can only specify `tfa`.
`resource`	You can specify either CPU or memory.

Example 9-71 getresourcelimit Example

```
# tfactl getresourcelimit
Tool TFA: Resource CPU: Limit value: 1
```

9.3.1.13 tfactl getupload

Use the `tfactl getupload` command to fetch the details of configured upload parameters.

> **Note:**
>
> The `tfactl getupload` command has been deprecated in 21.1. Oracle recommends using `ahfctl getupload` instead.

You can run the `getupload` command as `root` or a non-root user.

Syntax

```
tfactl getupload
[-h][--help]
[-all]
[-name NAME]
[-user USER]
[-password]
[-server SERVER]
[-url URL]
[-proxy PROXY]
[-noauth NOAUTH]
[-request REQUEST]
[-https_token HTTPS_TOKEN]
[-header HEADER]
[-secure SECURE]
[-connectstring CONNECTSTRING]
[-uploadtable UPLOADTABLE]
```

Parameters

Table 9-63 tfactl getupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`name`	Specify the name of your configuration. For example, *mosconfig*.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`server`	Specify the name of the server to which you have uploaded files. For example, *bugsftp.example.com*.
`url`	Specify the target URL in case of HTTPS type. For example, *https://samplehost.com*.
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`noauth`	Specify `true` and `false`. Default value is `false`. If `noauth` is set to `true`, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/password authentication is required.
`request`	Specify the request type, for example, `POST`.
`https_token`	Specify any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. You can also pass dynamic headers at upload time by passing the `-https_token` *`headers`* command option to `tfactl upload` command. For example: *`-H 'X-TFA-REQUESTID: 1'`*.

Table 9-63 (Cont.) tfactl getupload Command Parameters

Parameter	Description
header	Stores the executionId in the ahf.properties file. For example, to set the header:tfactl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025
secure	Specify true or false. Default value is true. Specifying the secure value checks for certificates. If secure is set to false, the upload command will run an unsecure upload.
connectstring	Specify the database connect string to log in to the database where you have uploaded files. For example, (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl))).
uploadtable	Specify the name of the table where you have uploaded files as BLOB type. For example, for uploading Oracle ORAchk collections to the Collection Manager it is set to RCA13_DOCS.

9.3.1.14 tfactl host

Use the tfactl host command to add hosts to, or remove hosts from the Oracle Trace File Analyzer configuration.

Syntax

```
tfactl host [add host_name | remove host_name]
```

Usage Notes

View the current list of hosts in the Oracle Trace File Analyzer configuration using the tfactl print hosts command. The tfactl print hosts command lists the hosts that are part of the Oracle Trace File Analyzer cluster:

```
$ tfactl print hosts
Host Name : node1
Host Name : node2
```

When you add a new host, Oracle Trace File Analyzer contacts the Oracle Trace File Analyzer instance on the other host. Oracle Trace File Analyzer authenticates the new host using certificates and both the Oracle Trace File Analyzer instances synchronize their respective hosts lists. Oracle Trace File Analyzer does not add the new host until the certificates are synchronized.

After you successfully add a host, all the cluster-wide commands are activated on all nodes registered in the Berkeley DB (BDB).

Example 9-72 tfactl host

Specify a host name to add:

```
$ tfactl host add myhost
```

Specify a host name to remove:

```
$ tfactl host remove myhost
```

9.3.1.16 tfactl index

Use the `tfactl index` command to index events.

Syntax

```
tfactl index [-json | -jsonfile json_file|string] -category result |
metadata
```

Parameters

Table 9-64 tfactl index Command Parameters

Parameter	Description
`-json`	Specify the JSON string to index.
`-jsonfile`	Specify the absolute path of the JSON file to index.
`-category result`	Indexes Oracle ORAchk and Oracle EXAchk compliance check run results.
`-category metadata`	Indexes Oracle ORAchk and Oracle EXAchk compliance check run metadata.

Example 9-73 tfactl index

```
tfactl index -jsonfile /home/dtayade/result.json -category result
JSON String Indexed Successfully.
```

9.3.1.17 tfactl print

Use the `tfactl print` command to print information from the Berkeley DB (BDB).

Syntax

```
tfactl print command [options]
Commands: status|components|config|directories|hosts|actions|repository|
runmode|suspendedips|protocols|smtp|collections
```

```
tfactl print status
```

```
tfactl print components [ [component_name1] [component_name2] ...
[component_nameN] ]
```

```
tfactl print config [ -node all | local | n1,n2,...  -name param]
```

```
tfactl print directories [ -node all | local | n1,n2,... ] [ -comp
component_name1,component_name2,... ] [ -policy exclusions | noexclusions ]
[ -permission public | private ]
```

```
tfactl print collections [ -status status ] [ -last <n><m|h|d> ] [-id] [ -
json ]
```

```
tfactl print hosts
```

```
tfactl print actions [ -status status ] [ -since nh|d ]
```

```
tfactl print repository
```

```
tfactl print runmode
```

```
tfactl print suspendedips
```

```
tfactl print protocols
```

```
tfactl print smtp
```

```
tfactl print collections -status QUEUED
```

```
tfactl print collections -status COMPLETED
```

Parameters

Table 9-65 tfactl print Command Parameters

Parameter	Description
`status`	Displays the status of Oracle Trace File Analyzer across all nodes in the cluster. Also, displays the Oracle Trace File Analyzer version and the port on which it is running.
`components`	Displays the desired components in the configuration.
`config`	Displays the current Oracle Trace File Analyzer configuration settings.
`directories`	Lists all the directories that Oracle Trace File Analyzer scans for trace or log file data. Also, displays the location of the trace directories allocated for the database, Oracle ASM, and instance.
`hosts`	Lists the hosts that are part of the Oracle Trace File Analyzer cluster, and that can receive cluster-wide commands.
`actions`	Lists all the actions submitted to Oracle Trace File Analyzer, such as diagnostic collection. By default, `tfactl print` commands only display actions that are running or that have completed in the last hour.
`repository`	Displays the current location and amount of used space of the repository directory. Initially, the maximum size of the repository directory is the smaller of either 10 GB or 50% of available file system space. If the maximum size is exceeded or the file system space gets to 1 GB or less, then Oracle Trace File Analyzer suspends operations and closes the repository. Use the `tfactl purge` command to clear collections from the repository.
`suspendedips`	Lists all paused Oracle Trace File Analyzer IPS collections.
`protocols`	Lists all available and restricted protocols.
`smtp`	Displays the SMTP server configuration

Options

```
tfactl print collections [ -status status ] [ -last <n><m|h|d> ] [ -
json ]
```

Option	Description
`-status` *`status`*	Collection status can be: • `running` • `queued` • `completed`
`-last` *`nh|d`*	Specify to print collections since the past *n* days or *n* hours.
`-since`	Same as `-last`. Kept for backward compatibility.
`-id`	Specify the collection ID to view its details.
`-json`	Specify to generate the output in JSON format.

Example 9-74 tfactl print runmode

```
tfactl print runmode
TFA Run Mode: COLLECTOR
```

Example 9-75 tfactl print smtp

```
tfactl print smtp
.---------------------------.
| SMTP Server Configuration |
+---------------+-----------+
| Parameter     | Value     |
+---------------+-----------+
| smtp.auth     | false     |
| smtp.from     | tfa       |
| smtp.user     | -         |
| smtp.cc       | -         |
| smtp.port     |        25 |
| smtp.bcc      | -         |
| smtp.password | *******   |
| smtp.host     | localhost |
| smtp.to       | -         |
| smtp.debug    | true      |
| smtp.ssl      | false     |
'---------------+-----------'
```

Example 9-76 tfactl print protocols

```
tfactl print protocols
.--------------------------------------------------.
|                    node1                         |
+--------------------------------------------------+
| Protocols                                        |
+--------------------------------------------------+
| Available : [TLSv1.2]                            |
| Restricted : [SSLv3, SSLv2Hello, TLSv1, TLSv1.1] |
'--------------------------------------------------'
```

Example 9-77 tfactl print components ASM

```
$ tfactl print components ASM
.--------------------------------------------------.
|                  XML Components                  |
+---------------+----------------------------------+
| Field         | Value                            |
+---------------+----------------------------------+
| Name          | ASM                              |
| Description   | ASM logs                         |
| Comp. Types   | collection action                |
| Configuration | all                              |
| Subcomponents | name:instance required: default: |
| Also collect  | TNS                              |
|               | AFD                              |
|               | ASMPROXY                         |
|               | ASMIO                            |
'---------------+----------------------------------'
```

Example 9-78 tfactl print components ODASTORAGE

```
$ tfactl print components ODASTORAGE
.-------------------------------------------.
|               XML Components              |
+---------------+---------------------------+
| Field         | Value                     |
+---------------+---------------------------+
| Name          | ODASTORAGE                |
| Description   | ODA Storage logs and Data |
| Comp. Types   | action                    |
| Configuration | ODA                       |
| Also collect  | OS                        |
|               | ODA                       |
|               | ASM                       |
|               | DCS                       |
'---------------+---------------------------'
```

Example 9-79 tfactl print collections -id -json

```
tfactl print collections -id 20240104010433stbm000004-vm18 -json
[
    {
        “CollectionId”: “20240104010433stbm000004-vm18",
        “InitiatedNode”: “stbm000004-vm18",
        “CollectionType”: “Manual Collection”,
        “RequestUser”: “root”,
        “NodeList”: “[stbm000004-vm17, stbm000004-vm18]“,
        “StartTime”: “2024-01-04T00:04:30.000-0600",
        “EndTime”: “2024-01-04T01:04:30.000-0600",
        “ComponentList”: “[omsi, emagent, acfs, asmproxy, sosreport, 
crsclient,
emagenti, oms, qos, dbwlm, ocm, cha, cfgtools, afd, avs, dbclient, 
rdbms, cvu,
os, crs, syslens, hami, em, chmos, goldengate, asmio, dataguard, 
install,
compliance, tns, asm, rhp, emplugins, wls]“,
        “UploadStatus”: “FAILED”,
        “CollectionStatus”: “COMPLETED”,
        “NodeCollection”: [
            {
                “Host”: “stbm000004-vm18”,
                “Tag”: 
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/“,
                “ZipFileName”: 
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/stbm000004-
vm18.tfa_Thu_Jan_04_01_04_36_CST_2024.zip”,
                “ZipFileSize”: “38896",
                “CollectionTime”: “183",
                “CheckSum”:
“d882835fe5bcee4b8d5381b59572f2b75dc7499ddf3adf5771e3ea75fa39e975",
                “checksum_algo”: “sha256"
            },
            {
                “Host”: “stbm000004-vm17",
                “Tag”:
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/“,
                “ZipFileName”:
“/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Jan_04_01_04_37_CST_2024_node_all/stbm000004-
vm17.tfa_Thu_Jan_04_01_04_36_CST_2024.zip”,
                “ZipFileSize”: “42759",
                “CollectionTime”: “186",
                “CheckSum”:
“b090611f11e94814782b12f798e60ef0e054fbad47e94d950a3a24c698a79986",
                “checksum_algo”: “sha256"
            }
        ]
    }
]
```

Example 9-80 tfactl print config

```
tfactl print config
.----------------------------------------------------------------------------
--------.
|
node1                                         |
+-----------------------------------------------------------------------
+------------+
| Configuration Parameter                                               |
Value      |
+-----------------------------------------------------------------------
+------------+
| TFA Version                                                           |
19.1.0.0.0 |
| Java Version                                                          |
1.8        |
| Public IP Network                                                     |
false      |
| Automatic Diagnostic Collection                                       |
true       |
| Alert Log Scan                                                        |
true       |
| Disk Usage Monitor                                                    |
true       |
| Managelogs Auto Purge                                                 |
false      |
| Trimming of files during diagcollection                               |
true       |
| Inventory Trace level                                                 |
1          |
| Collection Trace
level                                                 | 1          |
| Scan Trace
level                                                       |
1          |
| Other Trace
level                                                     | 1
|
| Granular
Tracing                                                       |
false      |
| Debug Mask
(Hex)                                                       |
0          |
| Repository current size
(MB)                                           | 146        |
| Repository maximum size
(MB)                                           | 10240      |
| Max Size of TFA Log
(MB)                                               | 50         |
| Max Number of TFA
Logs                                                 | 10         |
| Max Size of Core File
(MB)                                             | 50         |
| Max Collection Size of Core Files
(MB)                                 | 500        |
| Max File Collection Size
(MB)                                          | 5120       |
| Minimum Free Space to enable Alert Log Scan
(MB)                       | 500        |
| Time interval between consecutive Disk Usage
Snapshot(minutes)        | 60         |
| Time interval between consecutive Managelogs Auto
Purge(minutes)      | 60         |
| Logs older than the time period will be auto purged(days[d]|
hours[h]) | 30d        |
| Automatic
Purging                                                      |
true       |
| Age of Purging Collections
(Hours)                                    | 12         |
| TFA IPS Pool
Size                                                     | 5          |
| TFA ISA Purge Age
(seconds)                                            | 604800     |
| TFA ISA Purge
Mode                                                    | profile    |
| TFA ISA Purge Thread Delay
(minutes)                                  | 60         |
| Setting for ACR redaction (none|SANITIZE|
MASK)                         | none       |
| Email Notification will be sent for CHA EVENTS if address is
set      | false      |
| AUTO Collection will be generated for CHA
```

```
EVENTS                          | false       |
'-----------------------------------------------------------------
+------------'
```

In the preceding sample output:

- **`Automatic diagnostic collection`**: When `ON` (default is `OFF`), if scanning an alert log, then finding specific events in those logs triggers diagnostic collection.
- **`Trimming of files during diagcollection`**: Determines if Oracle Trace File Analyzer trims large files to contain only data that is within the specified time ranges. When trimming is `OFF`, no trimming of trace files occurs for automatic diagnostic collection.
- **`Repository current size in MB`**: How much space in the repository is used.
- **`Repository maximum size in MB`**: The maximum size of storage space in the repository. Initially, the maximum size is set to the smaller of either 10 GB or 50% of free space in the file system.
- **`Trace Level`**: 1 is the default, and the values 2, 3, and 4 have increasing verbosity. While you can set the trace level dynamically for running the Oracle Trace File Analyzer daemon, increasing the trace level significantly impacts the performance of Oracle Trace File Analyzer. Increase the trace level only at the request of My Oracle Support.
- **`Automatic Purging`**: Automatic purging of Oracle Trace File Analyzer collections is enabled by default. Oracle Trace File Analyzer collections are purged if their age exceeds the value of `Minimum Age of Collections to Purge`, and the repository space is exhausted.
- **`Minimum Age of Collections to Purge (Hours)`**: The minimum number of hours that Oracle Trace File Analyzer keeps a collection, after which Oracle Trace File Analyzer purges the collection. You can set the number of hours using the `tfactl set minagetopurge=`*`hours`* command.
- **`Minimum Space free to enable Alert Log Scan (MB)`**: The space limit, in MB, at which Oracle Trace File Analyzer temporarily suspends alert log scanning until space becomes free. Oracle Trace File Analyzer does not store alert log events if space on the file system used for the metadata database falls below the limit.

9.3.1.18 tfactl print inventory

Use the `tfactl print inventory` command delete file metadata.

Syntax

```
tfactl print inventory
[-file file_path]
[-node all | local | n1,n2,..]
```

Parameters

Table 9-66 tfactl print inventory Command Parameters

Parameter	Description
`-file`	Specify the path of file for which you the details.

Table 9-66 (Cont.) tfactl print inventory Command Parameters

Parameter	Description
`-node`	Specify `all`, `local`, or a comma-delimited list of nodes.

Example 9-81 tfactl print inventory

```
tfactl print inventory -file
/u01/app/giusr/diag/apx/+apx/+APX1/trace/alert_+APX1.log,/u01/app/
giusr/diag/crs/stbm000004-vm13/crs/trace/alert.log
| python -m json.tool
[
    {
        "Result": [
            {
                "absolute_path":
"/u01/app/giusr/diag/apx/+apx/+APX1/trace/alert_+APX1.log",
                "component": "ASMPROXY",
                "date_pattern":
"\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}\\.\\d{6}[\\+|-]\\d{2}:\
\d{2}",
                "file_name": "alert_+APX1.log",
                "last_modified": "05/26/2021 20:16:37"
            },
            {
                "absolute_path":
"/u01/app/giusr/diag/crs/stbm000004-vm13/crs/trace/alert.log",
                "component": "CRS",
                "date_pattern":
"\\d{4}-\\d{2}-\\d{2}\\s\\d{2}:\\d{2}:\\d{2}\\.\\d{3}",
                "file_name": "alert.log",
                "last_modified": "07/14/2021 14:18:59"
            }
        ],
        "hostname": "stbm000004-vm13"
    }
]
```

9.3.1.19 tfactl print syncstatus

Use the `tfactl print syncstatus` command to get the sync status of TFA on all cluster nodes.

Syntax

```
tfactl print syncstatus [-short]
```

Parameters

Table 9-67   tfactl print syncstatus Command Parameters

Parameter	Description
`-short`	Displays if the sync status is `TRUE` or `FALSE`. `TRUE` indicates TFA on all cluster nodes are in sync. `FALSE` indicates TFA on the cluster nodes are not in sync.

Example 9-82   tfactl print syncstatus

```
tfactl print syncstatus
SYNC MESSAGE : TFA Synced on all Cluster Nodes
.-------------------------------.
| Node            | Sync Status |
+-----------------+-------------+
| node1           | SYNCED      |
| node2           | SYNCED      |
'-----------------+-------------'


tfactl print syncstatus -short
Sync Status : TRUE


tfactl print syncstatus
SYNC FAILED : TFA not Synced on [stbm000004-vm18]
.-------------------------------------.
| Node            | Sync Status       |
+-----------------+-------------------+
| node3           | SYNCED            |
| node4           | Failed to Connect |
'-----------------+-------------------'


tfactl print syncstatus -short
Sync Status : FALSE
```

9.3.1.20 tfactl purgeindex

Use the `tfactl purgeindex` command to index events.

Syntax

```
tfactl purgeindex -category result | metadata
[-json JSON String]
[-last nh|d]
```

Parameters

Table 9-68   tfactl purgeindex Command Parameters

Parameter	Description
`-json`	Deletes the indexed events matching the JSON string specified.
`-last` *`nh|d`*`]`	Specify hours or days to delete index since the previous `n` hours or days.
`-category result`	Purges Oracle ORAchk and Oracle EXAchk compliance check run results.
`-category metadata`	Purges Oracle ORAchk and Oracle EXAchk compliance check run metadata.

Configure Compliance Index Threshold

You can set compliance index purge policy.

- If the compliance runs exceed the threshold (default 30), then delete all older records above the threshold (event based, that is, on every index request).
- If the compliance run is below the threshold and the size of index exceeds the threshold, then delete last run data (periodic).

Example 9-83   tfactl purgeindex

```
tfactl purgeindex -category result
Successfully deleted Index.
```

Example 9-84   Compliance Index Threshold

```
tfactl set maxcomplianceruns=60
Successfully set maxcomplianceruns=60
.----------------------------------------------------------------------.
|                           testhost                                   |
+--------------------------------------------------------------+-------+
| Configuration Parameter                                      | Value |
+--------------------------------------------------------------+-------+
| Maximum Compliance Runs to be Indexed ( maxcomplianceruns ) | 60    |
'--------------------------------------------------------------+-------'


tfactl set maxcompliancesize=100
Successfully set maxcompliancesize=100
.-------------------------------------------------------------------.
|                          testhost                                 |
+-----------------------------------------------------------+-------+
| Configuration Parameter                                   | Value |
+-----------------------------------------------------------+-------+
| Maximum Compliance Index Size (MB) ( maxcompliancesize ) | 100   |
'----------------------------------------------------------+-------'


tfactl get maxcompliancesize
.------------------------------------------------------------------.
|                          testhost                                |
+----------------------------------------------------------+-------+
| Configuration Parameter                                  | Value |
+----------------------------------------------------------+-------+
| Maximum Compliance Index Size (MB) ( maxcompliancesize ) | 150   |
'----------------------------------------------------------+-------'


tfactl get maxcomplianceruns
.---------------------------------------------------------------------.
|                            testhost                                 |
+-------------------------------------------------------------+-------+
| Configuration Parameter                                     | Value |
+-------------------------------------------------------------+-------+
| Maximum Compliance Runs to be Indexed ( maxcomplianceruns ) | 30    |
'-------------------------------------------------------------+-------'
```

9.3.1.21 tfactl purgeinventory

Use the `tfactl purgeinventory` command delete file metadata.

Syntax

```
tfactl purgeinventory
[-file file_path]
[-delayreload ]
[-node all | local | n1,n2,.. ]
```

Parameters

Table 9-69 tfactl purgeinventory Command Parameters

Parameter	Description
`-file`	Specify the path of file for which you want to delete the metadata.
`-delayreload`	Delays restoring file data until the next inventory.
`-node`	Specify `all`, `local`, or a comma-delimited list of nodes.

Example 9-85 tfactl purgeinventory

```
tfactl purgeinventory -file /u01/app/giusr/diag/crs/stbm000037-vm1/crs/trace/
alert.log
Successfully deleted file metadata
```

9.3.1.22 tfactl queryindex

Use the `tfactl queryindex` command to view stored events.

Syntax

```
tfactl queryindex -category result | metadata
[-checkid ID]
[-target target]
[-severity severity
[-name keywords
[-fields all | fields_list]
[-last nh|d | -from time -to time]
```

Parameters

Table 9-70 tfactl queryindex Command Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>

`-category`

</td><td>

Searches all metadata stored in the Oracle Trace File Analyzer index.

The compliance check run result consists of data like check ID, status, and so on while metadata consist of compliance run information like user, start time, end time, and so on.

Example Metadata

```
{
  "data_type": "compliance_metadata",
  "user": "dbusr",
  "run arguments": "-hardwaretype X4-2 -showpass -
localonly -silentforce -dball -check
C1AF676F0FB70BE1E053D498EB0A1971",
  "nodename": "testhost",
  "result_location": "/opt/rjtest/oracle.ahf/data/
testhost/exachk",
  "output zip name":
"exachk_testhost_sing11g_052721_03424",
  "start_time": "2021-06-16 01:13:18 EDT",
  "end_time": "2021-06-16 04:13:18 EDT",
  "health_score": 0
}
```

Example Result

```
{
  "modelVersion": "21.1.0_20210415",
  "RackType": "N/A",
  "EngineeredSystems": "Exadata",
  "RackIdentifier": "Cluster-c1",
  "OSVersion": "7",
  "DBVersion": "",
  "ExadataVersion": "211000",
  "HardwareType": "X4-2",
  "CoverageWindow": {
  "StartTime": "",
  "EndTime": ""
},
  "exachkExecTimestamp": "2021-06-16 01:35:39 EDT",
  "exachkID": "BEEC289AF1841071E053D498EB0A498D",
  "exachkType": "OS",
  "exachkName": "Verify v$asm_disk_stat os_mb and
total_mb values are the same",
  "exachkmessage": "v$asm_disk_stat os_mb and
total_mb values are the same",
  "exachkAlertType": "FAIL",
  "exachkTargetType": "ASM_HOME",
  "exachkExpectedValue": "0",
```

</td></tr>
</table>

Table 9-70 (Cont.) tfactl queryindex Command Parameters

Parameter	Description

	`  "exachkActualValue": "0",`
	`  "exachkStatus": "PASS",`
	`  "exachkStatusCode": "0",`
	`  "exachkReturnCode": "0",`
	`  "exachkMsgDetail": "'DATA FROM BUSM01CLIENT01 - VERIFY V$ASM_DISK_STAT OS_MB AND TOTAL_MB VALUES ARE THE SAME   \nSUCCESS:os_mb and total_mb values matched for all disks. Details:\nno rows selected'",`
	`  "NodeName": "testhost.example.com",`
	`  "exachkProfile": ""`
	`}`

`-checkid`	Searches results by check ID.
`-target`	Searches results by target. Specify a target, or a list of comma-delimited list of targets. **Note:** If you do not specify a target, then Oracle Trace File Analyzer displays data for all of the targets. Valid values: • `ASM` • `ASM_HOME` • `CLUSTER` • `CRS` • `CRS_HOME` • `HOST` • `RDBMS` • `RDBMS_HOME` • `STORAGE_CELL` • `SWITCH`
`-severity`	Searches results by severity. Valid values: • `CRITICAL` • `FAIL` • `INFO` • `PASS` • `WARNING`
`-name`	Searches results by check name. To query multiple check names, provide a space-delimited list of check names.

Table 9-70 (Cont.) tfactl queryindex Command Parameters

Parameter	Description
`-fields`	Specify the fields to restrict to a subset of attributes, for example, `–fields NodeName`. **Note:** Field names are case sensitive. By default, the field is set to `all`.

`-last` *nh*|*d* | `-from` *time* `-to` *time*	Specify hours or days to query data since the previous `n` hours or days.
	Specify the `-from` and `-to` parameters (you must use these two parameters together) to query data for a specific time interval.
	Valid date and time formats:
	`Mon/dd/yyyy hh:mm:ss`
	`yyyy-mm-dd hh:mm:ss`
	`yyyy-mm-ddThh:mm:ss`
	`yyyy-mm-dd`

Example 9-86 tfactl queryindex

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" | python -m json.tool
[
    {
        "Result": [
            {
                "ActualValue": "1",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:42:51 EDT",
                "ExpectedValue": "1",
                "HardwareType": "X4-2",
                "ID": "002331F422E014CAE05312C0E50AA2F3",
                "MsgDetail": "DATA FROM testhost - EXADATA DATABASE SERVER
ROLLING SWITCH PATCHING MINIMUM GI SOFTWARE REQUIREMENT //n32240590;TOMCAT
RELEASE UPDATE 19.0.0.0.0 (32240590)//n32222571;OCW Interim patch for
32222571//n32218663;ACFS RELEASE UPDATE 19.10.0.0.0 (32218663)//
n32218454;Database Release Update :19.10.0.0.210119 (32218454)//
n29340594;DBWLM RELEASE UPDATE 19.0.0.0.0 (29340594)//nOPatch succeeded.",
                "Name": "Exadata Database Server rolling switch patching
minimum GI software requirement",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "1",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "CRS_HOME",
                "Type": "OS",
                "message": "Exadata Database Server GI software 
version meets requirement for rolling switch patching",
                "modelVersion": "21.2.0(dev)_20210622"
            },
            {
                "ActualValue": "0",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:43:00 EDT",
                "ExpectedValue": "0",
                "HardwareType": "X4-2",
                "ID": "AA8C83A023362C5EE040E50A1EC0146A",
                "MsgDetail": "DATA FROM testhost - CDBM121 DATABASE - 
RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = 
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - CDBM122 
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - CDBM19C DATABASE - RECOVERY AND CREATE FILE 
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = 
+DATAC1//nDATA FROM testhost - RAC11G DATABASE - RECOVERY AND CREATE 
FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC12C DATABASE 
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = 
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC1 
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - SING11G DATABASE - RECOVERY AND CREATE FILE 
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = 
+DATAC1",
                "Name": "Recovery and Create File Destinations",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "0",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "RDBMS",
                "Type": "OS",
                "message": "Database DB_CREATE_FILE_DEST and 
DB_RECOVERY_FILE_DEST are in different diskgroups",
                "modelVersion": "21.2.0(dev)_20210622"
            }
        ],
        "hostname": "testhost1"
```

```
    }
]
```

```
tfactl queryindex -category metadata -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" | python -m json.tool
[
    {
        "Result": [
            {
                "end_time": "2021-06-29 09:33:27 UTC",
                "error": "somemsg",
                "health_score": "0",
                "nodename": "testhost",
                "output_zip_name": "exachk_testhost_rac19c_061421_093053",
                "result_location": "/opt/oracle.ahf/data/testhost/exachk/
user_root/output",
                "run_arguments": "-showpass -check
B407B045E9413B83E053D598EB0A8904 -excludeprofile storage,switch -dball  -
silentforce ",
                "run_type": "STANDALONE",
                "size": "45363",
                "start_time": "2021-06-29 09:31:35 UTC",
                "user": "root"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category metadata -last 20d | python -m json.tool
[
    {
        "Result": [
            {
                "end_time": "2021-06-29 09:33:27 UTC",
                "error": "somemsg",
                "health_score": "0",
                "nodename": "testhost",
                "output_zip_name": "exachk_testhost_rac19c_061421_093053",
                "result_location": "/opt/oracle.ahf/data/testhost/exachk/
user_root/output",
                "run_arguments": "-showpass -check
B407B045E9413B83E053D598EB0A8904 -excludeprofile storage,switch -dball  -
silentforce ",
                "run_type": "STANDALONE",
                "size": "45363",
                "start_time": "2021-06-29 09:31:35 UTC",
                "user": "root"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" -checkid 002331F422E014CAE05312C0E50AA2F3 |
python -m json.tool
[
    {
        "Result": [
            {
                "ActualValue": "1",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:42:51 EDT",
                "ExpectedValue": "1",
                "HardwareType": "X4-2",
                "ID": "002331F422E014CAE05312C0E50AA2F3",
                "MsgDetail": "DATA FROM testhost - EXADATA DATABASE
SERVER ROLLING SWITCH PATCHING MINIMUM GI SOFTWARE REQUIREMENT //
n32240590;TOMCAT RELEASE UPDATE 19.0.0.0.0 (32240590)//n32222571;OCW
Interim patch for 32222571//n32218663;ACFS RELEASE UPDATE 19.10.0.0.0
(32218663)//n32218454;Database Release Update :19.10.0.0.210119
(32218454)//n29340594;DBWLM RELEASE UPDATE 19.0.0.0.0 (29340594)//
nOPatch succeeded.",
                "Name": "Exadata Database Server rolling switch
patching minimum GI software requirement",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "1",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "CRS_HOME",
                "Type": "OS",
                "message": "Exadata Database Server GI software
version meets requirement for rolling switch patching",
                "modelVersion": "21.2.0(dev)_20210622"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" -target rdbms | python -m json.tool
[
    {
        "Result": [
            {
                "ActualValue": "0",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:43:00 EDT",
                "ExpectedValue": "0",
                "HardwareType": "X4-2",
                "ID": "AA8C83A023362C5EE040E50A1EC0146A",
                "MsgDetail": "DATA FROM testhost - CDBM121 DATABASE -
RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM BUSM01CLIENT01 - CDBM122 DATABASE
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM BUSM01CLIENT01 - CDBM19C DATABASE
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM BUSM01CLIENT01 - RAC11G DATABASE
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM BUSM01CLIENT01 - RAC12C DATABASE
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM BUSM01CLIENT01 - RAC1 DATABASE -
RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM BUSM01CLIENT01 - SING11G DATABASE
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1",
                "Name": "Recovery and Create File Destinations",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "0",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "RDBMS",
                "Type": "OS",
                "message": "Database DB_CREATE_FILE_DEST and
DB_RECOVERY_FILE_DEST are in different diskgroups",
                "modelVersion": "21.2.0(dev)_20210622"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" -severity critical | python -m json.tool
[
    {
        "Result": [
            {
                "ActualValue": "1",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:42:51 EDT",
                "ExpectedValue": "1",
                "HardwareType": "X4-2",
                "ID": "002331F422E014CAE05312C0E50AA2F3",
                "MsgDetail": "DATA FROM testhost - EXADATA DATABASE 
SERVER ROLLING SWITCH PATCHING MINIMUM GI SOFTWARE REQUIREMENT //
n32240590;TOMCAT RELEASE UPDATE 19.0.0.0.0 (32240590)//n32222571;OCW 
Interim patch for 32222571//n32218663;ACFS RELEASE UPDATE 19.10.0.0.0 
(32218663)//n32218454;Database Release Update :19.10.0.0.210119 
(32218454)//n29340594;DBWLM RELEASE UPDATE 19.0.0.0.0 (29340594)//
nOPatch succeeded.",
                "Name": "Exadata Database Server rolling switch 
patching minimum GI software requirement",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "1",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "CRS_HOME",
                "Type": "OS",
                "message": "Exadata Database Server GI software 
version meets requirement for rolling switch patching",
                "modelVersion": "21.2.0(dev)_20210622"
            },
            {
                "ActualValue": "0",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:43:00 EDT",
                "ExpectedValue": "0",
                "HardwareType": "X4-2",
                "ID": "AA8C83A023362C5EE040E50A1EC0146A",
                "MsgDetail": "DATA FROM testhost - CDBM121 DATABASE - 
RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = 
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - CDBM122 
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - CDBM19C DATABASE - RECOVERY AND CREATE FILE 
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = 
+DATAC1//nDATA FROM testhost - RAC11G DATABASE - RECOVERY AND CREATE 
FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC12C DATABASE 
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = 
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC1 
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - SING11G DATABASE - RECOVERY AND CREATE FILE 
```

```
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest =
+DATAC1",
                "Name": "Recovery and Create File Destinations",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "0",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "RDBMS",
                "Type": "OS",
                "message": "Database DB_CREATE_FILE_DEST and
DB_RECOVERY_FILE_DEST are in different diskgroups",
                "modelVersion": "21.2.0(dev)_20210622"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" -name "Exadata" | python -m json.tool
[
    {
        "Result": [
            {
                "ActualValue": "1",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:42:51 EDT",
                "ExpectedValue": "1",
                "HardwareType": "X4-2",
                "ID": "002331F422E014CAE05312C0E50AA2F3",
                "MsgDetail": "DATA FROM testhost - EXADATA DATABASE SERVER
ROLLING SWITCH PATCHING MINIMUM GI SOFTWARE REQUIREMENT //n32240590;TOMCAT
RELEASE UPDATE 19.0.0.0.0 (32240590)//n32222571;OCW Interim patch for
32222571//n32218663;ACFS RELEASE UPDATE 19.10.0.0.0 (32218663)//
n32218454;Database Release Update :19.10.0.0.210119 (32218454)//
n29340594;DBWLM RELEASE UPDATE 19.0.0.0.0 (29340594)//nOPatch succeeded.",
                "Name": "Exadata Database Server rolling switch patching
minimum GI software requirement",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "1",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "CRS_HOME",
                "Type": "OS",
                "message": "Exadata Database Server GI software
version meets requirement for rolling switch patching",
                "modelVersion": "21.2.0(dev)_20210622"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to
"2021-06-29 15:00:00" -name "Recovery Destinations" | python -m
json.tool
[
    {
        "Result": [
            {
                "ActualValue": "0",
                "AlertType": "CRITICAL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:43:00 EDT",
                "ExpectedValue": "0",
                "HardwareType": "X4-2",
                "ID": "AA8C83A023362C5EE040E50A1EC0146A",
                "MsgDetail": "DATA FROM testhost - CDBM121 DATABASE -
RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest =
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - CDBM122
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - CDBM19C DATABASE - RECOVERY AND CREATE FILE
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest =
+DATAC1//nDATA FROM testhost - RAC11G DATABASE - RECOVERY AND CREATE
FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC12C DATABASE
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest =
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC1
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - SING11G DATABASE - RECOVERY AND CREATE FILE
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest =
+DATAC1",
                "Name": "Recovery and Create File Destinations",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "0",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "RDBMS",
                "Type": "OS",
                "message": "Database DB_CREATE_FILE_DEST and 
DB_RECOVERY_FILE_DEST are in different diskgroups",
                "modelVersion": "21.2.0(dev)_20210622"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to 
"2021-06-29 15:00:00" -fields ID | python -m json.tool[
    {
        "Result": [
            {
                "ID": "002331F422E014CAE05312C0E50AA2F3"
            },
            {
                "ID": "AA8C83A023362C5EE040E50A1EC0146A"
            }
        ],
        "hostname": "testhost1"
    }
]
```

```
tfactl queryindex -category result -from "2021-06-29 09:00:00" -to 
"2021-06-29 15:00:00" -fields all | python -m json.tool
[
    {
        "Result": [
            {
                "ActualValue": "1",
                "AlertType": "CRITICAL",
                "CoverageWindow.EndTime": "NULL",
                "CoverageWindow.StartTime": "NULL",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:42:51 EDT",
                "ExpectedValue": "1",
                "HardwareType": "X4-2",
                "ID": "002331F422E014CAE05312C0E50AA2F3",
                "MsgDetail": "DATA FROM testhost - EXADATA DATABASE SERVER 
ROLLING SWITCH PATCHING MINIMUM GI SOFTWARE REQUIREMENT //n32240590;TOMCAT 
RELEASE UPDATE 19.0.0.0.0 (32240590)//n32222571;OCW Interim patch for 
32222571//n32218663;ACFS RELEASE UPDATE 19.10.0.0.0 (32218663)//
n32218454;Database Release Update :19.10.0.0.210119 (32218454)//
n29340594;DBWLM RELEASE UPDATE 19.0.0.0.0 (29340594)//nOPatch succeeded.",
                "Name": "Exadata Database Server rolling switch patching 
minimum GI software requirement",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "1",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "CRS_HOME",
                "Type": "OS",
                "data_type": "compliance_result",
                "message": "Exadata Database Server GI software 
version meets requirement for rolling switch patching",
                "modelVersion": "21.2.0(dev)_20210622",
                "timestamp": "20210629134251000",
                "user": "root"
            },
            {
                "ActualValue": "0",
                "AlertType": "CRITICAL",
                "CoverageWindow.EndTime": "NULL",
                "CoverageWindow.StartTime": "NULL",
                "DBName": "cdbm121",
                "DBVersion": "112040",
                "EngineeredSystems": "Exadata",
                "ExadataVersion": "NULL",
                "ExecTimestamp": "2021-06-29 09:43:00 EDT",
                "ExpectedValue": "0",
                "HardwareType": "X4-2",
                "ID": "AA8C83A023362C5EE040E50A1EC0146A",
                "InstanceName": "cdbm1211",
                "InstanceType": "CDB",
                "MsgDetail": "DATA FROM testhost - CDBM121 DATABASE - 
RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = 
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - CDBM122 
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - CDBM19C DATABASE - RECOVERY AND CREATE FILE 
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = 
+DATAC1//nDATA FROM testhost - RAC11G DATABASE - RECOVERY AND CREATE 
FILE DESTINATIONS//ndb_recovery_file_dest = +RECOC1//
ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC12C DATABASE 
- RECOVERY AND CREATE FILE DESTINATIONS//ndb_recovery_file_dest = 
+RECOC1//ndb_create_file_dest = +DATAC1//nDATA FROM testhost - RAC1 
DATABASE - RECOVERY AND CREATE FILE DESTINATIONS//
ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = +DATAC1//
nDATA FROM testhost - SING11G DATABASE - RECOVERY AND CREATE FILE 
DESTINATIONS//ndb_recovery_file_dest = +RECOC1//ndb_create_file_dest = 
+DATAC1",
                "Name": "Recovery and Create File Destinations",
                "NodeName": "testhost.example.com",
                "OSVersion": "7",
                "Profile": "dba",
                "RackIdentifier": "Cluster-c1",
                "RackType": "N/A",
                "ReturnCode": "0",
                "Status": "PASS",
                "StatusCode": "0",
                "TargetType": "RDBMS",
                "Type": "OS",
                "data_type": "compliance_result",
                "message": "Database DB_CREATE_FILE_DEST and 
DB_RECOVERY_FILE_DEST are in different diskgroups",
                "modelVersion": "21.2.0(dev)_20210622",
                "timestamp": "20210629134300000",
                "user": "root"
            }
        ],
        "hostname": "testhost1"
    }
]
```

9.3.1.23 tfactl rediscover

Use the `tfactl rediscover` command to discover new components and update inventory.

Syntax

```
tfactl rediscover [-mode <full|lite>]
```

Parameters

Table 9-71 tfactl rediscover Command Parameters

Parameter	Description
`-mode full`	(Default) Runs a full discovery.
`-mode lite`	Runs a lite discovery.

9.3.1.24 tfactl refreshconfig

Use the `tfactl refreshconfig` command to refresh and list Oracle Trace File Analyzer cron jobs.

Syntax

```
tfactl refreshconfig [cron|listcrons|modifycron|envrole]
```

Parameters

Table 9-72 tfactl refreshconfig Command Parameters

Parameter	Description
`cron`	Refreshes Oracle Trace File Analyzer cron jobs running in the background.

Table 9-72 (Cont.) tfactl refreshconfig Command Parameters

Parameter	Description

`listcrons`	Lists all Oracle Trace File Analyzer cron jobs.
	For example:
	`AUTOSTART_CLIENT`
	`AUTOSTART_CLIENT_ORATIER1`

`modifycron`	Reloads the cron jobs with the configuration changes.
`envrole`	Specifies Oracle Trace File Analyzer configuration type.

Example 9-87 tfactl refreshconfig cron

```
tfactl refreshconfig cron
refreshConfig() completed successfully.
```

Example 9-88 tfactl refreshconfig listcrons

```
tfactl refreshconfig listcrons

TFA CRON item:
Name:     AUTOSTART_CLIENT
Command:  /opt/oracle.ahf/bin/orachk -usediscovery -syslog -tag
autostart_client -readenvconfig -autorun_id AUTOSTART_CLIENT
Schedule: 3 3 * * 0

TFA CRON item:
Name:     AUTOSTART_CLIENT_ORATIER1
Command:  /opt/oracle.ahf/bin/orachk -usediscovery -profile oratier1 -
syslog -dball -showpass -tag autostart_client_oratier1 -readenvconfig -
autorun_id AUTOSTART_CLIENT_ORATIER1
Schedule: 3 2 * * 1,2,3,4,5,6

TFA CRON item:
Name:     id001
Command:  ahf analysis create --type insights --last 5m
Schedule: 0 3 * * 1
```

Example 9-89 tfactl refreshconfig modifycron

```
# tfactl refreshconfig modifycron -enable true -id id001 -valid For all
modifycron() completed successfully.
```

9.3.1.25 tfactl refreshconfig modifycron

Use the `tfactl refreshconfig modifycron` command to modify the Oracle Trace File Analyzer cron entry.

Syntax

```
tfactl refreshconfig modifycron [-h] -id ID -enabled {true,false}
[-validFor {all,dbcs,exacc,exacs,atp,fa} [{all,dbcs,exacc,exacs,atp,fa} ...]
| -validForClear]
[-excludeOn {all,dbcs,exacc,exacs,atp,fa}
[{all,dbcs,exacc,exacs,atp,fa} ...] | -excludeOnClear]
```

Parameters

Table 9-73 tfactl refreshconfig modifycron Command Parameters

Parameter	Description
`-id` *`ID`*	Specifies Oracle Trace File Analyzer cron identifier.
`-enabled {true,false}`	Enables or disables the cron entry.
`-validFor {all,dbcs,exacc,exacs,atp,fa} [{all,dbcs,exacc,exacs,atp,fa} ...]`	Sets the `validFor` cron attribute.
`-validForClear`	Clears the `validFor` cron attribute.
`-excludeOn {all,dbcs,exacc,exacs,atp,fa} [{all,dbcs,exacc,exacs,atp,fa} ...]`	Sets the `excludeOn` cron attribute.
`-excludeOnClear`	Clears the `excludeOn` cron attribute.

9.3.1.26 tfactl restrictprotocol

Use the `tfactl restrictprotocol` command to restrict certain protocols.

Syntax

```
tfactl restrictprotocol [-force] protocol
```

Example 9-90 tfactl restrictprotocol

```
$ tfactl restrictprotocol TLSv1
```

9.3.1.27 tfactl sendmail

Use the `tfactl sendmail` command to send a test email to verify SMTP configuration.

Syntax

```
tfactl sendmail email_address
```

9.3.1.28 tfactl set

Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.

Syntax

```
tfactl set [
smartprobclassifier=<ON|OFF>
| autodiagcollect=<ON|OFF>
| autoinsights=<ON|OFF>
| cron=<ON|OFF>
| trimfiles=<ON|OFF>
| tracelevel=<COLLECT|SCAN|INVENTORY|OTHER|ISA|HANDLER|CLUSTEREVENT|
MAIN|CONSOLE|CLIENT>:<FATAL|ERROR|WARN|INFO|DEBUG|TRACE>
| reposizeMB=<n> [repositorydir=<dir>] [-force]
| repositorydir=<dir> [reposizeMB=<n>] [-force]
| maxlogsize=<n> [-local]
| maxlogcount=<n> [-local]
| maxcorefilesize=<n> [-local]
| maxcorecollectionsize=<n> [-local]
| maxfilecollectionsize=<n>
| maxZipSize=<n>
| autopurge=<ON|OFF>
| purgestrategy=<SIZE|LRU|ALL>
| autosynccertificates=<ON|OFF>
| publicip=<ON|OFF>
| redact=<NONE|MASK|SANITIZE>
| minSpaceForRTScan=<n>
| maxcompliancesize=<n>
| maxcomplianceruns=<n>
| rtscan=<ON|OFF>
| diskUsageMon=<ON|OFF>
| diskUsage.snapshot.save=<ON|OFF>
| diskUsage.snapshot.interval=<n>
| diskUsage.snapshot.purgeInterval=<n>
| unreachableNodeSleepTime
| unreachableNodeTimeOut
| ipsAlertlogTrimsizeMB
| diskUsageMonInterval=<n>
| manageLogsAutoPurge=<ON|OFF>
| manageLogsAutoPurgeInterval=<n>
| manageLogsAutoPurgePolicyAge=<d|h>
| managelogs.adump=<ON|OFF>
| minfileagetopurge=<n>
| maxCollectionRetentionPeriod=<n>
| tfaIpsPoolSize=<n>
| tfaDbUtlPurgeAge=<n>
| tfaDbUtlPurgeMode=<simple|resource|profile>
| tfaDbUtlPurgeThreadDelay=<n>
| tfaDbUtlCrsProfileDelay=<n>
| indexRecoveryMode=<recreate|restore>
| rediscoveryInterval=<m|d|h>
| applin_incidents=<ON|OFF>
| scandiskmon=ON|OFF]
[-c]
```

Parameters

Table 9-74 tfactl set Command Parameters

Parameter	Description
`smartprobclassifier=ON|OFF`	Problem Classification feature for diagcollect (default ON)
`autodiagcollect=ON|OFF`	When set to `OFF` (default) automatic diagnostic collection is disabled. If set to `ON`, then Oracle Trace File Analyzer automatically collects diagnostics when certain patterns occur while Oracle Trace File Analyzer scans the alert logs. To set automatic collection for all nodes of the Oracle Trace File Analyzer cluster, you must specify the `-c` parameter.
`autoinsights=ON|OFF`	Specifies to include automatic AHF Insights report generation in the diagnostic collection. Default: `ON`.
`cron=ON|OFF`	Enables or disables Oracle Trace File Analyzer cron. Default: `OFF`.
`trimfiles=ON|OFF`	When set to `ON`, Oracle Trace File Analyzer trims the files to have only the relevant data when diagnostic collection is done as part of a scan. Note: When using `tfactl diagcollect`, you determine the time range for trimming with the parameters you specify. Oracle recommends that you *not* set this parameter to `OFF`, because untrimmed data can consume much space.
`tracelevel=COLLECT|SCAN|INVENTORY|OTHER|ISA|HANDLER|MAIN|CLIENT|CONSOLE:FATAL|ERROR|WARNING|INFO|DEBUG|TRACE`	Controls the trace level of log files. **Note:** Do not change the tracing level unless you are directed to do so by My Oracle Support.
`reposizeMB=`*`number`*	Sets the maximum size in MB of the collection repository.
`repositorydir=`*`directory`* `[-force]`	Specify the collection repository directory. Use the `-force` option to skip initial checks while changing the repository (Not Recommended)
`logsize=`*`n`* `[-local]`	Sets the maximum size, in MB, of each log before Oracle Trace File Analyzer rotates to a new log. • **Default:** 50 MB • **Minimum:** 10 MB • **Maximum:** 500 MB Use the `-local` parameter to apply the change only to the local node.

Table 9-74 (Cont.) tfactl set Command Parameters

Parameter	Description
`logcount=n [-local]`	Sets the maximum number of logs of specified size that Oracle Trace File Analyzer retains. • **Default:** 10 • **Minimum:** 5 • **Maximum:** 50 Use the `-local` option to apply the change only to the local node.
`port=n`	Specify the Oracle Trace File Analyzer port.
`maxcorefilesize=n [-local]`	Sets the maximum size of the core files to the size specified in MB. **Default:** 50 MB
`maxcorecollectionsize=n`	Sets the maximum collection size of the core files to the size specified in MB. **Default:** 500 MB
`maxfilecollectionsize=n`	Specify the file size in MB (5 GB by default). When you run the `tfactl diagcollect` command, it adds only the last 200 KB of the files that exceed the maximum file size to the diagnostic collection. The `tfactl diagcollect` command adds a new file, `skipped_files.txt` with the list of skipped files that are too large to add to the diagnostic collection.
`maxcompliancesize=n`	Sets the maximum size of `Compliance Index` directory in MB. **Default:** 150 MB
`maxcomplianceruns=n`	Sets the maximum number of compliance runs to be stored. **Default:** 30
`maxZipSize=n`	Sets the maximum size of single zip file in MB. **Default:** 1.8 GB
`autopurge=ON|OFF`	When set to `ON`, enables automatic purging of collections when Oracle Trace File Analyzer observes less space in the repository (`ON` by default).
`autosynccertificates=ON|OFF`	Specify to turn on or off auto-syncing TFA certificates.
`sslconfig`	Set the paths and passwords for the new SSL certificates to be used for TFA.
`ciphersuite`	Set cipher suite(s) for TLS communication between TFA client and daemon.
`publicip=ON|OFF`	Allows Oracle Trace File Analyzer to run on public network.
`redact <NONE|MASK|SANITIZE>`	Specify to set ACR redaction.
`smtp`	Specify the configuration details for the SMTP server to use for email notifications when prompted.
`minSpaceForRTScan=n`	Specify the minimum space required to run RT scan (500 by default).
`rtscan`	Specify to allow Oracle Trace File Analyzer to perform alert log scanning.

Table 9-74 (Cont.) tfactl set Command Parameters

Parameter	Description
`diskUsageMon=ON|OFF`	Turns `ON` or `OFF` monitoring disk usage and recording snapshots (`ON` by default). Oracle Trace File Analyzer stores the snapshots under `tfa/repository/suptools/`*`node`*`/managelogs/usage_snapshot/`.
`diskUsageMonInterval=`*`minutes`*	Specify the time interval between snapshots. **Default:** 60 minutes
`diskUsage.snapshot.save=ON|OFF`	Enables or disbales disk usage snapshots.
`diskUsage.snapshot.interval=`*`n`*	Set the time interval between consecutive Disk Usage Snapshot reports (minutes). **Default:** 60 minutes
`diskUsage.snapshot.purgeInterval=`*`n`*	Set the time interval between consecutive Disk Usage Snapshot Auto purge (hours). **Default:** 72 hours
`ipsAlertlogTrimsizeMB`	Trims `IpsAlertLog` files to a specified size.
`manageLogsAutoPurge=ON | OFF`	Turns automatic purging on or off (`ON` by default in DSC and `OFF` by default elsewhere).
`manageLogsAutoPurgeInterval=`*`minutes`*	Specify the purge frequency. **Default:** 60 minutes
`manageLogsAutoPurgePolicyAge=`*`n`*`d|h`	Age of logs to be purged. **Default:** 30 days
`managelogs.adump=<`*`ON|OFF`*`>`	Allow managelogs to purge audit dump destination.
`minfileagetopurge=`*`n`*	Set the minimum age, in hours, for a collection before Oracle Trace File Analyzer considers it for purging. • **Default:** 12 hours • **Minimum:** 12 hours • **Maximum:** 168 hours
`maxCollectionRetentionPeriod`	Maximum number of days a TFA collection will be retained. **Default:** 30 days
`tfaIpsPoolSize=`*`n`*	Sets the Incident Packaging Service (IPS) purge size.
`tfaDbUtlPurgeAge=`*`n`*	Sets the Oracle Trace File Analyzer ISA purge age in seconds. **Default:** 604800 seconds, that is, 7 days **Range:** 86400 (1 day) - 2592000 (1 month)
`tfaDbUtlPurgeMode=simple|resource|profile`	Sets the Oracle Trace File Analyzer ISA purge mode.
`tfaDbUtlPurgeThreadDelay=`*`n`*	Set the Oracle Trace Fils Analyzer ISA purge thread delay in minutes. **Default:** 60 minutes **Range:** 1 - 1440 (24 hours) minutes

Table 9-74 (Cont.) tfactl set Command Parameters

Parameter	Description
`tfaDbUtlCrsProfileDelay=`*n*	Set the Oracle Trace File Analyzer ISA CRS profile delay in minutes. **Default:** 30 minutes **Range:** 1 - 60 minutes
`indexRecoveryMode=recreate|restore`	Set the Lucene index recovery mode to recreate or restore. **Recreate:** If there's corruption, then index will be recreated with no recovery. **Restore:** If there's corruption, then index will be recovered from last backup and the latest changes are reapplied
`rediscoveryInterval`	Sets the time interval for running lite rediscovery. **Minimum:** 10 minutes **Maximum:** 1 day
`trimsize=`*n*`|`*n*`B|`*n*`K|`*n*`M|`*n*`G`	Sets the trimsize for diagnostic collection. The files of length lesser than the set trimsize will be excluded from trimming. **Default:** 488.28 KB **Range:** 100 KB - 50 MB
`-c`	Propagates the settings to all nodes in the Oracle Trace File Analyzer configuration.
`-local`	Sets the value on the local node. If this option is not included, then the value will be set on all the nodes.
`scandiskmon=ON|OFF`	Enables or disables monitoring `diskmon.trc` file.

Example 9-91 tfactl set

```
$ tfactl set autodiagcollect=ON reposizeMB=20480
$ tfactl set autodiagcollect=ON
$ tfactl set autopurge=ON
$ tfactl set tracelevel=INVENTORY:DEBUG
$ tfactl set reposizeMB=20480
$ tfactl set logsize=100
$ tfactl set port=5000
```

Example 9-92 tfactl set rediscoveryInterval

```
tfa/bin/tfactl set rediscoveryInterval=1m1h1d
Successfully set rediscoveryInterval=1m1h1d
.--------------------------------------------------------.
|                        node1                           |
+-----------------------------------------------+--------+
| Configuration Parameter                       | Value  |
+-----------------------------------------------+--------+
| Rediscovery Interval ( rediscoveryInterval )  | 1m1h1d |
'-----------------------------------------------+--------'
```

Example 9-93 tfactl set clustereventmonitor

```
tfactl set clustereventmonitor=on
Successfully set clustereventmonitor=ON
Changes will take effect at next restart.
.-------------------------------------------------------.
|                        node1                          |
+-----------------------------------------------+-------+
| Configuration Parameter                       | Value |
+-----------------------------------------------+-------+
| Cluster Event Monitor ( clustereventmonitor ) | ON    |
'-----------------------------------------------+-------'


tfactl set clustereventmonitor=off
Successfully set clustereventmonitor=OFF
Changes will take effect at next restart.
.-------------------------------------------------------.
|                        node1                          |
+-----------------------------------------------+-------+
| Configuration Parameter                       | Value |
+-----------------------------------------------+-------+
| Cluster Event Monitor ( clustereventmonitor ) | OFF   |
'-----------------------------------------------+-------'
```

Example 9-94 tfactl set ipsAlertlogTrimsizeMB

```
tfactl set ipsAlertlogTrimsizeMB=10
Successfully set ipsAlertlogTrimsizeMB=10
.----------------------------------------------------------------------------
----------------.
|
node1                                             |
+----------------------------------------------------------------------------
--------+-------+
| Configuration
Parameter                                                            | Value
|
+----------------------------------------------------------------------------
--------+-------+
| Maximum Size in MB allowed for alert file inside IPS Zip
( ipsAlertlogTrimsizeMB ) | 10    |
'----------------------------------------------------------------------------
--------+-------'
```

Example 9-95 tfactl set trimsize

```
tfactl set trimsize=10M
Successfully set trimsize=10M
.------------------------------------.
| node1                              |
+-------------------------+----------+
| Configuration Parameter | Value    |
+-------------------------+----------+
| Trim Size ( trimsize ) | 10.00 MB  |
'------------------------+-----------'
```

Example 9-96 tfactl set diskUsageMon

```
tfactl set diskUsageMon=ON
Successfully set diskUsageMon=ON
.---------------------------------------------.
|                testserver                   |
+-------------------------------------+-------+
| Configuration Parameter             | Value |
+-------------------------------------+-------+
| Disk Usage Monitor ( diskUsageMon ) | ON    |
'-------------------------------------+-------'
```

Example 9-97 tfactl set diskUsageMonInterval

```
tfactl set diskUsageMonInterval=0
Invalid value specified: 0
diskUsageMonInterval value should not be less than 1


tfactl set diskUsageMonInterval=5
Successfully set diskUsageMonInterval=5
.----------------------------------------------------------------------
---------------------------.
|
testserver                                             |
+----------------------------------------------------------------------
-------------------+-------+
| Configuration
Parameter
   | Value |
+----------------------------------------------------------------------
-------------------+-------+
| Time interval between consecutive Disk Usage Snapshot(minutes)
( diskUsageMonInterval ) | 5     |
'----------------------------------------------------------------------
-------------------+-------'
```

Example 9-98 tfactl set diskUsage.snapshot.save

```
tfactl set diskUsage.snapshot.save=ON
Successfully set diskUsage.snapshot.save=ON
.---------------------------------------------------------------.
|                         testserver                            |
+-------------------------------------------------------+-------+
| Configuration Parameter                               | Value |
+-------------------------------------------------------+-------+
| Save Disk Usage Snapshots ( diskUsage.snapshot.save ) | ON    |
'-------------------------------------------------------+-------'
```

Example 9-99 tfactl set diskUsage.snapshot.interval

```
tfactl set diskUsage.snapshot.interval=30
Successfully set diskUsage.snapshot.interval=30
.----------------------------------------------------------------------------
------------------------------------.
|
testserver                                                    |
+----------------------------------------------------------------------------
----------------------------+-------+
| Configuration
Parameter
            | Value |
+----------------------------------------------------------------------------
----------------------------+-------+
| Time interval between consecutive Disk Usage Snapshot(minutes) reports
( diskUsage.snapshot.interval ) | 30    |
'----------------------------------------------------------------------------
----------------------------+-------'
```

Example 9-100 tfactl set diskUsage.snapshot.purgeInterval

```
tfactl set diskUsage.snapshot.purgeInterval=70
Successfully set diskUsage.snapshot.purgeInterval=70
.----------------------------------------------------------------------------
------------------------------------------.
|
testserver                                                       |
+----------------------------------------------------------------------------
----------------------------------+-------+
| Configuration
Parameter
                  | Value |
+----------------------------------------------------------------------------
----------------------------------+-------+
| Time interval between consecutive Disk Usage Snapshot Auto Purge(Hours)
( diskUsage.snapshot.purgeInterval ) | 70    |
'----------------------------------------------------------------------------
----------------------------------+-------'
```

Example 9-101 tfactl set scandiskmon=ON

```
tfactl set scandiskmon=ON
Successfully set scandiskmon=ON
.---------------------------------.
|           testserver            |
+-------------------------+-------+
| Configuration Parameter | Value |
+-------------------------+-------+
| scandiskmon             | ON    |
'-------------------------+-------'
```

9.3.1.29 tfactl setresourcelimit

Use the `tfactl setresourcelimit` command to restrict the CPU and memory usage of Oracle Trace File Analyzer.

> **Note:**
>
> The `tfactl setresourcelimit` command has been deprecated in 21.1. Oracle recommends using `ahfctl setresourcelimit` instead.

Syntax

```
tfactl setresourcelimit
[-tool tool_name]
[-resource resource_type]
[-value value]
```

Parameters

Table 9-75 tfactl setresourcelimit Command Parameters

Parameter	Description
`value`	Set the limit to a minimum of 50% of a single CPU, and a maximum of 4 or 75% of the available CPUs, whichever is lower. By default, the CPU limit is set to the maximum. To limit TFA to a maximum of 50% of a single CPU: `tfactl setresourcelimit -value 0.5` You can limit memory usage either at the system level using `tfactl setresourcelimit -resource kmem` or combined system and swap memory using `tfactl setresourcelimit -resource swmem`.
`tool`	Currently, you can only specify `tfa`. Default: *`tfa`*
`resource`	You can specify either CPU or memory.

Example 9-102 setresourcelimit Examples

On a server with 10 CPUs, the default limit will be 4 CPUs:

```
# tfactl setresourcelimit
Tool TFA: Resource CPU: Limit value: 4
```

On a server with 4 CPUs, the default limit will be 3 CPUs (75% of available CPUs):

```
tfactl setresourcelimit
Tool TFA: Resource CPU: Limit value: 3


# tfactl setresourcelimit -value 2
Tool TFA: Resource CPU: Limit value: 2
```

To limit the memory usage to only 1 GB of system memory run:

```
tfactl setresourcelimit -resource kmem -value 1024
```

To limit the combined total of system memory and the swap memory to 2 GB run:

```
tfactl setresourcelimit -resource swmem -value 2048
```

9.3.1.30 tfactl setupload

Use the `tfactl setupload` command to set upload parameters.

> **Note:**
>
> The `tfactl setupload` command has been deprecated in 21.1. Oracle recommends using `ahfctl setupload` instead.

You can run the `setupload` command as `root` or a non-root user.

Syntax

```
tfactl setupload
[-h][--help]
[-all]
[-type TYPE]
[-name NAME]
[-user USER]
[-password]
[-server SERVER]
[-url URL]
[-proxy PROXY]
[-noauth NOAUTH]
[-https_token HTTPS_TOKEN]
[-request REQUEST]
[-header HEADER]
[-secure SECURE]
[-connectstring CONNECTSTRING]
[-uploadtable UPLOADTABLE]
```

Parameters

Table 9-76 tfactl setupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`type`	Specify the type of an endpoint. For example, `https`, `sftp`, or `sqlnet`.
`name`	Specify a unique descriptive name to your configuration. For example, *mosconfig* to upload to My Oracle Support.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`server`	Specify the name of the server to which you want to upload files. For example, *bugsftp.example.com*.
`url`	Specify the target URL to upload files in case of HTTPS type. For example, *https://samplehost.com*.
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`noauth`	Specify `true` and `false`. Default value is `false`. If `noauth` is set to `true`, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/password authentication is required.
`request`	Specify the request type, for example, `POST`.
`https_token`	Specify any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. For example, `tfactl setupload -name config -type https -https_token 'abc:13'`. You can also pass dynamic headers at upload time by passing the `-https_token` *`headers`* command option to `tfactl upload` command. For example: *`-H 'X-TFA-REQUESTID: 1'`*.
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`tfactl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.
`connectstring`	Specify the database connect string to log in to the database where you want to upload files. For example, `(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl)))`.

Table 9-76 (Cont.) tfactl setupload Command Parameters

Parameter	Description
`uploadtable`	Specify the name of the table where you want to upload files as `BLOB` type. For example, for uploading Oracle ORAchk collections to the Collection Manager it is set to `RCA13_DOCS`.

To setup MOS configuration:

```
tfactl setupload -name mos -type https -user sample_user@domain.com -url
https://transport.oracle.com/upload/issue
```

To set proxy for MOS configuration:

```
tfactl setupload -name mos -type https -proxy www-proxy.server.com:80
```

To upload to MOS using `tfactl upload`:

```
tfactl upload -name mos -id 3-23104325631 -file /opt/oracle.ahf/data/
repository/auto_srdc_ORA-00600_20200706T18:58:09_myserver1.zip
```

To upload to MOS using `tfactl diagcollect`:

```
tfactl diagcollect -upload mos -srdc ORA-00600 -id 3-23104325631
```

or

```
tfactl diagcollect -srdc ORA-00600 -sr 3-23104325631
```

> **Note:**
>
> Ensure that the configuration name is `mos`.

9.3.1.31 tfactl showrepo

Use the `tfactl showrepo` command to get the repository locations of Oracle Autonomous Health Framework components.

> **Note:**
>
> The `tfactl showrepo` command has been deprecated in 21.1. Oracle recommends using `ahfctl showrepo` instead.

Syntax

```
tfactl showrepo
[-h]
[-all]
[-tfa]
[-compliance]
```

Parameters

Table 9-77 tfactl showrepo Command Parameters

Parameter	Description
`-all`	Displays the repository locations of Oracle Autonomous Health Framework components.
`-tfa`	Displays the repository locations of Oracle Trace File Analyzer.
`-compliance`	Displays the repository locations of Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components.

9.3.1.32 tfactl start

Use the `tfactl start` command to start the Oracle Trace File Analyzer daemon on the local node, and also to start the desired support tool.

Syntax

```
tfactl start [tool]
```

9.3.1.33 tfactl startahf

Use the `tfactl startahf` command to start the scheduler for Oracle Autonomous Health Framework components.

> **Note:**
>
> The `tfactl startahf` command has been deprecated in 21.1. Oracle recommends using `ahfctl startahf` instead.

Syntax

```
tfactl startahf
[-h]
[-all]
[-tfa tfa_start_args]
[-compliance compliance_autostart_args]
```

Parameters

Table 9-78 tfactl startahf Command Parameters

Parameter	Description
`-all`	Starts the Oracle Trace File Analyzer and Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons.
`-tfa`	Starts the Oracle Trace File Analyzer daemon.
`-tfa` *`tfa_start_args`*	Starts the Oracle Trace File Analyzer daemon with the option specified. You can specify all Oracle Trace File Analyzer supported options. For example: `tfactl startahf -tfa "`*`tfa_start_args`*`"`
`-compliance`	Starts the Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons.

`-compliance` *`compliance_autostart_args`*	Starts the Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons with the option specified. Prepend the argument with a space followed by an hyphen and then wrap it with double quotes. You can specify all Oracle ORAchk and Oracle EXAchk supported options. For example:
	`tfactl startahf -compliance " -`*`compliance_autostart_args`*`"`
	`tfactl startahf -compliance -cargs " -c X4-2,EXAMAA"`
	`tfactl startahf -compliance -cargs " -debug"`
	`tfactl startahf -compliance -cagrs " -withisa"`

9.3.1.34 tfactl status

Use the `tfactl status` command to check the run status of Oracle Trace File Analyzer.

Syntax

```
tfactl status
```

9.3.1.35 tfactl statusahf

Use the `tfactl statusahf` command to check the shceduler status for Oracle Autonomous Health Framework components.

> **Note:**
>
> The `tfactl statusahf` command has been deprecated in 21.1. Oracle recommends using `ahfctl statusahf` instead.

Syntax

```
tfactl statusahf [-h]
[-all]
[-tfa]
[-compliance]
```

Parameters

Table 9-79 tfactl statusahf Command Parameters

Parameter	Description
`-all`	Checks and displays the status of Oracle Trace File Analyzer and Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons.
`-tfa`	Checks and displays the status of Oracle Trace File Analyzer daemon.
`-compliance`	Checks and displays the status of Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons.

9.3.1.36 tfactl stop

Use the `tfactl stop` command to stop the Oracle Trace File Analyzer daemon on the local node, and also to stop the desired support tool.

Syntax

```
tfactl stop [tool]
```

9.3.1.37 tfactl stopahf

Use the `tfactl stopahf` command to stop the scheduler for Oracle Autonomous Health Framework components.

> **Note:**
>
> The `tfactl stopahf` command has been deprecated in 21.1. Oracle recommends using `ahfctl stopahf` instead.

Syntax

```
tfactl stopahf [-h]
[-all]
[-tfa]
[-compliance]
```

Parameters

Table 9-80   tfactl stopahf Command Parameters

Parameter	Description
`-all`	Stops the Oracle Trace File Analyzer and Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons.
`-tfa`	Stops the Oracle Trace File Analyzer daemon.
`-compliance`	Stops the the Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components daemons.

9.3.1.38 tfactl syncnodes

Use the `tfactl syncnodes` command to generate and copy Oracle Trace File Analyzer certificates to other Oracle Trace File Analyzer nodes.

Syntax

```
tfactl syncnodes [-regenerate]
```

Parameters

Table 9-81   tfactl syncnodes Command Parameters

Parameter	Description
`-regenerate`	Regenerates Oracle Trace File Analyzer certificates.

9.3.1.39 tfactl uninstall

Use the `tfactl uninstall` command to uninstall Oracle Autonomous Health Framework.

Running the command:

- Stops Oracle Orachk
- Stops Oracle Trace File Analyzer
- Deletes the Oracle Autonomous Health Framework installation directory

Syntax

```
tfactl uninstall
[-local]
[-silent]
[-deleterepo]
```

Parameters

Table 9-82   tfactl uninstallahf Command Parameters

Parameter	Description
`-local`	Uninstalls Oracle Autonomous Health Framework only on the local node. **Note:** If you do not specify the `-local` option, then the uninstaller script uninstalls Oracle Autonomous Health Framework from all of the configured nodes.
`-silent`	Specify to not ask any uninstall questions.
`-deleterepo`	Deletes the Oracle Autonomous Health Framework repository.

9.3.1.40 tfactl upload

Use the `tfactl upload` command to upload collections or files on demand.

You can run the `upload` command as `root` or a non-root user.

Syntax

```
tfactl upload
[-sr sr_number]
[-name config_name]
```

```
[-id the location or target where you want to upload your files to]
[-file file_name]
```

Parameters

Table 9-83 tfactl upload Command Parameters

Parameter	Description
`-sr` *`sr_number`*	Specify the SR number.
`-name` *`config_name`*	Specify a unique name for the configuration.
`-id` *`The location or target where you want to upload your files to.`*	Specify the location or target where you want to upload your files to.
`-file` *`file_name`*	Specify the name of the file to upload.

Example 9-103 Upload to MOS using tfactl upload Example

```
tfactl upload -name mos -id 3-23104325631 -file /opt/oracle.ahf/data/
repository/auto_srdc_ORA-00600_20200706T18:58:09_myserver1.zip
```

Example 9-104 Upload to MOS using tfactl diagcollect Example

```
tfactl diagcollect -upload mos -srdc ORA-00600 -id 3-23104325631


tfactl diagcollect -srdc ORA-00600 -sr 3-23104325631
```

> **Note:**
>
> Ensure that the configuration name is `mos`.

For more information on configuration setup, run `tfactl setupload -h`.

9.3.1.41 tfactl unsetresourcelimit

Use the `tfactl unsetresourcelimit` command to unset the limitations set on Oracle Trace File Analyzer CPU and memory usage.

> **Note:**
>
> The `tfactl unsetresourcelimit` command has been deprecated in 21.1. Oracle recommends using `ahfctl unsetresourcelimit` instead.

Syntax

```
tfactl unsetresourcelimit
[-tool tool_name]
[-resource resource_type]
```

Parameters

Table 9-84 tfactl unsetresourcelimit Command Parameters

Parameter	Description
`tool`	Currently, you can only specify `tfa`.
`resource`	You can specify either CPU or memory.

Example 9-105 unsetresourcelimit Example

```
# tfactl unsetresourcelimit -tool tfa -resource cpu
```

9.3.1.42 tfactl unsetupload

Use the `tfactl unsetupload` command to unset the configured upload parameters.

> **Note:**
>
> The `tfactl unsetupload` command has been deprecated in 21.1. Oracle recommends using `ahfctl unsetupload` instead.

You can run the `unsetupload` command as `root` or a non-root user.

Syntax

```
tfactl unsetupload
[-h][--help]
[-all]
[-name NAME]
[-user USER]
[-password]
[-server SERVER]
[-url URL]
[-proxy PROXY]
[-noauth NOAUTH]
[-https_token HTTPS_TOKEN]
[-request REQUEST]
[-header HEADER]
[-secure SECURE]
[-connectstring CONNECTSTRING]
[-uploadtable UPLOADTABLE]
```

Parameters

Table 9-85 tfactl unsetupload Command Parameters

Parameter	Description
`all`	All of the parameters.
`name`	Specify the name of your configuration. For example, *mosconfig* to upload to My Oracle Support.
`user`	Specify the user who has the privileges to access the endpoint. For example, *upload.user@example.com*.
`password`	Specify the password of the user.
`server`	Specify the name of the server to which you have uploaded the files. For example, *bugsftp.example.com*.
`url`	Specify the target URL to which you have uploaded the files in case of HTTPS type. For example, *https://samplehost.com*.
`proxy`	Specify the URL of the proxy server. For example, *www.example.com:80*.
`noauth`	Specify `true` and `false`. Default value is `false`. If `noauth` is set to `true`, then HTTPS upload will skip authentication. For example, upload files to PAR, Pre Authenticated URL where no user/password authentication is required.
`request`	Specify the request type, for example, `POST`.
`https_token`	Specify any static header values while configuring. For example, set auth tokens while configuring the HTTPS end point. You can also pass dynamic headers at upload time by passing the `-https_token` *`headers`* command option to `tfactl upload` command. For example: *`-H 'X-TFA-REQUESTID: 1'`*.
`header`	Stores the `executionId` in the `ahf.properties` file. For example, to set the header:`tfactl setupload -name a1 -type https -header X-TFA-HEADERS:executionId=aeldb1db01_2020.06.16_19.20.55.15336025`
`secure`	Specify `true` or `false`. Default value is `true`. Specifying the secure value checks for certificates. If `secure` is set to `false`, then the `upload` command will run an unsecure upload.
`connectstring`	Specify the database connect string to log in to the database where you have uploaded files. For example, `(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = 1521))(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = orcl)))`.
`uploadtable`	Specify the name of the table where you have uploaded the files as `BLOB` type. For example, for uploading Oracle ORAchk collections to the Collection Manager it is set to `RCA13_DOCS`.

9.3.1.43 tfactl version

Use the `tfactl version` command to check the version of Oracle Autonomous Health Framework components.

Syntax

```
tfactl version
[-h]
[-all]
[-tfa]
[-compliance]
```

Parameters

Table 9-86 tfactl version Command Parameters

Parameter	Description
`-all`	Checks and displays the version of Oracle Autonomous Health Framework components.
`-tfa`	Checks and displays the version of Oracle Trace File Analyzer.
`-compliance`	Checks and displays the version of Oracle Autonomous Health Framework compliance (Oracle ORAchk and Oracle EXAchk) components.

9.3.2 Running Oracle Trace File Analyzer Summary and Analysis Commands

Use these commands to view the summary of deployment and status of Oracle Trace File Analyzer, and changes and events detected by Oracle Trace File Analyzer.

- tfactl analyze
  Use the `tfactl analyze` command to obtain analysis of your system by parsing the database, Oracle Automatic Storage Management (Oracle ASM), and Oracle Grid Infrastructure alert logs, system message logs, OSWatcher Top, and OSWatcher Slabinfo files.
- tfactl changes
  Use the `tfactl changes` command to view the changes detected by Oracle Trace File Analyzer.
- tfactl events
  Use the `tfactl events` command to view the events detected by Oracle Trace File Analyzer.
- tfactl isa
  Use the `tfactl isa` command to view the Infrastructure Service Automation (ISA) score.
- tfactl param
  Use the `tfactl param` command to view the values of operating system and database parameters specified.

- tfactl run
  Use the `tfactl run` command to run the requested action (can be inventory or scan or any support tool).
- tfactl search
  Use the `tfactl search` command to search all metadata stored in the Oracle Trace File Analyzer index.
- tfactl summary
  Use the `tfactl summary` command to view the summary of Oracle Trace File Analyzer deployment.
- tfactl toolstatus
  Use the `tfactl toolstatus` command to view the status of Oracle Trace File Analyzer Support Tools across all nodes.

9.3.2.1 tfactl analyze

Use the `tfactl analyze` command to obtain analysis of your system by parsing the database, Oracle Automatic Storage Management (Oracle ASM), and Oracle Grid Infrastructure alert logs, system message logs, OSWatcher Top, and OSWatcher Slabinfo files.

Filter the output of the command by component, error type, and time.

With the `tfactl analyze` command, you can choose from the following types of log file analysis:

- **Show the most common messages within the logs**: This analysis provides a quick indication of where larger issues are occurring. Oracle Trace File Analyzer takes important messages out of the alert logs and strips the extraneous information from the log messages, organizes the most commonly occurring messages, and displays them in the order from most common to least common. By default, Oracle Trace File Analyzer analyzes error messages, but you can specify a particular type of message for analysis.
- **Search for text within log messages**: This is similar to using the `grep` utility to search, only faster because Oracle Trace File Analyzer checks the time of each message and only shows those matching the last *x* number of minutes or any interval of time.
- **Analyze the Oracle OSWatcher log statistics**: Oracle Trace File Analyzer reads the various statistics available in the `OSWatcher` log files and provides detailed analysis showing first, highest, lowest, average, and the last three readings of each statistic. Choose any interval down to a specific minute or second. Oracle Trace File Analyzer optionally provides the original data from the `OSWatcher` logs for each value reported on (data point).

Syntax

```
tfactl analyze
[-search "pattern"]
[-comp db|asm|crs|acfs|os|osw|oswslabinfo|oratop|all]
[-type error|warning|generic]
[-last n[h|d]]
[-from time]
[-to time]
[-for time]
[-node all|local|n1,n2,...]
[-verbose]
```

```
[-o file]
[timeline [-l n] f1 f2...fn]
[-examples]
```

Parameters

Table 9-87 tfactl analyze Command Parameters

Parameter	Description
`-search "pattern"`	Searches for a pattern enclosed in double quotation marks ("") in system and alert logs within a specified time range. This parameter supports both case-sensitive and case-insensitive search in alert and system message files across the cluster within the specified filters. Default is case insensitive. If you do not specify the `-search` parameter, then Oracle Trace File Analyzer provides a summary of messages within specified filters from alert and system log messages across the cluster. Oracle Trace File Analyzer displays message counts grouped by type (`error`, `warning`, and `generic`) and shows unique messages in a table organized by message type selected for analysis. The `generic` message type is assigned to all messages which are not either an `error` or `warning` message type.
`[-comp db|asm|crs|acfs|os|osw|oswslabinfo|oratop|all]`	Select which components you want Oracle Trace File Analyzer to analyze. Default is `all`. • `db`: Database alert logs • `asm`: Oracle ASM alert logs • `crs`: Oracle Grid Infrastructure alert logs • `acfs`: Oracle ACFS alert logs • `os`: System message files • `osw`: OSW Top output • `oswlabinfo`: OSW Slabinfo output When `OSWatcher` data is available, `OSW` and `OSWSLABINFO` components provide summary views of OSWatcher data.
`-type error | warning | generic`	Select what type of messages Oracle Trace File Analyzer analyzes. Default is `error`.
`[-last n[h|d]]`	Specify an amount of time, in hours or days, before current time that you want Oracle Trace File Analyzer to analyze.

Table 9-87 (Cont.) tfactl analyze Command Parameters

Parameter	Description

`-from | -to | -for` *`time`*	Specify a time interval, using the `-from` and `-to` parameters together.
	Supported time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`
	Or, a specific time using the `-for` parameter that you want Oracle Trace File Analyzer to analyze.
	Supported time formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`

`[-node all|local|`*`n1`*`,` *`n2`*`,...]`	Specify a comma-separated list of host names. Use `-local` to analyze files on the local node. Default is all.
`-verbose`	Displays verbose output.
`-o` *`file`*	Specify a file where Oracle Trace File Analyzer writes the output instead of displaying on the screen.
`timeline`	Displays timeline for the specified trace or alert log files. `-l`*`n`*: Specify debug level, for example, `l 3`. Debug levels: • 1 – FATAL • 2 – ERROR • 3 – WARNING • 4 – INFO (default) • 5 – DEBUG • 6 – TRACE *`f1 f2...fn`*: Specify a space-delimited list of file names.
`[-examples]`	Specify this parameter to view `analyze` usage examples.

-type Parameter Arguments

The `tfactl analyze` command classifies all the messages into different categories when you specify the `-type` parameter. The analysis component provides count of messages by the message type you configure and lists all unique messages grouped by count within specified filters. The message type patterns for each argument are listed in the following table.

Table 9-88 tfactl analyze -type Parameter Arguments

<table>
<tr><th>Argument</th><th>Description</th></tr>
<tr><td>error</td><td>Error message patterns for Oracle Database and Oracle ASM alert logs:

.*ORA-00600:.*
.*ORA-07445:.*
.*IPC Send timeout detected. Sender: ospid.*
.*Direct NFS: channel id .* path .* to filer .* PING timeout.*
.*Direct NFS: channel id .* path .* to filer .* is DOWN.*
.*ospid: .* has not called a wait for .* secs.*
.*IPC Send timeout to .* inc .* for msg type .* from opid.*
.*IPC Send timeout: Terminating pid.*
.*Receiver: inst .* binc .* ospid.*
.* terminating instance due to error.*
.*: terminating the instance due to error.*
.*Global Enqueue Services Deadlock detected
.*ORA-031(13|37):.*
.*ORA-00603:.*
.*ORA-0035(3|5|6):.*
.*ORA-00700:.*
.*ORA-040(20|36):.*
.*ORA-0403(0|1):.*
.*ORA-002(27|39|40|55):.*
.*ORA-01578:.*
.*ORA-2(5319|4982):.*
.*ORA-56729:.*
.*ORA-00445:.*

Error message patterns for Oracle Grid Infrastructure alert logs:

.*CRS-8011:.*
.*CRS-8013:.*
.*CRS-1607:.*
.*CRS-1615:.*
.*CRS-1714:.*
.*CRS-1656:.*
.*PRVF-5305:.*
.*CRS-1601:.*
.*CRS-1610:.*
.*PANIC. CRSD exiting:.*
.*Fatal Error from AGFW Proxy:.*
.*CRS-1603:.*
.*CRS-10051:.*
.*CRS-2409:.*
.*CRS-1625:.*</td></tr>
</table>

Table 9-88 (Cont.) tfactl analyze -type Parameter Arguments

Argument	Description

`warning`	Warning message patterns for database and Oracle ASM alert logs:
	`NOTE: process .* initiating offline of disk .*`
	`.*WARNING: cache read a corrupted block group.*`
	`.*NOTE: a corrupted block from group FRA was dumped to`

`generic`	Any messages that do not match any of the preceding patterns.

oratop options

The options available when using `-comp oratop`:

```
-database dbname oratop options logon
```

Table 9-89 tfactl analyze -comp oratop options

Argument	Description
`-database` *`dbname`*	Specify the name of the Oracle Database to run `oratop`.
`logon`	Default is `/ as sysdba`. Specify a different user using, `{username[/password][@connect_identifier] | / } [AS {SYSDBA|SYSOPER}]` Connect Identifier: *`host`*`[:`*`port`*`]/[`*`service_name`*`]`

Table 9-90 oratop options

Argument	Description
`-b`	Specify the batch mode. Default: text-based user interface.
`-n`	Specify the maximum number of iterations.
`-o`	Writes console output to a file (in batch mode).
`-i`	Specify the interval delay in seconds. Default: 5 seconds.
`-r`	Real-time (RT) wait events. (sec 3, default: Cumulative)
`-m`	Specify `MODULE`/`ACTION` (section 4). Default: `USERNAME`/`PROGRAM`.
`-s`	Specify the SQL mode (section 4). Default: process mode.

Table 9-90 (Cont.) oratop options

Argument	Description
`-f`	Specify the detailed format (132 columns). Default: standard (80 columns).
`-v`	Displays `oratop` release version number.

Examples

The following command examples demonstrate how to use Oracle Trace File Analyzer to search collected data:

- `tfactl analyze -search "error" -last 2d`

  Oracle Trace File Analyzer searches database alert and system log files collected since the past two days for messages that contain case-insensitive string "error".
- `tfactl analyze -comp os -for "Jul/01/2021 11" -search "."`

  Oracle Trace File Analyzer displays all system log messages collected at the date and time specified, that is, July 1, 2021 at 11 am.
- `tfactl analyze -search "/ORA-/c" -comp db -last 2d`

  Oracle Trace File Analyzer searches database alert and system log files collected since the past two days for messages that contain case-sensitive string "ORA-".
- `tfactl analyze -search "ORA-00600" -last 8h`

  Oracle Trace File Analyzer searches database alert and system log files collected since the last eight hours for the messages that contain case-insensitive string "ORA-00600".

The following command examples demonstrate how to use Oracle Trace File Analyzer to analyze collected data:

- `tfactl analyze -last 5h`

  Oracle Trace File Analyzer displays a summary of events from all alert logs and system messages collected since the past five hours.
- `tfactl analyze -comp os -last 1d`

  Oracle Trace File Analyzer displays a summary of events from system messages collected since the past day.
- `tfactl analyze -last 1h -type generic`

  Oracle Trace File Analyzer analyzes all generic messages collected since the last hour.
- `tfactl analyze -type generic -last 1d`

  Oracle Trace File Analyzer analyzes all generic messages collected since the past day.
- `tfactl analyze -last 1d -node $HOSTNAME`

  Oracle Trace File Analyzer displays a summary of events for the past day from all database alert and system log files collected on the node specified.
- `tfactl analyze -database $ORACLE_SID`

Oracle Trace File Analyzer displays a summary of events from all database alert and system log files for the database instance specified.

The following command examples demonstrate how to use Oracle Trace File Analyzer to analyze `OSWatcher` Top and Slabinfo:

- `tfactl analyze -comp osw -last 6h`

  Oracle Trace File Analyzer displays `OSWatcher` Top summary for the past six hours.
- `tfactl analyze -comp oswslabinfo -from "2021-07-01" -to "2021-07-03"`

  Oracle Trace File Analyzer displays `OSWatcher` Slabinfo summary for time period specified.

9.3.2.2 tfactl changes

Use the `tfactl changes` command to view the changes detected by Oracle Trace File Analyzer.

Syntax

```
tfactl changes
[-from time -to time | -for time | last time_length]
```

Parameters

Option	Description

`from` *`time`* `-to` *`time`*	Specify the `-from` and `-to` parameters (you must use these two parameters together) to view changes that occurred during a specific time interval.
	Supported time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`

`for` *`time`*	Specify the `-for` parameter to view the changes that occurred at the time given.
	Supported time formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`

`-last` *`nh|d`*	Specify the `-last` parameter to view changes for the past specific number of hours (h), or days (d).

Option	Description
`-type`	Supported values: - `databaseParameters` - `OSParameters` - `OSPackages` - `oracleHomes` - `OracleHomePatches` Default value: `all`
`-node`	Specify the node for which you want to generate the report. Supported values: `local` or `all`.
`-json`	Specify to generate the report in JSON format.

Example

```
$ tfactl changes
Output from host : myserver69
------------------------------

Output from host : myserver70
------------------------------
Jul/26/2016 10:20:35 : Parameter 'sunrpc.transports' value changed :
tcp 1048576 => udp 32768
Jul/26/2016 10:20:35 : Parameter 'sunrpc.transports' value changed :
tcp 1048576 => tcp-bc 1048576

Output from host : myserver71
------------------------------
Jul/26/2016 10:21:06 : Parameter 'sunrpc.transports' value changed :
tcp 1048576 => udp 32768
Jul/26/2016 10:21:06 : Parameter 'sunrpc.transports' value changed :
tcp 1048576 => tcp-bc 1048576


tfactl changes -last 24h -node all -json
Generating System Changes From 05/11/2023 05:11:24.927 To 05/12/2023
05:11:24.927

{
  "snapshotTimestamp": "2023-05-12 05:11:24.000000",
  "timePeriodOfChange": "1 Days",
  "changeRecords": {
    "node1": [],
    "node2": []
  }
}


tfactl changes -last 1h -node local
Generating System Changes From 05/12/2023 04:10:43.844 To 05/12/2023
05:10:43.845
```

```
Snapshot Timestamp for Changes:2023-05-12 05:10:43.000000
Duration for Changes: 1 Hours

Change Records for host: node1
No Changes Found


tfactl changes -last 10h -node all
Generating System Changes From 05/11/2023 19:11:01.188 To 05/12/2023
05:11:01.188

Snapshot Timestamp for Changes:2023-05-12 05:11:01.000000
Duration for Changes: 10 Hours

Change Records for host: node1
===========================================
No Changes Found

Change Records for host: node2
===========================================
No Changes Found
```

9.3.2.3 tfactl events

Use the `tfactl events` command to view the events detected by Oracle Trace File Analyzer.

Syntax

```
tfactl events
[-search keyword | -component ASM|CRS | -database db_name | -instance
db_instance_name | -source filename | -from time -to time | -json | -fields
all|fields_list]
```

Parameters

Option	Description
`component [ASM|CRS]`	Searches all Oracle Automatic Storage Management (Oracle ASM) or Oracle Clusterware events.
`database` *db_name*	Specify the name of an Oracle Database to search all events from that Oracle Database.
`instance` *db_instance_name*	Specify the name of an Oracle Database instance to search all events from that Oracle Database instance.
`source` *filename*	Specify the source file name to search all events from that alert file.
`json`	Displays event information in JSON format.

Option	Description

`-last` *`nh`*`|`*`d`* `| -from` *`time`* `-to` *`time`* `| -for` *`time`*`]`	• Specify the `-last` parameter to view events for the past specific number of hours (*h*) or days (*d*).
	• Specify the `-from` and `-to` parameters (you must use these two parameters together) to view events that occurred during a specific time interval.
	Supported time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`
	• Specify the `-for` parameter to view events for the time given.
	Supported time formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`
	Note:
	If you specify both date and time, then you must enclose both the values in double quotation marks (""). If you specify only the date or the time, then you do not have to enclose the single value in quotation marks.

`fields all|` *`fields_list`*	When provided with the `-json` option, the command returns only the requested fields

Oracle Trace File Analyzer detects the following events:

```
ORA-03113
ORA-03137
ORA-00603
ORA-00700
ORA-00353
ORA-00355
ORA-00356
ORA-04020
ORA-04036
ORA-04030
ORA-04031
ORA-00227
ORA-00239
ORA-00240
ORA-00255
ORA-00257
ORA-01578
ORA-25319
ORA-24982
```

```
ORA-56729
ORA-00445
ORA-5014
ORA-27300
ORA-27301
ORA-27302
ORA-00060
ORA-16038
ORA-15338
ORA-15064
ORA-19815
ORA-19804
ORA-19809
ORA-15196
ORA-08101
ORA-08102
ORA-08103
ORA-04021
ORA-15311
ORA-00600
ORA-07445
ORA-00469
ORA-00470
ORA-00471
ORA-00472
ORA-00473
ORA-00474
ORA-00475
ORA-00476
ORA-00478
ORA-00479
ORA-00480
ORA-00481
ORA-00482
ORA-00483
ORA-00484
ORA-00485
ORA-00486
ORA-00487
ORA-00488
ORA-00489
ORA-00490
ORA-00491
ORA-00492
ORA-00493
ORA-00495
ORA-00496
ORA-00497
ORA-00498
ORA-00499
ORA-29701
ORA-29702
ORA-29703
ORA-29708
ORA-29709
```

```
ORA-29710
ORA-29740
ORA-29770
ORA-29771
ORA-32701
ORA-32703
ORA-32704
ORA-00494
```

Example

```
$ tfactl events
Output from host : node1
------------------------------
Event Summary:
INFO    :15
ERROR   :105
WARNING :2
Event Timeline:
[Aug/24/2020 20:03:01.000]: [db.db0422_iad33r.DB04221]: ORA-00600:
internal error code, arguments: [kghfrf1], [], [], []
[Aug/24/2020 20:03:01.000]: [db.db0422_iad33r.DB04221]: ORA-07445:
exception encountered: core dump [] [] [] [] [] []
[Aug/24/2020 20:03:01.000]: [db.db0422_iad33r.DB04221]: ORA-29708:
error occurred in Cluster Synchronization Services
[Aug/24/2020 20:05:00.000]: [db.db0422_iad33r.DB04221]: ORA-00257:
archiver error
[Aug/24/2020 20:05:00.000]: [db.db0422_iad33r.DB04221]: ORA-01578:
ORACLE data block corrupted file 1, block 57371
[Aug/24/2020 20:05:00.000]: [db.db0422_iad33r.DB04221]: ORA-32701:
Possible hangs up to hang ID= detected
[Aug/24/2020 20:07:01.000]: [db.db0422_iad33r.DB04221]: Instance
terminated by USER, pid = 49334
[Aug/24/2020 20:10:09.000]: [db.db0422_iad33r.DB04221]: Starting
ORACLE instance (normal) (OS id: 52489)
[Aug/24/2020 20:10:14.000]: [db.db0422_iad33r.DB04221]:
Reconfiguration started (old inc 0, new inc 44)
[Aug/24/2020 23:22:00.000]: [db.db0422_iad33r.DB04221]: ORA-00600:
internal error code, arguments: [kghfrf1], [], [], []
[Aug/24/2020 23:22:00.000]: [db.db0422_iad33r.DB04221]: ORA-07445:
exception encountered: core dump [] [] [] [] [] []
[Aug/24/2020 23:22:00.000]: [db.db0422_iad33r.DB04221]: ORA-29708:
error occurred in Cluster Synchronization Services
[Aug/24/2020 23:24:01.000]: [db.db0422_iad33r.DB04221]: ORA-00257:
archiver error
[Aug/24/2020 23:24:01.000]: [db.db0422_iad33r.DB04221]: ORA-01578:
ORACLE data block corrupted file 1, block 57371
[Aug/24/2020 23:24:01.000]: [db.db0422_iad33r.DB04221]: ORA-32701:
Possible hangs up to hang ID= detected
[Aug/24/2020 23:26:02.000]: [asm.+ASM1]: Instance terminated by USER,
pid = 83183
[Aug/24/2020 23:29:15.000]: [asm.+ASM1]: Starting ORACLE instance
(normal) (OS id: 98769)
[Aug/24/2020 23:29:20.000]: [asm.+ASM1]: Reconfiguration started (old
inc 0, new inc 188)
[Aug/24/2020 23:37:02.000]: [db.db0422_iad33r.DB04221]: Instance terminated
by USER, pid = 7260
[Aug/24/2020 23:40:15.000]: [db.db0422_iad33r.DB04221]: Starting ORACLE
instance (normal) (OS id: 19279)
[Aug/24/2020 23:40:21.000]: [db.db0422_iad33r.DB04221]: Reconfiguration
started (old inc 0, new inc 48)
[Aug/24/2020 23:48:07.000]: [asm.+ASM1]: Starting ORACLE instance (normal)
(OS id: 33507)
[Aug/24/2020 23:48:11.000]: [asm.+ASM1]: Reconfiguration started (old inc 0,
new inc 192)
[Aug/24/2020 23:48:16.000]: [db.db0422_iad33r.DB04221]: ORA-15064:
communication failure with ASM instance
[Aug/24/2020 23:52:02.000]: [db.db0422_iad33r.DB04221]: Instance terminated
by USER, pid = 20510
[Aug/24/2020 23:52:35.088]: [crs]: 2020-08-24 23:52:35.088
[OCSSD(31306)]CRS-1603: CSSD on node racgi-kumar1 has been shut down.
[Aug/24/2020 23:55:57.333]: [crs]: 2020-08-24 23:55:57.333
[OCSSD(46179)]CRS-1601: CSSD Reconfiguration complete. Active nodes are
racgi-kumar1 racgi-kumar2 .
[Aug/24/2020 23:56:19.000]: [asm.+ASM1]: Starting ORACLE instance (normal)
(OS id: 47183)
[Aug/24/2020 23:56:24.000]: [asm.+ASM1]: Reconfiguration started (old inc 0,
new inc 196)
[Aug/24/2020 23:56:32.000]: [apx.+APX1]: Starting ORACLE instance (normal)
(OS id: 47673)
[Aug/24/2020 23:56:35.000]: [db.db0422_iad33r.DB04221]: Starting ORACLE
instance (normal) (OS id: 47714)
[Aug/24/2020 23:56:41.000]: [db.db0422_iad33r.DB04221]: Reconfiguration
started (old inc 0, new inc 52)
[Aug/25/2020 11:25:00.000]: [db.db0422_iad33r.DB04221]: ORA-00600: internal
error code, arguments: [kghfrf1], [], [], []
[Aug/25/2020 11:25:00.000]: [db.db0422_iad33r.DB04221]: ORA-07445: exception
encountered: core dump [] [] [] [] [] []
[Aug/25/2020 11:25:00.000]: [db.db0422_iad33r.DB04221]: ORA-29708: error
occurred in Cluster Synchronization Services
[Aug/25/2020 11:27:01.000]: [db.db0422_iad33r.DB04221]: ORA-00257: archiver
error
[Aug/25/2020 11:27:01.000]: [db.db0422_iad33r.DB04221]: ORA-01578: ORACLE
data block corrupted file 1, block 57371
[Aug/25/2020 11:27:01.000]: [db.db0422_iad33r.DB04221]: ORA-32701: Possible
hangs up to hang ID= detected
[Aug/25/2020 11:29:02.000]: [db.db0422_iad33r.DB04221]: Instance terminated
by USER, pid = 59035
[Aug/25/2020 11:32:09.000]: [db.db0422_iad33r.DB04221]: Starting ORACLE
instance (normal) (OS id: 62205)
[Aug/25/2020 11:32:14.000]: [db.db0422_iad33r.DB04221]: Reconfiguration
started (old inc 0, new inc 56)
```

9.3.2.4 tfactl isa

Use the `tfactl isa` command to view the Infrastructure Service Automation (ISA) score.

Syntax

```
tfactl isa
[-availability]
[-all]
[-node all|local|n1,n2,...]
```

Parameters

Table 9-91 tfactl run Command Parameters

Parameter	Description
`availability`	Includes the Availability Score.
`all`	Displays all the details.
`node`	Specify a comma-separated list of host names.

9.3.2.5 tfactl param

Use the `tfactl param` command to view the values of operating system and database parameters specified.

> **Note:**
>
> `tfactl param` replaces `tfactl run param`.

Syntax

```
tfactl param [-type TYPE] [-parameter PARAMETER] [-database DATABASE]
[-node NODE] [-json] [-refresh]
```

Parameters

Table 9-92 tfactl param Command Parameters

Parameter	Description
`-type` *`TYPE`*	Specify the parameter type. **Valid values:** • `databaseParameters` • `OSParameters` **Default:** `all`

Table 9-92 (Cont.) tfactl param Command Parameters

Parameter	Description
`-parameter` *`PARAMETER`*	Specify the name or part of the name of the parameter. If not specified, then all parameters of the parameter type specified will be displayed. **Valid values:** • `sga_max` • `sga_min` • `db_unique` • `shmmax`
`-database DATABASE`	Specify the name of the database. This option can be used only when the parameter type specified is `databaseParameters` or `all`.
`-node` *`NODE`*	Specify the node. **Valid values:** • `local` • `all`
`-json`	Specify to print the values in JSON format.
`-refresh`	Specify to refresh param data.

Example 9-106 tfactl param

```
tfactl param sga_max


tfactl param sga_min


tfactl param db-unique


tfactl param shmmax
```

9.3.2.6 tfactl run

Use the `tfactl run` command to run the requested action (can be inventory or scan or any support tool).

> **Note:**
>
> `tfactl run param` will be deprecated in a future release. It will be replaced by `tfactl param`.

Syntax

```
tfactl [run [inventory | scan | <tool>]] | [<tool>]
```

Parameters

Table 9-93 tfactl run Command Parameters

Parameter	Description
`inventory`	Inventory of all trace file directories.
`scan`	Runs a one off scan.
`tool`	Runs the desired analysis tool.

Analysis Tools

Table 9-94 tfactl run Analysis Tools Parameters

Parameter	Description
`orachk`	Runs `Oracle ORAchk`.
`oratop`	Runs `oratop`.
`oswbb`	Runs `OSWatcher Analyzer`.
`prw`	Runs `Procwatcher`.
`alertsummary`	Prints summary of important events in Oracle Database / ASM alert logs.
`calog`	Prints Oracle Clusterware activity logs.
`dbglevel`	Sets Oracle Clusterware log / trace levels using profiles.
`grep`	`grep` for input string in logs.
`history`	Lists commands run in current Oracle Trace File Analyzer shell session.
`ls`	Searches files in Oracle Trace File Analyzer.
`managelogs`	Purge slogs.
`menu`	Oracle Trace File Analyzer Collector menu system.
`param`	Prints parameter value.
`ps`	Finds a process.
`pstack`	Runs `pstack` on a process.
`summary`	Prints system summary.
`tail`	Tails log files.
`triage`	Summarize `OSWatcher` / `ExaWatcher` data.
`vi`	Searches and opens files in the `vi` editor.

Profiling Tools

Table 9-95 tfactl run Profiling Tools Parameters

Parameter	Description
`dbglevel`	Sets Oracle Clusterware log and trace levels using profiles.

Related Topics

- tfactl param
  Use the `tfactl param` command to view the values of operating system and database parameters specified.

9.3.2.7 tfactl search

Use the `tfactl search` command to search all metadata stored in the Oracle Trace File Analyzer index.

Syntax

```
tfactl search
[-json json_string | -fields all|fields_list | -showdatatypes | -showfields
datatype]
```

Parameters

Table 9-96 tfactl search Command Parameters

Parameter	Description
`json`	JSON string containing the search criteria.
`fields`	Returns the JSON output with only the requested fields.
`showdatatypes`	Displays the list of all available datatypes.
`showfields`	Displays the list of fields available in a datatype.

9.3.2.8 tfactl summary

Use the `tfactl summary` command to view the summary of Oracle Trace File Analyzer deployment.

Syntax

```
tfactl [run] summary [OPTIONS]
```

Options

Option	Description
`[no_components]`	[Default] Complete summary collection
`-overview`	[Optional/Default] Complete summary collection - overview.
`-crs`	[Optional/Default] Oracle Clusterware status summary.
`-asm`	[Optional/Default] Oracle ASM status summary.
`-acfs`	[Optional/Default] Oracle ACFS status Summary.
`-database`	[Optional/Default] Oracle Database status summary.
`-exadata`	[Optional/Default] Oracle Exadata status summary. Not enabled/ignored in Microsoft Windows and Non-Exadata machine

Option	Description
`-patch`	[Optional/Default] Patch details.
`-listener`	[Optional/Default] LISTENER status summary.
`-network`	[Optional/Default] NETWORK status summary.
`-os`	[Optional/Default] Operating system status summary.
`-tfa`	[Optional/Default] Oracle Trace File Analyzer status summary.
`-summary`	[Optional/Default] Summary tool metadata.
`-json`	[Optional] - Prepare JSON report.
`-html`	[Optional] - Prepare HTML report.
`-print`	[Optional] - Display [HTML or JSON] report at console.
`-silent`	[Optional] - Interactive console by default.
`-history` *`num`*	[Optional] - View Previous *numberof* summary collection history in interpreter.
`-node`	*node(s)* : [Optional] - local or comma-separated list of names of nodes.
`-help`	Usage/help

9.3.2.9 tfactl toolstatus

Use the `tfactl toolstatus` command to view the status of Oracle Trace File Analyzer Support Tools across all nodes.

Syntax

```
$ tfactl toolstatus
```

Example 9-107 tfactl toolstatus

The `tfactl toolstatus` command returns output similar to the following, showing which tool is deployed and where the tool is deployed.

```
.------------------------------------------------------------------.
|                 TOOLS STATUS - HOST : myhost                     |
+----------------------+--------------+--------------+-------------+
| Tool Type            | Tool         | Version      | Status      |
+----------------------+--------------+--------------+-------------+
| Development Tools    | orachk       |   12.2.0.1.3 | DEPLOYED    |
|                      | oratop       |       14.1.2 | DEPLOYED    |
+----------------------+--------------+--------------+-------------+
| Support Tools Bundle | darda        | 2.10.0.R6036 | DEPLOYED    |
|                      | oswbb        |        8.1.2 | RUNNING     |
|                      | prw          | 12.1.13.11.4 | NOT RUNNING |
+----------------------+--------------+--------------+-------------+
| TFA Utilities        | alertsummary |   12.2.1.1.0 | DEPLOYED    |
|                      | calog        |   12.2.0.1.0 | DEPLOYED    |
|                      | dbcheck      |   18.3.0.0.0 | DEPLOYED    |
|                      | dbglevel     |   12.2.1.1.0 | DEPLOYED    |
|                      | grep         |   12.2.1.1.0 | DEPLOYED    |
|                      | history      |   12.2.1.1.0 | DEPLOYED    |
|                      | ls           |   12.2.1.1.0 | DEPLOYED    |
|                      | managelogs   |   12.2.1.1.0 | DEPLOYED    |
|                      | menu         |   12.2.1.1.0 | DEPLOYED    |
|                      | param        |   12.2.1.1.0 | DEPLOYED    |
|                      | ps           |   12.2.1.1.0 | DEPLOYED    |
|                      | pstack       |   12.2.1.1.0 | DEPLOYED    |
|                      | summary      |   12.2.1.1.0 | DEPLOYED    |
|                      | tail         |   12.2.1.1.0 | DEPLOYED    |
|                      | triage       |   12.2.1.1.0 | DEPLOYED    |
|                      | vi           |   12.2.1.1.0 | DEPLOYED    |
'----------------------+--------------+--------------+-------------'

Note :-
  DEPLOYED    : Installed and Available - To be configured or run
interactively.
  NOT RUNNING : Configured and Available - Currently turned off
interactively.
  RUNNING     : Configured and Available.
```

9.3.3 Running Oracle Trace File Analyzer Diagnostic Collection Commands

Run the diagnostic collection commands to collect diagnostic data.

- tfactl collection
  Use the `tfactl collection` command to manage Oracle Trace File Analyzer collections.
- tfactl dbglevel
  Use the `tfactl dbglevel` command to set Oracle Grid Infrastructure trace levels.
- tfactl diagcollect
  Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.
- tfactl diagcollect -srdc
  Use the `tfactl diagcollect -srdc` command to run a Service Request Data Collection (SRDC).
- tfactl directory
  Use the `tfactl directory` command to add a directory to, or remove a directory from the list of directories to analyze their trace or log files.
- tfactl ips
  Use the `tfactl ips` command to collect Automatic Diagnostic Repository diagnostic data.
- tfactl managelogs
  Use the `tfactl managelogs` command to manage Automatic Diagnostic Repository log and trace files.
- tfactl purge
  Use the `tfactl purge` command to delete collections and log files from AHF components from the local node.

9.3.3.1 tfactl collection

Use the `tfactl collection` command to manage Oracle Trace File Analyzer collections.

Syntax

```
tfactl collection [-h] [stop collection_id] [list-contents -
collectionname COLLECTIONNAME | -collectionzip COLLECTIONZIP]
```

- To stop a collection, use:

  ```
  tfactl collection stop collection_id
  ```

  Run the `tfactl print` command to get the collection ID.
- To list the contents of diagnostic collection including any nested zip files, use:

  ```
  tfactl collection list-contents -collectionzip zip
  ```

- To list the contents of all zip files within a specific collection, use:

  ```
  tfactl collection list-contents -collectionname collection-name
  ```

9.3.3.2 tfactl dbglevel

Use the `tfactl dbglevel` command to set Oracle Grid Infrastructure trace levels.

Syntax

```
tfactl [run] dbglevel
[ {-set|-unset} profile_name
-dependency [dep1,dep2,...|all]
-dependency_type [type1,type2,type3,...|all]
| {-view|-drop} profile_name
| -lsprofiles
| -lsmodules
| -lscomponents [module_name]
| -lsres
| -create profile_name [ -desc description
| [-includeunset] [-includetrace]
| -debugstate | -timeout time ]
| -modify profile_name [-includeunset] [-includetrace]
| -getstate [ -module module_name ]
| -active [profile_name]
| -describe [profile_name] ] ]
```

Parameters

Table 9-97 tfactl dbglevel Command Parameters

Parameter	Description
`profile_name`	Specify the name of the profile.
`active`	Displays the list of active profiles.
`set`	Sets the trace or log levels for the profile specified.
`unset`	Unsets the trace or log levels for the profile specified.
`view`	Displays the trace or log entries for the profile specified.
`create`	Creates a profile.
`drop`	Drops the profile specified.
`modify`	Modifies the profile specified.
`describe`	Describes the profiles specified.
`lsprofiles`	Lists all the available profiles.
`lsmodules`	Lists all the discovered Oracle Clusterware modules.
`lscomponents`	Lists all the components associated with the Oracle Clusterware module.
`lsres`	Lists all the discovered Oracle Clusterware resources.
`getstate`	Displays the current trace or log levels for the Oracle Clusterware components or resources.
`module`	Specify the Oracle Clusterware module.
`dependency`	Specify the dependencies to consider, start, or stop dependencies, or both.
`dependency_type`	Specify the type of dependencies to be consider.
`debugstate`	Generates a System State Dump for all the available levels.
`includeunset`	Adds or modifies an unset value for the Oracle Clusterware components or resources.
`includetrace`	Adds or modifies a trace value for the Oracle Clusterware components.

> **WARNING:**
>
> Set the profiles only at the direction of Oracle Support.

9.3.3.3 tfactl diagcollect

Use the `tfactl diagcollect` command to perform on-demand diagnostic collection.

AHF 23.8

Starting in AHF 23.8, you will be able to upload to pre-authenticated (PAR) URL. Uploading AHF Insights reports helps Oracle Cloud Operations to identify, investigate, track, and resolve system health issues and divergences in best practice configurations quickly and effectively.

Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D) and Oracle Base Database Service

To upload AHF Insights report to PAR location, run:

```
tfactl diagcollect -insight -last 1h -par <par_url>
```

```
tfactl insight -last 1h -par <par_url>
```

Oracle Trace File Analyzer Collector can perform three types of on-demand collections:

- Default collections
- Event-driven Support Service Request Data Collection (SRDC) collections
- Custom collections

Syntax

```
tfactl diagcollect [ [-insight | -noinsight] [component_name1]
[component_name2] ... [component_nameN] | [-srdc <srdc_profile>] | [-
defips]]
[-sr <SR#>]
[-node <all|local|n1,n2,..>]
[-tag <tagname>]
[-z <filename>]
[-acrlevel <system,database,userdata>]
[-last <n><m|h|d>| -from <time> -to <time> | -for <time>]
[-nocopy]
[-notrim]
[-dryrun]
[-silent]
[-cores]
[-collectalldirs]
[-collectdir <dir1,dir2..>]
[-collectfiles <file1,..,fileN,dir1,..,dirN> [-onlycollectfiles]]
[-par <par_url>]
[-onlyinsights]
[-request_from <requestor>]
[-examples]
[-singlearchive]
```

Components:

```
-ips|-database|-asm|-crsclient|-dbclient|-dbwlm|-tns|-rhp|-procinfo|-
cvu|-afd|-crs|-cha|-wls|-emagenti|-emagent|-oms|-omsi|-ocm|-emplugins|-
em|-acfs|-install|-cfgtools|-os|-ashhtml|-ashtext|-awrhtml|-awrtext|-
sosreport|-qos|-ahf|-dataguard|-syslens|-hami|-asr|-oda
```

For detailed help on each component, use `tfactl diagcollect [component_name1] [component_name2] ... [component_nameN] -help`

Parameters

Prefix each option with a minus sign (-).

Option	Description
`[ [-insight | -noinsight] [`*`component_name1`*`] [`*`component_name2`*`] ... [`*`component_nameN`*`] | [-srdc `*`srdc_profile`*`] | [-defips]]`	Specify the list of components for which you want to obtain collections, or specify the SRDC name, or specify to include Incident Packaging Service (IPS) Packages for Oracle Automatic Storage Management (Oracle ASM), Oracle Clusterware, and Oracle Databases in the default collection. `-insight`: Specify to include the AHF Insights Report in the diagnostic collection. `-noinsight`: Specify not to include the AHF Insights Report in the diagnostic collection. `[-defips]`: Specify to Include in the default collection the IPS Packages for ASM, CRS, and Databases.
`[-sr `*`SR#`*`]`	Specify the Service Request number to which Oracle Trace File Analyzer automatically uploads all collections.
`-node all|local|`*`n1,n2,...`*	Collects diagnostics from the nodes specified. Specify a comma-delimited list of nodes. If you do not specify, then the commands collects diagnostics for all the nodes by default. For example: `tfactl diagcollect -node node1`
`-tag `*`description`*	Use this parameter to create a subdirectory for the resulting collection in the Oracle Trace File Analyzer repository.
`-z `*`file_name`*	Use this parameter to specify an output file name.

Option	Description

`[-last` *`nh`*`|`*`d`* `| -from` *`time`* `-to` *`time`* `| -for` *`time`*`]`	• Specify the `-last` parameter to collect files that have relevant data for the past specific number of hours (*h*) or days (*d*). By default, using the command with this parameter also trims files that are large and shows files only from the specified interval.
	You can also use `-since`, which has the same functionality as `-last`. This option is included for backward compatibility.
	• Specify the `-from` and `-to` parameters (you must use these two parameters together) to collect files that have relevant data during a specific time interval, and trim data before this time where files are large.
	Supported time formats:
	`"Mon/dd/yyyy hh:mm:ss"`
	`"yyyy-mm-dd hh:mm:ss"`
	`"yyyy-mm-ddThh:mm:ss"`
	`"yyyy-mm-dd"`
	• Specify the `-for` parameter to collect files that have relevant data for the time given. The files `tfactl` collects will have timestamps in between which the time you specify after `-for` is included. No data trimming is done for this option.
	Supported time formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`
	Note:
	If you specify both date and time, then you must enclose both the values in double quotation marks (""). If you specify only the date or the time, then you do not have to enclose the single value in quotation marks.

`-nocopy`	Specify this parameter to stop the resultant trace file collection from being copied back to the initiating node. The file remains in the Oracle Trace File Analyzer repository on the executing node.
`-notrim`	Specify this parameter to stop trimming the files collected.
`-dryrun`	Creates a text file that contains a list of all the files that would have been collected and which scripts would be run for the specific diagcollect command without actually doing the collection.
`-silent`	Specify this parameter to run diagnostic collection as a background process
`-cores`	Specify this parameter to collect core files when it would normally have not been collected.
`-collectalldirs`	Specify this parameter to collect all files from a directory that has `Collect All` flag marked true.
`-collectdir` *`dir1,dir2,...dirn`*	Specify a comma-delimited list of directories and collection includes all files from these directories irrespective of type and time constraints in addition to the components specified.

Option	Description
`[-collectfiles` *`file1,..,fileN,dir1,..,dirN`* `[-onlycollectfiles]]`	Specify a comma-delimited list of files and directories and the collection will include the files and directories in addition to the components specified. If `-onlycollectfiles` is also used, then no other components will be collected.
`[-acrlevel` *`system,database,userdata`*`]`	Use this parameter to specify the ACR level(s) for redaction. ACR supports the following three levels: • `system`: For entity types such as hostname, IP, port, and user name. • `database`: For entity types such as `dbname`, `tbsname`, `svcname`, and `sqlstmt`. • `userdata`: For block dumps and redo log dumps.
`-sanitize`	**Note:** Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release. For more information, see Deprecated Oracle Trace File Analyzer Masking in Release 24.1 Sanitize sensitive values in the collection using Adaptive Classification and Redaction (ACR). This option will significantly increase the elapsed and actual processor time required to complete the collection.
`-mask`	**Note:** Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release. For more information, see Deprecated Oracle Trace File Analyzer Masking in Release 24.1 Mask sensitive values in the collection using Adaptive Classification and Redaction (ACR). This option will significantly increase the elapsed and actual processor time required to complete the collection.
`-examples`	Specify this parameter to view `diagcollect` usage examples.
`-singlearchive`	Specify this parameter to merge remote zip files into a single zip file on the initiating node.

Example 9-108 tfactl diagcollect -onlycollectfiles -collectfiles

```
tfactl diagcollect -onlycollectfiles -collectfiles
/tmp/tfa/tracedir,/tmp/tfa/tracedir/trace1.log,/tmp/tfa/tracedir2/
trace2_dir2.log
-node local -since 1h
Collecting data for local node(s).

TFA is using system timezone for collection, All times shown in UTC.

Collection Id : 20210721225241<hostname>

Detailed Logging at :
/opt/oracle.ahf/data/repository/
collection_Wed_Jul_21_22_52_46_UTC_2021_node_local/
diagcollect_20210721225241_<hostname>.log
2021/07/21 22:52:51 UTC : NOTE : Any file or directory name containing
the
string .com will be renamed to replace .com with dotcom
2021/07/21 22:52:51 UTC : Collection Name :
tfa_Wed_Jul_21_22_52_44_UTC_2021.zip
2021/07/21 22:52:51 UTC : Getting list of files satisfying time range
[07/21/2021 21:52:51 UTC, 07/21/2021 22:52:51 UTC]
2021/07/21 22:52:51 UTC : Collecting additional diagnostic
information...
2021/07/21 22:52:53 UTC : Collecting ADR incident files...
2021/07/21 22:53:15 UTC : Completed collection of additional diagnostic
information...
2021/07/21 22:53:18 UTC : Completed Local Collection
2021/07/21 22:53:18 UTC : Redacting the collection...
2021/07/21 22:55:06 UTC : Redacted masked Host name :owlo000037-vm1
2021/07/21 22:55:06 UTC : Successfully redacted the collection
.--------------------------------------------.
|             Collection Summary             |
+-----------------+-----------+-------+------+
| Host            | Status    | Size  | Time |
+-----------------+-----------+-------+------+
| <hostname> | Completed | 1.6MB |  27s |
'-----------------+-----------+-------+------'

Logs are being collected to:
/opt/oracle.ahf/data/repository/
collection_Wed_Jul_21_22_52_46_UTC_2021_node_local
/opt/oracle.ahf/data/repository/
collection_Wed_Jul_21_22_52_46_UTC_2021_node_local/owlo000037-
vm1.tfa_Wed_Jul_21_22_52_44_UTC_2021.zip
```

- Smart Problem Classification to Help Oracle Support Resolve Service Requests Faster
  AHF diagnostic collection now uses Smart Problem Classification to pinpoint the specific problem for which the diagnostic collection is being performed.

Related Topics

- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=1513912.2

9.3.3.3.1 Smart Problem Classification to Help Oracle Support Resolve Service Requests Faster

AHF diagnostic collection now uses Smart Problem Classification to pinpoint the specific problem for which the diagnostic collection is being performed.

You are often required to collect generic collections for all components over a wide range of times. The logs collected as part of diagnostic collections often reveal evidence of multiple types of problems. Consequently, automated log analysis is limited in its effectiveness because of the significant amount of time required to process and analyze log files.

By intelligently presenting you with a list of detected events relevant to the type of collection being performed, Smart Problem Classification allows you to identify the problem by selecting one from the list.

In addition to recording the type of problem, AHF also records the time and location. This information is made available to Oracle Support to help them resolve Service Requests faster. To ensure that the correct targeted collection is made, you can drill down by problem category if the problem you are looking for is not displayed.

Smart Problem Classification is enabled by default when you run `tfactl diagcollect`. You can, however, disable it when necessary.

> **Note:**
>
> Currently, Smart Problem Classification is not enabled on systems running AIX and Microsoft Windows operating systems.

How to use Smart Problem Classification

1. When you initiate a diagnostic collection, Oracle Trace File Analyzer queries events pertinent to the type of collection occurred during the specified time range. If you do not specify the time range, then by default Oracle Trace Files Analyzer queries events occurred duing the last four hours.
2. Oracle Trace Files Analyzer displays the list of events to pick.
   a. Select one event from the list. Oracle Trace Files Analyzer will initiate a collection to collect data for the selected event.
   b. If you opt to enter a new time range, then Oracle Trace Files Analyzer will prompt you to enter the new time range and will be redirect to step 2.
   c. If you opt to choose to display problem categories, then Oracle Trace Files Analyzer will display a list of categories. Selecting one of them will display sub-categories. After getting the information needed (directed to a problem), Oracle Trace File Analyzer will prompt you to enter the following details:
      i. Time range
      ii. Name of the database, if the problem maps to a database.

   Setting this will trigger an SRDC for the details provided.

At any point in time, you can exit from the classification process by selecting "X" from the menu.

> **Note:**
>
> The following collection options do not honor Smart Problem Classification:
>
> - **Collection switches:** [-ips, -syslens, -ahf, -awrhtml, -awrtext, -sosreport, -ashhtml, -ashtext]
> - **Collection modules:** [-srdc, -insight, -em, -emagenti, -emagent, -oms, -omsi]

Example 9-109   Smart Problem Classification - Examples

To check if Smart Problem Classification is enabled or disabled:

```
# tfactl get smartprobclassifier
.----------------------------------.
|              node1               |
+-------------------------+--------+
| Configuration Parameter | Value  |
+-------------------------+--------+
| smartprobclassifier     | ON     |
'-------------------------+--------'
```

To collect diagnostics when Smart Problem Classification is enabled:

```
# tfactl diagcollect -last 1h

AHF has detected following events from 2022-11-04 12:01:56.768 to
2022-11-04 13:01:56.768
All events are displayed in UTC time zone

Choose an event to perform a diagnostic collection:
1   . 2022-11-04 13:01:43.000 [RDBMS.orcl.orcl1] ORA-00600: internal
error code, arguments: [kjb], [ch11], [ch24], [], ...
2   . Show problem categories
3   . Enter a different event time
X   . Exit
Please choose the option [1-3]:2

Problem Categories:
1   . ACFS
2   . ASM Configuration
3   . ASM Errors/Other
4   . ASM Instance Crash
5   . CRS Client
6   . CRS Errors/Other
7   . Clusterware Installation
8   . Clusterware Patching
9   . Clusterware Startup
10  . Clusterware Upgrade
```

```
11 . Database Corruption
12 . Database Errors/Other
13 . Database Install
14 . Database Instance Eviction/Crash
15 . Database Internal Error
16 . Database Memory
17 . Database Patching
18 . Database Performance
19 . Database RMAN
20 . Database Storage (ASM)
21 . Database Streams/AQ
22 . Database Upgrade
23 . Dataguard
24 . GoldenGate
25 . Node Eviction/Reboot
26 . Problem not listed, provide problem description
X  . Exit
Please select the category of your problem [1-26]:
...
...
```

To bypass Smart Problem Classification:

```
# tfactl diagcollect -last 1h -noclassify
Collecting data for all nodes
TFA is using system timezone for collection, All times shown in UTC.
Collection Id: 20221104125517stbm000004-vm15
```

To bypass Smart Problem Classification, use the flags `-silent` and `-noclassify`.

```
# tfactl diagcollect -last 1h -silent
Smart Problem Classifier is ON. Since -silent is passed, Problem Classifier
is not processing the request.
```

To disable Smart Problem Classification:

```
# tfactl set smartprobclassifier=off
Successfully set smartprobclassifier=OFF
.----------------------------------.
|               node1              |
+--------------------------+-------+
| Configuration Parameter  | Value |
+--------------------------+-------+
| smartprobclassifier      | OFF   |
'--------------------------+-------'
```

To enable Smart Problem Classification:

```
# tfactl set smartprobclassifier=on
Successfully set smartprobclassifier=ON
.----------------------------------.
|               node1              |
+-------------------------+-------+
| Configuration Parameter | Value |
+-------------------------+-------+
| smartprobclassifier     | ON    |
'-------------------------+-------'
```

9.3.3.4 tfactl diagcollect -srdc

Use the `tfactl diagcollect -srdc` command to run a Service Request Data Collection (SRDC).

Syntax

```
tfactl diagcollect -srdc srdc_profile
[-tag tagname]
[-z filename]
[-last nh|d | -from time -to time | -for date]
-database database
```

Parameters

Each option must be prefixed with a minus sign (-).

Option	Description
`[-srdc srdc_profile]`	Specify the SRDC profile.
`-tag description`	Use this parameter to create a subdirectory for the resulting collection in the Oracle Trace File Analyzer repository.
`-z file_name`	Use this parameter to specify an output file name.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>[-last <i>nh</i>|<i>d</i> | -from <i>time</i> -to <i>time</i> | -for <i>date</i>]</td><td>
<ul>
<li>Specify the -last parameter to collect files that have relevant data for the past specific number of hours (<i>h</i>) or days (<i>d</i>). By default, using the command with this parameter also trims files that are large and shows files only from the specified interval.
You can also use -since, which has the same functionality as -last. This option is included for backward compatibility.</li>
<li>Specify the -from and -to parameters (you must use these two parameters together) to collect files that have relevant data during a specific time interval, and trim data before this time where files are large.
Supported time formats:
"Mon/dd/yyyy hh:mm:ss"
"yyyy-mm-dd hh:mm:ss"
"yyyy-mm-ddThh:mm:ss"
"yyyy-mm-dd"</li>
<li>Specify the -for parameter to collect files that have relevant data for the date specified. The files tfactl collects will have timestamps in between which the time you specify after -for is included. No data trimming is done for this option.
Supported time formats:
"Mon/dd/yyyy"
"yyyy-mm-dd"</li>
</ul>
<b>Note:</b>
If you specify both date and time, then you must enclose both the values in double quotation marks (""). If you specify only the date or the time, then you do not have to enclose the single value in quotation marks.
</td></tr>
<tr><td>-database <i>database</i></td><td>Specify the name of the database.</td></tr>
</table>

SRDC Profiles

SRDC Profile	Description
`listener_services`	Collects data for listener services errors: `TNS-12514` / `TNS-12516` / `TNS-12518` / `TNS-12519` / `TNS-12520` / `TNS-12528`.
`naming_services`	Collects data for naming services errors: `ORA-12514` / `ORA-12528`.
`ORA-00020`	Collects data regarding maximum number of processes exceeded.
`ORA-00060`, `ORA-00600`	Collects data for internal errors.
`ORA-00700`	Collects data for soft internal error.
`ORA-01031`	Collects standard information for `ORA-1031` / `ORA-1017` during SYSDBA connections

SRDC Profile	Description
ORA-01555	Collects data for Oracle Database Snapshot too old error.
ORA-01578	Collects data for NOLOGGING ORA-1578 / ORA-26040 DBV-00201.
ORA-01628	Collects data for Oracle Database Snapshot too old error.
ORA-04030	Collects data for OS process private memory was exhausted error.
ORA-04031	Collects data for More shared memory is needed in the shared/streams pool. error.
ORA-07445	Collects data for Exception encountered, core dump. error.
ORA-08102	Collects data for ORA error ORA-08102.
ORA-08103	Collects data for ORA error ORA-08103.
ORA-27300	Collects data for OS system dependent operation: open failed with status: (status). error.
ORA-27301	Collects data for OS failure message: (message). error.
ORA-27302	Collects data for Failure occurred at: (module). error.
ORA-30036	Collects data for Oracle Database Unable to extend Undo Tablespace error.
dbasm	Collects data for Oracle Database storage problems.
dbaudit	Collects standard information for Oracle Database auditing.
dbawrspace	Collects data for Oracle Database Automatic Workload Repository (AWR) space problems.
dbexp	Collects information for troubleshooting original Export (exp) related problems.
dbexpdp	Collects data for Data Pump Export generic issues.
dbexpdpapi	Collects data for Data Pump Export API Issues.
dbexpdpperf	Collects data for Data Pump Export performance issues.
dbexpdptts	Collects data to supply for Transportable Tablespace Data Pump and original EXPORT, IMPORT.
dbfs	Collects data for dbfs issues.
dbggclassicmode	Collects data for Oracle GoldenGate Classic Mode issues.
dbggintegratedmode	Collects data for Oracle GoldenGate Extract / Replicat abends problems.
dbimp	Collects data for troubleshooting original Import (imp) releated problems.
dbimpdp	Collects data for Data Pump Import generic issues.
dbimpdpperf	Collects data for Data Pump Import performance issues.
dbinstall	Collects data for Oracle Database install / upgrade problems.
dbpartition	Collects data for Create / maintain partitioned / subpartitioned table / index problems.
dbpartitionperf	Collects data for slow Create / Alter / Drop commands against partitioned table / index problems.
dbpatchconflict	Collects data for Oracle Database patch conflict problems.
dbpatchinstall	Collects data for Oracle Database patch install problems.
dbperf	Collects data for Oracle Database performance problems.

SRDC Profile	Description
`dbpreupgrade`	Collects data for Oracle Database preupgrade problems.
`dbrman`	Collects data for RMAN related issues, such as backup, maintenance, restore and recover, `RMAN-08137`, or `RMAN-08120`.
`dbrman600`	Collects data for `RMAN-00600` error (My Oracle Support note 2045195.1).
`dbrmanperf`	Collects data for RMAN Performance error (My Oracle Support note 1671509.1).
`dbscn`	Collects data for Oracle Database SCN problems.
`dbshutdown`	Collects data for single instance Oracle Database shutdown problems.
`dbsqlperf`	Collects data for an SQL performance problem using Oracle Trace File Analyzer Collector.
`dbstartup`	Collects data for single instance Oracle Database startup problems.
`dbtde`	Collects data for Transparent Data Encryption (TDE) (My Oracle Support note 1905607.1)
`dbunixresources`	Collects data for Oracle Database issues related to operating system resources.
`dbupgrade`	Collects data for Oracle Database upgrade problems.
`dbxdb`	Collects data Oracle Database XDB installation and invalid object problems.
`dnfs`	Collects data for DNFS problems.
`emagentperf`	Collects data for Enterprise Manager Agent performance issues.
`emcliadd`	Collects data for Enterprise Manager errors while adding an Oracle Database, a listener, or an ASM target using Enterprise Manager command-line.
`emclusdisc`	Collects data for cluster target, cluster (RAC) Oracle Database, or an ASM target is not discovered issue.
`emdbsys`	Collects data for Enterprise Manager Oracle Database system target is not discovered, detected, removed, or renamed correctly issue.
`emdebugoff`	Collects data for unsetting Enterprise Manager debug.
`emdebugon`	Collects data for setting Enterprise Manager debug.
`emgendisc`	Collects data for Enterprise Manager generic error while discovering, or removing an Oracle Database, a listener, or an ASM target.
`emmetricalert`	Collects data for Enterprise Manager metric events not raised and general metric alert related issues.
`emomscrash`	Collects for all Enterprise Manager OMS crash or restart performance issues.
`emomsheap`	Collects data for Enterprise Manager OMS heap usage alert performance issues.
`emomshungcpu`	Collects data for Enterprise Manager OMS hung or high CPU usage performance issues.
`emprocdisc`	Collects data for Enterprise Manager Oracle Database, listener, or an ASM target is not discovered or detected by the discovery process issues.
`emrestartoms`	Collects data for Enterprise Manager restart OMS crash problems.

SRDC Profile	Description
`emtbsmetric`	Collects data for Enterprise Manager Tablespace space used metric issues.
`esexalogic`	Collects data for Oracle Exalogic Full Exalogs problems.
`ggintegratedmodenodb`	Collects data for Oracle GoldenGate Extract/Replicat abends problems.
`internalerror`	Collects data for all other types of internal Oracle Database errors.

Related Topics

- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=2175568.1
- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=2045195.1
- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=1671509.1
- https://support.oracle.com/epmos/faces/DocumentDisplay?cmd=show&type=NOT&id=1905607.1

9.3.3.5 tfactl directory

Use the `tfactl directory` command to add a directory to, or remove a directory from the list of directories to analyze their trace or log files.

Also, use the `tfactl directory` command to change the directory permissions. When automatic discovery adds a directory, the directory is added as public. Any user who has sufficient permissions to run the `tfactl diagcollect` command collects any file in that directory. This is only important when non-root or `sudo` users run `tfactl` commands.

If a directory is marked as private, then Oracle Trace File Analyzer, before allowing any files to be collected:

- Determines which user is running `tfactl` commands
- Verifies if the user has permissions to see the files in the directory

> **Note:**
>
> A user can only add a directory to Oracle Trace File Analyzer to which they have read access. If you have automatic diagnostic collections configured, then Oracle Trace File Analyzer runs as `root`, and can collect all available files.

The `tfactl directory` command includes three verbs with which you can manage directories: `add`, `remove`, and `modify`.

Syntax

```
tfactl directory add directory [-public] [-exclusions | -noexclusions | -
collectall] [-node all | n1,n2...]
```

```
tfactl directory remove directory [-node all | n1,n2...]
```

```
tfactl directory modify directory [-private | -public] [-exclusions | -
noexclusions | -collectall]
```

```
tfactl directory list
```

For each of the three syntax models, you must specify a directory path where Oracle Trace File Analyzer stores collections.

Parameters

Table 9-98 tfactl directory Command Parameters

Parameter	Description
`-public`	Use the `-public` parameter to make the files contained in the directory available for collection by any Oracle Trace File Analyzer user.
`-private`	Use the `-private` parameter to prevent an Oracle Trace File Analyzer user who does not have permission to see the files in a directory (and any subdirectories) you are adding or modifying, from running a command to collect files from the specified directory.
`-exclusions`	Use the `-exclusions` parameter to specify that files in this directory are eligible for collection if the files satisfy type, name, and time range restrictions.
`-noexclusions`	Use the `-noexclusions` parameter to specify that files in this directory are eligible for collection if the files satisfy time range restrictions.
`-collectall`	Use the `-collectall` parameter to specify that files in this directory are eligible for collection irrespective of type and time range when the user specifies the `-collectalldirs` parameter with the `tfactl diagcollect` command.
`-node all | n1,n2...`	Add or remove directories from every node in the cluster or use a comma-delimited list to add or remove directories from specific nodes.

Usage Notes

You must add all trace directory names to the Berkeley DB (BDB) so that Oracle Trace File Analyzer can collect file metadata in that directory. The discovery process finds most directories, but if new or undiscovered directories are required, then you can add these manually using the `tfactl directory` command.

When you add a directory using tfactl, then Oracle Trace File Analyzer attempts to determine whether the directory is for

- Oracle Database

- Oracle Grid Infrastructure
- Operating system logs
- Some other component
- Which database or instance

If Oracle Trace File Analyzer cannot determine this information, then Oracle Trace File Analyzer returns an error and requests that you enter the information, similar to the following:

```
# tfactl directory add /tmp

Failed to add directory to TFA. Unable to determine parameters for
directory: /tmp
Please enter component for this Directory [RDBMS|CRS|ASM|INSTALL|OS|
CFGTOOLS|TNS|DBWLM|ACFS|ALL] : RDBMS
Please enter database name for this Directory :MYDB
Please enter instance name for this Directory :MYDB1
```

> **Note:**
>
> For OS, CRS, CFGTOOLS, ACFS, ALL, or INSTALL files, only the component is requested and for Oracle ASM only the instance is created. No verification is done for these entries so use caution when entering this data.

Example 9-110 tfactl directory

To add a directory:

```
# tfactl directory add /u01/app/grid/diag/asm/+ASM1/trace
```

To modify a directory and make the contents available for collection only to Oracle Trace File Analyzer users with sufficient permissions:

```
# tfactl directory modify /u01/app/grid/diag/asm/+ASM1/trace -private
```

To remove a directory from all nodes in the cluster:

```
# tfactl directory remove /u01/app/grid/diag/asm/+ASM1/trace -node all
```

To list all Oracle Trace File Analyzer directories:

```
tfactl directory list
```

9.3.3.6 tfactl ips

Use the `tfactl ips` command to collect Automatic Diagnostic Repository diagnostic data.

Syntax

```
tfactl ips
[ADD]
[ADD FILE]
[ADD NEW INCIDENTS]
[CHECK REMOTE KEYS]
[COPY IN FILE]
[COPY OUT FILE]
[CREATE PACKAGE]
[DELETE PACKAGE]
[FINALIZE PACKAGE]
[GENERATE PACKAGE]
[GET MANIFEST]
[GET METADATA]
[GET REMOTE KEYS]
[PACK]
[REMOVE]
[REMOVE FILE]
[SET CONFIGURATION]
[SHOW CONFIGURATION]
[SHOW FILES]
[SHOW INCIDENTS]
[SHOW PROBLEMS]
[SHOW PACKAGE]
[UNPACK FILE]
[UNPACK PACKAGE]
[USE REMOTE KEYS]
[options]
```

For detailed help on each topic use:

```
help ips topic
```

Parameters

Table 9-99 tfactl ips Command Parameters

Parameter	Description
`ADD`	Adds incidents to an existing package.
`ADD FILE`	Adds a file to an existing package.
`ADD NEW INCIDENTS`	Finds new incidents for the problems and add the latest ones to the package.
`CHECK REMOTE KEYS`	Creates a file with keys matching incidents in specified package.
`COPY IN FILE`	Copies an external file into Automatic Diagnostic Repository, and associates it with a package and (optionally) an incident.
`COPY OUT FILE`	Copies an Automatic Diagnostic Repository file to a location outside Automatic Diagnostic Repository.
`CREATE PACKAGE`	Creates a package, and optionally select contents for the package.

Table 9-99 (Cont.) tfactl ips Command Parameters

Parameter	Description
`DELETE PACKAGE`	Drops a package and its contents from Automatic Diagnostic Repository.
`FINALIZE PACKAGE`	Gets a package ready for shipping by automatically including correlated contents.
`GENERATE PACKAGE`	Creates a physical package (`zip` file) in target directory.
`GET MANIFEST`	Extracts the manifest from a package file and displays it.
`GET METADATA`	Extracts the metadata XML document from a package file and displays it.
`GET REMOTE KEYS`	Creates a file with keys matching incidents in specified package.
`PACK`	Creates a package, and immediately generates the physical package.
`REMOVE`	Removes incidents from an existing package.
`REMOVE FILE`	Removes a file from an existing package.
`SET CONFIGURATION`	Changes the value of an Incident Packaging Service configuration parameter.
`SHOW CONFIGURATION`	Shows the current Incident Packaging Service settings.
`SHOW FILES`	Shows the files included in the specified package.
`SHOW INCIDENTS`	Shows incidents included in the specified package.
`SHOW PROBLEMS`	Shows problems for the current Automatic Diagnostic Repository home.
`SHOW PACKAGE`	Shows details for the specified package.
`UNPACK FILE`	Unpackages a physical file into the specified path.
`UNPACK PACKAGE`	Unpackages physical files in the current directory into the specified path, if they match the package name.
`USE REMOTE KEYS`	Adds incidents matching the keys in the specified file to the specified package.

- tfactl ips ADD
  Use the `tfactl ips ADD` command to add incidents to an existing package.
- tfactl ips ADD FILE
  Use the `tfactl ADD FILE` command to add a file to an existing package.
- tfactl ips ADD NEW INCIDENTS
  Use the `tfactl ips ADD NEW INCIDENTS` command to find new incidents for the problems in a specific package, and add the latest ones to the package.
- tfactl ips CHECK REMOTE KEYS
  Use the `tfactl ips CHECK REMOTE KEYS` command to create a file with keys matching incidents in a specified package.
- tfactl ips COPY IN FILE
  Use the `tfactl ips COPY IN FILE` command to copy an external file into Automatic Diagnostic Repository, and associate the file with a package and (optionally) an incident.
- tfactl ips COPY OUT FILE
  Use the `tfactl ips COPY OUT FILE` command to copy an Automatic Diagnostic Repository file to a location outside Automatic Diagnostic Repository.

- tfactl ips CREATE PACKAGE
  Use the `tfactl ips CREATE PACKAGE` command to create a package, and optionally select the contents for the package.
- tfactl ips DELETE PACKAGE
  Use the `tfactl ips DELETE PACKAGE` command to drop a package and its contents from the Automatic Diagnostic Repository.
- tfactl ips FINALIZE PACKAGE
  Use the `tfactl ips FINALIZE PACKAGE` command to get a package ready for shipping by automatically including correlated contents.
- tfactl ips GENERATE PACKAGE
  Use the `tfactl ips GENERATE PACKAGE` command to create a physical package (`zip` file) in the target directory.
- tfactl ips GET MANIFEST
  Use the `tfactl ips GET MANIFEST` command to extract the manifest from a package file and view it.
- tfactl ips GET METADATA
  Use the `tfactl ips GET METADATA` command to extract the metadata XML document from a package file and view it.
- tfactl ips GET REMOTE KEYS
  Use the `tfactl ips GET REMOTE KEYS` command to create a file with keys matching incidents in a specific package.
- tfactl ips PACK
  Use the `tfactl ips PACK` command to create a package and immediately generate the physical package.
- tfactl ips REMOVE
  Use the `tfactl ips REMOVE` command to remove incidents from an existing package.
- tfactl ips REMOVE FILE
  Use the `tfactl ips REMOVE FILE` command to remove a file from an existing package.
- tfactl ips SET CONFIGURATION
  Use the `tfactl ips SET CONFIGURATION` command to change the value of an Incident Packaging Service configuration parameter.
- tfactl ips SHOW CONFIGURATION
  Use the `tfactl ips SHOW CONFIGURATION` command to view the current Incident Packaging Service settings.
- tfactl ips SHOW FILES
  Use the `tfactl ips SHOW FILES` command to view the files included in a specific package.
- tfactl ips SHOW INCIDENTS
  Use the `tfactl ips SHOW INCIDENTS` command to view the incidents included in a specific package.
- tfactl ips SHOW PROBLEMS
  Use the `tfactl ips SHOW PROBLEMS` command to view the problems for the current Automatic Diagnostic Repository home.
- tfactl ips SHOW PACKAGE
  Use the `tfactl ips SHOW PACKAGE` command to view the details of a specific package.

- tfactl ips UNPACK FILE
  Use the `tfactl ips UNPACK FILE` command to unpack a physical file into a specific path.
- tfactl ips UNPACK PACKAGE
  Use the `tfactl ips UNPACK PACKAGE` command to unpack physical files in the current directory into a specific path, if they match the package name.
- tfactl ips USE REMOTE KEYS
  Use the `tfactl ips USE REMOTE KEYS` command to add incidents matching the keys in a specific file to a specific package.

9.3.3.6.1 tfactl ips ADD

Use the `tfactl ips ADD` command to add incidents to an existing package.

Syntax

```
tfactl ips ADD [INCIDENT incid | PROBLEM prob_id | PROBLEMKEY prob_key
| SECONDS seconds | TIME start_time TO end_time] PACKAGE package_id
```

Parameters

Table 9-100 tfactl ips ADD Command Parameters

Parameter	Description
incid	Specify the ID of the incident to add to the package contents.
prob_id	Specify the ID of the problem to add to the package contents.
prob_key	Specify the problem key to add to the package contents.
seconds	Specify the number of seconds before now for adding package contents.
start_time	Specify the start of time range to look for incidents in.
end_time	Specify the end of time range to look for incidents in.

Example 9-111 tfactl ips ADD

```
$ tfactl ips add incident 22 package 12
```

9.3.3.6.2 tfactl ips ADD FILE

Use the `tfactl ADD FILE` command to add a file to an existing package.

Syntax

The file must be in the same `ADR_BASE` as the package.

```
tfactl ips ADD FILE file_spec PACKAGE pkgid
```

Parameters

Table 9-101   tfactl ips ADD FILE Command Parameters

Parameter	Description
file_spec	Specify the file with file and path (full or relative).
package_id	Specify the ID of the package to add the file to.

Example 9-112   tfactl ips ADD FILE

```
$ tfactl ips add file ADR_HOME/trace/mydb1_ora_13579.trc package 12
```

9.3.3.6.3 tfactl ips ADD NEW INCIDENTS

Use the `tfactl ips ADD NEW INCIDENTS` command to find new incidents for the problems in a specific package, and add the latest ones to the package.

Syntax

```
tfactl ips ADD NEW INCIDENTS package_id
```

Parameters

Table 9-102   tfactl ips ADD NEW INCIDENTS Command Parameters

Parameter	Description
package_id	Specify the ID of the package to add the incidents to.

9.3.3.6.4 tfactl ips CHECK REMOTE KEYS

Use the `tfactl ips CHECK REMOTE KEYS` command to create a file with keys matching incidents in a specified package.

Syntax

```
tfactl ips CHECK REMOTE KEYS file_spec PACKAGE package_id
```

Parameters

Table 9-103   tfactl ips CHECK REMOTE KEYS Command Parameters

Parameter	Description
file_spec	Specify the file with file name and full path.
package_id	Specify the ID of the package to get the keys for.

9.3.3.6.5 tfactl ips COPY IN FILE

Use the `tfactl ips COPY IN FILE` command to copy an external file into Automatic Diagnostic Repository, and associate the file with a package and (optionally) an incident.

Syntax

```
tfactl ips COPY IN FILE file [TO new_name] [OVERWRITE] PACKAGE pkgid
[INCIDENT incid]
```

Parameters

Table 9-104 tfactl ips COPY IN FILE Command Parameters

Parameter	Description
file	Specify the file with file name and full path (full or relative).
new_name	Specify a name for the copy of the file.
pkgid	Specify the ID of the package to associate the file with.
incid	Specify the ID of the incident to associate the file with.

Options

`OVERWRITE`: If the file exists, then use the `OVERWRITE` option to overwrite the file.

Example 9-113 tfactl ips COPY IN FILE

```
$ tfactl ips copy in file /tmp/key_file.txt to new_file.txt package 12
incident 62
```

9.3.3.6.6 tfactl ips COPY OUT FILE

Use the `tfactl ips COPY OUT FILE` command to copy an Automatic Diagnostic Repository file to a location outside Automatic Diagnostic Repository.

Syntax

```
tfactl IPS COPY OUT FILE source TO target [OVERWRITE]
```

Parameters

Table 9-105 tfactl ips COPY OUT FILE Command Parameters

Parameter	Description
source	Specify the file with file name and full path (full or relative). This file must be inside ADR.
target	Specify the file with file name and full path (full or relative). This file must be outside ADR.

Options

OVERWRITE: If the file exists, then use the OVERWRITE option to overwrite the file.

Example 9-114 tfactl ips COPY OUT FILE

```
$ tfactl ips copy out file ADR_HOME/trace/ora_26201 to /tmp/trace_26201.txt
```

9.3.3.6.7 tfactl ips CREATE PACKAGE

Use the `tfactl ips CREATE PACKAGE` command to create a package, and optionally select the contents for the package.

Syntax

```
tfactl ips CREATE PACKAGE [INCIDENT inc_id | PROBLEM prob_id
| PROBLEMKEY prob_key | SECONDS seconds | TIME start_time TO end_time]
[CORRELATE BASIC | TYPICAL | ALL] [MANIFEST file_spec]
[KEYFILE file_spec]
```

Parameters

Table 9-106 tfactl ips CREATE PACKAGE Command Parameters

Parameter	Description
incid	Specify the ID of the incident to use for selecting the package contents.
prob_id	Specify the ID of the problem to use for selecting the package contents.
prob_key	Specify the problem key to use for selecting the package contents.
seconds	Specify the number of seconds before now for selecting the package contents.
start_time	Specify the start of time range to look for the incidents in.
end_time	Specify the end of time range to look for the incidents in.

Options

- CORRELATE BASIC: The package includes the incident dumps and the incident process trace files. If the incidents share relevant correlation keys, then more incidents are included automatically.
- CORRELATE TYPICAL: The package includes the incident dumps and all trace files that were modified in a time window around each incident. If the incidents share relevant correlation keys, or occurred in a time window around the main incidents, then more incidents are included automatically.
- CORRELATE ALL: The package includes the incident dumps and all trace files that were modified between the first selected incident and the last selected incident. If the incidents occurred in the same time range, then more incidents are included automatically.
- MANIFEST file_spec: Generates the XML format package manifest file.
- KEYFILE file_spec: Generates the remote key file.

Note:

- If you do not specify package contents, such as incident, problem, and so on, then Oracle Trace File Analyzer creates an empty package.

  You can add files and incidents later.
- If you do not specify the correlation level, then Oracle Trace File Analyzer uses the default level.
- The default is normally **TYPICAL**, but you can change using the `IPS SET CONFIGURATION` command.

Example 9-115 tfactl ips CREATE PACKAGE

```
$ tfactl ips create package incident 861
```

```
$ tfactl ips create package time '2006-12-31 23:59:59.00 -07:00' to
'2007-01-01 01:01:01.00 -07:00'
```

9.3.3.6.8 tfactl ips DELETE PACKAGE

Use the `tfactl ips DELETE PACKAGE` command to drop a package and its contents from the Automatic Diagnostic Repository.

Syntax

```
tfactl ips DELETE PACKAGE package_id
```

Parameters

Table 9-107 tfactl ips DELETE PACKAGE Command Parameters

Parameter	Description
package_id	Specify the ID of the package to delete.

Example 9-116 tfactl ips DELETE PACKAGE

```
$ tfactl ips delete package 12
```

9.3.3.6.9 tfactl ips FINALIZE PACKAGE

Use the `tfactl ips FINALIZE PACKAGE` command to get a package ready for shipping by automatically including correlated contents.

Syntax

```
tfactl ips FINALIZE PACKAGE package_id
```

Example 9-117   tfactl ips FINALIZE PACKAGE

```
$ tfactl ips finalize package 12
```

9.3.3.6.10 tfactl ips GENERATE PACKAGE

Use the `tfactl ips GENERATE PACKAGE` command to create a physical package (`zip` file) in the target directory.

Syntax

```
tfactl ips GENERATE PACKAGE package_id [IN path][COMPLETE | INCREMENTAL]
```

Parameters

Table 9-108   tfactl ips GENERATE PACKAGE Command Parameters

Parameter	Description
package_id	Specify the ID of the package to create physical package file for.
path	Specify the path where the physical package file must be generated.

Options

- `COMPLETE`: (Default) The package includes all package files even if a previous package sequence was generated.
- `INCREMENTAL`: The package includes only the files that have been added or changed since the last package was generated.

> **Note:**
>
> If no target path is specified, then Oracle Trace File Analyzer generates the physical package file in the current working directory.

Example 9-118   tfactl ips GENERATE PACKAGE

```
$ tfactl ips generate package 12 in /tmp
```

9.3.3.6.11 tfactl ips GET MANIFEST

Use the `tfactl ips GET MANIFEST` command to extract the manifest from a package file and view it.

Syntax

```
tfactl ips GET MANIFEST FROM FILE file
```

Parameters

Table 9-109   tfactl ips GET MANIFEST FROM FILE Command Parameters

Parameter	Description
file	Specify the external file with file name and full path.

Example 9-119   tfactl ips GET MANIFEST

```
$ tfactl ips get manifest from file /tmp/IPSPKG_200704130121_COM_1.zip
```

9.3.3.6.12 tfactl ips GET METADATA

Use the `tfactl ips GET METADATA` command to extract the metadata XML document from a package file and view it.

Syntax

```
tfactl ips GET METADATA [FROM FILE file | FROM ADR]
```

Parameters

Table 9-110   tfactl ips GET METADATA Command Parameters

Parameter	Description
file	Specify the external file with file name and full path.

Example 9-120   tfactl ips GET METADATA

```
$ tfactl ips get metadata from file /tmp/IPSPKG_200704130121_COM_1.zip
```

9.3.3.6.13 tfactl ips GET REMOTE KEYS

Use the `tfactl ips GET REMOTE KEYS` command to create a file with keys matching incidents in a specific package.

Syntax

```
tfactl ips GET REMOTE KEYS FILE file_spec PACKAGE package_id
```

Parameters

Table 9-111   tfactl ips GET REMOTE KEYS FILE Command Parameters

Parameter	Description
file_spec	Specify the file with file name and full path (full or relative).
package_id	Specify the ID of the package to get keys for.

Example 9-121 tfactl ips GET REMOTE KEYS

```
$ tfactl ips get remote keys file /tmp/key_file.txt package 12
```

9.3.3.6.14 tfactl ips PACK

Use the `tfactl ips PACK` command to create a package and immediately generate the physical package.

Syntax

```
tfactl ips PACK [INCIDENT incid | PROBLEM prob_id | PROBLEMKEY prob_key |
SECONDS seconds | TIME start_time TO end_time]
[CORRELATE BASIC | TYPICAL | ALL] [MANIFEST file_spec] [KEYFILE file_spec]
```

Parameters

Table 9-112 tfactl ips PACK Command Parameters

Parameter	Description
incid	Specify the ID of the incident to use for selecting the package contents.
prob_id	Specify the ID of the problem to use for selecting the package contents.
prob_key	Specify the problem key to use for selecting the package contents.
seconds	Specify the number of seconds before the current time for selecting the package contents.
start_time	Specify the start of time range to look for the incidents in.
end_time	Specify the end of time range to look for the incidents in.
path	Specify the path where the physical package file must be generated.

Options

- **`CORRELATE BASIC`**: The package includes the incident dumps and the incident process trace files. If the incidents share relevant correlation keys, then more incidents are included automatically.
- `CORRELATE TYPICAL`: The package includes the incident dumps and all trace files that were modified in a time window around each incident. If the incidents share relevant correlation keys, or occurred in a time window around the main incidents, then more incidents are included automatically.
- `CORRELATE ALL`: The package includes the incident dumps and all trace files that were modified between the first selected incident and the last selected incident. If the incidents occurred in the same time range, then more incidents are included automatically.
- `MANIFEST file_spec`: Generate the XML format package manifest file.
- `KEYFILE file_spec`: Generate remote key file.

> **Note:**
>
> If you do not specify package contents, such as incident, problem, and so on, then Oracle Trace File Analyzer creates an empty package.
>
> You can add files and incidents later.
>
> If you do not specify the correlation level, then Oracle Trace File Analyzer uses the default level.
>
> The default is normally **TYPICAL**, but you can change using the `IPS SET CONFIGURATION` command.

Example 9-122 tfactl ips PACK

```
$ tfactl ips pack incident 861

$ tfactl ips pack time '2006-12-31 23:59:59.00 -07:00' to '2007-01-01
01:01:01.00 -07:00'
```

9.3.3.6.15 tfactl ips REMOVE

Use the `tfactl ips REMOVE` command to remove incidents from an existing package.

Syntax

The incidents remain associated with the package, but not included in the physical package file.

```
tfactl ips REMOVE [INCIDENT incid | PROBLEM prob_id | PROBLEMKEY
prob_key] PACKAGE package_id
```

Parameters

Table 9-113 tfactl ips REMOVE Command Parameters

Parameter	Description
incid	Specify the ID of the incident to add to the package contents.
prob_id	Specify the ID of the problem to add to the package contents.
prob_key	Specify the problem key to add to the package contents.

Example 9-123 tfactl ips REMOVE

```
$ tfactl ips remove incident 22 package 12
```

9.3.3.6.16 tfactl ips REMOVE FILE

Use the `tfactl ips REMOVE FILE` command to remove a file from an existing package.

Syntax

The file must be in the same `ADR_BASE` as the package. The file remains associated with the package, but not included in the physical package file.

```
tfactl ips REMOVE FILE file_spec PACKAGE pkgid
```

Parameters

Table 9-114 tfactl ips REMOVE FILE Command Parameters

Parameter	Description
file_spec	Specify the file with file name and full path (full or relative).
package_id	Specify the ID of the package to remove the file from.

Example 9-124 tfactl ips REMOVE FILE

```
$ tfactl ips remove file ADR_HOME/trace/mydb1_ora_13579.trc package 12
```

9.3.3.6.17 tfactl ips SET CONFIGURATION

Use the `tfactl ips SET CONFIGURATION` command to change the value of an Incident Packaging Service configuration parameter.

Syntax

```
tfactl ips SET CONFIGURATION parameter_id value
```

Parameters

Table 9-115 tfactl ips SET CONFIGURATION Command Parameters

Parameter	Description
parameter_id	Specify the ID of the parameter to change.
value	Specify the new value for the parameter.

Example 9-125 tfactl ips SET CONFIGURATION

```
$ tfactl ips set configuration 6 2
```

9.3.3.6.18 tfactl ips SHOW CONFIGURATION

Use the `tfactl ips SHOW CONFIGURATION` command to view the current Incident Packaging Service settings.

Syntax

```
tfactl ips SHOW CONFIGURATION parameter_id
```

Example 9-126 tfactl ips SHOW CONFIGURATION

```
$ tfactl ips show configuration

Multiple ORACLE HOMES were found, please select one ...

option[0] /scratch/app/oradb/product/11.2.0/dbhome_11204
option[1] /scratch/app/11.2.0.4/grid

Pls select an ORACLE_HOME to be used for the ADRCI binary [0] ?0
/scratch/app/oradb/product/11.2.0/dbhome_11204 was selected


Multiple ADR basepaths were found, please select one ...

( ) option[0] /scratch/app/oradb
( ) option[1] /scratch/app/oragrid

Pls select an ADR basepath [0..1] ?0
/scratch/app/oradb was selected


Multiple ADR homepaths were found for /scratch/app/oradb, please
select one ...

( ) option[0] diag/rdbms/racone/racone_2
( ) option[1] diag/rdbms/rdb11204/rdb112041
( ) option[2] diag/rdbms/ogg11204/ogg112041
( ) option[3] diag/rdbms/apxcmupg/apxcmupg_1
( ) option[4] diag/rdbms/apxcmupg/apxcmupg_2
    option[5] Done

Pls select a homepath [5] ?0
diag/rdbms/racone/racone_2 was selected

PARAMETER INFORMATION:
   PARAMETER_ID           1
   NAME                   CUTOFF_TIME
   DESCRIPTION            Maximum age for an incident to be considered
for inclusion
   UNIT                   Days
   VALUE                  90
   DEFAULT_VALUE          90
   MINIMUM                1
   MAXIMUM                4294967295
   FLAGS                  0

PARAMETER INFORMATION:
   PARAMETER_ID           2
   NAME                   NUM_EARLY_INCIDENTS
   DESCRIPTION            How many incidents to get in the early part
of the range
   UNIT                   Number
   VALUE                  3
   DEFAULT_VALUE          3
   MINIMUM                 1
   MAXIMUM                 4294967295
   FLAGS                   0

PARAMETER INFORMATION:
   PARAMETER_ID            3
   NAME                    NUM_LATE_INCIDENTS
   DESCRIPTION             How many incidents to get in the late part of the
range
   UNIT                    Number
   VALUE                   3
   DEFAULT_VALUE           3
   MINIMUM                 1
   MAXIMUM                 4294967295
   FLAGS                   0

PARAMETER INFORMATION:
   PARAMETER_ID            4
   NAME                    INCIDENT_TIME_WINDOW
   DESCRIPTION             Incidents this close to each other are considered
correlated
   UNIT                    Minutes
   VALUE                   5
   DEFAULT_VALUE           5
   MINIMUM                 1
   MAXIMUM                 4294967295
   FLAGS                   0

PARAMETER INFORMATION:
   PARAMETER_ID            5
   NAME                    PACKAGE_TIME_WINDOW
   DESCRIPTION             Time window for content inclusion is from x hours
before first included incident to x hours after last incident
   UNIT                    Hours
   VALUE                   24
   DEFAULT_VALUE           24
   MINIMUM                 1
   MAXIMUM                 4294967295
   FLAGS                   0

PARAMETER INFORMATION:
   PARAMETER_ID            6
   NAME                    DEFAULT_CORRELATION_LEVEL
   DESCRIPTION             Default correlation level for packages
   UNIT                    Number
   VALUE                   2
   DEFAULT_VALUE           2
   MINIMUM                 1
   MAXIMUM                 4
   FLAGS                   0
```

9.3.3.6.19 tfactl ips SHOW FILES

Use the `tfactl ips SHOW FILES` command to view the files included in a specific package.

Syntax

```
tfactl ips SHOW FILES PACKAGE package_id
```

Example 9-127 tfactl ips SHOW FILES

```
$ tfactl ips show files package 12
```

9.3.3.6.20 tfactl ips SHOW INCIDENTS

Use the `tfactl ips SHOW INCIDENTS` command to view the incidents included in a specific package.

Syntax

```
tfactl ips SHOW INCIDENTS PACKAGE package_id
```

Example 9-128 tfactl ips SHOW INCIDENTS

```
$ tfactl ips show incidents package 12
```

9.3.3.6.21 tfactl ips SHOW PROBLEMS

Use the `tfactl ips SHOW PROBLEMS` command to view the problems for the current Automatic Diagnostic Repository home.

Syntax

```
tfactl ips SHOW PROBLEMS
```

Example 9-129 tfactl ips SHOW PROBLEMS

```
tfactl ips show problems

Multiple ADR basepaths were found, please select one ...

( ) option[0] /scratch/app/oradb
( ) option[1] /scratch/app/oragrid

Pls select an ADR basepath [0..1] ?0
/scratch/app/oradb was selected


ADR Home = /scratch/app/oradb/diag/rdbms/racone/racone_2:
***********************************************************************
**
0 rows fetched

ADR Home = /scratch/app/oradb/diag/rdbms/rdb11204/rdb112041:
***********************************************************************
```

```
**
PROBLEM_ID
PROBLEM_KEY
LAST_INCIDENT        LASTINC_TIME
--------------------
-----------------------------------------------------------
-------------------- ----------------------------------------
2                    ORA 700
[kgerev1]                                           42605
2016-07-05 07:53:28.578000 -07:00
1                    ORA
600                                                     42606
2016-07-05 07:53:30.427000 -07:00

ADR Home = /scratch/app/oradb/diag/rdbms/ogg11204/ogg112041:
*************************************************************************
PROBLEM_ID
PROBLEM_KEY
LAST_INCIDENT        LASTINC_TIME
--------------------
-----------------------------------------------------------
-------------------- ----------------------------------------
3                    ORA
4030                                                    51504
2017-09-26 10:03:03.922000 -07:00
2                    ORA 700
[kgerev1]                                           54401
2017-09-26 10:03:10.371000 -07:00
1                    ORA
600                                                     54402
2017-09-26 10:03:11.446000 -07:00
6                    ORA 600
[gc_test_error]                                     54691
2017-10-23 03:03:40.599000 -07:00
5                    ORA
4031                                                    64277
2017-12-13 04:48:16.035000 -08:00
4                    ORA
7445                                                    96286
2018-05-29 08:26:11.326000 -07:00

ADR Home = /scratch/app/oradb/diag/rdbms/apxcmupg/apxcmupg_1:
*************************************************************************
0 rows fetched

ADR Home = /scratch/app/oradb/diag/rdbms/apxcmupg/apxcmupg_2:
*************************************************************************
0 rows fetched
```

9.3.3.6.22 tfactl ips SHOW PACKAGE

Use the `tfactl ips SHOW PACKAGE` command to view the details of a specific package.

Syntax

```
tfactl ips SHOW PACKAGE package_id [BASIC | BRIEF | DETAIL]
```

> **Note:**
>
> It is possible to specify the level of detail to use with this command.

`BASIC` : Shows a minimal amount of information. It is the default when no package ID is specified.

`BRIEF` : Shows a more extensive amount of information. It is the default when a package ID is specified.

`DETAIL` : Shows the same information as `BRIEF`, and also some package history and information on included incidents and files.

Example 9-130 tfactl ips SHOW PACKAGE

```
$ tfactl ips show package

Multiple ADR basepaths were found, please select one ...

( ) option[0] /scratch/app/oradb
( ) option[1] /scratch/app/oragrid

Pls select an ADR basepath [0..1] ?0
/scratch/app/oradb was selected


Multiple ADR homepaths were found for /scratch/app/oradb, please
select one ...

( ) option[0] diag/rdbms/racone/racone_2
( ) option[1] diag/rdbms/rdb11204/rdb112041
( ) option[2] diag/rdbms/ogg11204/ogg112041
( ) option[3] diag/rdbms/apxcmupg/apxcmupg_1
( ) option[4] diag/rdbms/apxcmupg/apxcmupg_2
    option[5] Done

Pls select a homepath [5] ?1
diag/rdbms/rdb11204/rdb112041 was selected

   PACKAGE_ID             1
   PACKAGE_NAME           IPSPKG_20160731165615
   PACKAGE_DESCRIPTION
   DRIVING_PROBLEM        N/A
   DRIVING_PROBLEM_KEY    N/A
   DRIVING_INCIDENT       N/A
   DRIVING_INCIDENT_TIME  N/A
   STATUS                 Generated (4)
   CORRELATION_LEVEL      Typical (2)
   PROBLEMS               0 main problems, 0 correlated problems
   INCIDENTS              0 main incidents, 0 correlated incidents
   INCLUDED_FILES         27

   PACKAGE_ID             2
   PACKAGE_NAME           IPSPKG_20160731170111
   PACKAGE_DESCRIPTION
   DRIVING_PROBLEM        N/A
   DRIVING_PROBLEM_KEY    N/A
   DRIVING_INCIDENT       N/A
   DRIVING_INCIDENT_TIME  N/A
   STATUS                 Generated (4)
   CORRELATION_LEVEL      Typical (2)
   PROBLEMS               0 main problems, 0 correlated problems
   INCIDENTS              0 main incidents, 0 correlated incidents
   INCLUDED_FILES         27

   PACKAGE_ID             3
   PACKAGE_NAME           ORA700kge_20160731211334
   PACKAGE_DESCRIPTION
   DRIVING_PROBLEM        2
   DRIVING_PROBLEM_KEY    ORA 700 [kgerev1]
   DRIVING_INCIDENT       42605
   DRIVING_INCIDENT_TIME  N/A
   STATUS                 Generated (4)
   CORRELATION_LEVEL      Typical (2)
   PROBLEMS               2 main problems, 0 correlated problems
   INCIDENTS              2 main incidents, 0 correlated incidents
   INCLUDED_FILES         84

   PACKAGE_ID             4
   PACKAGE_NAME           IPSPKG_20160801203518
   PACKAGE_DESCRIPTION
   DRIVING_PROBLEM        N/A
   DRIVING_PROBLEM_KEY    N/A
   DRIVING_INCIDENT       N/A
   DRIVING_INCIDENT_TIME  N/A
   STATUS                 Generated (4)
   CORRELATION_LEVEL      Typical (2)
   PROBLEMS               0 main problems, 0 correlated problems
   INCIDENTS              0 main incidents, 0 correlated incidents
   INCLUDED_FILES         27
```

```
$ tfactl ips show package 4 detail

Multiple ADR basepaths were found, please select one ...

( ) option[0] /scratch/app/oradb
( ) option[1] /scratch/app/oragrid

Pls select an ADR basepath [0..1] ?0
/scratch/app/oradb was selected
```

```
Multiple ADR homepaths were found for /scratch/app/oradb, please
select one ...

( ) option[0] diag/rdbms/racone/racone_2
( ) option[1] diag/rdbms/rdb11204/rdb112041
( ) option[2] diag/rdbms/ogg11204/ogg112041
( ) option[3] diag/rdbms/apxcmupg/apxcmupg_1
( ) option[4] diag/rdbms/apxcmupg/apxcmupg_2
    option[5] Done

Pls select a homepath [5] ?1
diag/rdbms/rdb11204/rdb112041 was selected

DETAILS FOR PACKAGE 4:
   PACKAGE_ID             4
   PACKAGE_NAME           IPSPKG_20160801203518
   PACKAGE_DESCRIPTION
   DRIVING_PROBLEM        N/A
   DRIVING_PROBLEM_KEY    N/A
   DRIVING_INCIDENT       N/A
   DRIVING_INCIDENT_TIME  N/A
   STATUS                 Generated (4)
   CORRELATION_LEVEL      Typical (2)
   PROBLEMS               0 main problems, 0 correlated problems
   INCIDENTS              0 main incidents, 0 correlated incidents
   INCLUDED_FILES         27
   SEQUENCES              Last 1, last full 1, last base 0
   UNPACKED               FALSE
   CREATE_TIME            2016-08-01 20:35:18.684231 -07:00
   UPDATE_TIME            N/A
   BEGIN_TIME             2016-08-01 13:59:04.000000 -07:00
   END_TIME               2016-08-01 20:34:50.000000 -07:00
   FLAGS                  0

HISTORY FOR PACKAGE 4:
   SEQUENCE               1
   BASE_SEQUENCE          1
   MODE                   Complete (0)
   STATUS                 Generated (4)
   FILENAME               /scratch/app/oragrid/tfa/repository/suptools/
srdc/user_oradb/IPSPKG_20160801203518_COM_1.zip
   ARCHIVE_TIME           2016-08-01 20:35:21.899095 -07:00
   UPLOAD_TIME            N/A
   UNPACK_TIME            N/A
   FORCE                  FALSE
   GENERATE_FLAGS         0
   UNPACK_FLAGS           0

MAIN INCIDENTS FOR PACKAGE 4:
CORRELATED INCIDENTS FOR PACKAGE 4:

FILES FOR PACKAGE 4:
   FILE_ID                1
   FILE_LOCATION          <ADR_HOME>/trace
```

```
FILE_NAME              alert_rdb112041.log
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2087
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_CONFIGURATION.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2088
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_PACKAGE.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2089
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_PACKAGE_INCIDENT.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2090
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_PACKAGE_FILE.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2091
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_PACKAGE_HISTORY.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2092
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_FILE_METADATA.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2093
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              IPS_FILE_COPY_LOG.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2094
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              DDE_USER_ACTION_DEF.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2095
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              DDE_USER_ACTION_PARAMETER_DEF.dmp
```

```
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2096
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              DDE_USER_ACTION.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2097
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              DDE_USER_ACTION_PARAMETER.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2098
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              DDE_USER_INCIDENT_TYPE.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2099
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              DDE_USER_INCIDENT_ACTION_MAP.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2100
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              INCIDENT.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2101
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              INCCKEY.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2102
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              INCIDENT_FILE.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2103
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              PROBLEM.dmp
LAST_SEQUENCE          1
EXCLUDE                Included

FILE_ID                2104
FILE_LOCATION          <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME              HM_RUN.dmp
LAST_SEQUENCE          1
```

```
EXCLUDE                 Included

FILE_ID                 2105
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1/export
FILE_NAME               EM_USER_ACTIVITY.dmp
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2106
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1
FILE_NAME               config.xml
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2107
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1/opatch
FILE_NAME               opatch.log
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2108
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1/opatch
FILE_NAME               opatch.xml
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2109
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1
FILE_NAME               metadata.xml
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2110
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1
FILE_NAME               manifest_4_1.xml
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2111
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1
FILE_NAME               manifest_4_1.html
LAST_SEQUENCE           1
EXCLUDE                 Included

FILE_ID                 2112
FILE_LOCATION           <ADR_HOME>/incpkg/pkg_4/seq_1
FILE_NAME               manifest_4_1.txt
LAST_SEQUENCE           1
EXCLUDE                 Included
```

9.3.3.6.23 tfactl ips UNPACK FILE

Use the `tfactl ips UNPACK FILE` command to unpack a physical file into a specific path.

Syntax

Running the following command automatically creates a valid ADR_HOME structure. The path must exist and be writable.

```
tfactl ips UNPACK FILE file_spec [INTO path]
```

Parameters

Table 9-116 tfactl ips UNPACK FILE Command Parameters

Parameter	Description
file_spec	Specify the file with file name and full path.
path	Specify the path where the physical package file should be unpacked.

Example 9-131 tfactl ips UNPACK FILE

```
$ tfactl ips unpack file /tmp/IPSPKG_20061026010203_COM_1.zip
into /tmp/newadr
```

9.3.3.6.24 tfactl ips UNPACK PACKAGE

Use the tfactl ips UNPACK PACKAGE command to unpack physical files in the current directory into a specific path, if they match the package name.

Syntax

Running the following command automatically creates a valid ADR_HOME structure. The path must exist and be writable.

```
tfactl ips UNPACK PACKAGE pkg_name [INTO path]
```

Parameters

Table 9-117 tfactl ips UNPACK PACKAGE Command Parameters

Parameter	Description
pkg_name	Specify the name of the package.
path	Specify the path where the physical package files should be unpacked.

Example 9-132 tfactl ips UNPACK PACKAGE

```
$ tfactl ips unpack package IPSPKG_20061026010203 into /tmp/newadr
```

9.3.3.6.25 tfactl ips USE REMOTE KEYS

Use the `tfactl ips USE REMOTE KEYS` command to add incidents matching the keys in a specific file to a specific package.

Syntax

```
tfactl ips USE REMOTE KEYS FILE file_spec PACKAGE package_id
```

Parameters

Table 9-118 tfactl ips USE REMOTE KEYS Command Parameters

Parameter	Description
`file_spec`	Specify the file with file name and full path.
`package_id`	Specify the ID of the package to add the incidents to.

Example 9-133 tfactl ips USE REMOTE KEYS

```
$ tfactl ips use remote keys file /tmp/key_file.txt package 12
```

9.3.3.7 tfactl managelogs

Use the `tfactl managelogs` command to manage Automatic Diagnostic Repository log and trace files.

Syntax

```
tfactl managelogs
[-purge [[-older nm|h|d] | [-gi] | [-database all|d1,d2,...]]]
[-show [usage|variation] [[-older nd] | [-gi] | [-database all|d1,d2,...]]]
```

Parameters

Table 9-119 tfactl managelogs Purge Options

Purge Option	Description
`-older`	Time period for purging logs.
`-gi`	Purges Oracle Grid Infrastructure logs (all Automatic Diagnostic Repository homes under `GIBASE/diag` and `crsdata (cvu dirs)`).
`-database`	Purges Oracle database logs (Default is all, else provide a list).
`-dryrun`	Estimates logs cleared by `purge` command.

Table 9-120   tfactl managelogs Show Options

Show Option	Description
`-older`	Time period for change in log volume.
`-gi`	Space utilization under `GIBASE`.
`-database`	Space utilization for Oracle database logs (Default is all, else provide a list).

9.3.3.8 tfactl purge

Use the `tfactl purge` command to delete collections and log files from AHF components from the local node.

Syntax

```
tfactl purge [tfa|compliance|collections <-tfa>|oswatcher|managelogs|
supporttools] -older n[h|d] [-dryrun]
```

Parameters

Table 9-121   tfactl purge Command Parameters

Parameter	Description
`tfa`	Purges collections and log files of the TFA component.
`compliance`	Purges collections and log files of the compliance component.
`collections`	Purges collections of the passed component.
`-tfa`	Purge collections for the TFA component. Only supported with collections.
`oswatcher`	Purges files from the `oswatcher` tool directory.
`managelogs`	Purges files from the `managelogs` tool directory.
`supporttools`	Purges files from all the support tools directory except from `oswatcher` and `managelogs`.
`-older` *n*[*h*|*d*]	Purges files older than *n* hours or days.
`-dryrun`	Lists files that would be purged without purging the files.

Example 9-134   tfactl purge

```
# tfactl purge tfa -older 1h
/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Nov_23_13_31_27_CST_2023_node_all
/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Nov_23_14_33_05_CST_2023_node_all
```

```
/u01/app/giusr/oracle.ahf/data/repository/suptools/srdc/user_root/
GJxkypiOn.sh
/u01/app/giusr/oracle.ahf/data/test-node/diag/acr/user_root/diag/acr/test-
node/acrctl/trace/acrctl_131098.trc

Successfully deleted above files.


# tfactl purge oswatcher -older 12h -dryrun

List of files older than 12h considered for purge :
/u01/app/giusr/oracle.ahf/data/repository/suptools/test-node/oswbb/root/
run_oswbb1310.log
/u01/app/giusr/oracle.ahf/data/repository/suptools/test-node/oswbb/root/
archive/oswbuddy/oswbb_buddy131098.gz


# tfactl purge -older 1h
/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Nov_23_13_31_27_CST_2023_node_all
/u01/app/giusr/oracle.ahf/data/repository/
collection_Thu_Nov_23_14_33_05_CST_2023_node_all
/u01/app/giusr/oracle.ahf/data/repository/suptools/srdc/user_root/
GJxkypiOn.sh
/u01/app/giusr/oracle.ahf/data/test-node/diag/acr/user_root/diag/acr/test-
node/acrctl/trace/acrctl_131098.trc
/u01/app/giusr/oracle.ahf/data/test-node/orachk/user_root/
output/.input_131098
/u01/app/giusr/oracle.ahf/data/test-node/orachk/user_root/output/
orachk_131098
/u01/app/giusr/oracle.ahf/data/test-node/orachk/user_root/output/
orachk_131098.zip
/u01/app/giusr/oracle.ahf/data/test-node/orachk/user_root/output/
orachk_debug131098.log

Successfully deleted above files.
```

9.4 Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options

Review the list of commands that you can use to run compliance checks on Oracle Engineered and non-engineered systems.

- Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options
  Review the list of Compliance Framework (Oracle Orachk and Oracle Exachk) command-line options.
- Running Generic Compliance Framework (Oracle Orachk and Oracle Exachk) Commands
  Review the list of generic Oracle Orachk and Oracle Exachk command options.
- Controlling the Scope of Checks
  Use the list of commands to control the scope of checks.

- Managing the Report Output
  Use the list of commands to manage compliance checks report output.
- Uploading Results to Database
  Use the list of commands to upload results to the database.
- Controlling the Behavior of the Daemon
  Use the list of commands to control the behavior of the daemon.
- Tracking File Attribute Differences
  Use the list of commands to track file attribute differences.
- Running Oracle Health Check Collections Manager Commands
  Use the `-cmupgrade` command to upgrade Oracle Health Check Collections Manager.
- Command-Line Options to Generate Password Protected Collection zip Files
  Use the list of commands to encrypt or decrypt diagnostic collection `zip` files.
- Caching Discovery Data
  Use the list of commands to manage caching of discovery data.
- Running Cluster Verification Utility (CVU) Compliance Checks
  Run Cluster Verification Utility (CVU) to perform system checks in preparation for installation, patch updates, or other system changes.
- Running Auto Start
  Use the list of commands to start or stop auto start.
- ZFS Storage Appliance Options
  Use the `-zfssa` command to run compliance checks on Oracle ZFS Storage Appliances.

9.4.1 Compliance Framework (Oracle Orachk and Oracle Exachk) Command-Line Options

Review the list of Compliance Framework (Oracle Orachk and Oracle Exachk) command-line options.

Syntax

```
$ orachk [options]


[-h] [-a] [-b] [-v] [-p] [-m] [-u] [-f] [-o]
[-clusternodes clusternames]
[-failedchecks previous_result]
[-nordbms]
[-output path]
[-dbnames dbnames]
[-localonly]
[-debug]
[-dbnone | -dball]
[-c]
[-upgrade | -noupgrade]
[-syslog]
[-skip_usr_def_checks]
[-checkfaileduploads]
```

```
[-uploadfailed all | comma-delimited list of collections]
[-fileattr [start | check | remove ] [-includedir path ] [-excludediscovery]
[-baseline path [-fileattronly]
[-testemail all | "NOTIFICATION_EMAIL=comma-delimited list of email 
addresses"]
[-setdbupload all | db upload variable, for example, 
RAT_UPLOAD_CONNECT_STRING, RAT_UPLOAD_PASSWORD]
[-unsetdbupload all | db upload variable, for example, 
RAT_UPLOAD_CONNECT_STRING, RAT_UPLOAD_PASSWORD]
[-checkdbupload]
[-getdbupload]
[-cmupgrade]
[-sendemail "NOTIFICATION_EMAIL=comma-delimited list of email addresses"]
[-nopass]
[-noscore]
[-showpass]
[-show_critical]
[-diff Old Report New Report [-outfile Output HTML] [-force]]
[-merge report 1 report 2 [-force]]
[-tag tagname]
[-nodaemon]
[-profile asm | clusterware | corroborate | dba | ebs | emagent | emoms | em 
| goldengate | hardware | maa | oam | oim | oud | ovn | peoplesoft | 
preinstall | prepatch | security | siebel | solaris_cluster | storage | 
switch | sysadmin | timesten | user_defined_checks |  zfs ]
[-excludeprofile asm | clusterware | corroborate | dba | ebs | emagent | 
emoms | em | goldengate | hardware | maa | oam | oim | oud | ovn | peoplesoft 
| preinstall | prepatch | security | siebel | solaris_cluster | storage | 
switch | sysadmin | timesten | user_defined_checks | zfs ]
[-includeprofile asm | clusterware | corroborate | dba | ebs | emagent | 
emoms | em | goldengate | hardware | maa | oam | oim | oud | ovn | peoplesoft 
| preinstall | prepatch | security | siebel | solaris_cluster | storage | 
switch | sysadmin | timesten | user_defined_checks | zfs ]
[-acchk -javahome path to jdk8 
-asmhome path to asm-all-5.0.3.jar -appjar directory where jar files are 
present for concrete class -apptrc directory where trace files are present 
for coverage class]
[-check check ids | -excludecheck check ids]
[-zfsnodes nodes]
[-zfssa appliance names]
[-dbserial | -dbparallel [n] | -dbparallelmax]
[-idmpreinstall | -idmpostinstall | -idmruntime] [-topology topology.xml | 
-credconfig credconfig] | -idmdbpreinstall | -idmdbpostinstall | -
idmdbruntime]
[-idm_config IDMCONFIG] [-idmdiscargs IDMDISCARGS]
[-idmhcargs IDMHCARGS | -h]
```

Syntax

```
$ exachk [options]


[-h] [-a] [-b] [-v] [-p] [-m] [-u] [-f] [-o]
[-clusternodes clusternames]
```

```
[-failedchecks previous_result]
[-nordbms]
[-output path]
[-dbnames dbnames]
[-localonly]
[-debug]
[-dbnone | -dball]
[-c]
[-upgrade | -noupgrade]
[-syslog] [-skip_usr_def_checks]
[-checkfaileduploads]
[-uploadfailed all | comma-delimited list of collections]
[-fileattr start | check | remove [-includedir path [-
excludediscovery] [-baseline path[-fileattronly]
[-testemail all | "NOTIFICATION_EMAIL=comma-delimited list of email
addresses"]
[-setdbupload all | db upload variable, for example,
RAT_UPLOAD_CONNECT_STRING, RAT_UPLOAD_PASSWORD]
[-unsetdbupload all | db upload variable, for example,
RAT_UPLOAD_CONNECT_STRING, RAT_UPLOAD_PASSWORD]
[-checkdbupload]
[-getdbupload]
[-cmupgrade] [-sendemail "NOTIFICATION_EMAIL=comma-delimited list of
email addresses"]
[-nopass]
[-noscore]
[-showpass]
[-show_critical]
[-diff Old Report New Report [-outfile Output HTML] [-force]]
[-merge report 1 report 2 [-force]]
[-tag tagname]
[-auto_restart -initsetup | -initdebugsetup | -initrmsetup | -
initcheck | -h]
[-d start|start -debug|stop|status|info|stop_client|nextautorun|-h]
[-nodaemon]
[-unlockcells all | -cells comma-delimited list of names or IPs of
cells] [-lockcells all | -cells comma-delimited list of names or IPs
of cells]
[-usecompute]
[-exadiff Exalogic collection1 Exalogic collection2]
[-vmguest]
[-hybrid [-phy nodes]]
[-profile asm | bi_middleware | clusterware | compute_node | exatier1 |
control_VM | corroborate | dba | ebs | el_extensive | el_lite |
el_rackcompare | emagent | emoms | em | goldengate | hardware | maa |
nimbula | obiee | ovn | peoplesoft | platinum | preinstall | prepatch |
security | siebel | solaris_cluster | storage | switch | sysadmin |
timesten | user_defined_checks | virtual_infra]
[-excludeprofile asm | bi_middleware | clusterware | compute_node |
exatier1 | control_VM | corroborate | dba | ebs | el_extensive |
el_lite | el_rackcompare | emagent | emoms | em | goldengate | hardware
| maa | nimbula | obiee | ovn | peoplesoft | platinum | preinstall |
prepatch | security | siebel | solaris_cluster | storage | switch |
sysadmin | timesten | user_defined_checks | virtual_infra]
[-includeprofile asm | clusterware | corroborate | dba | ebs | emagent
| emoms | em | goldengate | hardware | maa | oam | oim | oud | ovn |
peoplesoft | preinstall | prepatch | security | siebel | solaris_cluster |
storage | switch | sysadmin | timesten | user_defined_checks | zfs ]
[-check check ids | -excludecheck check ids]
[-cells cells]
[-ibswitches switches]
[-torswitches]
[-extzfsnodes nodes]
[-dbserial | -dbparallel [n] | -dbparallelmax | -allserial]
[-allserial | -dbnodeserial |-cellserial | -switchserial]
```

9.4.2 Running Generic Compliance Framework (Oracle Orachk and Oracle Exachk) Commands

Review the list of generic Oracle Orachk and Oracle Exachk command options.

Syntax

```
[-a]
[-v]
[-debug]
[-nodaemon]
[-f]
[-upgrade]
[-noupgrade]
[-testemail all | "NOTIFICATION_EMAIL=comma-delimited list of email
addresses"]
[-sendemail "NOTIFICATION_EMAIL=comma-delimited list of email addresses"]
[-dbserial]
[-dbparallel [n]]
[-dbparallelmax]
[-readenvconfig]
```

Parameters

Table 9-122 Generic Commands

Option	Description
`-a`	Runs all checks, including the best practice checks and the recommended patch check. If you do not specify any options, then the tools run all checks by default.
`-v`	Shows the version of Oracle Autonomous Health Framework compliance tools.
`-debug`	Runs in debug mode. The generated `.zip` file contains a debug log and other files useful for Oracle Support.
`-nodaemon`	Does not send commands to the daemon, usage is interactive.
`-f`	Runs Offline. The tools perform health checks on the data already collected from the system.
`-upgrade`	Forces an upgrade of the version of the tools being run.

Table 9-122 (Cont.) Generic Commands

Option	Description
`-noupgrade`	`-noupgrade` is for when you have the latest version in `RAT_UPGRADE_LOC` and do not yet want to upgrade. Adding `-noupgrade` without having the latest version in `RAT_UPGRADE_LOC` will still prompt you to download the latest version.
`-testemail all | "NOTIFICATION_EMAIL=`*`comma-delimited list of email addresses`*`"`	Sends a test email to validate email configuration.
`-sendemail “NOTIFICATION_EMAIL=`*`comma-delimited list of email addresses`*`"`	Specify a comma-delimited list of email addresses. Emails the generated HTML report on completion to the specified email addresses.
`-dbserial`	Runs the `SQL`, `SQL_COLLECT`, and `OS` health checks in serial.
`-dbparallel [`*`n`*`]`	Runs the `SQL`, `SQL_COLLECT`, and `OS` health checks in parallel, using *n* number of child processes. Default is 25% of CPUs.
`-dbparallelmax`	Runs the `SQL`, `SQL_COLLECT`, and `OS` health checks in parallel, using the maximum number of child processes.

`-readenvconfig`	Read the configuration file `conf_file` under `DATA_DIR/`*`SERVER_NAME`*`/common/config/user_`*`username`*.
	You cannot set the environment variables `RAT_SSH`, `RAT_SSHELL`, and `RAT_SCOPY` using the export option. You will have to create the configuration file and add them manually.
	To read configuration file, run:
	`./exachk -readenvconfig`
	`./orachk -readenvconfig`

9.4.3 Controlling the Scope of Checks

Use the list of commands to control the scope of checks.

Syntax

```
[-b]
[-p]
[-m]
[-u -o pre]
[-u -o post]
[-clusternodes nodes]
[-failedchecks previous_result]
[-nordbms]
[-dbnames db_names]
```

```
[-dbnone]
[-dball]
[-localonly]
[-cells cells]
[-ibswitches switches]
[-profile profile]
[-excludeprofile asm | clusterware | corroborate | dba | ebs | emagent |
emoms | em | goldengate | hardware | maa | oam | oim | oud | ovn | peoplesoft
| preinstall | prepatch | security | siebel | solaris_cluster | storage |
switch | sysadmin | timesten | user_defined_checks | zfs ]
[-includeprofile asm | clusterware | corroborate | dba | ebs | emagent |
emoms | em | goldengate | hardware | maa | oam | oim | oud | ovn | peoplesoft
| preinstall | prepatch | security | siebel | solaris_cluster | storage |
switch | sysadmin | timesten | user_defined_checks | zfs ]
[-check check_id]
[-excludecheck check_id]
[-skip_usr_def_checks]
```

Parameters

Table 9-123 Scope of Checks

Command	Description
`-b`	Runs only the best practice checks. Does not run the recommended patch checks.
`-p`	Runs only the patch checks.
`-m`	Excludes the checks for Maximum Availability Architecture (MAA) scorecards.
`-u -o pre`	Runs the pre-upgrade checks for Oracle Clusterware and Oracle Database.
`-u -o post`	Runs the post-upgrade checks for Oracle Clusterware and Oracle Database.
`-clusternodes` *`nodes`*	Specify a comma-delimited list of node names to run only on a subset of nodes.
`-failedchecks` *`previous_result`*	Runs only checks from the *presious_result*, which had failed.
`-nordbms`	Runs Oracle Grid Infrastructure checks only in environments with no Oracle Database checks performed.
`-dbnames` *`db_names`*	Specify a comma-delimited list of database names to run only on a subset of databases.
`-dbnone`	Does not prompt for database selection and skips all the database checks.
`-dball`	Does not prompt for database selection and runs the database checks on all databases discovered on the system.
`-localonly`	Runs only on the local node.
`-cells` *`cells`*	Specify a comma-delimited list of storage server names to run the checks only on a subset of storage servers.
`-ibswitches` *`switches`*	Specify a comma-delimited list of InfiniBand switch names to run the checks only on a subset of InfiniBand switches.

Table 9-123 (Cont.) Scope of Checks

Command	Description
`-profile` *`profile`*	Specify a comma-delimited list of profiles to run only the checks in the specified profiles.
`-excludeprofile` *`profile`*	Specify a comma-delimited list of profiles to exclude the checks in the specified profiles.
`-includeprofile` *`profile`*	Specify a comma-delimited list of profiles to include the checks in the specified profiles.
`-check` *`check_id`*	Specify a comma-delimited list of check IDs to run only the checks specified in the list check IDs.
`-excludecheck` *`check_id`*	Specify a comma-delimited list of check IDs to exclude the checks specified in the list of check IDs.
`-skip_usr_def_checks`	Does not run the checks specified in the user-defined `xml` file.

Related Topics

- Oracle Clusterware and Oracle Database Pre-Upgrade Checks
  During your pre-upgrade planning phase, run Oracle Autonomous Health Framework in pre-upgrade mode as the Oracle Database owner or as `root`.
- Oracle Clusterware and Oracle Database Post-Upgrade Checks
  After performing the upgrade, you can run in post-upgrade mode as the Oracle Database software owner or `root` to see further recommendations.
- Running Database Checks
  During Oracle Autonomous Health Framework system checks, all Oracle Database logins are performed by using local connections.
- Running Switch Checks
  Limit the scope of compliance checks to a subset of switches by using the `-ibswitches` *`switch`* option.
- Running Cell Checks
  Limit the scope of compliance checks to a subset of storage servers by using the `-cell` *`cell`* option.
- Using Profiles with Oracle Autonomous Health Framework
  Profiles are logical groupings of related checks. These related checks are grouped by a particular role, a task, or a technology.
- Excluding Individual Checks
  Excluding checks is recommended in situations where you have reviewed all check output and determined a particular check is not relevant for some particular business reason.
- Running Individual Checks
  There are times when you may want to run only specific checks.

9.4.4 Managing the Report Output

Use the list of commands to manage compliance checks report output.

Syntax

```
[-syslog] [-tag tagname]
[-o]
[-nopass]
[-noscore]
[-diff old_report new_report [-outfile output_HTML]]
[-merge [-force] collections]
```

Parameters

Table 9-124 Managing Output

Option	Description
`-syslog`	Writes JSON results to Syslog.
`-tag` *`tagname`*	Appends the *`tagname`* specified to the output report name. The *`tagname`* must contain only alphanumeric characters.
`-o`	Argument to an option. If `-o` is followed by `v`, (or `verbose`, and neither option is case-sensitive), then the command prints passed checks on the screen. If the `-o` option is not specified, then the command prints only the failed checks on the screen.
`-nopass`	Does not show passed checks in the generated output.
`-noscore`	Does not print health score in the HTML report.
`-diff` *`old_report new_report`* `[-outfile` *`output_HTML`*`]`	Reports the difference between the two HTML reports. Specify a directory name or a ZIP file or an HTML report file as *`old_report`* and *`new_report`*.
`-merge [-force]` *`collections`*	Merges a comma-delimited list of collections and prepares a single report.

Related Topics

- Tagging Reports
  The compliance check HTML report is typically named: `orachk_`*`hostname_database_date_timestamp`*`.html` or `exachk_`*`hostname_database_date_timestamp`*`.html`.
- Comparing Two Reports
  Oracle Autonomous Health Framework automatically compare the two most recent HTML reports and generate a third diff report, when run in automated daemon mode.
- Merging Reports
  Merging reports is useful in role-separated environments where different users are run different subsets of checks and then you want to view everything as a whole.
- Integrating Compliance Check Results with Third-Party Tool
  Integrate Oracle Orachk and Oracle Exachk compliance check results into various third-party log monitoring and analytics tools, such as Elasticsearch and Kibana.

9.4.5 Uploading Results to Database

Use the list of commands to upload results to the database.

Syntax

```
[-setdbupload all|list of variable names]
[-unsetdbupload all|list of variable names]
[-checkdbupload]
[-getdbupload]
[-checkfaileduploads]
[-uploadfailed all|list of failed collections]
```

Parameters

Table 9-125 Uploading Results to Database

Option	Description
`-setdbupload all|` *`variable_names`*	Sets the values in the wallet to upload compliance check run results to the database. `all`: Sets all the variables in the wallet. *variable_names*: Specify a comma-delimited list of variables to set.
`-unsetdbupload all|` *`variable_names`*	Unsets the values in the wallet to upload compliance check run results to the database. `all`: Unsets all the variables in the wallet. *variable_names*: Specify a comma-delimited list of variables to unset.
`-checkdbupload`	Checks if the variables are set correctly for uploading the compliance check run results to the database.
`-getdbupload`	Prints the variables with their values from wallet for uploading the compliance check run result to the database.
`-checkfaileduploads`	Reports any failed collection uploads.
`-uploadfailed all|` *`list of failed collections`*	Reattempts to upload one or more failed collection uploads. `all`: Reattempts to upload all the filed collection uploads. *list of failed collections*: Specify a comma-delimited list of collections to upload.

Related Topics

- Integrating Compliance Check Results with Custom Application
  Oracle Orachk and Oracle Exachk upload collection results from multiple instances into a single database for easier consumption of check results across your enterprise.

9.4.6 Controlling the Behavior of the Daemon

Use the list of commands to control the behavior of the daemon.

Syntax

```
[-autostart] [-autostart reset] [-autostop] [-autostop unset] [-autostatus]
[-autorestart] [-id id] -set daemon_option
[-id id] -unset daemon_option | all
[-id id] -get parameter | all
```

Parameters

Table 9-126 Daemon Options

Option	Description
`-autostart`	Starts the daemon.
`-autostart reset`	Starts and loads the default schedulers.
`-autostop`	Stops the daemon.
`-autostop unset`	Removes all default unmodified schedulers.
`-autostatus`	Checks the current status of the daemon.
`-autorestart`	Restarts the daemon.
`[-id` *`id`*`] -set` *`daemon_option`*	Optionally use `id` with the `set` command to set specific daemon usage profiles.
`[-id` *`id`*`] -unset` *`daemon_option`* `| all`	Unsets the parameter. Use with `-id` *`id`* to set a daemon profile-specific value.
`[-id` *`id`*`] -get` *`parameter`* `| all`	Displays the value of the specified parameter or all the parameters. Use with `-id` *`id`* to set a daemon profile-specific value.

Related Topics

- Running Compliance Checks Automatically
  Oracle recommends that you use the daemon process to schedule recurring compliance checks at regular intervals.
- Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands in 22.2
  Starting with the AHF 22.2 (2022-09-14), commands to run the Oracle Orachk or Oracle Exachk scheduler without the Oracle Trace File Analyzer daemon are deprecated. These commands are completely removed in AHF 23.8 (2023-08-28).
- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

9.4.7 Tracking File Attribute Differences

Use the list of commands to track file attribute differences.

Parameters

Table 9-127 File Attribute Differences

Option	Description
`-fileattr start`	Takes file attributes snapshot of discovered directories and stores the snapshot in the output directory. By default, the tool takes snapshot of Oracle Grid Infrastructure home and all the installed database homes. If the user doesn't own a particular directory, then the tool does not take snapshot of the directory.
`-fileattr check`	Takes a recent snapshot of discovered directories and compares with the previous snapshot
`-fileattr remove`	Removes the file attribute snapshots and related files.

`-fileattr [start|check] -includedir` *`directories`*	Includes the directories specified at the command-line to check file attributes.
	For example:
	`orachk -fileattr start -includedir "/root/home,/etc"`
	`orachk -fileattr check -includedir "/root/home,/etc"`

`-fileattr [start|check] -excludediscovery`	Excludes the discovered directories. `orachk -fileattr start -includedir "/root/home,/etc" -excludediscovery`
`-fileattr check -baseline` *`baseline snapshot path`*	For example: `orachk -fileattr check -baseline "/tmp/Snapshot"`
`-fileattr -check -fileattronly`	Performs file attributes check and exits Oracle Orachk. `orachk -fileattr check -fileattronly`

9.4.8 Running Oracle Health Check Collections Manager Commands

Use the `-cmupgrade` command to upgrade Oracle Health Check Collections Manager.

Table 9-128   Oracle Health Check Collections Manager Commands

Command	Description

`orachk -cmupgrade`
or
`exachk -cmupgrade`
	Upgrades Oracle Health Check Collections Manager from Oracle Orachk or Oracle Exachk.
	Oracle Health Check Collections Manager upgrades to the latest version of whichever application your database supports.
	You get the new theme interface only if you have APEX 5.

9.4.9 Command-Line Options to Generate Password Protected Collection zip Files

Use the list of commands to encrypt or decrypt diagnostic collection `zip` files.

Table 9-129   Encrypt and Decrypt Diagnostic Collection zip Files

Option	Description

`orachk -d start -encryptzip`
`exachk -d start -encryptzip`
	Starts the daemon with `-encryptzip` option.
	The daemon prompts for a password when it starts. The daemon then encrypts the subsequent on-demand and scheduled runs collections with that password.
	Note:
	When `-encryptzip` is passed, Oracle Orachk and Oracle Exachk after successfully encrypting the diagnostic collection `zip` file deletes the collections directory.

Table 9-129 (Cont.) Encrypt and Decrypt Diagnostic Collection zip Files

Option	Description
orachk [-option *value*] -encryptzip exachk [-option *value*] -encryptzip	Encrypts the run result. Prompts for the password, and encrypts the collections created at the end of the run with that password. You can use -encryptzip with other Oracle Orachk and Oracle Exachk options that generate a collection. For example: orachk -profile *profile-name* -encryptzip orachk -profile sysadmin -encryptzip orachk -check *check-id* -encryptzip orachk -check D47661C55B1A291AE0431EC0E50A5C53 -encryptzip **Note:** When -encryptzip is passed, Oracle Orachk and Oracle Exachk after successfully encrypting the diagnostic collection zip file deletes the collections directory.
orachk -encryptzip *zip_file* exachk -encryptzip *zip_file*	Encrypts the already generated collection. Prompts for the password, encrypts the zip file specified with that password, and then renames the collections as, for example, orachk_*host*_*db*_encrypted_*date*_*time*.zip. **Note:** When -encryptzip is passed, Oracle Orachk and Oracle Exachk after successfully encrypting the diagnostic collection zip file deletes the collections directory.
orachk -decryptzip *zip_file* exachk -decryptzip *zip_file*	Decrypts the encrypted collection. Prompts for the password, decrypts the zip file specified with that password, and then renames the collections as, for example, orachk_*host*_*db*_*date*_*time*.zip.

9.4.10 Caching Discovery Data

Use the list of commands to manage caching of discovery data.

Syntax

```
orachk -discovery -discoverydir location
exachk -discovery -discoverydir location


orachk -checkdiscovery
exachk -checkdiscovery


orachk -usediscovery -discoverydir location
exachk -usediscovery -discoverydir location


orachk -rediscovery
exachk -rediscovery


orachk -rmdiscovery
exachk -rmdiscovery
```

Table 9-130 Manage Caching of Discovery Data

Command	Description
`-discovery`	Caches discovery data, which Oracle Orachk and Oracle Exachk can use for future runs. `-discoverydir`: Specify the location to store the discovery data.
`-checkdiscovery`	Verifies the discovery data.
`-usediscovery`	Uses the discovery data. `-discoverydir`: Specify the location where you have cached the discovery data.
`-rediscovery`	Refreshes the cache discovery data.
`-rmdiscovery`	Removes the cached discovery data.

9.4.11 Running Cluster Verification Utility (CVU) Compliance Checks

Run Cluster Verification Utility (CVU) to perform system checks in preparation for installation, patch updates, or other system changes.

Note:

You can run CVU check as `root` or a non-root user. Currently, running CVU checks are limited to Linux and Solaris.

CVU is integrated into Oracle Orachk and Oracle Exachk. By default,

- CVU health checks are run when you run Oracle Orachk on Oracle RAC, Oracle Restart, and Oracle Database Appliance (ODA).
- A full Oracle Exachk run includes CVU health checks.

Oracle Orachk and Oracle Exachk include the Cluster Verification Utility (CVU) compliance check results in the following reports:

- Oracle RAC Assessment Report
- Oracle RAC Upgrade Readiness Report
- Oracle Exadata Assessment Report

When you run the `-profile preinstall` command, preinstallation related CVU checks are run for Oracle Database and Oracle Clusterware.

When you run Oracle Orachk and Oracle EXAchk in pre-upgrade mode, pre-upgrade related CVU checks are run for Oracle Database and Oracle Clusterware.

When you run Oracle Orachk and Oracle Exachk in normal or pre-upgrade mode, CVU will only be used if the tools find CVU is available, recent and valid for the situation you are using it in.

These are the checks performed to validate CVU:

- CVU exists in `ahf_dir/common/cvu` directory or the path specified using the `-cvuhome` option.
- The CVU pack is less than 180 days. Note that you can modify this value by setting the `RAT_STALE_DAYS=`*n* environment variable.
- If the CVU version is equal or higher than the CRS version.
- If the CVU version is equal or higher than the upgrade target version.

If you are running as `root` and one of the above validations fail, then the tools will prompt to download the latest CVU from My Oracle Support. If My Oracle Support credentials are already configured in the wallet, then these will be used. If not, then the tools will prompt for My Oracle Support username and password.

After downloading a new CVU pack the tools automatically distribute this to all nodes in the cluster. By default this cluster distribution is done through the TFA secure socket connection. Distribution through the TFA secure socket connection is only possible if:

- The tools were installed through a full installation and not using the `-extract` option, or installed as non-root.
- The Oracle Trace File Analyzer daemon has not been shutdown.

CVU pack cluster distribution can be done through passwordless SSH if the originating Oracle Orachk or Oracle Exachk command was run with the `-usessh` option for example:

```
orachk -usessh
orachk -preupgrade -usessh


exachk -usessh
exachk -preupgrade -usessh
```

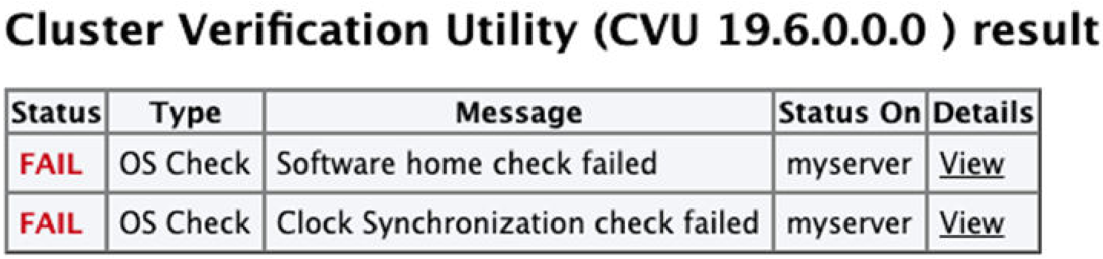
You can prevent the prompting for CVU upgrade using any one of the following options:

- Set the `RAT_NOCVU_UPGRADE` environment variable to 1, for example, `RAT_NOCVU_UPGRADE=1`.
- Set the `RAT_NOUPGRADE` environment variable to 1, for example, `RAT_NOUPGRADE=1`.
- Run Oracle Orachk and Oracle Exachk with the `-noupgrade` option.
  For example:

```
orachk -noupgrade
orachk -preupgrade -noupgrade


exachk -noupgrade
exachk -preupgrade -noupgrade
```

Oracle Orachk and Oracle Exachk report includes the CVU version and the CVU checks result.

Figure 9-1   CVU Result

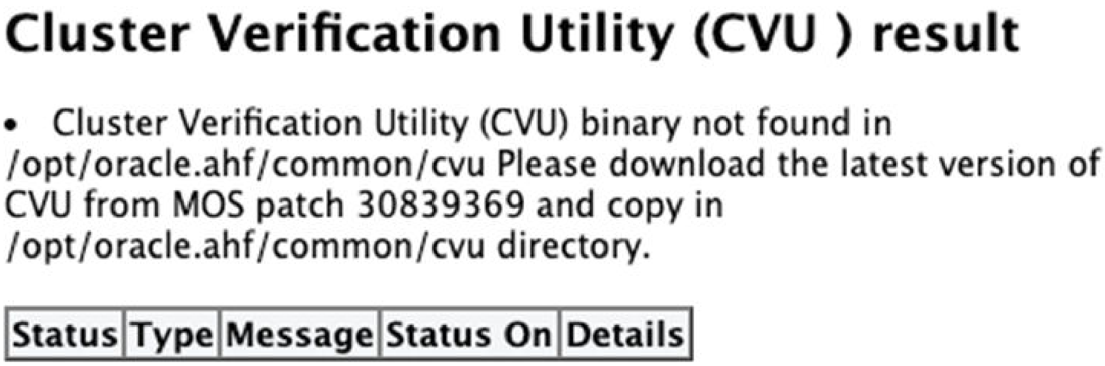


Cluster Verification Utility (CVU 19.6.0.0.0) result

Status	Type	Message	Status On	Details
FAIL	OS Check	Software home check failed	myserver	View
FAIL	OS Check	Clock Synchronization check failed	myserver	View

If CVU pack is not found or if the latest version is not available, then Oracle Orachk and Oracle Exachk logs the message and add an entry within the report.

Figure 9-2   No CVU Result



Cluster Verification Utility (CVU) result

- Cluster Verification Utility (CVU) binary not found in /opt/oracle.ahf/common/cvu Please download the latest version of CVU from MOS patch 30839369 and copy in /opt/oracle.ahf/common/cvu directory.

Status	Type	Message	Status On	Details

Syntax

```
orachk [-cvuhome] [-cvuonly] [-includecvu] [-excludecvu]
exachk [-cvuhome] [-cvuonly] [-includecvu] [-excludecvu]
```

Parameters

Table 9-131 Running CVU Compliance Checks

Option	Description

`-cvuhome`	Specify the location of the zipped file `cvupack.zip` or the directory where you have unzipped the `cvupack.zip` file.
	`orachk -cvuhome` *gi_home*
	`exachk -cvuhome` *gi_home*
	`orachk -cvuhome` *path to cvu_zip*
	`exachk -cvuhome` *path to cvu_zip*
	`orachk -cvuhome` *path to unzipped cvupack*
	`exachk -cvuhome` *path to unzipped cvupack*
	`orachk -cvuhome` *location_of_file_or_directory*
	`exachk -cvuhome` *location_of_file_or_directory*
	`orachk -profile preinstall -cvuhome` *location_of_file_or_directory*
	`exachk -profile preinstall -cvuhome` *location_of_file_or_directory*
	`orachk -preupgrade -cvuhome` *location_of_file_or_directory*
	`exachk -preupgrade -cvuhome` *location_of_file_or_directory*
	For example:
	`orachk -cvuhome /tmp/cvupack.zip`
	`orachk -cvuhome /tmp/cvupack`
	`orachk -profile preinstall -cvuhome /tmp/cvupack.zip`
	`orachk -profile preinstall -cvuhome /tmp/cvupack`
	`orachk -preupgrade -cvuhome /tmp/cvupack.zip`
	`orachk -preupgrade -cvuhome /tmp/cvupack`

`-cvuonly`	Use the `-cvuonly` command option to run only the CVU checks. Running the `-cvuonly` command does not run Oracle Orachk and Oracle Exachk related compliance checks.
`-excludecvu`	Use the `-excludecvu` command option to exclude CVU checks.

Reviewing Cluster Verification Utility (CVU) Output

By default, a full Oracle Exachk run calls CVU and displays the results in a separate section of the report. To review the CVU output, run Oracle Exachk and review the provided report. Also by default, only the FAIL items are displayed, so the expected output (all PASS results) in the Oracle Exachk report displays only the header information similar to:

```
Cluster Verification Utility (CVU 19.4.0.0.0 ) result
Status    Type    Message    Status On    Details
```

If you wish to view the specific CVU verifications, select **PASS** or **ALL** in the Oracle Exachk report header section, and you will see output similar to:

```
Cluster Verification Utility (CVU 19.4.0.0.0 ) result
Status    Type    Message    Status On    Details
PASS   OS Check   Node Connectivity check passed   random01client01   View
PASS   OS Check   Multicast or broadcast check check passed
random01client01   View
PASS   OS Check   Time zone consistency check passed   random01client01
View
PASS   OS Check   Cluster Manager Integrity check passed
random01client01   View
PASS   OS Check   Cluster Integrity check passed   random01client01   View
PASS   OS Check   CRS Integrity check passed   random01client01   View
PASS   OS Check   Node Application Existence check passed
random01client01   View
PASS   OS Check   Single Client Access Name (SCAN) check passed
random01client01   View
PASS   OS Check   OLR Integrity check passed   random01client01   View
PASS   OS Check   ASM Integrity check passed   random01client01   View
PASS   OS Check   User Not In Group "root": grid check passed
random01client01   View
PASS   OS Check   Clock Synchronization check passed   random01client01
View
PASS   OS Check   VIP Subnet configuration check check passed
random01client01   View
PASS   OS Check   Network configuration consistency checks check passed
random01client01   View
PASS   OS Check   Package: psmisc-22.6-19 check passed   random01client01
View
PASS   OS Check   File system mount options for path GI_HOME check passed
random01client01   View
PASS   OS Check   ACFS device special file check passed   random01client01
View
```

In this section of the report, click the **View** link to view more details. For example, in the **Node Connectivity check passed** entry above:

```
Description   This is a prerequisite condition to test whether connectivity
exists amongst all the nodes.
The connectivity is being tested for the subnets
"98.450.312.0,98.450.312.0,98.450.312.0,99.475.0.0"
```

```
Links   None

Needs attention on   -
Passed on   random01client01

Status on random01client01:
PASS => Node Connectivity check passed
```

If there are any CVU issues reported, then the default report will show an expanded table similar to the following:

```
Cluster Verification Utility (CVU 19.4.0.0.0 ) result
Status    Type    Message    Status On    Details
FAIL   OS Check   Node Connectivity check failed   random01client01
View
```

Examine the additional information in the **View** detail section for root cause and take appropriate corrective action.

Note:

For additional information on the Cluster Verification Utility, see *Cluster Verification Utility Referece* section of the appropriate *Clusterware Administration and Deployment Guide* for the installed Oracle Database version.

Note:

If you wish to review the CVU output without a full Oracle Exachk run after completing the corrective actions, then as `root` run the following command in the directory in which Oracle Exachk was installed:

```
exachk -cvuonly
```

Related Topics

- Cluster Verification Utility Reference

9.4.12 Running Auto Start

Use the list of commands to start or stop auto start.

Table 9-132 Auto start

Option	Description
`-autostart`	Configures auto start. You must run this command as `root`. The daemon runs a full local Oracle Orachk check once every week at 3 AM, and a partial run of the most impactful checks at 2 AM every day through the `oratier1` or `exatier1` profiles. The daemon automatically purges the `oratier1` or `exatier1` profile run that runs daily, after a week. The daemon also automatically purges the full local run after 2 weeks. You can change the daemon settings after enabling auto start. **Note:** Daemon mode is supported only on the Linux and Solaris operating systems. • `$ orachk -autostart` • `$ exachk -autostart`
`-autostart reset`	Starts and loads the default schedulers.
`-autostart -monthly`	Use the `-monthly` option to configure the daemon to run a full local Oracle Orachk once every month, and a partial run of the most important checks at 2 AM every day through the `oratier1` or `exatier1` profiles. • `$ orachk -autostart -monthly` • `$ exachk -autostart -monthly`
`-autostop`	Removes auto start configuration. You must run this command as `root`.
`-autostop unset`	Removes all default unmodified schedulers.

Related Topics

- Behavior of Oracle Orachk or Oracle Exachk Daemon
  AHF 23.9 includes a new command option `reset` to change the behavior of Oracle Orachk or Oracle Exachk daemon during `autostart`, `autostop`, and `upgrade`.

9.4.13 ZFS Storage Appliance Options

Use the `-zfssa` command to run compliance checks on Oracle ZFS Storage Appliances.

Table 9-133 ZFS Storage Appliance Options

Option	Description
`-zfssa` *`node`*	Runs Oracle Orachk only on selected ZFS appliance nodes, where *node* is a comma-delimited list of ZFS Storage Appliance names. For example: `orachk -zfssa` *`node1,node2`*

Related Topics

- Running Oracle ZFS Storage Appliance Compliance Checks
  Learn to run the compliance checks for Oracle ZFS Storage Appliances.

9.5 Running Unified AHF CLI Administration Commands

Currently, the unified AHF CLI is supported only for Linux platforms.

- ahf
  Use the `ahf` command to generate diagnostic analysis report, generate AHF Balance reports, and query the version of AHF running on the local node.
- ahf analysis
  Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.
- ahf configuration
  Use the `ahf configuration` command to change AHF configuration.
- ahf observer
  Use the `ahf observer` command to retrieve status of AHF components.
- ahf software
  Use the `ahf software` command to retrieve the details of AHF software and Monthly Recommended Patches (MRP).
- ahf data
  Use the `ahf data` command to retrieve information about AHF repositories.

9.5.1 ahf

Use the `ahf` command to generate diagnostic analysis report, generate AHF Balance reports, and query the version of AHF running on the local node.

Syntax

```
ahf category action [options]
category: {analysis,configuration,observer,software,data}
```

- **analysis**: Use to analyze an environment for problems and provide recommendations for corrective actions.
- **configuration**: Use to change AHF configuration.
- **observer**: Use to interact with AHF processes.
- **software**: Use to retrieve software information about AHF and Monthly Recommended Patches (MRP).
- **data**: Use to retrieve information about AHF repositories.

Parameters

Table 9-134 ahf Command Parameters

Parameter	Description
`-h`, `--help`	Show this help and exit.
`--version`, `-v`	Queries the version of AHF installed on the local node.
`--debug, -d`	Show additional debug information in log file.
Category: `software` • **Action:** `get-version` • **Options:** – `--component {ahf,tfa,compliance,all}` – `--local`	Queries the version of AHF installed on the local node.
Category: `software` • **Action:** – `get-mrp-level` – `compare-mrp-level` – `get-latest-mrp-level` – `apply-update`	`get-mrp-level`: gets the Monthly Recommended Patches (MRP) level the Oracle home is at • **Options:** – `--oracle-home` *`ORACLE_HOME`*: gets the MRP level for the specified Oracle Home – `-all`: gets the MRP level for all Oracle Home on the system `compare-mrp-level`: compares an Oracle home against a specific MRP level to retrieve installed and missing patches • **Options:** – `--oracle-home` *`ORACLE_HOME`*: Specify the Oracle home for which you want to query the information for – `--mrp-level` *`MRP_LEVEL`*: Specify the MRP level for which you want to check. **Default:** Latest applicable MRP level. `get-latest-mrp-level`: gets the latest MRP level name • **Option:** `--ru` *`RU`* Specify the RU for which you want to query information. `apply-update`: applies the update provided to the AHF installation on the local node • **Option:** `--update-file` *`<zip-file-name>`* Specify the zip file name.
Category: `analysis` • **Action:** `create` • **AHF Insights Options:** [`--type insights`] [`--last` *`n{m|h}`* | `--for` *`<DATETIME>`* | `--from` *`<DATETIME>`* `--to` *`<DATETIME>`*]	Generates AHF Insights analysis report.
Category: `analysis` • **Action:** `create` • **AHF Balance Options:** [`--type impact`] `--scope` [`fleet`|`cluster`|`database`] `--name` *`NAME`*	Generates AHF Balance reports: Fleet Report, Cluster Report, and Database Report.

Table 9-134 (Cont.) ahf Command Parameters

Parameter	Description
Category: `analysis` - **Action:** `explore` - **AHF Scope Options:** [`--with scope`] [`--from-file` *`FILE`*]	Launches exploratory analysis with the specified tool.
Category: `configuration` - **Action:** `set` - **AHF Balance Options:** [`--type impact`][`--connect-string` *`CONNECT-STRING`*] [`--user-name` *`USER-NAME`*]	Configures a connection to an Oracle Enterprise Manager repository.
Category: `data` - **Action:** `get-repository` - **Options:** , – `--component {all,compliance,tfa}` – `--local`	Retrieves information about AHF repositories. `--local`: Retrieves information about AHF repositories only from the local node.
Category: `observer` - **Action:** `status`	Retrieves the status of AHF components.

Example 9-135 ahf software get-version --component all

```
ahf software get-version --component all
AHF version: 24.2.0
Build Timestamp: 20240224222447
TFA version: 24.2.0
Compliance version: 24.2.0
Compliance metadata version: 20240224
```

9.5.2 ahf analysis

Use the `ahf analysis` command to generate AHF Insights and AHF Balance reports.

AHF 23.8

Starting in AHF 23.8, you will be able to upload AHF Insights report automatically if Object Store is configured as part of AHF. Uploading AHF Insights reports helps Oracle Cloud Operations to identify, investigate, track, and resolve system health issues and divergences in best practice configurations quickly and effectively.

Oracle Autonomous Database on Dedicated Exadata Infrastructure and Oracle SaaS

To set REST endpoints (Object Store's), run:

```
ahfctl setupload -name oss -type https -user <user> -url <object_store> -
password
```

To upload AHF Insights report to Object Store, run:

```
ahf analysis create --type insights
```

.

ahf analysis create

```
ahf analysis create [-h] [--type {insights|impact}] [[--last n{m|h} [--
refresh] | --for DATETIME | --from DATETIME --to DATETIME] [--tag TAGNAME] |
[--scope SCOPE --name NAME --cluster CLUSTER --clusters CLUSTER_LIST]][--
output-file PATH] [--to-json]
```

Syntax: AHF Balance

```
ahf analysis create [-h] --type impact --scope [fleet|cluster|database] [--
cluster CLUSTER_NAME] [--clusters space-delimited list of clusters
] --name NAME
```

Parameters

Table 9-135 ahf analysis create --type impact Command Parameters

Parameter	Description
`-h, --help`	Show this help and exit.
`--type impact`	Specify the type of report to generate.
`--scope [fleet|cluster|database]`	Specify to generate AHF Balance reports - Fleet Report, Cluster Report, and Database Report Specify the `--scope` and `--name` options to create an impact analysis. The `--cluster` option is required for database impact analysis.
`--output-file` *PATH*	Specify to create output file in the specified location.
`--clusters` *clu1 clu2 clu3*	Specify a space-delimited list of clusters to include in the fleet scope.
`--name` *NAME*	Specify the name of the fleet, cluster, or database to report on.
`--user-name` *USER_NAME*	Specify the Oracle Enterprise Manager Repository user name.
`--connect-string` *CONNECT_STRING*	Specify the connect string for the Oracle Enterprise Manager Repository.

Syntax: AHF Insights

```
ahf analysis create [-h] --type insights [--last n{m|h} | --for
DATETIME | --from DATETIME --to DATETIME] [--refresh] [--tag TAGNAME
]
```

Parameters

Table 9-136 ahf analysis create --type insights Command Parameters

Parameter	Description
`-h, --help`	Show this help and exit.
`--type insights`	Specify the type of report to generate.
`--last` *n*{*m*|*h*}	Specify the `--last` parameter to analyze data for the past number of minutes (m) or hours (h). `--last` cannot be greater than 12 hours.

`--for` *<DATETIME>*	Specify the `--for` parameter to analyze data for a 2 hour period before and after the timestamp specified.
	Supported time formats:
	`"YYYY-MM-DDTHH:MM:SS"`
	`"YYYY-MM-DD HH:MM:SS"`

`--from` *<DATETIME>*
`--to` *<DATETIME>*
	Specify the `--from` and `--to` parameters (you must use these two parameters together) to analyze data for a specific time interval.
	Supported time formats:
	`"YYYY-MM-DDTHH:MM:SS"`
	`"YYYY-MM-DD HH:MM:SS"`
	`"YYYY-MM-DD"`
	Time difference between from and to time should not be more than 4 hours.

`--refresh`	Provides fresh data from AHF Insights sources. Specify `--refresh` alone or together with `--last` to provide fresh data from AHF Insights sources.
`--include-cell-data`	Specify to include data from cell into AHF Insights sources.
`--tag` *TAGNAME*	Specify to collect the files into the *TAGNAME* directory inside the repository.

Syntax: ahf analysis explore

```
ahf analysis explore [-h] [--with scope] [--from-file FILE]
```

Parameters

Table 9-137   ahf analysis explore Command Parameters

Parameter	Description
`-h`, `--help`	Show this help and exit.
`--from-file FILE`	Specify to read from a file. If you do not specify the file extension, then AHF Scope assumes `.mdb` as the file extension.

Example 9-136   AHF Insights Analysis Usage Examples

Specify `[--last | --for | --from --to]` to create an analysis for a given period of time. Maximum time interval allowed is 4 hrs.

Specify `[--refresh]` alone or together with `[--last]` to provide fresh data from AHF Insights sources.

- Create analysis report from the data collected in the last 3 hours:

  ```
  ahf analysis create --type insights --last 3h
  ```

- Create analysis for a 2-hour period centered at the specified timestamp:

  ```
  ahf analysis create --type insights --for 2022-10-10T14:00:00
  ```

- Create analysis for a given time range:

  ```
  ahf analysis create --type insights --from 2022-10-10T14:00:00 --to
  2022-10-10T15:30:00
  ```

- Create analysis specifying a timezone:

  ```
  ahf analysis create --type insights --from 2022-10-10T14:00:00 --to
  2022-10-11T13:30:00
  ```

- Create analysis with most recent data:

  ```
  ahf analysis create --type insights --refresh
  ```

- Create analysis with a tag:

  ```
  ahf analysis create --type insights --tag my_tag
  ```

Example 9-137   AHF Balance Usage Examples

Specify `[--scope]` and `[--name]` options to create an impact analysis.

The `[--cluster]` option is required for database impact analysis.

- Create analysis for a fleet (all clusters):

  ```
  ahf analysis create --type impact --scope fleet --name fleet1
  ```

- Create analysis for a fleet (cluster list):

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --
  clusters clu1 clu2 clu3
  ```

- Create analysis for a cluster:

  ```
  ahf analysis create --type impact --scope cluster --name cluster1
  ```

- Create analysis for a database:

  ```
  ahf analysis create --type impact --scope database --cluster
  cluster1 --name database1
  ```

- Create analysis specifying the output directory:

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --
  output-file /custom_path/custom_name.html
  ```

- Create analysis specifying EM repository user name and password:

  ```
  ahf analysis create --type impact --scope fleet --name fleet1 --
  user-name oracle --connect-string <cs>
  ```

9.5.3 ahf configuration

Use the `ahf configuration` command to change AHF configuration.

Syntax: ahf configuration

```
ahf configuration action [options]
```

Actions	Description
`set`	Sets configuration property and value.
`get`	Gets configuration property and value.
`unset`	Unsets configuration property and value.
`check`	Checks configuration.

ahf configuration set

```
ahf configuration set --type CONFIGURATION_TYPE [OPTIONS]
```

Parameter	Description
`-h`, `--help`	Show this help and exit.
`--to-json`	Specify to display the output in JSON format.
`--type` *`TYPE`*	Specify the type of configuration to access.
`--name` *`NAME`*	Specify the name of the component or configuration.
`--property` *`NAME`*	Specify the name of the property to set.
`--value` *`VALUE`*	Specify the value of the property.
`--type impact`	`--user-name` *`USER_NAME`*: Specify the user name which the command requires. `--connect-string` *`CONNECT_STRING`*: Specify the connect string for the Oracle Enterprise Manager repository.
`--type fleet-insights`	`--url` *`URL`*: Specify the full fleet insights registration URL. `--user-name USER_NAME`: Specify the user name which the command requires.
`--type repository`	`--location` *`LOCATION`*: Specify a new location for the repository. `--size` *`SIZE`*: Specify the maximum size of repository (MB).
`--type goldengate`	`--all`: Specify to set all parameters interactively. `--host-name` *`HOST_NAME`*: Specify the fully qualified host name with domain name. `--db-name` *`DB_NAME`*: Specify the database name. `--port` *`PORT`*: Specify GoldenGate Service Manager port.

Parameter	Description
`--type upload`	`--endpoint-type {https,bugdb,sqlnet,sftp}`: Specify the upload endpoint type. `--all`: Specify to set all parameters interactively. `--host-name` *`HOST_NAME`*: Specify the fully qualified host name with domain name `--user-name` *`USER_NAME`*: Specify the user name which the command requires. `--password`: Specify to prompt for password. `--url` *`URL`*: Specify the full registration or upload URL `--port` *`PORT`*: Specify the service port number. `--store-type` *`STORE_TYPE`*: Specify the store type. `--proxy` *`PROXY`*: Specify the proxy URL `--connect-string` *`CONNECT_STRING`*: Specify the Connect string for the Oracle Enterprise Manager Repository `--upload-table` *`UPLOAD_TABLE`*: Spefiy the upload table name. `--no-authentication`: Specify if no authentication is required. `--https-token` *`HTTPS_TOKEN`*: Specify the HTTPS token to log in. `--https-header` *`HTTPS_HEADER`*: Specify the HTTPS header string. `--request-type` *`REQUEST_TYPE`*: Specify the HTTPS request type.

> **Note:**
>
> - `--user-name` is the Oracle Enterprise Manager Repository user name if `--type impact`
> - `--user-name` is the API registration user if `--type fleet-insights`
> - `--user-name` is the upload configuration user if `--type upload`
> - `--user-name` is the login user if `--type impact`
> - `--user-name` is the GoldenGate service manager user if `--type goldengate`
> - `--name` is the component name if `--type repository`
> - `--name` is the configuration name if `--type goldengate`

Values supported for `--property`:

- Repository properties:

  - `reposizeMB`
  - `repositorydir`
- Global properties: `gather_ahf_feature_usage`
- User properties: `ahf.insights.max-collection-interval`

Syntax: ahf configuration get

```
ahf configuration get [OPTIONS]
```

Parameter	Description
`--type` *`TYPE`*	Specify the type of configuration to get. Valid values: • GoldenGate microservice: `goldengate` • Upload configuration: `upload`
`--name` *`CONFIG_NAME`*	Specify unique configuration name for `--type goldengate` or `--type upload`.
`--property` *`PROPERTY_NAME`*	Specify the name of the property.
`--type upload`	`--endpoint-type {https,bugdb,sqlnet,sftp}`: Specify the upload endpoint type. `--all`: Specify to set all parameters interactively. `--host-name` *`HOST_NAME`*: Specify the fully qualified host name with domain name `--user-name` *`USER_NAME`*: Specify the user name which the command requires. `--password`: Specify to prompt for password. `--url` *`URL`*: Specify the full registration or upload URL `--port` *`PORT`*: Specify the service port number. `--store-type` *`STORE_TYPE`*: Specify the store type. `--proxy` *`PROXY`*: Specify the proxy URL `--connect-string` *`CONNECT_STRING`*: Specify the Connect string for the Oracle Enterprise Manager Repository `--upload-table` *`UPLOAD_TABLE`*: Spefiy the upload table name. `--no-authentication`: Specify if no authentication is required. `--https-token` *`HTTPS_TOKEN`*: Specify the HTTPS token to log in. `--https-header` *`HTTPS_HEADER`*: Specify the HTTPS header string. `--request-type` *`REQUEST_TYPE`*: Specify the HTTPS request type.

Syntax: ahf configuration check

```
ahf configuration check [OPTIONS]
```

Parameter	Description
`--type` *`TYPE`*	Specify the type of configuration to check.
`--to-json`	Specify to display the output in JSON format.
`--name` *`CONFIG_NAME`*	Specify configuration name to check if `--type goldengate` or `--type upload`.

Syntax: ahf configuration unset

```
ahf configuration unset [OPTIONS]
```

Parameter	Description
`--type` *`TYPE`*	Specify the type of configuration to unset.
`--type fleet-insights`	`--user-name` *`USER_NAME`*: API registration user. `--url` *`URL`*: Full fleet insights registration URL.
`--type goldengate`	`--name` *`CONFIG_NAME`*: Configuration name.

Parameter	Description
--type upload	--endpoint-type {https,bugdb,sqlnet,sftp}: Specify the upload endpoint type. --all: Specify to set all parameters interactively. --host-name *HOST_NAME*: Specify the fully qualified host name with domain name --user-name *USER_NAME*: Specify the user name which the command requires. --password: Specify to prompt for password. --url *URL*: Specify the full registration or upload URL --port *PORT*: Specify the service port number. --store-type *STORE_TYPE*: Specify the store type. --proxy *PROXY*: Specify the proxy URL --connect-string *CONNECT_STRING*: Specify the Connect string for the Oracle Enterprise Manager Repository --upload-table *UPLOAD_TABLE*: Spefiy the upload table name. --no-authentication: Specify if no authentication is required. --https-token *HTTPS_TOKEN*: Specify the HTTPS token to log in. --https-header *HTTPS_HEADER*: Specify the HTTPS header string. --request-type *REQUEST_TYPE*: Specify the HTTPS request type.

Syntax: AHF Balance

```
ahf configuration set --type CONFIGURATION_TYPE [OPTIONS]
```

Parameters

Table 9-138 ahf configuration set Command Parameters

Parameter	Description
-h, --help	Show this help and exit.
--type *CONFIGURATION_TYPE*	Specify the type of configuration (impact) to access.

Table 9-138 (Cont.) ahf configuration set Command Parameters

Parameter	Description
`--connect-string` *`CONNECT-STRING`*	Specify the connect string for the Oracle Enterprise Manager repository. **Note:** Ensure that the connect string does not contain any spaces.
`--user-name` *`USER-NAME`*	Specify Oracle Enterprise Manager repository user name.

> **Note:**
>
> Running this command will prompt you to enter the password for the Oracle Enterprise Manager repository user. The Oracle Enterprise Manager repository user can be any Enterprise Manager (EM) user with Target Privilege: `View any Target`. AHF Balance connects to an EM repository instance as the specified user.

9.5.4 ahf observer

Use the `ahf observer` command to retrieve status of AHF components.

Syntax: ahf observer

```
ahf observer action [options]
```

Action: status

Options: `--to-json`: displays the output in JSON format.

Example 9-138 ahf observer status

```
ahf observer status
+---------------+---------------+---------------+
|  Observer Type|      Host     |     Status    |
+---------------+---------------+---------------+
|    COMPLIANCE |  hostname     |   NOT RUNNING |
+---------------+---------------+---------------+
```

9.5.5 ahf software

Use the `ahf software` command to retrieve the details of AHF software and Monthly Recommended Patches (MRP).

Use the `ahf software` command:

- to query the version of AHF installed
- to find the Monthly Recommended Patches (MRP) level the Oracle home is at
- to fetch the list of installed and missing patches for a specific MRP level. This will help you determine whether an Oracle home has all an MRP's patches installed or not.

Use the `--to-json` option with the following commands to get output in the JSON format.

- `ahf software get-version`
- `ahf software compare-mrp-level`
- `ahf software get-latest-mrp-level`

Syntax: ahf software

- To get AHF installed version:

  ```
  ahf software get-version --component all
  ```

  For example:

  ```
  ahf software get-version --component all
  AHF version: 24.2.0
  Build Timestamp: 20240224222447
  TFA version: 24.2.0
  Compliance version: 24.2.0
  Compliance metadata version: 20240224
  ```

- To get the MRP level for a given Oracle home:

  ```
  ahf software get-mrp-level --oracle_home ORACLE_HOME
  ```

  For example:

  - **Database:** compliant and no missing patches

    ```
    ahf software get-mrp-level --oracle-home /u01/oracle
    Database MRP 19.17.0.0.221115
    ```

  - **Grid Infrastructure:** compliant and no missing patches

    ```
    ahf software get-mrp-level --oracle-home /u01/oracle/grid
    GI MRP 19.17.0.0.230221
    ```

  - **Oracle Home:** No MRP installed

    ```
    ahf software get-mrp-level --oracle-home /u01/oracle
    No MRP installed in the Oracle Home
    ```

- To compare an Oracle home against a specific MRP level to retrieve installed and missing patches:

  ```
  ahf software compare-mrp-level --oracle-home TEXT --mrp-level TEXT
  ```

For example:

- **Database:** comparing to a specific level

  ```
  ahf software compare-mrp-level --oracle-home /u01/oracle --mrp-
  level "Database MRP 19.17.0.0.221220"
  Installed:
      <bug-id-1>
      <bug-id-2>
        ...
      <bug-id-5>
   Missing:
      <bug-id-8>
      <bug-id-9>
        ...
      <bug-id-10>
  ```

- **Grid Infrastructure:** comparing to a specific level

  ```
  ahf software compare-mrp-level --oracle-home /u01/oracle/grid --
  mrp-level "GI MRP 19.17.0.0.230321"
  Installed:
      <bug-id-1>
      <bug-id-2>
        ...
      <bug-id-5>
   Missing:
      <bug-id-8>
      <bug-id-9>
        ...
      <bug-id-10>
  ```

- To query the latest MRP level:

  ```
  ahf software get-latest-mrp-level
  19.22
      Database: Database MRP 19.22.0.0.240220
      GI      : None
  19.21
      Database: Database MRP 19.21.0.0.240220
      GI      : GI MRP 19.21.0.0.240116
  19.20
      Database: Database MRP 19.20.0.0.240116
      GI      : GI MRP 19.20.0.0.240116
  19.19
      Database: Database MRP 19.19.0.0.231017
      GI      : GI MRP 19.19.0.0.231017
  19.18
      Database: Database MRP 19.18.0.0.230718
      GI      : GI MRP 19.18.0.0.230718
  19.17
  ```

```
    Database: Database MRP 19.17.0.0.230418
    GI      : GI MRP 19.17.0.0.230418


ahf software get-latest-mrp-level --ru 19.21
19.21
    Database: Database MRP 19.21.0.0.240220
    GI      : GI MRP 19.21.0.0.240116


ahf software get-latest-mrp-level --ru 19.22
19.22
    Database: Database MRP 19.22.0.0.240220
    GI      : None
```

- To apply update using a specific file:

  ```
  ahf software apply-update --update-file <zip-file-name>
  ```

  For example:

  ```
  ahf software apply-update --update-file /tmp/ahf_data_20240127.zip
  Successfully updated Data files from version 20240111 to 20240127
  ```

9.5.6 ahf data

Use the `ahf data` command to retrieve information about AHF repositories.

Syntax: ahf data

```
ahf data action [options]
Action: get-repository
Option: --component {all,compliance,tfa}, --local, --to-json
```

Action	Description
`get-repository`	Gets the repository information.

Options	Description
`--to-json`	Prints the output in JSON format.
`--local`	Gets information about the repositories for the local AHF installation.
`--component {all,tfa,compliance}`	Gets repository information for a component {`tfa`|`compliance`|`all`}

```
ahf data get-repository --component all
tfa
--------------------    -----
Repository parameter    Value
location                /opt/oracle.ahf/data/repository
```

```
max_size                6171
size                    7
free_size               6164
status                  OPEN

compliance
--------------------    -----
Repository parameter    Value
location                /opt/oracle.ahf/data/<host_name>/orachk/
user_root/output


ahf data get-repository --component tfa
tfa
--------------------    -----
Repository parameter    Value
location                /scratch/repository
max_size                15000
size                    0
free_size               15000
status                  OPEN


ahf data get-repository --component compliance
compliance
--------------------    -----
Repository parameter    Value
location                /opt/oracle.ahf/data/<host_name>/orachk/
user_root/output
```

9.6 OCLUMON Command Reference

Use the command-line tool to query the Cluster Health Monitor repository to display node-specific metrics for a specific time period.

Use OCLUMON to perform miscellaneous administrative tasks, such as changing the debug levels, querying the version of Cluster Health Monitor, and changing the metrics database size.

- oclumon analyze
  Use the `oclumon analyze` command to analyze CHM metrics.
- oclumon dumpnodeview
  Use the `oclumon dumpnodeview` command to view log information from the system monitor service in the form of a node view.
- oclumon chmdiag
  Use the `oclumon chmdiag` to get a detailed description of all the supported events and actions, query CHMDiag events/actions sent by various components and generate an HTML or a text report, and to collect all events/actions data generated by CHMDiag into the specified output directory location.
- oclumon localrepo
  Use the `oclumon localrepo` command to view and change the configuration of local repository.

- oclumon version
  Use the `oclumon version` command to obtain the version of Cluster Health Monitor that you are using.
- oclumon debug
  Use the `oclumon debug` command to set the log level for the Cluster Health Monitor services.

9.6.1 oclumon analyze

Use the `oclumon analyze` command to analyze CHM metrics.

Syntax

```
oclumon analyze [-h] [-i CHM_METRICS_DIR] -o OUT_DIR [-l LOG_DIR] [--
log_level {DEBUG,INFO,WARNING,ERROR}] [-s START_TIME] [-e END_TIME] [-f
FORMAT] [--version]
```

Parameters

Table 9-139 oclumon analyze Command Parameters

Parameter	Description

`-i` *`CHM_METRICS_DIR`*
`--chm_metrics_dir` *`CHM_METRICS_DIR`*
	Specify the directory containing CHM metrics.

`-o` *`OUT_DIR`*
`--out_dir` *`OUT_DIR`*
	Specify the output directory for the results.

`-l` *`LOG_DIR`*
`--log_dir` *`LOG_DIR`*
	Specify the log directory.

`--log_level {DEBUG,INFO,WARNING,ERROR}`	Specify the log level.

`-s` *`START_TIME`*
`--start_time` *`START_TIME`*
	Specify the start time for analysis in `YYYY-MM-DDTHH:MM:SS` format.

`-e` *`END_TIME`*
`--end_time` *`END_TIME`*
	Specify the end time for analysis in `YYYY-MM-DDTHH:MM:SS` format.

`-f` *`FORMAT`*
`--format` *`FORMAT`*
	Specify a comma-delimited report format (`text`,`html`). Defaults to `text` format if not specified. Can either `text` or `html` or both

`--version`	Displays the program's version number and exits.

Example 9-139 oclumon analyze Examples

To generate text analysis report for the entire CHM repository:

```
oclumon analyze -o /<outpur-dir>
```

To generate text analysis report from 2024-03-14T05:00:00 to 2024-03-14T05:15:00 duration:

```
oclumon analyze -o /<output-dir> -s 2024-03-14T05:00:00 -e
2024-03-14T05:15:00
```

To generate an HTML analysis report for the entire CHM repository:

```
oclumon analyze -o /<output-dir> -f html
```

To generate the analysis report from an archived CHM dataset:

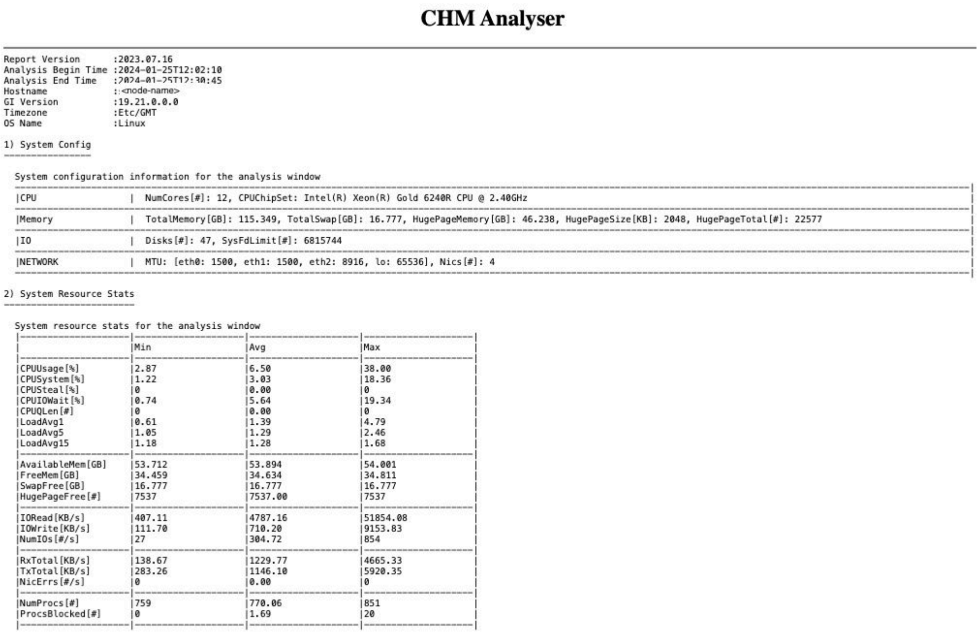
```
oclumon analyze -i /<chm-data-dir> -o /<output-dir>
```

Example 9-140 Sample CHM Analysis Report

CHM analysis report contains following sections:

- **Header section:** Contains info about the node, analysis time period, system configuration and system resource stats.

Figure 9-3 System Configuration and System resource stats

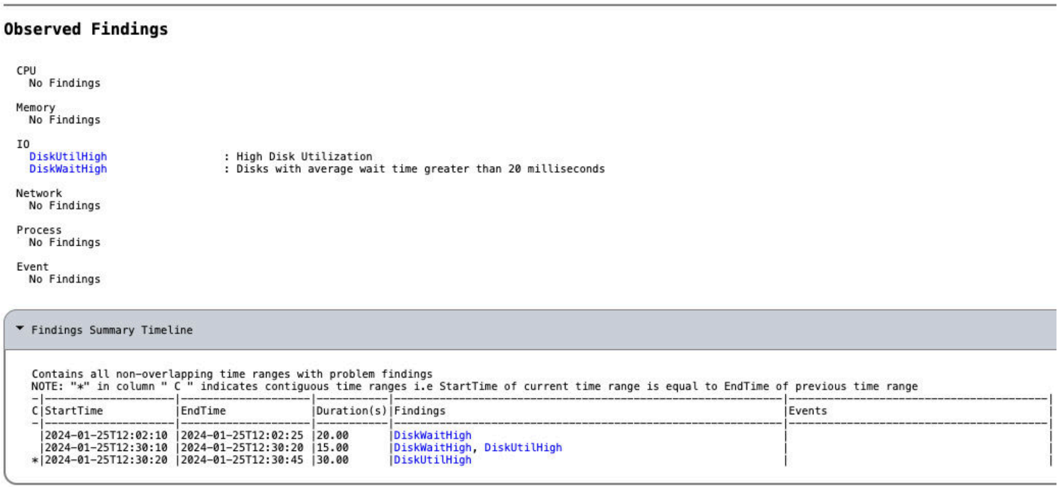


CHM Analyser

```
Report Version      :2023.07.16
Analysis Begin Time :2024-01-25T12:02:10
Analysis End Time   :2024-01-25T12:30:45
Hostname            :<node-name>
GI Version          :19.21.0.0.0
Timezone            :Etc/GMT
OS Name             :Linux

1) System Config
----------------

  System configuration information for the analysis window
  -------------------------------------------------------------------------------------------------------------------------------------------|
  |CPU              |  NumCores[#]: 12, CPUChipSet: Intel(R) Xeon(R) Gold 6240R CPU @ 2.40GHz                                                 |
  -------------------------------------------------------------------------------------------------------------------------------------------|
  |Memory           |  TotalMemory[GB]: 115.349, TotalSwap[GB]: 16.777, HugePageMemory[GB]: 46.238, HugePageSize[KB]: 2048, HugePageTotal[#]: 22577  |
  -------------------------------------------------------------------------------------------------------------------------------------------|
  |IO               |  Disks[#]: 47, SysFdLimit[#]: 6815744                                                                                     |
  -------------------------------------------------------------------------------------------------------------------------------------------|
  |NETWORK          |  MTU: [eth0: 1500, eth1: 1500, eth2: 8916, lo: 65536], Nics[#]: 4                                                      |
  -------------------------------------------------------------------------------------------------------------------------------------------|

2) System Resource Stats
------------------------

  System resource stats for the analysis window
  |--------------------|--------------------|--------------------|--------------------|
  |                    |Min                 |Avg                 |Max                 |
  |--------------------|--------------------|--------------------|--------------------|
  |CPUUsage[%]         |2.87                |6.50                |38.00               |
  |CPUSystem[%]        |1.22                |3.03                |18.36               |
  |CPUSteal[%]         |0                   |0.00                |0                   |
  |CPUIOWait[%]        |0.74                |5.64                |19.34               |
  |CPUQLen[#]          |0                   |0.00                |0                   |
  |LoadAvg1            |0.61                |1.39                |4.79                |
  |LoadAvg5            |1.05                |1.29                |2.46                |
  |LoadAvg15           |1.18                |1.28                |1.68                |
  |--------------------|--------------------|--------------------|--------------------|
  |AvailableMem[GB]    |53.712              |53.894              |54.001              |
  |FreeMem[GB]         |34.459              |34.634              |34.811              |
  |SwapFree[GB]        |16.777              |16.777              |16.777              |
  |HugePageFree[#]     |7537                |7537.00             |7537                |
  |--------------------|--------------------|--------------------|--------------------|
  |IORead[KB/s]        |407.11              |4787.16             |51854.08            |
  |IOWrite[KB/s]       |111.70              |710.20              |9153.83             |
  |NumIOs[#/s]         |27                  |304.72              |854                 |
  |--------------------|--------------------|--------------------|--------------------|
  |RxTotal[KB/s]       |138.67              |1229.77             |4665.33             |
  |TxTotal[KB/s]       |283.26              |1146.10             |5920.35             |
  |NicErrs[#/s]        |0                   |0.00                |0                   |
  |--------------------|--------------------|--------------------|--------------------|
  |NumProcs[#]         |759                 |770.06              |851                 |
  |ProcsBlocked[#]     |0                   |1.69                |20                  |
  |--------------------|--------------------|--------------------|--------------------|
```

- **Observed findings and findings summary timeline section:** Contains the list of observed problems, along with a summary timeline of the problems.

Figure 9-4   Problematic findings and summary timeline

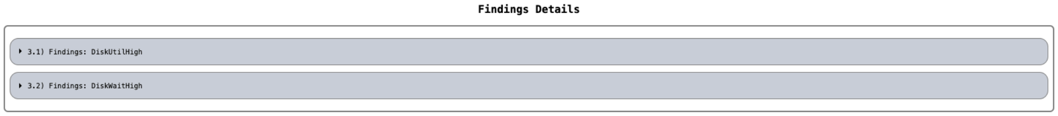


```
Observed Findings

  CPU
    No Findings

  Memory
    No Findings

  IO
    DiskUtilHigh                : High Disk Utilization
    DiskWaitHigh                : Disks with average wait time greater than 20 milliseconds

  Network
    No Findings

  Process
    No Findings

  Event
    No Findings
```

```
▼ Findings Summary Timeline

  Contains all non-overlapping time ranges with problem findings
  NOTE: "*" in column " C " indicates contiguous time ranges i.e StartTime of current time range is equal to EndTime of previous time range
  -|--------------------|--------------------|-----------|-----------------------------------------------------------|----------------------------------------|
  C|StartTime           |EndTime             |Duration(s)|Findings                                                   |Events                                  |
  -|--------------------|--------------------|-----------|-----------------------------------------------------------|----------------------------------------|
   |2024-01-25T12:02:10 |2024-01-25T12:02:25 |20.00      |DiskWaitHigh                                               |                                        |
   |2024-01-25T12:30:10 |2024-01-25T12:30:20 |15.00      |DiskWaitHigh, DiskUtilHigh                                 |                                        |
  *|2024-01-25T12:30:20 |2024-01-25T12:30:45 |30.00      |DiskUtilHigh                                               |                                        |
```

- **Findings details section:** Contains detailed contextual information for each of the problems observed above.

Figure 9-5   Problematic findings - details



```
                              Findings Details

 ▸ 3.1) Findings: DiskUtilHigh
 ▸ 3.2) Findings: DiskWaitHigh
```

9.6.2 oclumon dumpnodeview

Use the `oclumon dumpnodeview` command to view log information from the system monitor service in the form of a node view.

Syntax

```
oclumon dumpnodeview [[([(-system | -protocols | -v)] |
     [(-cpu | -process | -procagg | -device | -nic | -filesystem | -thread |
-nfs)
     [-detail] [-all] [-pinned_only] [-sort <metric_name>] [-filter
<string>] [-head <rows_count>] [-i <seconds>]])
     [([-s <start_time>  -e <end_time>] | -last <duration>)]] |
     [-inputDataDir <absolute_path> -logDir <absolute_path>]
     [-h]]
```

Parameters

Table 9-140 oclumon dumpnodeview Command Parameters

Parameter	Description
`-system`	Dumps system metrics. For example: `oclumon dumpnodeview -system` .
`-cpu`	Dumps CPU metrics. For example: `oclumon dumpnodeview -cpu` .
`-process`	Dumps process metrics. For example: `oclumon dumpnodeview -process` .
`-procagg`	Dumps process aggregate metrics. For example: `oclumon dumpnodeview -procagg` .
`-device`	Dumps disk metrics. For example: `oclumon dumpnodeview -device` .
`-nic`	Dumps network interface metrics. For example: `oclumon dumpnodeview -nic` .
`-filesystem`	Dumps filesystem metrics. For example: `oclumon dumpnodeview -filesystem` .
`-thread`	Dumps thread metrics for pinned processes. For example: `oclumon dumpnodeview -thread`

Table 9-140 (Cont.) oclumon dumpnodeview Command Parameters

Parameter	Description
`-nfs`	Dumps NFS metrics. For example: `oclumon dumpnodeview -nfs` .
`-protocols`	Dumps network protocol metrics, cumulative values from system start. For example: `oclumon dumpnodeview -protocols` .
`-v`	Displays verbose node view output. For example: `oclumon dumpnodeview -v` .
`-h, --help`	Displays the command-line help and exits.

Table 9-141 oclumon dumpnodeview Command Flags

Flag	Description
`-detail`	Use this option to dump detailed metrics. Applicable to the `-process` and `-nic` options. For example: `oclumon dumpnodeview -process -detail` .
`-all`	Use this option to dump the node views of all entries. Applicable to the `-process` option. For example: `oclumon dumpnodeview -process -all` .
`-pinned_only`	Use this option to dump the node views of all pinned processes. Applicable to the `-process` option. For example: `oclumon dumpnodeview -process -pinned_only`

Table 9-141 (Cont.) oclumon dumpnodeview Command Flags

Flag	Description
`-head` *`rows_count`*	Use this option to dump the node view of the specified number of metrics rows in the result. Applicable to the `-process` option. Default is set to 5. For example: `oclumon dumpnodeview -process -head 7` .
`-sort` *`metric_name`*	Use this option to sort based on the specified metric name, supported with the `-process`, `-device`, `-nic`, `-cpu`, `-procagg`, `-filesystem`, `-nfs` options. For example: `oclumon dumpnodeview -device -sort "ioR"` .
`-i` *`seconds`*	Display data separated by the specified interval in seconds. Must be a multiple of 5. Applicable to continuous mode query. For example: `oclumon dumpnodeview -device -i 5`
`-filter` *`string`*	Use this option to search for a filter string in the Name column of the respective metric. For example, `-process -filter "ora"` will display the process metrics, which contain "`ora`" substring in their name. Supported with the `-process`, `-device`, `-nic`, `-cpu`, `-procagg`, `-filesystem`, `-nfs` options. For example: `oclumon dumpnodeview -process -filter "ora"` .

Table 9-141 (Cont.) oclumon dumpnodeview Command Flags

Flag	Description
`-show_all_sample_with_filter`	All samples where filter doesn't matches will also show in the output. Can be used only with the –`filter` option. For example: `oclumon dumpnodeview -filter` *`filter_criteria`* `-show_all_sample_with_filter`

Table 9-142 oclumon dumpnodeview Command Log File Directories

Directory	Description
`-inputDataDir` *`absolute_dir_path`*	Specifies absolute path of the directory that contains JSON logs files. For example: `oclumon dumpnodeview -cpu -inputDataDir` *`absolute_path`*
`-logDir` *`absolute_log_dir_path`*	Specifies absolute path of the directory, which will contain the script run logs. For example: `oclumon dumpnodeview -cpu -inputDataDir` *`absolute_path`* `-logDir` *`absolute_log_dir_path`*

Table 9-143 oclumon dumpnodeview Command Historical Query Options

Flag	Description

`-s` *`start_time`*
`-e` *`end_time`*
	Use the `-s` option to specify a time stamp from which to start a range of queries and use the `-e` option to specify a time stamp to end the range of queries.
	Specify time in the `YYYY-MM-DD HH24:MM:SS` format surrounded by double quotation marks ("").
	Specify these two options together to obtain a range.
	For example:
	`oclumon dumpnodeview -cpu -s "2019-07-10 03:40:25" -e "2019-07-10 03:45:25"`

`-last` *`duration`*	Use this option to specify a time, given in `HH24:MM:SS` format surrounded by double quotation marks (""), to retrieve the last metrics. Specifying "*`00:45:00`*" will dump metrics for the last 45 minutes. For example: `oclumon dumpnodeview -nic -last "00:45:00"` .

9.6.3 oclumon chmdiag

Use the `oclumon chmdiag` to get a detailed description of all the supported events and actions, query CHMDiag events/actions sent by various components and generate an HTML or a text report, and to collect all events/actions data generated by CHMDiag into the specified output directory location.

- oclumon chmdiag description
  Use the `oclumon chmdiag description` command to get a detailed description of all the supported events and actions.
- oclumon chmdiag query
  Use the `oclumon chmdiag query` command to query CHMDiag events/actions sent by various components and generate an HTML or a text report.
- oclumon chmdiag collect
  Use the `oclumon chmdiag collect` command to collect all events/actions data generated by CHMDiag into the specified output directory location. This command will primarily be used by Oracle Trace File Analyzer to collect all events/actions that fall within a problematic window.

9.6.3.1 oclumon chmdiag description

Use the `oclumon chmdiag description` command to get a detailed description of all the supported events and actions.

Syntax

```
oclumon chmdiag description
[-h]
[-f {text,html} | --format {text,html}]
[--outdir OUTDIR]
```

Parameters

Table 9-144 oclumon chmdiag description Command Parameters

Parameter	Description
`-f {text,html}` | `--format {text,html}`	Specify to generate a report in the Text or HTML format. Note that you need to specify the `--outdir` if you need the report in the HTML format. HTML report is an interactive `html` page, which has support for easy navigation and filtering of data. It also has built-in help, which describes the events/actions.
`--outdir` *`OUTDIR`*	Specify the location of the directory where the description data (text/html) will be written.

9.6.3.2 oclumon chmdiag query

Use the `oclumon chmdiag query` command to query CHMDiag events/actions sent by various components and generate an HTML or a text report.

Syntax

```
oclumon chmdiag query
[-h]
[-f {text,html} | --format {text,html}]
[--outdir OUTDIR]
[--summary]
[-s S]
[-e E]
[--last LAST]
[--evtids EVTIDS [EVTIDS,...]]
[--actids ACTIDS [ACTIDS,...]]
[--compids COMPIDS [COMPIDS,...]]
[--inputdir INPUTDIR]
[--logdir LOGDIR]
```

Parameters

Table 9-145 oclumon chmdiag query Command Parameters

Parameter	Description
`-f {text,html}|--format {text,html}`	Specify to generate a report in the Text or HTML format. Note that you need to specify the `--outdir` if you need the report in the HTML format. HTML report is an interactive `html` page, which has support for easy navigation and filtering of data. It also has built-in help, which describes the events/actions.
`--outdir` *`OUTDIR`*	Specify the location of the directory where the queried data report (text/html) will be written.
`--summary`	Specify to display only the summary of the query result.
`-s` *`S`*	Specify the start timestamp for the query in the `YYYY-MM-DDTHH24:MI:SS-z` format.
`-e` *`E`*	Specify the end timestamp for the query in the `YYYY-MM-DDTHH24:MI:SS-z` format.
`--last` *`LAST`*	Specify to query logs for a specific duration.The duration can be specified as `nd`|`h`|`m`|`s`. Where: • `d` stands for Days • `h` stands for Hours • `m` stands for Minutes • `s` stands for Seconds • `n` can be a floating number For example, `--last` *`1d2h3m1s`*.
`--evtids EVTIDS`	Specify to query only the events with the specified event IDs.
`--actids ACTIDS`	Specify to query only the actions with the specified action IDs.
`--compids COMPIDS`	Specify to query all events/actions generated by the specified set of components.
`--inputdir` *`INPUTDIR`*	Specify the absolute path of the directory that contains `chmdiag` logs files.
`--logdir` *`LOGDIR`*	Specify the absolute path of the directory, whcih will contain the script run logs.

Action Status can be one of the following:

- **Succeeded:** Action completed with success return code.
- **Failed:** Action returned a non-success return code
- **NotRunExceededMaxLimit:** Action has not been run as the maximum number of allowed concurrent runs for this action has been exceeded.
- **Purged:** Action results have been purged, that is, the results have been recycled based on the set retention policy for this Action ID.
- **ExceededMaxRunTime:** This action has not completed within the configured maximum run time and hence the action has been killed. Whatever the output that gets generated by the command will be captured in the `cmd.out` file.

Example 9-141 oclumon chmdiag query

```
oclumon chmdiag query -f html --outdir /outdir/path/


oclumon chmdiag query --last 1h30m


oclumon chmdiag query -s 2018-06-20T10:30:00 -e 2018-06-20T11:30:00
```

9.6.3.3 oclumon chmdiag collect

Use the `oclumon chmdiag collect` command to collect all events/actions data generated by CHMDiag into the specified output directory location. This command will primarily be used by Oracle Trace File Analyzer to collect all events/actions that fall within a problematic window.

Syntax

```
oclumon chmdiag collect
[-h]
[--outdir OUTDIR]
[--gzip]
[-s S]
[-e E]
[--last LAST]
[--evtids EVTIDS [EVTIDS,...]]
[--actids ACTIDS [ACTIDS,...]]
[--compids COMPIDS [COMPIDS,...]]
[--inputdir INPUTDIR]
[--logdir LOGDIR]
```

Parameters

Table 9-146 oclumon chmdiag collect Command Parameters

Parameter	Description
`--outdir` *`OUTDIR`*	Specify the location of the directory where the collected data will be written.
`-gzip`	Specify to compress the output directory data into a `gzip` file.
`-s` *`S`*	Specify the start timestamp for the collection in the `YYYY-MM-DDTHH24:MI:SS-z` format.
`-e` *`E`*	Specify the end timestamp for the collection in the `YYYY-MM-DDTHH24:MI:SS-z` format.

Table 9-146 (Cont.) oclumon chmdiag collect Command Parameters

Parameter	Description
`--last` *`LAST`*	Specify to collect logs for a specific duration.The duration can be specified as `nd`|`h`|`m`|`s`. Where: • `d` stands for Days • `h` stands for Hours • `m` stands for Minutes • `s` stands for Seconds • `n` can be a floating number For example, `--last` *`1d2h3m1s`*.
`--evtids EVTIDS`	Specify to collect only the events with the specified event IDs.
`--actids ACTIDS`	Specify to collect only the actions with the specified action IDs.
`--compids COMPIDS`	Specify to collect all events/actions generated by the specified set of components.
`--inputdir` *`INPUTDIR`*	Specify the absolute path of the directory that contains `chmdiag` logs files.
`--logdir` *`LOGDIR`*	Specify the absolute path of the directory, whcih will contain the script run logs.

Example 9-142 oclumon chmdiag collect

```
oclumon chmdiag collect --outdir /outdir/path/


oclumon chmdiag collect --last 1.5h --outdir /outdir/path/
```

9.6.4 oclumon localrepo

Use the `oclumon localrepo` command to view and change the configuration of local repository.

- oclumon localrepo getconfig
  Use the `oclumon localrepo getconfig` to get the configuration of repositories for all the nodes.
- oclumon localrepo setconfig
  Use the `oclumon localrepo setconfig` command to change the configuration of local repository.

9.6.4.1 oclumon localrepo getconfig

Use the `oclumon localrepo getconfig` to get the configuration of repositories for all the nodes.

Syntax

```
oclumon localrepo getconfig [-reposize] [-repopath] [-retentiontime] [-local
| -n <node1> ...]
```

Parameters

Parameter	Description
`-reposize`	Gets the repository size in MB.
`-repopath`	Gets the repository path.
`-retentiontime`	Gets an estimation of local repository retention in time units based on the historical data of the currently configured repository size.
`-local`	Gets the configuration only for the local node.
`-n`	Gets the configuration for a desired list of nodes.

Example 9-143 To view full configuration of repositories for all nodes

```
oclumon localrepo getconfig
Node: <node-name1>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name1>/crf/db/json
Repository retention time: 246 Hours

Node: <node-name2>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name2>/crf/db/json
Repository retention time: 240 Hours
```

Example 9-144 To view only the repository path and size of repositories in all nodes

```
oclumon localrepo getconfig -reposize -repopath
Node: <node-name1>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name1>/crf/db/json

Node: <node-name2>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name2>/crf/db/json
```

Example 9-145 To view full configuration of the repository for the local node

```
oclumon localrepo getconfig -local
Node: <node-name>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name>/crf/db/json
Repository retention time: 246 Hours
```

Example 9-146 To view full configuration for the repositories on specific nodes <node-name1> and <node-name2>

```
oclumon localrepo getconfig -n <node-name1> <node-name2>
Node: <node-name1>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name1>/crf/db/json
Repository retention time: 246 Hours

Node: <node-name2>
Repository size: 500 MB
Repository path: $ORACLE_HOME/crsdata/<node-name2>/crf/db/json
Repository retention time: 240 Hours
```

9.6.4.2 oclumon localrepo setconfig

Use the `oclumon localrepo setconfig` command to change the configuration of local repository.

Syntax

```
oclumon localrepo setconfig -reposize <size>
```

Where, `setconfig` sets the repository size in MB for all the nodes.

Example 9-147 To set the repository size for all the nodes

```
oclumon localrepo setconfig -reposize 200
json dump log event is sent successfully on <node-name1>
json dump log event is sent successfully on <node-name2>
```

9.6.5 oclumon version

Use the `oclumon version` command to obtain the version of Cluster Health Monitor that you are using.

Syntax

```
oclumon version
```

Example 9-148 oclumon version

This command produces output similar to the following:

```
Cluster Health Monitor (OS), Release 20.0.0.0.0
Version : 20.3.0.0.0
```

9.6.6 oclumon debug

Use the `oclumon debug` command to set the log level for the Cluster Health Monitor services.

Syntax

```
oclumon debug [log daemon module:log_level] [version]
```

Parameters

Table 9-147 oclumon debug Command Parameters

Parameter	Description

`log daemon module:log_level`	Use this option change the log level of daemons and daemon modules.
	Supported daemons are:
	`osysmond`
	`client`
	`all`
	Supported daemon modules are:
	`osysmond`: `CRFMOND`, `CRFM`, and `allcomp`
	`client`: `OCLUMON`, `CRFM`, and `allcomp`
	`all`: `allcomp`
	Supported *log_level* values are `0`, `1`, `2`, and `3`.
	Where level 0 is lowest default level with minimal logging and level 3 is highest level with maximum logging.

`version`	Use this option to display the versions of the daemons.

Example 9-149 oclumon debug

The following example sets the log level of the system monitor service (`osysmond`):

```
$ oclumon debug log osysmond CRFMOND:3
```

The following example displays the versions of the daemons:

```
$ oclumon debug version

Cluster Health Monitor (OS), Release 20.0.0.0.0
Version            : 20.3.0.0.0
NODEVIEW Version   : 19.03
Label Date         : 200116
```

9.7 Querying Cluster Resource Activity Log

Oracle Clusterware stores logs about resource state changes in the cluster resource activity log.

Failures can occur as a result of a problem with a resource, a hosting node, or the network.

The cluster resource activity log provides precise and specific information about a resource failure, separate from diagnostic logs. The cluster resource activity log also provides a unified view of the cause of resource failure.

Use the following commands to view the contents of the cluster resource activity log:

- crsctl query calog
  Query the cluster resource activity logs matching specific criteria.

9.7.1 crsctl query calog

Query the cluster resource activity logs matching specific criteria.

Syntax

```
crsctl query calog
[-aftertime "timestamp"]
[-beforetime "timestamp"]
[-days "number_of_days"]
[-duration "time_interval" | -follow]
[-filter "filter_expression"]
[-processname "writer_process"]
[-processid "writer_process_id"]
[-node "entity_hostname"]
[-fullfmt | -xmlfmt]
```

Parameters

Table 9-148 crsctl query calog Command Parameters

Parameter	Description
`-aftertime "timestamp"`	Displays the activities logged after a specific time. Specify the timestamp in the `YYYY-MM-DD HH24:MI:SS[.FF][TZH:TZM]` or `YYYY-MM-DD` or `YYYY-MM` or `YYYY` or `HH24:MI:SS[.FF][TZH:TZM]` format. `TZH` and `TZM` stands for time zone hour and minute, and `FF` stands for microseconds. If you specify `[TZH:TZM]`, then the `crsctl` command assumes UTC as time zone. If you do not specify `[TZH:TZM]`, then the `crsctl` command assumes the local time zone of the cluster node from where the `crsctl` command is run. Use this parameter with `-beforetime` to query the activities logged at a specific time interval.
`-beforetime "timestamp"`	Displays the activities logged before a specific time. Specify the timestamp in the `YYYY-MM-DD HH24:MI:SS[.FF][TZH:TZM]` or `YYYY-MM-DD` or `YYYY-MM` or `YYYY` or `HH24:MI:SS[.FF][TZH:TZM]` format. `TZH` and `TZM` stands for time zone hour and minute, and `FF` stands for microseconds. If you specify `[TZH:TZM]`, then the `crsctl` command assumes UTC as time zone. If you do not specify `[TZH:TZM]`, then the `crsctl` command assumes the local time zone of the cluster node from where the `crsctl` command is run. Use this parameter with `-aftertime` to query the activities logged at a specific time interval.

Table 9-148 (Cont.) crsctl query calog Command Parameters

Parameter	Description
`-days "number_of_days"`	Displays the activities logged in the last number of days specified. The number of days are specified as an integer value.
`-duration "time_interval" | -follow`	Use `-duration` to specify a time interval that you want to query when you use the `-aftertime` parameter. Specify the timestamp in the `DD HH:MM:SS` format. Use `-follow` to display a continuous stream of activities as they occur.
`-filter "filter_expression"`	Query any number of fields in the cluster resource activity log using the `-filter` parameter. To specify multiple filters, use a comma-delimited list of filter expressions surrounded by double quotation marks (`""`).
`-processname "writer_process"`	Displays the activities logged by a specific process identified by name.
`-processid "writer_process_id"`	Displays the activities logged by a specific process identified by ID.
`-node "entity_hostname"`	Displays the activities logged by a specific host.
`-fullfmt | -xmlfmt`	To display cluster resource activity log data, choose full or XML format.

Cluster Resource Activity Log Fields

Query any number of fields in the cluster resource activity log using the `-filter` parameter.

Table 9-149 Cluster Resource Activity Log Fields

Field	Description	Use Case
`timestamp`	The time when the cluster resource activities were logged.	Use this filter to query all the activities logged at a specific time. This is an alternative to `-aftertime`, `-beforetime`, and `-duration` command parameters.
`writer_process_id`	The ID of the process that is writing to the cluster resource activity log.	Query only the activities spawned by a specific process.
`writer_process_name`	The name of the process that is writing to the cluster resource activity log.	When you query a specific process, CRSCTL returns all the activities for a specific process.
`writer_user`	The name of the user who is writing to the cluster resource activity log.	Query all the activities written by a specific user.
`writer_group`	The name of the group to which a user belongs who is writing to the cluster resource activity log.	Query all the activities written by users belonging to a specific user group.
`writer_hostname`	The name of the host on which the cluster resource activity log is written.	Query all the activities written by a specific host.

Table 9-149 (Cont.) Cluster Resource Activity Log Fields

Field	Description	Use Case
`writer_clustername`	The name of the cluster on which the cluster resource activity log is written.	Query all the activities written by a specific cluster.
`nls_product`	The product of the NLS message, for example, `CRS`, `ORA`, or `srvm`.	Query all the activities that have a specific product name.
`nls_facility`	The facility of the NLS message, for example, `CRS` or `PROC`.	Query all the activities that have a specific facility name.
`nls_id`	The ID of the NLS message, for example *42008*.	Query all the activities that have a specific message ID.
`nls_field_count`	The number of fields in the NLS message.	Query all the activities that correspond to NLS messages with more than, less than, or equal to `nls_field_count` command parameters.
`nls_field1`	The first field of the NLS message.	Query all the activities that match the first parameter of an NLS message.
`nls_field1_type`	The type of the first field in the NLS message.	Query all the activities that match a specific type of the first parameter of an NLS message.
`nls_format`	The format of the NLS message, for example, `Resource '%s' has been modified`.	Query all the activities that match a specific format of an NLS message.
`nls_message`	The entire NLS message that was written to the cluster resource activity log, for example, `Resource 'ora.cvu' has been modified`.	Query all the activities that match a specific NLS message.
`actid`	The unique activity ID of every cluster activity log.	Query all the activities that match a specific ID. Also, specify only partial `actid` and list all activities where the `actid` is a subset of the activity ID.
`is_planned`	Confirms if the activity is planned or not. For example, if a user issues the command `crsctl stop crs` on a node, then the stack stops and resources bounce. Running the `crsctl stop crs` command generates activities and logged in the `calog`. Since this is a planned action, the `is_planned` field is set to true (1). Otherwise, the `is_planned` field is set to false (0).	Query all the planned or unplanned activities.

Table 9-149 (Cont.) Cluster Resource Activity Log Fields

Field	Description	Use Case
`onbehalfof_user`	The name of the user on behalf of whom the cluster activity log is written.	Query all the activities written on behalf of a specific user.
`entity_isoraentity`	Confirms if the entity for which the calog activities are being logged is an oracle entity or not. If a resource, such as `ora.***`, is started or stopped, for example, then all those activities are logged in the cluster resource activity log. Since `ora.***` is an Oracle entity, the `entity_isoraentity` field is set to true (1). Otherwise the `entity_isoraentity` field is set to false (0).	Query all the activities logged by Oracle or non-Oracle entities.
`entity_type`	The type of the entity, such as *server*, for which the cluster activity log is written. Entity types that can be used to filter activities • `resource` • `resource_type` • `resource_group` • `server_category` • `ohasd` - activities generated by `ohasd` and resources it manages • `crsd` - activities generated by `crsd` and resources it manages In addition, GI components can choose to use their own names for entities when they write to activity log.	Query all the activities that match a specific entity.
`entity_name`	The name of the entity, for example, *foo* for which the cluster activity log is written.	Query all the cluster activities that match a specific entity name.
`entity_hostname`	The name of the host, for example, `node1`, associated with the entity for which the cluster activity log is written.	Query all the cluster activities that match a specific host name.
`entity_clustername`	The name of the cluster, for example, *cluster1* associated with the entity for which the cluster activity log is written.	Query all the cluster activities that match a specific cluster name. .

Usage Notes

- Combine simple filters into expressions called expression filters using Boolean operators.
- Enclose timestamps and time intervals in double quotation marks ("").
- Enclose the filter expressions in double quotation marks ("").
- Enclose the values that contain parentheses or spaces in single quotation marks ('').
- If no matching records are found, then the Oracle Clusterware Control (CRSCTL) utility displays the following message:

  ```
  CRS-40002: No activities match the query.
  ```

Examples

Examples of filters include:

- `"writer_user==root"`: Limits the display to only root user.
- `"customer_data=='GEN_RESTART@SERVERNAME(rwsbi08)=StartCompleted~'"`: Limits the display to `customer_data` that has the specified value `GEN_RESTART@SERVERNAME(node1)=StartCompleted~`.

To query all the resource activities and display the output in full format:

```
$ crsctl query calog -fullfmt

----ACTIVITY START----
timestamp                : 2016-09-27 17:55:43.152000
writer_process_id        : 6538
writer_process_name      : crsd.bin
writer_user              : root
writer_group             : root
writer_hostname          : node1
writer_clustername       : cluster1-mb1
customer_data            : CHECK_RESULTS=-408040060~
nls_product              : CRS
nls_facility             : CRS
nls_id                   : 2938
nls_field_count          : 1
nls_field1               : ora.cvu
nls_field1_type          : 25
nls_field1_len           : 0
nls_format               : Resource '%s' has been modified.
nls_message              : Resource 'ora.cvu' has been modified.
actid                    : 14732093665106538/1816699/1
is_planned               : 1
onbehalfof_user          : grid
onbehalfof_hostname      : node1
entity_isoraentity       : 1
entity_type              : resource
entity_name              : ora.cvu
entity_hostname          : node1
entity_clustername       : cluster1-mb1
```

```
nls_severity            : INFO
----ACTIVITY END----
```

To query all the resource activities and display the output in XML format:

```
$ crsctl query calog -xmlfmt

<?xml version="1.0" encoding="UTF-8"?>
<activities>
  <activity>
    <timestamp>2016-09-27 17:55:43.152000</timestamp>
    <writer_process_id>6538</writer_process_id>
    <writer_process_name>crsd.bin</writer_process_name>
    <writer_user>root</writer_user>
    <writer_group>root</writer_group>
    <writer_hostname>node1</writer_hostname>
    <writer_clustername>cluster1-mb1</writer_clustername>
    <customer_data>CHECK_RESULTS=-408040060~</customer_data>
    <nls_product>CRS</nls_product>
    <nls_facility>CRS</nls_facility>
    <nls_id>2938</nls_id>
    <nls_field_count>1</nls_field_count>
    <nls_field1>ora.cvu</nls_field1>
    <nls_field1_type>25</nls_field1_type>
    <nls_field1_len>0</nls_field1_len>
    <nls_format>Resource '%s' has been modified.</nls_format>
    <nls_message>Resource 'ora.cvu' has been modified.</nls_message>
    <actid>14732093665106538/1816699/1</actid>
    <is_planned>1</is_planned>
    <onbehalfof_user>grid</onbehalfof_user>
    <onbehalfof_hostname>node1</onbehalfof_hostname>
    <entity_isoraentity>1</entity_isoraentity>
    <entity_type>resource</entity_type>
    <entity_name>ora.cvu</entity_name>
    <entity_hostname>node1</entity_hostname>
    <entity_clustername>cluster1-mb1</entity_clustername>
    <nls_severity>INFO</nls_severity>
  </activity>
</activities>
```

To query resource activities for a two-hour interval after a specific time and display the output in XML format:

```
$ crsctl query calog -aftertime "2016-09-28 17:55:43" -duration "0 02:00:00"
-xmlfmt
<?xml version="1.0" encoding="UTF-8"?>
<activities>
  <activity>
    <timestamp>2016-09-28 17:55:45.992000</timestamp>
    <writer_process_id>6538</writer_process_id>
    <writer_process_name>crsd.bin</writer_process_name>
    <writer_user>root</writer_user>
    <writer_group>root</writer_group>
    <writer_hostname>node1</writer_hostname>
    <writer_clustername>cluster1-mb1</writer_clustername>
    <customer_data>CHECK_RESULTS=1718139884~</customer_data>
    <nls_product>CRS</nls_product>
    <nls_facility>CRS</nls_facility>
    <nls_id>2938</nls_id>
    <nls_field_count>1</nls_field_count>
    <nls_field1>ora.cvu</nls_field1>
    <nls_field1_type>25</nls_field1_type>
    <nls_field1_len>0</nls_field1_len>
    <nls_format>Resource '%s' has been modified.</nls_format>
    <nls_message>Resource 'ora.cvu' has been modified.</nls_message>
    <actid>14732093665106538/1942009/1</actid>
    <is_planned>1</is_planned>
    <onbehalfof_user>grid</onbehalfof_user>
    <onbehalfof_hostname>node1</onbehalfof_hostname>
    <entity_isoraentity>1</entity_isoraentity>
    <entity_type>resource</entity_type>
    <entity_name>ora.cvu</entity_name>
    <entity_hostname>node1</entity_hostname>
    <entity_clustername>cluster1-mb1</entity_clustername>
    <nls_severity>INFO</nls_severity>
  </activity>
</activities>
```

To query resource activities at a specific time:

```
$ crsctl query calog -filter "timestamp=='2016-09-28 17:55:45.992000'"

2016-09-28 17:55:45.992000 : node1 : INFO : Resource 'ora.cvu' has
been modified. : 14732093665106538/1942009/1 :
```

To query resource activities using filters `writer_user` and `customer_data`:

```
$ crsctl query calog -filter "writer_user==root AND
customer_data=='GEN_RESTART@SERVERNAME(node1)=StartCompleted~'" -
fullfmt
```

or

```
$ crsctl query calog -filter "(writer_user==root) AND
(customer_data=='GEN_RESTART@SERVERNAME(node1)=StartCompleted~')" -
fullfmt


----ACTIVITY START----
timestamp                : 2016-09-15 17:42:57.517000
writer_process_id        : 6538
writer_process_name      : crsd.bin
writer_user              : root
writer_group             : root
writer_hostname          : node1
writer_clustername       : cluster1-mb1
customer_data            :
```

```
GEN_RESTART@SERVERNAME(rwsbi08)=StartCompleted~
nls_product              : CRS
nls_facility             : CRS
nls_id                   : 2938
nls_field_count          : 1
nls_field1               : ora.testdb.db
nls_field1_type          : 25
nls_field1_len           : 0
nls_format               : Resource '%s' has been modified.
nls_message              : Resource 'ora.devdb.db' has been modified.
actid                    : 14732093665106538/659678/1
is_planned               : 1
onbehalfof_user          : oracle
onbehalfof_hostname      : node1
entity_isoraentity       : 1
entity_type              : resource
entity_name              : ora.testdb.db
entity_hostname          : node1
entity_clustername       : cluster1-mb1
nls_severity             : INFO
----ACTIVITY END----
```

To query all the calogs that were generated after UTC+08:00 time "2016-11-15 22:53:08":

```
$ crsctl query calog -aftertime "2016-11-15 22:53:08+08:00"
```

To query all the calogs that were generated after UTC-08:00 time "2016-11-15 22:53:08":

```
$ crsctl query calog -aftertime "2016-11-15 22:53:08-08:00"
```

To query all the calogs by specifying the timestamp with microseconds:

```
$ crsctl query calog -aftertime "2016-11-16 01:07:53.063000"
2016-11-16 01:07:53.558000 : node1 : INFO : Resource 'ora.cvu' has been
modified. : 14792791129816600/2580/7 :
2016-11-16 01:07:53.562000 : node2 : INFO : Clean of 'ora.cvu' on 'node2'
succeeded : 14792791129816600/2580/8 :
```

To query all the activities that were written by a specific process by name:

```
$  crsctl query calog -processname crsd.bin

2016-11-16 01:07:53.558000 : node1 : INFO : Resource 'ora.cvu' has been
modified. : 14792791129816600/2580/7 :
2016-11-16 01:07:53.562000 : node2 : INFO : Clean of 'ora.cvu' on 'node2'
succeeded : 14792791129816600/2580/8 :
```

To query all the activities that were written by a specific process by ID:

```
$ crsctl query calog -processid 6538

2016-11-16 01:07:53.558000 : node1 : INFO : Resource 'ora.cvu' has been
```

```
modified. : 14792791129816600/2580/7 :
2016-11-16 01:07:53.562000 : node2 : INFO : Clean of 'ora.cvu' on
'node2' succeeded : 14792791129816600/2580/8 :
```

To query all the activities that were written by a specific node:

```
$ crsctl query calog -node node2
2016-11-16 01:07:53.562000 : node2 : INFO : Clean of 'ora.cvu' on
'node2' succeeded : 14792791129816600/2580/8 :
```

9.8 chactl Command Reference

The Oracle Cluster Health Advisor commands enable the Oracle Grid Infrastructure user to administer basic monitoring functionality on the targets.

- chactl monitor
  Use the `chactl monitor` command to start monitoring all the instances of a specific Oracle Real Application Clusters (Oracle RAC) database using the current set model.
- chactl unmonitor
  Use the `chactl unmonitor` command to stop monitoring all the instances of a specific database.
- chactl status
  Use the `chactl status` command to check monitoring status of the running targets.
- chactl config
  Use the `chactl config` command to list all the targets being monitored, along with the current model of each target.
- chactl calibrate
  Use the `chactl calibrate` command to create a new model that has greater sensitivity and accuracy.
- chactl query diagnosis
  Use the `chactl query diagnosis` command to return problems and diagnosis, and suggested corrective actions associated with the problem for specific cluster nodes or Oracle Real Application Clusters (Oracle RAC) databases.
- chactl query model
  Use the `chactl query model` command to list all Oracle Cluster Health Advisor models or to view detailed information about a specific Oracle Cluster Health Advisor model.
- chactl query repository
  Use the `chactl query repository` command to view the maximum retention time, number of targets, and the size of the Oracle Cluster Health Advisor repository.
- chactl query calibration
  Use the `chactl query calibration` command to view detailed information about the calibration data of a specific target.

- chactl remove model
  Use the `chactl remove model` command to delete an Oracle Cluster Health Advisor model along with the calibration data and metadata of the model from the Oracle Cluster Health Advisor repository.
- chactl rename model
  Use the `chactl rename model` command to rename an Oracle Cluster Health Advisor model in the Oracle Cluster Health Advisor repository.
- chactl export model
  Use the `chactl export model` command to export Oracle Cluster Health Advisor models.
- chactl import model
  Use the `chactl import model` command to import Oracle Cluster Health Advisor models.
- chactl set maxretention
  Use the `chactl set maxretention` command to set the maximum retention time for the diagnostic data.
- chactl resize repository
  Use the `chactl resize repository` command to resize the tablespace of the Oracle Cluster Health Advisor repository based on the current retention time and the number of targets.

9.8.1 chactl monitor

Use the `chactl monitor` command to start monitoring all the instances of a specific Oracle Real Application Clusters (Oracle RAC) database using the current set model.

Oracle Cluster Health Advisor monitors all instances of this database using the same model assigned to the database.

Oracle Cluster Health Advisor uses Oracle-supplied gold model when you start monitoring a target for the first time. Oracle Cluster Health Advisor stores monitoring status of the target in the internal store. Oracle Cluster Health Advisor starts monitoring any new database instance when Oracle Cluster Health Advisor detects or redetects the new instance.

Syntax

```
chactl monitor database -db db_unique_name [-model model_name [-force]][-
help]


chactl monitor cluster [-model model_name [-force]]
```

Parameters

Table 9-150 chactl monitor Command Parameters

Parameter	Description
`db_unique_name`	Specify the name of the database.
`model_name`	Specify the name of the model.

Table 9-150   (Cont.) chactl monitor Command Parameters

Parameter	Description
`force`	Use the `-force` option to monitor with the specified model without stopping monitoring the target. Without the `-force` option, run `chactl unmonitor` first, and then `chactl monitor` with the model name.

Examples

- To monitor the *`SalesDB`* database using the *`BlkFridayShopping`* default model:

```
$ chactl monitor database -db SalesDB -model BlkFridayShopping
```

- To monitor the *`InventoryDB`* database using the *`Nov2014`* model:

```
$ chactl monitor database -db InventoryDB -model Nov2014
```

If you specify the *`model_name`*, then Oracle Cluster Health Advisor starts monitoring with the specified model and stores the model in the Oracle Cluster Health Advisor internal store.

If you use both the *`-model`* and *`-force`* options, then Oracle Cluster Health Advisor stops monitoring and restarts monitoring with the specified model.

- To monitor the *`SalesDB`* database using the *`Dec2014`* model:

```
$ chactl monitor database -db SalesDB -model Dec2014
```

- To monitor the *`InventoryDB`* database using the *`Dec2014`* model and the `-force` option:

```
$ chactl monitor database -db InventoryDB -model Dec2014 -force
```

Error Messages

Error: `no CHA resource is running in the cluster.`

Description: Returns when there is no hub or leaf node running the Oracle Cluster Health Advisor service.

Error: `the database is not configured.`

Description: Returns when the database is not found in either the Oracle Cluster Health Advisor configuration repository or as a CRS resource.

Error: `input string “xc#? %” is invalid.`

Description: Returns when the command-line cannot be parsed. Also displays the top-level help text.

Error: `CHA is already monitoring target <dbname>.`

Description: Returns when the database is already monitored.

9.8.2 chactl unmonitor

Use the `chactl unmonitor` command to stop monitoring all the instances of a specific database.

Syntax

```
chactl unmonitor database -db db_unique_name [-help]
```

Examples

To stop monitoring the *SalesDB* database:

```
$ chactl unmonitor database -db SalesDB
Database SalesDB is not monitored
```

9.8.3 chactl status

Use the `chactl status` command to check monitoring status of the running targets.

If you do not specify any parameters, then the `chactl status` command returns the status of all running targets.

The monitoring status of an Oracle Cluster Health Advisor target can be either `Monitoring` *or* `Not Monitoring`. The `chactl status` command shows four types of results and depends on whether you specify a target and `-verbose` option.

The `-verbose` option of the command also displays the monitoring status of targets contained within the specified target and the names of executing models of each printed target. The `chactl status` command displays targets with positive monitoring status only. The `chactl status` command displays negative monitoring status only when the corresponding target is explicitly specified on the command-line.

Syntax

```
chactl status {cluster|database [-db db_unique_name]} [-verbose][-help]
```

Examples

- To display the list of cluster nodes and databases being monitored:

  ```
  #chactl status
  Monitoring nodes rac1Node1, rac1Node2
  Monitoring databases SalesDB, HRdb
  ```

> **Note:**
>
> A database is displayed with **Monitoring** status, if Oracle Cluster Health Advisor is monitoring one or more of the instances of the database, even if some of the instances of the database are not running.

- To display the status of Oracle Cluster Health Advisor:

  ```
  $ chactl status
  Cluster Health Advisor service is offline.
  ```

  No target or the `-verbose` option is specified on the command-line. Oracle Cluster Health Advisor is not running on any node of the cluster.

- To display various Oracle Cluster Health Advisor monitoring states for cluster nodes and databases:

  ```
  $ chactl status database -db SalesDB
  Monitoring database SalesDB
  ```

  ```
  $ chactl status database -db bogusDB
  Not Monitoring database bogusDB
  ```

  ```
  $ chactl status cluster
  Monitoring nodes rac1,rac2
  Not Monitoring node rac3
  ```

  or

  ```
  $ chactl status cluster
  Cluster Health Advisor is offline
  ```

- To display the detailed Oracle Cluster Health Advisor monitoring status for the entire cluster:

  ```
  $ chactl status -verbose
  Monitoring node(s) racNd1, racNd2, racNd3, racNd4 using model
  MidSparc

  Monitoring database HRdb2, Instances HRdb2I1, HRdb2I2 in server
  pool SilverPool using model M6
  Monitoring database HRdb, Instances HRdbI4, HRdbI6 in server pool
  SilverPool using model M23
  Monitoring database testHR, Instances inst3 on node racN7 using
  model TestM13
  Monitoring database testHR, Instances inst4 on node racN8 using
  model TestM14
  ```

When the target is not specified and the `-verbose` option is specified, the `chactl status` command displays the status of the database instances and names of the models.

9.8.4 chactl config

Use the `chactl config` command to list all the targets being monitored, along with the current model of each target.

If the specified target is a multitenant container database (CDB) or a cluster, then the `chactl config` command also displays the configuration data status.

Syntax

```
chactl config {cluster|database -db db_unique_name}[-help]
```

Examples

To display the monitor configuration and the specified model of each target:

```
$ chactl config
Databases monitored: prodDB, hrDB


$ chactl config database -db prodDB
Monitor: Enabled
Model: GoldDB


$ chactl config cluster
Monitor: Enabled
Model: DEFAULT_CLUSTER
```

9.8.5 chactl calibrate

Use the `chactl calibrate` command to create a new model that has greater sensitivity and accuracy.

The user-generated models are effective for Oracle Real Application Clusters (Oracle RAC) monitored systems in your operating environment as the user-generated models use calibration data from the target. Oracle Cluster Health Advisor adds the user-generated model to the list of available models and stores the new model in the Oracle Cluster Health Advisor repository.

If a model with the same name exists, then overwrite the old model with the new one by using the `-force` option.

Key Performance and Workload Indicators

A set of metrics or Key Performance Indicators describe high-level constraints to the training data selected for calibration. This set consists of relevant metrics to describe performance goals and resource utilization bandwidth, for example, response times or CPU utilization.

The Key Performance Indicators are also operating system and database signals which are monitored, estimated, and associated with fault detection logic. Most of these Key

Performance Indicators are also either predictors, that is, their state is correlated with the state of other signals, or predicted by other signals. The fact that the Key Performance Indicators correlate with other signals makes them useful as filters for the training or calibration data.

The Key Performance Indicators ranges are used in the `query calibrate` and `calibrate` commands to filter out data points.

The following Key Performance Indicators are supported for database:

- `CPUPERCENT` - CPU utilization - Percent
- `IOREAD` - Disk read - Mbyte/sec
- `DBTIMEPERCALL` - Database time per user call - usec/call
- `IOWRITE` - Disk write - Mbyte/sec
- `IOTHROUGHPUT` - Disk throughput - IO/sec

The following Key Performance Indicators are supported for cluster:

- `CPUPERCENT` - CPU utilization - Percent
- `IOREAD` - Disk read - Mbyte/sec
- `IOWRITE` - Disk write - Mbyte/sec
- `IOTHROUGHPUT` - Disk throughput - IO/sec

Syntax

```
chactl calibrate {cluster|database -db db_unique_name} -model
model_name
[-force] [-timeranges 'start=time_stamp,end=time_stamp,...']
[-kpiset 'name=kpi_name min=val max=val,...' ][-help]
```

Specify timestamp in the `YYYY-MM-DD HH24:MI:SS` format.

Examples

```
chactl calibrate database -db oracle -model weekday
-timeranges 'start=start=2016-09-09 16:00:00,end=2016-09-09 23:00:00'
```

```
chactl calibrate database -db oracle -model weekday
-timeranges 'start=start=2016-09-09 16:00:00,end=2016-09-09 23:00:00'
-kpiset 'name=CPUPERCENT min=10 max=60'
```

Error Messages

Error: `input string “xc#? %” is misconstructed`

Description: Confirm if the given model name exists with `Warning: `*`model_name`*` already exists, please use [-force]` message.

Error: *`start_time`*` and/or `*`end_time`*` are misconstructed`

Description: Input time specifiers are badly constructed.

Error: `no sufficient calibration data exists for the specified period, please reselect another period`

Description: Evaluator couldn’t find enough calibration data.

9.8.6 chactl query diagnosis

Use the `chactl query diagnosis` command to return problems and diagnosis, and suggested corrective actions associated with the problem for specific cluster nodes or Oracle Real Application Clusters (Oracle RAC) databases.

Syntax

```
chactl query diagnosis [-cluster|-db db_unique_name] [-start time -end time]
[-htmlfile file_name][-help]
```

Specify date and time in the `YYYY-MM-DD HH24:MI:SS` format.

In the preceding syntax, you must consider the following points:

- If you do not provide any options, then the `chactl query diagnosis` command returns the current state of all monitored nodes and databases. The `chactl query diagnosis` command reports general state of the targets, for example, **ABNORMAL** by showing their diagnostic identifier, for example, `Storage Bandwidth Saturation`. This is a quick way to check for any **ABNORMAL** state in a database or cluster.
- If you provide a time option after the target name, then the `chactl query diagnosis` command returns the state of the specified target restricted to the conditions in the time interval specified. The compressed time series lists the identifiers of the causes for distinct incidents which occurred in the time interval, its start and end time.
- If an incident and cause recur in a specific time interval, then the problem is reported only once. The start time is the start time of the first occurrence of the incident and the end time is the end time of the last occurrence of the incident in the particular time interval.
- If you specify the `-db` option without a database name, then the `chactl query diagnosis` command displays diagnostic information for all databases. However, if a database name is specified, then the `chactl query diagnosis` command displays diagnostic information for all instances of the database that are being monitored.
- If you specify the `-cluster` option without a host name, then the `chactl query diagnosis` command displays diagnostic information for all hosts in that cluster.
- If you do not specify a time interval, then the `chactl query diagnosis` command displays only the current issues for all or the specified targets. The `chactl query diagnosis` command does not display the frequency statistics explicitly. However, you can count the number of normal and abnormal events that occurred in a target in the last 24 hours.
- If no incidents have occurred during the specified time interval, then the `chactl query diagnosis` command returns a text message, for example, `Database/host is operating NORMALLY`, or `no incidents were found`.
- If the state of a target is **NORMAL**, the command does not report it. The `chactl query diagnosis` command reports only the targets with **ABNORMAL** state for the specified time interval.

Output parameters:

- Incident start Time
- Incident end time (only for the default database and/or host, non-verbose output)
- Target (for example, database, host)
- Problem

  Description: Detailed description of the problem

  Cause: Root cause of the problem and contributing factors
- Action: an action that corrects the abnormal state covered in the diagnosis

Reporting Format: The diagnostic information is displayed in a time compressed or time series order, grouped by components.

Examples

To display diagnostic information of a database for a specific time interval:

```
$ chactl query diagnosis -db oltpacdb -start "2016-02-01 02:52:50.0" -
end "2016-02-01 03:19:15.0"
2016-02-01 01:47:10.0  Database oltpacdb  DB Control File IO
Performance (oltpacdb_1) [detected]
2016-02-01 01:47:10.0  Database oltpacdb  DB Control File IO
Performance (oltpacdb_2) [detected]
2016-02-01 02:52:15.0  Database oltpacdb  DB CPU Utilization
(oltpacdb_2) [detected]
2016-02-01 02:52:50.0  Database oltpacdb  DB CPU Utilization
(oltpacdb_1) [detected]
2016-02-01 02:59:35.0  Database oltpacdb  DB Log File Switch
(oltpacdb_1) [detected]
2016-02-01 02:59:45.0  Database oltpacdb  DB Log File Switch
(oltpacdb_2) [detected]

Problem: DB Control File IO Performance
Description: CHA has detected that reads or writes to the control
files are slower than expected.
Cause: The Cluster Health Advisor (CHA) detected that reads or writes
to the control files were slow
because of an increase in disk IO.
The slow control file reads and writes may have an impact on
checkpoint and Log Writer (LGWR) performance.
Action: Separate the control files from other database files and move
them to faster disks or Solid State Devices.

Problem: DB CPU Utilization
Description: CHA detected larger than expected CPU utilization for
this database.
Cause: The Cluster Health Advisor (CHA) detected an increase in
database CPU utilization
because of an increase in the database workload.
Action: Identify the CPU intensive queries by using the Automatic
Diagnostic and Defect Manager (ADDM)
and follow the recommendations given there. Limit the number of CPU
intensive queries
or relocate sessions to less busymachines. Add CPUs if the CPU
capacity is insufficent to support the load
```

```
without a performance degradation or effects on other databases.

Problem: DB Log File Switch
Description: CHA detected that database sessions are waiting longer than
expected for log switch completions.
Cause: The Cluster Health Advisor (CHA) detected high contention during log
switches
because the redo log files were small and the redo logs switched frequently.
Action: Increase the size of the redo logs.
```

Error Message

Message: `*Target* is operating normally`

Description: No incidents are found on the target.

Message: `No data was found for active *Target*`

Description: No data was found, but the target was operating or active at the time of the query.

Message: `Target is not active or was not being monitored.`

Description: No data was found because the target was not monitored at the time of the query.

9.8.7 chactl query model

Use the `chactl query model` command to list all Oracle Cluster Health Advisor models or to view detailed information about a specific Oracle Cluster Health Advisor model.

Syntax

```
chactl query model [-name model_name [-verbose]][-help]
```

Examples

- To list all base Oracle Cluster Health Advisor models:

  ```
  $ chactl query model
  Models: MOD1, MOD2, MOD3, MOD4, MOD5, MOD6, MOD7


  $ chactl query model -name weekday
  Model: weekday
  Target Type: DATABASE
  Version: 12.2.0.1_0
  OS Calibrated on: Linux amd64
  Calibration Target Name: prod
  Calibration Date: 2016-09-10 12:59:49
  Calibration Time Ranges: start=2016-09-09 16:00:00,end=2016-09-09 23:00:00
  Calibration KPIs: not specified
  ```

- To view detailed information, including calibration metadata, about the specific Oracle Cluster Health Advisor model:

  ```
  $ chactl query model -name MOD5 -verbose
  Model: MOD5
  CREATION_DATE:          Jan 10,2016 10:10
  VALIDATION_STATUS:      Validated
  DATA_FROM_TARGET :      inst72, inst75
  USED_IN_TARGET :        inst76, inst75, prodDB, evalDB-evalSP
  CAL_DATA_FROM_DATE:     Jan 05,2016 10:00
  CAL_DATA_TO_DATE:       Jan 07,2016 13:00
  CAL_DATA_FROM_TARGETS   inst73, inst75
  ...
  ```

9.8.8 chactl query repository

Use the `chactl query repository` command to view the maximum retention time, number of targets, and the size of the Oracle Cluster Health Advisor repository.

> **Note:**
>
> Applicable only if GIMR is configured. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.

Syntax

```
chactl query repository [-help]
```

Examples

To view information about the Oracle Cluster Health Advisor repository:

```
$ chactl query repository
specified max retention time(hrs) : 72
available retention time(hrs)     : 212
available number of entities      : 2
allocated number of entities      : 0
total repository size(gb)         : 2.00
allocated repository size(gb)     : 0.07
```

9.8.9 chactl query calibration

Use the `chactl query calibration` command to view detailed information about the calibration data of a specific target.

Syntax

> **Note:**
>
> Applicable only if GIMR is configured. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.

```
chactl query calibration {-cluster|-db db_unique_name} [-timeranges
'start=time_stamp,end=time_stamp,...'] [-kpiset 'name=kpi_name min=val
max=val,...' ] [-interval val][-help]
```

Specify the interval in hours.

Specify date and time in the `YYYY-MM-DD HH24:MI:SS` format.

> **Note:**
>
> If you do not specify a time interval, then the `chactl query calibration` command displays all the calibration data collected for a specific target.

The following Key Performance Indicators are supported for database:

- `CPUPERCENT` - CPU utilization - Percent
- `IOREAD` - Disk read - Mbyte/sec
- `DBTIMEPERCALL` - Database time per user call - usec/call
- `IOWRITE` - Disk write - Mbyte/sec
- `IOTHROUGHPUT` - Disk throughput - IO/sec

The following Key Performance Indicators are supported for cluster:

- `CPUPERCENT` - CPU utilization - Percent
- `IOREAD` - Disk read - Mbyte/sec
- `IOWRITE` - Disk write - Mbyte/sec
- `IOTHROUGHPUT` - Disk throughput - IO/sec

Examples

To view detailed information about the calibration data of the specified target:

```
$ chactl query calibration -db oltpacdb -timeranges
'start=2016-07-26 01:00:00,end=2016-07-26 02:00:00,start=2016-07-26
03:00:00,end=2016-07-26 04:00:00'
-kpiset 'name=CPUPERCENT min=20 max=40, name=IOTHROUGHPUT min=500 max=9000' -
interval 2

Database name : oltpacdb
```

```
Start time : 2016-07-26 01:03:10
End time : 2016-07-26 01:57:25
Total Samples : 120
Percentage of filtered data : 8.32%
The number of data samples may not be sufficient for calibration.

1) Disk read (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
4.96      0.20      8.98      0.06      25.68

<25       <50       <75       <100      >=100
97.50%    2.50%     0.00%     0.00%     0.00%

2) Disk write (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
27.73     9.72      31.75     4.16      109.39

<50       <100      <150      <200      >=200
73.33%    22.50%    4.17%     0.00%     0.00%

3) Disk throughput (ASM) (IO/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
2407.50   1500.00   1978.55   700.00    7800.00

<5000     <10000    <15000    <20000    >=20000
83.33%    16.67%    0.00%     0.00%     0.00%

4) CPU utilization (total) (%)

MEAN      MEDIAN    STDDEV    MIN       MAX
21.99     21.75     1.36      20.00     26.80

<20       <40       <60       <80       >=80
0.00%     100.00%   0.00%     0.00%     0.00%

5) Database time per user call (usec/call)

MEAN      MEDIAN    STDDEV    MIN       MAX
267.39    264.87    32.05     205.80    484.57

<10000000  <20000000  <30000000  <40000000  <50000000  <60000000
<70000000  >=70000000
100.00%   0.00%     0.00%     0.00%     0.00%     0.00%     0.00%
0.00%

Database name : oltpacdb
Start time : 2016-07-26 03:00:00
End time : 2016-07-26 03:53:30
Total Samples : 342
Percentage of filtered data : 23.72%
The number of data samples may not be sufficient for calibration.
```

```
1) Disk read (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
12.18     0.28      16.07     0.05      60.98

<25       <50       <75       <100      >=100
64.33%    34.50%    1.17%     0.00%     0.00%

2) Disk write (ASM) (Mbyte/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
57.57     51.14     34.12     16.10     135.29

<50       <100      <150      <200      >=200
49.12%    38.30%    12.57%    0.00%     0.00%

3) Disk throughput (ASM) (IO/sec)

MEAN      MEDIAN    STDDEV    MIN       MAX
5048.83   4300.00   1730.17   2700.00   9000.00

<5000     <10000    <15000    <20000    >=20000
63.74%    36.26%    0.00%     0.00%     0.00%

4) CPU utilization (total) (%)

MEAN      MEDIAN    STDDEV    MIN       MAX
23.10     22.80     1.88      20.00     31.40

<20       <40       <60       <80       >=80
0.00%     100.00%   0.00%     0.00%     0.00%

5) Database time per user call (usec/call)

MEAN      MEDIAN    STDDEV    MIN       MAX
744.39    256.47    2892.71   211.45    45438.35

<10000000  <20000000  <30000000  <40000000  <50000000  <60000000  <70000000
>=70000000
100.00%   0.00%     0.00%     0.00%     0.00%     0.00%     0.00%     0.00%
```

9.8.10 chactl remove model

Use the `chactl remove model` command to delete an Oracle Cluster Health Advisor model along with the calibration data and metadata of the model from the Oracle Cluster Health Advisor repository.

Note:

If the model is being used to monitor the targets, then the `chactl remove model` command cannot delete any model.

Syntax

```
chactl remove model -name model_name [-help]
```

Error Message

Error: *model_name* does not exist

Description: The specified Oracle Cluster Health Advisor model does not exist in the Oracle Cluster Health Advisor repository.

9.8.11 chactl rename model

Use the `chactl rename model` command to rename an Oracle Cluster Health Advisor model in the Oracle Cluster Health Advisor repository.

Assign a descriptive and unique name to the model. Oracle Cluster Health Advisor preserves all the links related to the renamed model.

Syntax

```
chactl rename model -from model_name -to model_name [-help]
```

Error Messages

Error: *model_name* does not exist

Description: The specified model name does not exist in the Oracle Cluster Health Advisor repository.

Error: *dest_name* already exist

Description: The specified model name already exists in the Oracle Cluster Health Advisor repository.

9.8.12 chactl export model

Use the `chactl export model` command to export Oracle Cluster Health Advisor models.

Syntax

> **Note:**
>
> Applicable only if GIMR is configured. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.

```
chactl export model -name model_name -file output_file [-help]
```

Example

```
$ chactl export model -name weekday -file /tmp//weekday.mod
```

9.8.13 chactl import model

Use the `chactl import model` command to import Oracle Cluster Health Advisor models.

Syntax

> **Note:**
>
> Applicable only if GIMR is configured. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.

```
chactl import model -name model_name -file model_file [-force] [-help]
```

While importing, if there is an existing model with the same name as the model being imported, then use the `-force` option to overwrite.

Example 9-150 Example

```
$ chactl import model -name weekday -file /tmp//weekday.mod
```

9.8.14 chactl set maxretention

Use the `chactl set maxretention` command to set the maximum retention time for the diagnostic data.

The default and minimum retention time is 72 hours. If the Oracle Cluster Health Advisor repository does not have enough space, then the retention time is decreased for all the targets.

> **Note:**
>
> Oracle Cluster Health Advisor stops monitoring if the retention time is less than 24 hours.

Syntax

```
chactl set maxretention -time retention_time [-help]
```

Specify the retention time in hours.

Examples

To set the maximum retention time to 80 hours:

```
$ chactl set maxretention -time 80
max retention successfully set to 80 hours
```

Error Message

Error: `Specified time is smaller than the allowed minimum`

Description: This message is returned if the input value for maximum retention time is smaller than the minimum value.

9.8.15 chactl resize repository

Use the `chactl resize repository` command to resize the tablespace of the Oracle Cluster Health Advisor repository based on the current retention time and the number of targets.

> **Note:**
>
> - Applicable only if GIMR is configured. GIMR is optionally supported in Oracle Database 19c. However, it's desupported in Oracle Database 23c.
> - The `chactl resize repository` command fails if your system does not have enough free disk space or if the tablespace contains data beyond requested resize value.

Syntax

```
chactl resize repository -entities total number of hosts and database
instances [-force | -eval] [-help]
```

Examples

To set the number of targets in the tablespace to 32:

```
chactl resize repository -entities 32
repository successfully resized for 32 targets
```

10 Behavior Changes, Deprecated and Desupported Features

Review information about changes, deprecations, and desupports.

- Oracle E-Business Suite (EBS) Support is Deprecated in Release 18.3.0
  Starting with 18.3.0 release, the Oracle Orachk and Oracle Exachk checks for EBS feature has been deprecated.
- Deprecated tfactl Upload Commands in Release 20.2
  Starting with 20.2 release, the following `tfactl upload` commands have been deprecated.
- Deprecated SRDCs in Release 20.2
  Starting with 20.2 release, SRDCs `dbdataguard` and `dbblockcorruption` have been deprecated.
- Deprecated tfactl Commands in Release 21.1
  Starting with the 21.1 release, all AHF functionalities that are available in `tfactl` command-line interface have been deprecated and will completely be removed in the 22.1 release.
- Deprecated Oracle Orachk and Oracle Exachk Commands to Manage Patches in Release 21.1
  Starting with the 21.1 release, Oracle Orachk and Oracle Exachk commands to manage patches have been deprecated and these commands will be completely removed in the 22.1 release.
- Deprecated Oracle Trace File Analyzer Utilities in Release 21.1
  Oracle Trace File Analyzer Utilities `summary` and `dbcheck` will be removed and replaced with new command-line with enhanced functionality.
- Deprecated Oracle Trace File Analyzer Receiver in Release 21.1
  Starting with 21.1 release, Oracle Trace File Analyzer Receiver has been deprecated and being replaced by enhanced Oracle AHF Collections Manager.
- Deprecated tfactl Commands in Release 22.1.0
  Starting with 22.1.0 release, the following tfactl upload commands have been deprecated and removed.
- Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands in 22.2
  Starting with the AHF 22.2 (2022-09-14), commands to run the Oracle Orachk or Oracle Exachk scheduler without the Oracle Trace File Analyzer daemon are deprecated. These commands are completely removed in AHF 23.8 (2023-08-28).
- Deprecated ahfctl Commands in Release 23.1.0
  Starting with the 23.1.0 release, the `ahfctl applypatch`, `ahfctl querypatch`, and `ahfctl rollbackpatch` commands have been deprecated and completely be removed.
- Deprecated AHF REST Services
  AHF REST is deprecated and will be desupported in AHF release 24.3.0.

- Deprecated Oracle Trace File Analyzer Masking in Release 24.1
  Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release.
- Oracle Database Quality of Service (QoS) Management is Deprecated in Release 21c
  Starting in Oracle Database release 21c, Oracle Database Quality of Service (QoS) Management is deprecated and will be desupported in a future release.

10.1 Oracle E-Business Suite (EBS) Support is Deprecated in Release 18.3.0

Starting with 18.3.0 release, the Oracle Orachk and Oracle Exachk checks for EBS feature has been deprecated.

Deprecating Oracle E-Business Suite (EBS) checks means that running health checks against EBS feature is no longer enhanced, but it is still supported until the Oracle Orachk and Oracle Exachk 19.3.0 release (approximately one year).

In the Oracle Orachk and Oracle Exachk 19.3.0 release, the EBS checks feature will be desupported, meaning Oracle will no longer fix bugs in Oracle Orachk and Oracle Exachk related to EBS checks, and the EBS checking feature will be removed altogether.

Run all EBS health checks using the EBS Analyzers, which is available at My Oracle Support note 1545562.1.

Related Topics

- https://support.oracle.com/rs?type=doc&id=1545562.1

10.2 Deprecated tfactl Upload Commands in Release 20.2

Starting with 20.2 release, the following `tfactl upload` commands have been deprecated.

- Upload Using Wallet: `tfactl upload -sr` *`SR#`* `-wallet` *`Space separated list of files to upload`*
- Upload without Wallet: `tfactl upload -sr` *`SR#`* `-user` *`UserId Space separated list of files to upload`*
- `tfactl setupmos`
- `tfactl setmosupload`
- `tfactl getmosupload`
- `tfactl unsetmosupload`
- `tfactl checkmosupload`
- `tfactl setdbupload`
- `tfactl getdbupload`
- `tfactl unsetdbupload`

- `tfactl checkdbupload`

Oracle recommends using the new generic upload mechanism.

Related Topics

- Diagnostic Upload
  Diagnostic upload eliminates the need for different set of commands to upload Oracle ORAchk, Oracle EXAchk, and Oracle Trace File Analyzer diagnostic collections to AHF Service, database, and Oracle Support.

10.3 Deprecated SRDCs in Release 20.2

Starting with 20.2 release, SRDCs `dbdataguard` and `dbblockcorruption` have been deprecated.

10.4 Deprecated tfactl Commands in Release 21.1

Starting with the 21.1 release, all AHF functionalities that are available in `tfactl` command-line interface have been deprecated and will completely be removed in the 22.1 release.

Oracle recommends using `ahfctl` to perform AHF functionalities instead of `tfactl`.

Deprecated `tfactl` commands:

- `compliance`
- `celldiagcollect`
- `applypatch`
- `querypatch`
- `rollbackpatch`
- `startahf`
- `stopahf`
- `statusahf`
- `showrepo`
- `import`
- `unset`
- `setupload`
- `getupload`
- `unsetupload`
- `checkupload`
- `setpassword`
- `unsetpassword`
- `checkpassword`
- `upgrade`
- `setupgrade`

- `unsetupgrade`
- `getupgrade`
- `setresourcelimit`
- `getresourcelimit`
- `unsetresourcelimit`
- `printresourcestats`
- `setserviceupload`
- `getserviceupload`
- `unsetserviceupload`

10.5 Deprecated Oracle Orachk and Oracle Exachk Commands to Manage Patches in Release 21.1

Starting with the 21.1 release, Oracle Orachk and Oracle Exachk commands to manage patches have been deprecated and these commands will be completely removed in the 22.1 release.

Deprecated Oracle Orachk and Oracle Exachk commands to manage patches:

- `-applypatch`
- `-querypatch`
- `-rollbackpatch`

10.6 Deprecated Oracle Trace File Analyzer Utilities in Release 21.1

Oracle Trace File Analyzer Utilities `summary` and `dbcheck` will be removed and replaced with new command-line with enhanced functionality.

10.7 Deprecated Oracle Trace File Analyzer Receiver in Release 21.1

Starting with 21.1 release, Oracle Trace File Analyzer Receiver has been deprecated and being replaced by enhanced Oracle AHF Collections Manager.

10.8 Deprecated tfactl Commands in Release 22.1.0

Starting with 22.1.0 release, the following tfactl upload commands have been deprecated and removed.

Deprecated tfactl command	Replaced with
`tfactl startahf`	`ahfctl startahf`

Deprecated tfactl command	Replaced with
`tfactl stopahf`	`ahfctl stopahf`
`tfactl statusahf`	`ahfctl statusahf`
`tfactl sendmail`	`ahfctl sendmail`
`tfactl showrepo`	`ahfctl showrepo`

Related Topics

- ahfctl startahf
  Use the `ahfctl startahf` command to start the scheduler for Oracle Autonomous Health Framework components.
- ahfctl stopahf
  Use the `ahfctl stopahf` command to stop the scheduler for Oracle Autonomous Health Framework components.
- ahfctl statusahf
  Use the `ahfctl statusahf` command to check the scheduler status for Oracle Autonomous Health Framework components.
- ahfctl sendmail
  Use the `ahfctl sendmail` command to send a test email to verify SMTP configuration.
- ahfctl showrepo
  Use the `ahfctl showrepo` command to get the repository locations of Oracle Autonomous Health Framework components.

10.9 Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands in 22.2

Starting with the AHF 22.2 (2022-09-14), commands to run the Oracle Orachk or Oracle Exachk scheduler without the Oracle Trace File Analyzer daemon are deprecated. These commands are completely removed in AHF 23.8 (2023-08-28).

Deprecated Legacy Oracle Orachk and Oracle Exachk Scheduler Commands:

- `-switch_scheduler`
- `-use_legacy_scheduler`
- `-xmlstart_scheduler`
- `-xmlstart_scheduler_debug`

Running the aforementioned commands would terminate with a deprecation notice. For example:

```
orachk -use_legacy_scheduler
Option '-use_legacy_scheduler' is deprecated and no longger supported.
Please run 'orachk -h' to see a list of available options
```

```
orachk -switch_scheduler
Option '-switch_scheduler' is deprecated and no longger supported.
Please run 'orachk -h' to see a list of available options
```

Changes also include the replacement of Oracle Orachk/Oracle Exachk daemon commands.

Table 10-1   Substituted Oracle Orachk and Oracle Exachk Daemon Commands

Deprecated Oracle Orachk and Oracle Exachk Daemon Commands	Replaced With

`exachk -d start`
`orachk -d start`
	`exachk -autostart`
	`orachk -autostart`

`exachk -d start_debug`
`orachk -d start_debug`	

`exachk -initsetup`
`orachk -initsetup`	

`exachk -initdebugsetup`
`orachk -initdebugsetup`	

`exachk -d stop`
`orachk -d stop`
	`exachk -autostop`
	`orachk -autostop`

`exachk -d stop_client`
`orachk -d stop_client`	

`exachk -initrmsetup`
`orachk -initrmsetup`	

`exachk -d info`
`orachk -d info`
	`exachk -autostatus`
	`orachk -autostatus`

`exachk -d status`
`orachk -d status`	

`exachk -d nextautorun`
`orachk -d nextautorun`	

`exachk -initcheck`
`orachk -initcheck`	

Running obsolete daemon commands will print a deprecation notice and an INFO message suggesting that you run equivalent commands. Then `orachk` and `exachk` will execute the respective equivalent commands. For example:

```
orachk -d start
'orachk -d start' is deprecated and will be removed in a future release.
Please start using 'orachk -autostart' instead.
Running 'orachk -autostart' for this operation. Run 'orachk -autostart -h'
for further help.


orachk -initrmsetup
'orachk -initrmsetup' is deprecated and will be removed in a future release.
Please start using 'orachk -autostop' instead.
Running 'orachk -autostop' for this operation. Run 'orachk -autostop -h' for
further help.


orachk -d info
'orachk -d info' is deprecated and will be removed in a future release.
Please start using 'orachk -autostatus' instead.
Running 'orachk -autostatus' for this operation. Run 'orachk -autostop -h'
for further help.
```

When the `-autostart` option is called and the TFA Scheduler is not running, you will receive a warning message suggesting that you start it.

```
ahfctl stopahf

Stopping TFA from the Command Line
Stopped OSWatcher
Nothing to do !
Please wait while TFA stops
Please wait while TFA stops
TFA-00002 Oracle Trace File Analyzer (TFA) is not running
TFA Stopped Successfully
Telemetry adapter is not running
Successfully stopped TFA..

No active orachk manual runs found

Stopping orachk scheduler ...
Removing orachk cache discovery....
No orachk cache discovery found.

Unable to send message to TFA

Removed orachk from inittab
```

```
Stopped orachk
```

```
orachk -autostart
TFA scheduler is not running. Please start TFA scheduler, by running
'ahfctl startahf', before configuring orachk to consume it.
```

Changes for legacy scheduler deprecation also include the ability to clean up legacy scheduler processes and remove `orachk`/`exachk` scheduler files upon an AHF upgrade, and/or by calling the `-autostart` or `-autostop` options.

10.10 Deprecated ahfctl Commands in Release 23.1.0

Starting with the 23.1.0 release, the `ahfctl applypatch`, `ahfctl querypatch`, and `ahfctl rollbackpatch` commands have been deprecated and completely be removed.

Deprecated `ahfctl` commands:

- `ahfctl applypatch`: Oracle recommends using `ahfctl applyupdate` instead.
- `ahfctl querypatch`: Oracle recommends using `ahfctl queryupdate` instead.
- `ahfctl rollbackpatch`: Oracle recommends using `ahfctl rollbackupdate` instead.

10.11 Deprecated AHF REST Services

AHF REST is deprecated and will be desupported in AHF release 24.3.0.

Download ORDS and provide the `ords.war` path to start AHF REST services.

10.12 Deprecated Oracle Trace File Analyzer Masking in Release 24.1

Starting with Oracle Autonomous Health Framework 24.1, the Oracle Trace File Analyzer masking feature is deprecated, and can be desupported in a future release.

Deprecating certain AHF features with limited adoption enables Oracle to focus on improving core features and functionality of AHF. Instructing TFA to mask sensitive data was an optional configuration choice enabled by creating a file named `mask_strings.xml` in the directory `tfa_home/resources`. Oracle recommends the AHF feature Adaptive Classification and Redaction (ACR) that is used to mask or redact sensitive data. The mask operation is enacted for all diagnostic collections with the command: `tfactl set redact=mask|sanitize`. Enable for a single collection by adding `-mask` or `-sanitize` to `tfactl diagcollect`. ACR is installed with AHF.

Related Topics

- Sanitizing Sensitive Information in Oracle Trace File Analyzer Collections
  After collecting copies of diagnostic data, Oracle Trace File Analyzer uses Adaptive Classification and Redaction (ACR) to sanitize sensitive data in the collections.

10.13 Oracle Database Quality of Service (QoS) Management is Deprecated in Release 21c

Starting in Oracle Database release 21c, Oracle Database Quality of Service (QoS) Management is deprecated and will be desupported in a future release.

Oracle Database Quality of Service (QoS) Management automates the workload management for an entire system by adjusting the system configuration based on pre-defined policies to keep applications running at the performance levels needed. Applications and databases are increasingly deployed in systems that provide some of the resource management capabilities of Oracle Database Quality of Service (QoS) Management. At the same time, Oracle's Autonomous Health Framework has been enhanced to adjust and provide recommendations to mitigate events and conditions that impact the health and operational capability of a system and its associated components. For those reasons, Oracle Database Quality of Service (QoS) Management has been deprecated with Oracle Database 21c.