Oracle® Trace File Analyzer

Collecting and Analyzing Oracle Database Diagnostic Data

18c
E90669-09
September 2018

Oracle Trace File Analyzer Collecting and Analyzing Oracle Database Diagnostic Data, 18c

E90669-09

Primary Author: Nirmal Kumar

Contributing Authors: Mark Bauer, Doug Williams

Contributors: Gareth Chapman, Bill Burton

Contents

2 Automatic Diagnostic Collections

3 On-demand Analysis and Diagnostic Collection

4 REST Service

Index

List of Examples

List of Figures

List of Tables

Preface

Oracle Trace File Analyzer User's Guide explains how to use the Oracle Trace File Analyzer diagnostic utility.

This Preface contains these topics:

Audience

Database administrators can use this guide to understand how to use the Oracle Trace File Analyzer. 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.

Related Documentation

For more information, see the following Oracle resources:

Related Topics

- *Oracle Automatic Storage Management Administrator's Guide*
- *Oracle Database 2 Day DBA*
- *Oracle Database Concepts*
- *Oracle Database Examples Installation Guide*

- *Oracle Database Licensing Information User Manual*
- *Oracle Database Release Notes*
- *Oracle Database Upgrade Guide*
- *Oracle Grid Infrastructure Installation and Upgrade Guide*
- *Oracle Real Application Clusters Installation Guide*

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 ORAchk and Oracle EXAchk consume 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.

Python

Python version 3.6.4 license, https://documentation.help/Python-3.6.4/license.html

pexpect

pexpect version 4.4.0 license, http://pexpect.readthedocs.io/en/latest/api/pexpect.html?highlight=license

ptyprocess

ptyprocess version 0.5.1 license, https://github.com/pexpect/ptyprocess/blob/master/LICENSE

Changes in this Release for Oracle Trace File Analyzer User's Guide 18.3.0

This preface lists changes in Oracle® Trace File Analyzer User's Guide 18.3.0.

- Automatic SRDCs
  Oracle Trace File Analyzer will now automatically run the relevant SRDC when it detects the following events:
- REST Service Extensions
  The REST service API includes new run commands.
- Configuring REST Service Using Apache Tomcat
  The Oracle Trace File Analyzer install includes a Web Application Resource (WAR) file to enable the REST service via Apache Tomcat.
- New SRDCs
  This release includes new SRDCs.
- Automatic Start from Oracle Trace File Analyzer Install
  Installing Oracle Trace File Analyzer as `root` on Linux or Solaris on non-engineered systems automatically sets up and runs the Oracle ORAchk daemon.

Automatic SRDCs

Oracle Trace File Analyzer will now automatically run the relevant SRDC when it detects the following events:

- `ORA-00600`
- `ORA-04030`
- `ORA-04031`
- `ORA-07445`

This means the diagnostic collections captured will be automatically targeted specifically to the event that occurred.

When other critical events are detected, Oracle Trace File Analyzer performs a default diagnostic collection.

Over future releases the automatic collection of specific SRDCs will be extended to cover other events.

REST Service Extensions

The REST service API includes new run commands.

You can access the new run commands as follows:

```
https://host:port/ords/tfactl/run/alertsummary
https://host:port/ords/tfactl/run/calog
https://host:port/ords/tfactl/run/changes
https://host:port/ords/tfactl/run/events
https://host:port/ords/tfactl/run/history
```

There is also a new upgrade feature for the existing ORDS REST implementations.

```
tfactl rest -upgrade
```

Running the commands `tfactl rest -upgrade` stops ORDS, upgrades it to support the latest API updates, and then restarts it again.

Configuring REST Service Using Apache Tomcat

The Oracle Trace File Analyzer install includes a Web Application Resource (WAR) file to enable the REST service via Apache Tomcat.

To enable the REST service using Apache Tomcat:

1. Deploy the WAR file located at `TFA_HOME/jlib/tfa.war` to your Tomcat server.
2. Change the `tfaadmin` user password.

   ```
   curl -k --user tfaadmin:tfaadmin -X POST "https://host/tfa/tfactl/user/update"
   '{ "password" : "some_new_password" }'
   ```

3. Change the `tfarest` user password.

   ```
   curl -k --user tfarest:tfarest -X POST "https://host/tfa/tfactl/user/update"
   '{ "password" : "some_new_password" }'
   ```

4. Add the Tomcat user to the Oracle Trace File Analyzer access list.

   ```
   tfactl access add -user tomcat_user
   ```

New SRDCs

This release includes new SRDCs.

- `dbimpdpperf` for Data Pump import performance problems.
- `dbsqlperf` for SQL performance problems.
- `dbtde` for Transparent Data Encryption (TDE) problems.
- `emagentperf` for Enterprise Manager Agent performance problems.
- `emomscrash` for Enterprise Manager crash problems.
- `emomsheap` for Enterprise Manager java heap usage, or performance problems.
- `emomshungcpu` for Enterprise Manager OMS crash, restart, or performance problems.

As with all other SRDCs use `tfactl diagcollect -srdc srdc_name`.

Automatic Start from Oracle Trace File Analyzer Install

Installing Oracle Trace File Analyzer as `root` on Linux or Solaris on non-engineered systems automatically sets up and runs the Oracle ORAchk daemon.

The daemon restarts at 1 am every day to discover any environment changes. The daemon runs a full local Oracle ORAchk check at 2 am every day, and a partial run of the most impactful checks every 6 hours through the `oratier1` profile.

The daemon automatically purges any collections older than 2 weeks.

You can change the daemon settings after enabling auto start. To remove auto start any time, run `tfactl run orachk -autostop`.

1

Getting Started with Oracle Trace File Analyzer

This section explains how to install Oracle Trace File Analyzer on different operating systems.

- Oracle Trace File Analyzer
  Oracle Trace File Analyzer helps you collect and analyze diagnostic data.
- Supported Environments
  You can use Oracle Trace File Analyzer with all supported versions of Oracle Database and Oracle Grid Infrastructure.
- Installing Oracle Trace File Analyzer on Linux or UNIX as root User in Daemon Mode
  To obtain the fullest capabilities of Oracle Trace File Analyzer, install it as `root`.
- Installing Oracle Trace File Analyzer on Linux or UNIX as Non-root User in Non-Daemon Mode
  If you are unable to install as `root`, then install Oracle Trace File Analyzer as the Oracle home owner.
- Installing Oracle Trace File Analyzer on Microsoft Windows
- Installing Oracle Trace File Analyzer on Microsoft Windows in Non-Daemon Mode
- Oracle Trace File Analyzer Key Directories
  Based on your installation type, the `ora_home` and the `bin` directories can differ.
- Oracle Trace File Analyzer Command Interfaces
  The `tfactl` tool functions as command-line interface, shell interface, and menu interface.
- Masking Sensitive Data
  Masking sensitive data is an optional feature that you can configure Oracle Trace File Analyzer to mask sensitive data in log files.
- Securing Access to Oracle Trace File Analyzer
  Running `tfactl` commands is restricted to authorized users.
- Uninstalling Oracle Trace File Analyzer

1.1 Oracle Trace File Analyzer

Oracle Trace File Analyzer helps you collect and analyze diagnostic data.

As a DBA, you are expected to do more work with fewer resources all the time. You are under pressure to keep the mission-critical applications up and running. When something goes wrong, everyone looks to you to understand what went wrong and how to fix it.

It is not always easy. You have to run the right tools at the right time. If you're using Oracle Grid Infrastructure, then you also have to collect diagnostic data from all the

database nodes. Collecting this data can require you to use tools that you rarely use. Needless to say, each tool has its own syntax.

The amount of data you collect can be huge. Only a fraction of the data that you collect is useful, but how can you know which part is relevant? You must collect it all, quickly, before the data is overwritten. In the meantime, you have still got a problem that costs your company time and money.

Oracle Trace File Analyzer enables you to collect diagnostic data. Collecting diagnostic data is a crucial step to resolving problems that occur with your Oracle Database.

Oracle Trace File Analyzer monitors your logs for significant problems that potentially impact your service. Oracle Trace File Analyzer also automatically collects relevant diagnostics when it detects any potential problems.

Oracle Trace File Analyzer can identify the relevant information in log files. It trims log files to just the parts that are necessary to resolve an issue. Oracle Trace File Analyzer also collects data across cluster nodes and consolidates everything in one place.

Using important database diagnostic tools is easy with Oracle Trace File Analyzer. Oracle Trace File Analyzer hides the complexity by providing a single interface and syntax for them all.

1.2 Supported Environments

You can use Oracle Trace File Analyzer with all supported versions of Oracle Database and Oracle Grid Infrastructure.

Oracle Trace File Analyzer works on the following operating systems:

- Linux OEL
- Linux RedHat
- Linux SuSE
- Linux Itanium
- zLinux
- Oracle Solaris SPARC
- Oracle Solaris x86-64
- AIX
- HPUX Itanium
- HPUX PA-RISC
- Microsoft Windows 64-bit

Oracle Trace File Analyzer is supported on the operating system versions supported by Oracle Database. Use a Java Runtime Edition of version 1.8.

Oracle Trace File Analyzer is shipped with Oracle Gird Infrastructure since versions 11.2.0.4 and 12.1.0.2. However, this install does not include many of the Oracle Database tools. Oracle releases new versions of Oracle Trace File Analyzer several times a year. These new releases include new features and bug fixes.

Ensure that you get the latest Oracle Trace File Analyzer with Oracle Database support tools bundle from My Oracle Support note 1513912.1.

Related Topics

- https://support.oracle.com/rs?type=doc&id=1513912.1

1.3 Installing Oracle Trace File Analyzer on Linux or UNIX as root User in Daemon Mode

To obtain the fullest capabilities of Oracle Trace File Analyzer, install it as `root`.

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

If Oracle Trace File Analyzer is already installed, then reinstalling performs an upgrade to the existing location. If Oracle Trace File Analyzer is not already installed, then the recommended location is `/opt/oracle.tfa`.

To install as `root`:

1. Download appropriate Oracle Trace File Analyzer zipped file, copy the downloaded file to the required machine, and then unzip.
2. Run the `installTFA` command:

   ```
   $ ./installTFA-platform
   ```

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

Cluster install requires passwordless SSH user equivalency for `root` to all cluster nodes. If not already configured, 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 on each host using a local install. Run the `tfactl syncnodes` command to generate and deploy relevant SSL certificates.

The Cluster Ready Services (CRS) do not manage Oracle Trace File Analyzer because Oracle Trace File Analyzer must be available if CRS goes down.

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

Installing Oracle Trace File Analyzer as root on Linux or Solaris on non-engineered systems automatically sets up and runs the Oracle ORAchk daemon.

The daemon restarts at 1 am every day to discover any environment changes. The daemon runs a full local Oracle ORAchk check at 2 am every day, and a partial run of the most impactful checks every 6 hours through the `oratier1` profile.

The daemon automatically purges any collections older than 2 weeks.

You can change the daemon settings after enabling auto start. To remove auto start any time, run `tfactl run orachk -autostop`.

Related Topics

- Installing Oracle Trace File Analyzer
  Understand the options that you can supply to the Oracle Trace File Analyzer installer script to customize the installation.
- Securing Access to Oracle Trace File Analyzer
  Running `tfactl` commands is restricted to authorized users.

1.4 Installing Oracle Trace File Analyzer on Linux or UNIX as Non-root User in Non-Daemon Mode

If you are unable to install as `root`, then install Oracle Trace File Analyzer as the Oracle home owner.

Oracle Trace File Analyzer has reduced capabilities in this installation mode.

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 `-extractto` option. Using the `-extractto` option tells Oracle Trace File Analyzer where to install to. Also, use the `-javahome` option to indicate which JRE to use. Use the JRE already available in the Oracle home, unless you have a later version available.

`./installTFA-`*`platform`* `-extractto` *`install_dir`* `-javahome` *`jre_home`*

Related Topics

- Installing Oracle Trace File Analyzer
  Understand the options that you can supply to the Oracle Trace File Analyzer installer script to customize the installation.

1.5 Installing Oracle Trace File Analyzer on Microsoft Windows

> **Note:**
>
> .NET Framework version 4.0.30319 or later is required to install Oracle Trace File Analyzer. If you experience installation errors, then ensure that you have the correct .NET Framework version installed.

1. Download appropriate Oracle Trace File Analyzer zipped file, copy the downloaded file to one of the required machines, and then unzip.
2. Open a command prompt as administrator and then run the installation script by specifying a Perl home.

For example:

```
install.bat -perlhome D:\oracle\product\12.2.0\dbhome_1\perl
```

The installer prompts you to do a local or cluster install. If you select cluster install, then the installer installs Oracle Trace File Analyzer on local and remote cluster nodes.

Alternatively, you can perform a local install on each host. Run the `tfactl syncnodes` command to generate and deploy relevant SSL certificates.

Related Topics

- Determine which .NET Framework versions are installed

1.6 Installing Oracle Trace File Analyzer on Microsoft Windows in Non-Daemon Mode

If you do not want Oracle Trace File Analyzer to run automatically as a windows service, then install it in non-daemon mode. Oracle Trace File Analyzer has reduced capabilities in this installation mode.

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

1. Download appropriate Oracle Trace File Analyzer zipped file, copy the downloaded file to one of the required machines, and then unzip.
2. Open a command prompt as administrator and then run the installation script.

   ```
   tfa_home\bin\tfactl.bat -setupnd
   ```

1.7 Oracle Trace File Analyzer Key Directories

Based on your installation type, the `ora_home` and the `bin` directories can differ.

If you have installed Oracle Trace File Analyzer with Oracle Grid Infrastructure, then `TFA_HOME` will be `GRID_HOME/tfa/hostname/tfa_home`.

Table 1-1 Key Oracle Trace File Analyzer Directories

Directory	Description
`tfa/bin`	Contains the command-line interface `tfactl` If Oracle Grid Infrastructure is installed, then `tfactl` is also installed in the `GRID_HOME/bin` directory.
`tfa/repository`	Directory where Oracle Trace File Analyzer stores diagnostic collections.
`tfa/node/tfa_home/database`	Contains Berkeley database that stores data about the system.

Table 1-1 (Cont.) Key Oracle Trace File Analyzer Directories

Directory	Description
`tfa/node/tfa_home/diag`	Tools for troubleshooting Oracle Trace File Analyzer.
`tfa/node/tfa_home/diagnostics_to_collect`	Place files here to include them in the next collection, then have them deleted afterwards.
`tfa/node/tfa_home/log`	Contains logs about Oracle Trace File Analyzer operation.
`tfa/node/tfa_home/resources`	Contains resource files, for example, the log masking control file.
`tfa/node/tfa_home/output`	Contains extra metadata about the environment.

1.8 Oracle Trace File Analyzer Command Interfaces

The `tfactl` tool functions as command-line interface, shell interface, and menu interface.

Table 1-2 Oracle Trace File 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.

1.9 Masking Sensitive Data

Masking sensitive data is an optional feature that you can configure Oracle Trace File Analyzer to mask sensitive data in log files.

Oracle Trace File Analyzer masks information such as host names or IP addresses and replaces sensitive data consistently throughout all files. Replacing consistently means that the information is still relevant and useful for the purposes of diagnosis without sharing any sensitive data.

To configure masking:

1. Create a file called `mask_strings.xml` in the directory `tfa_home/resources`.
2. Define a *`mask_strings`* element then within that a *`mask_string`* element, with *`original`* and *`replacement`* for each string you wish to replace:

   For example:

```
<mask_strings>
     <mask_string>
```

```
        <original>WidgetNode1</original>
        <replacement>Node1</replacement>
    </mask_string>
    <mask_string>
        <original>192.168.5.1</original>
        <replacement>Node1-IP</replacement>
    </mask_string>
    <mask_string>
        <original>WidgetNode2</original>
        <replacement>Node2</replacement>
    </mask_string>
    <mask_string>
        <original>192.168.5.2</original>
        <replacement>Node2-IP</replacement>
    </mask_string>
</mask_strings>
```

Oracle Trace File Analyzer automatically locates the `mask_strings.xml` files, and starts replacing the sensitive data in the diagnostics it collects.

1.10 Securing Access to Oracle Trace File Analyzer

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 around the time, collecting 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 any `tfactl` command.

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.

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 apply to cluster-wide unless `-local` is used to restrict 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
  ```

- To enable user access:

  ```
  tfactl access enable
  ```

- To disable user access:

  ```
  tfactl access disable
  ```

Related Topics

- tfactl access
  Use the `tfactl access` command to allow non-root users to have controlled access to Oracle Trace File Analyzer, and to run diagnostic collections.

1.11 Uninstalling Oracle Trace File Analyzer

1. To uninstall Oracle Trace File Analyzer, run the `uninstall` command as `root`, or install user.

   ```
   $ tfactl uninstall
   ```

2
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.

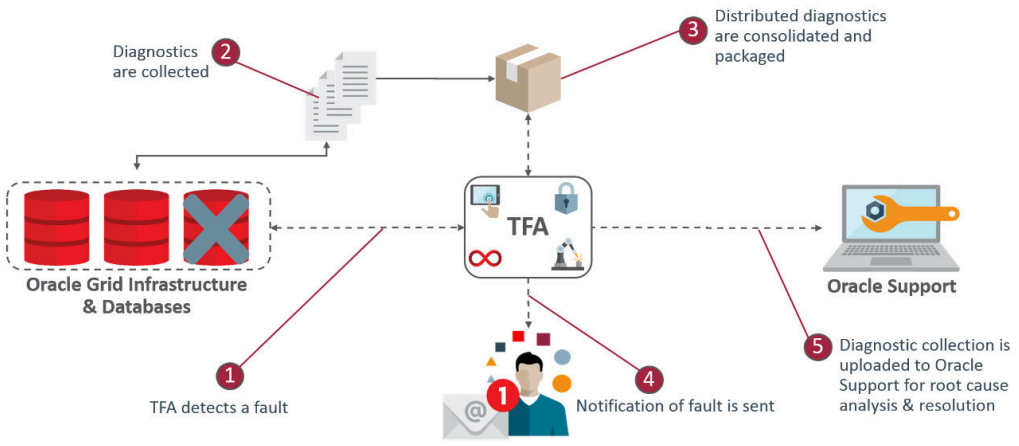
2.1 Collecting Diagnostics Automatically

This section explains automatic diagnostic collection concepts.

If Oracle Trace File Analyzer detects any problems, then it carries out the following actions:

- Runs necessary diagnostics and collects all relevant log data at the time of a problem
- Trims log files around the time of the problem so that Oracle Trace File Analyzer collects 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 2-1 Automatic Diagnostic Collections



Oracle Trace File Analyzer uses a flood control mechanism. Repeated errors do not flood the system with 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 is to capture any other relevant events together. 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 a further five minutes.

If events are still occurring after 10 minutes, then a diagnostic collection happens. A new collection point starts.

After the collection is complete, Oracle Trace File Analyzer sends email notification that includes the location of the collection, to the relevant recipients.

If your environment can make a connection to **oracle.com**, you can then 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 2-1 Log Entries that Trigger Automatic collection

String Pattern	Log Monitored
`ORA-297(01|02|03|08|09|10|40)`	Alert Log - Oracle Database
`ORA-00600`	Alert Log - Oracle ASM
`ORA-07445`	Alert Log - Oracle ASM Proxy
`ORA-04(69|([7-8][0-9]|9([0-3]|[5-8])))`	Alert Log - Oracle ASM IO Server
`ORA-32701`	
`ORA-00494`	
System State dumped	
`CRS-016(07|10|11|12)`	Alert Log - CRS

Additionally, when Oracle Cluster Health Advisor detects a problem event, Oracle Trace File Analyzer automatically triggers the relevant diagnostic collection.

Related Topics

- Uploading Collections to Oracle Support
  To enable collection uploads, configure Oracle Trace File Analyzer with your My Oracle Support user name and password.

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 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 2-2 tfactl diagnosetfa Command Parameters

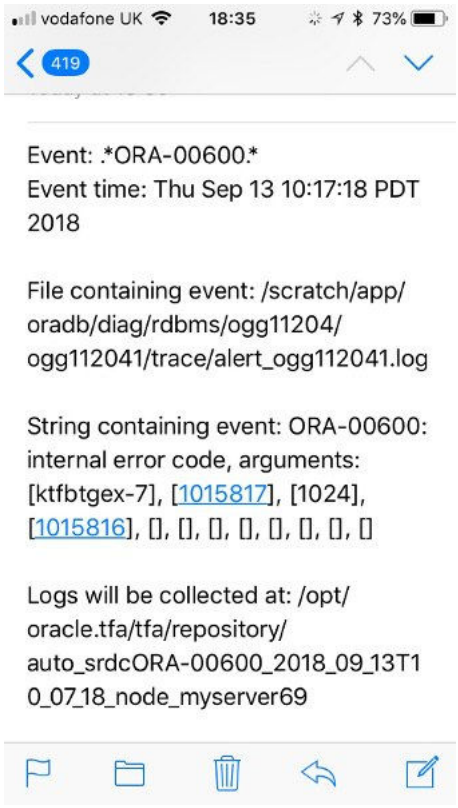
Parameter	Description
`smtp.host`	Specify the SMTP server host name.
`smtp.port`	Specify the SMTP server port.
`smtp.user`	Specify the SMTP user.
`smtp.password`	Specify password for the SMTP user.
`smtp.auth`	Set the Authentication flag to true or false.
`smtp.ssl`	Set the SSL flag to true or false.
`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 2-2 Email Notification



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.

Example 2-1 tfactl set smtp

```
# /u01/app/11.2.0.4/grid/bin/tfactl set 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 | true |
'---------------+-----------'

Enter the SMTP property you want to update : smtp.host
```

```
Enter value for smtp.host : myhost.domain.com

SMTP Property smtp.host updated with myhost.domain.com

Do you want to continue ? [Y]|N : N

#
```

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
   ```

3
On-demand Analysis and Diagnostic Collection

Run Oracle Trace File Analyzer on demand using `tfactl` command-line tool.

- Collecting Diagnostics and Analyzing Logs On-Demand
  The `tfactl` command can use a combination of different database command 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 your logs across your cluster to identify recent errors.
- Analyzing Logs Using the Included Tools
  Oracle Database support tools bundle is available only when you download Oracle Trace File Analyzer from My Oracle Support note 1513912.1.
- 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]`.
- Collecting Diagnostic Data and Using One Command Service Request Data Collections
- Uploading Collections to Oracle Support
  To enable collection uploads, configure Oracle Trace File Analyzer with your My Oracle Support user name and password.
- Changing Oracle Grid Infrastructure Trace Levels
  Enabling trace levels enables you to collect enough diagnostics to diagnose the cause of the problem.

3.1 Collecting Diagnostics and Analyzing Logs On-Demand

The `tfactl` command can use a combination of different database command tools when it performs analysis.

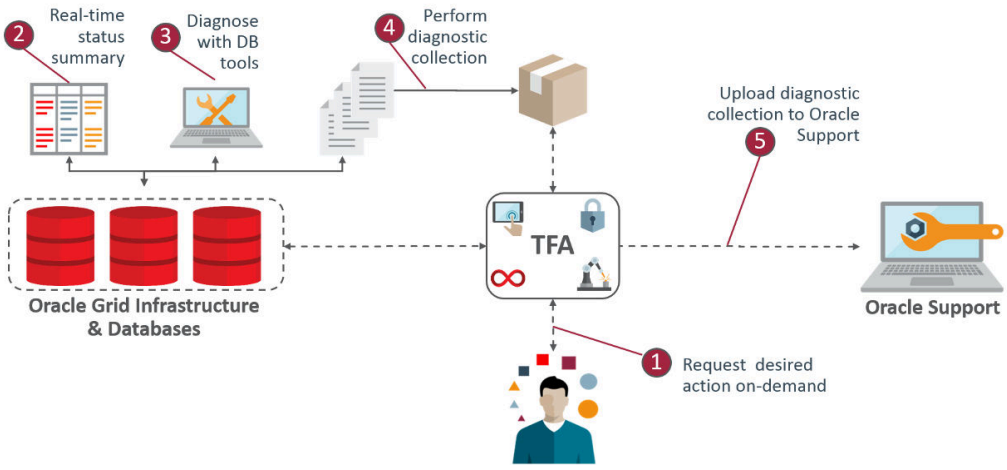
The `tfactl` command enables you to access all tools using common syntax. Using common syntax hides the complexity of the syntax differences between the tools.

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 around the time, collecting only what is necessary for diagnosis.
- Packages all diagnostics on the node where `tfactl` was run from.

Figure 3-1 On-Demand Collections



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
```

3.3 Investigating Logs for Errors

Use Oracle Trace File Analyzer to analyze all 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
   ```

Example 3-1 Analyzing logs

```
tfactl analyze –last 14d

Jun/02/2016 11:44:39 to Jun/16/2016 11:44:39 tfactl> analyze -last 14d
INFO: analyzing all (Alert and Unix System Logs) logs for the last 20160 minutes...
Please wait...
INFO: analyzing host: myserver69

                        Report title: Analysis of Alert,System Logs
```

```
                 Report date range: last ~14 day(s)
          Report (default) time zone: EST - Eastern Standard Time
                 Analysis started at: 16-Jun-2016 02:45:02 PM EDT
               Elapsed analysis time: 0 second(s).
                  Configuration file:
/u01/app/tfa/myserver69/tfa_home/ext/tnt/conf/tnt.prop
                 Configuration group: all
                 Total message count:            957, from 02-May-2016
09:04:07 PM EDT to 16-Jun-2016 12:45:41 PM EDT
   Messages matching last ~14 day(s):            225, from 03-Jun-2016
02:17:32 PM EDT to 16-Jun-2016 12:45:41 PM EDT
         last ~14 day(s) error count:              2, from 09-Jun-2016
09:56:47 AM EDT to 09-Jun-2016 09:56:58 AM EDT last ~14 day(s) ignored error count: 0
  last ~14 day(s) unique error count: 2

Message types for last ~14 day(s)
    Occurrences percent  server name          type
    ----------- -------  -------------------- -----
            223   99.1%  myserver69           generic
              2    0.9%  myserver69           ERROR
    ----------- -------
            225  100.0%

Unique error messages for last ~14 day(s)
    Occurrences percent  server name          error
    ----------- -------  -------------------- -----
              1   50.0%  myserver69           Errors in file
/u01/app/racusr/diag/rdbms/rdb11204/RDB112041/trace/RDB112041_ora_25401.trc
(incident=6398):
                                              ORA-07445: exception
encountered: core dump [] [] [] [] [] []
                                              Incident details in:
/u01/app/racusr/diag/rdbms/rdb11204/RDB112041/incident/incdir_6398/
RDB112041_ora_25401_i6398.trc

                                              Use ADRCI or Support Workbench to
package the incident.
                                              See Note 411.1 at My Oracle Support
for error and packaging details.

              1   50.0%  myserver69           Errors in file
/u01/app/racusr/diag/rdbms/rdb11204/RDB112041/trace/RDB112041_ora_25351.trc
(incident=6394):
                                              ORA-00700: soft internal error,
arguments: [kgerev1], [600], [600], [700], [], [], [], [], [], [], [], []
                                              Incident details in:
/u01/app/racusr/diag/rdbms/rdb11204/RDB112041/incident/incdir_6394/
RDB112041_ora_25351_i6394.trc

                                              Errors in file /u01/app/racusr/diag/
rdbms/rdb11204/RDB112041/trace/RDB112041_ora_25351.trc
(incident=6395):
                                              ORA-00600: internal error code,
arguments: [], [], [], [], [], [], [], [], [], [], [], []
                                              Incident details in:
/u01/app/racusr/diag/rdbms/rdb11204/RDB112041/incident/incdir_6395/
RDB112041_ora_25351_i6395.trc

                                              Dumping diagnostic data in
directory=[cdmp_20160609095648], requested by (instance=1, osid=25351),
summary=[incident=6394].
```

```
                                                    Use ADRCI or Support Workbench to
package the incident.
                                                    See Note 411.1 at My Oracle Support
for error and packaging details.

    ----------- -------
              2  100.0%
 See Change Which Directories Get Collected for more details.
```

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 ASM, and Oracle Grid Infrastructure alert logs, system message logs, OSWatcher Top, and OSWatcher Slabinfo files.

3.4 Analyzing Logs Using the Included Tools

Oracle Database support tools bundle is available only when you download Oracle Trace File Analyzer from My Oracle Support note 1513912.1.

Oracle Trace File Analyzer with Oracle Database support tools bundle includes the following tools:

Table 3-1 Tools included in Linux and UNIX

Tool	Description
`orachk` or `exachk`	Provides health checks for the Oracle stack. Oracle Trace File Analyzer 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 1268927.2.
`oswatcher`	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`	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 ASM alert files from all nodes.
`ls`	Lists all files 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.

Table 3-1 (Cont.) Tools included in Linux and UNIX

Tool	Description
`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 CRS 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 applied.
`calog`	Reports major events from the cluster event log.
`events`	Reports warnings and errors seen in the logs.
`managelogs`	Shows disk space usage and purges ADR log and trace files.
`ps`	Finds processes.
`triage`	Summarizes `oswatcher` or `exawatcher` data.

Table 3-2 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=1513912.1
- https://support.oracle.com/rs?type=doc&id=1070954.1
- https://support.oracle.com/rs?type=doc&id=1268927.2
- https://support.oracle.com/rs?type=doc&id=301137.1
- https://support.oracle.com/rs?type=doc&id=459694.1
- https://support.oracle.com/rs?type=doc&id=1500864.1
- https://support.oracle.com/rs?type=doc&id=215187.1

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,

```
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: `tfactl search -json '{"data_type":"event"}'`

To list all available datatypes: `tfactl search -showdatatypes`

3.6 Collecting Diagnostic Data and Using One Command Service Request Data Collections

To perform an on-demand diagnostic collection:

```
$ tfactl diagcollect
```

Running the command trims and collects all important log files updated in the past 12 hours across the whole cluster. Oracle Trace File Analyzer stores collections in the

repository directory. 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 you experienced. It 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_type –sr sr_number
```

To run SRDCs, use one of the Oracle privileged user accounts:

- `ORACLE_HOME` owner
- `GRID_HOME` owner

Table 3-3 One Command Service Request Data Collections

Type of Problem	Available SRDCs	Collection Scope
ORA Errors	`ORA-00020` `ORA-00060` `ORA-00600` `ORA-00700` `ORA-01031` `ORA-01555` `ORA-01578` `ORA-01628` `ORA-04030` `ORA-04031` `ORA-07445` `ORA-08102` `ORA-08103` `ORA-27300` `ORA-27301` `ORA-27302` `ORA-29548` `ORA-30036`	Local-only
Oracle Database performance problems	`dbperf`	Cluster-wide
Data Pump Import performance problems	`dbimpdpperf`	Local-only
SQL performance problems	`dbsqlperf`	Local-only
Transparent Data Encryption (TDE) problems	`dbtde`	Local-only
Oracle Database resource problems	`dbunixresources`	Local-only
Other internal Oracle Database errors	`internalerror`	Local-only
Oracle Database patching problems	`dbpatchinstall` `dbpatchconflict`	Local-only

Table 3-3 (Cont.) One Command Service Request Data Collections

Type of Problem	Available SRDCs	Collection Scope

Original Oracle Database Export (exp)	`dbexp`
	`dbexpdp`
	`dbexpdpapi`
	`dbexpdpperf`
	`dbexpdptts`
		Local-only

Original Oracle Database Import (imp)	`dbimp`
	`dbimpdp`
	`dbimpdpperf`
		Local-only

RMAN	`dbrman`
	`dbrman600`
	`dbrmanperf`
		Local-only

System change number	`dbscn`	Local-only
Oracle GoldenGate	`dbggclassicmode` `dbggintegratedmode`	Local-only

Oracle Database install / upgrade problems	`dbinstall`
	`dbupgrade`
	`dbpreupgrade`
		Local-only

Oracle Database storage problems	`dbasm`	Local-only
Excessive SYSAUX space is used by the Automatic Workload Repository (AWR)	`dbawrspace`	Local-only
Oracle Database startup / shutdown problems	`dbshutdown` `dbstartup`	
XDB Installation or invalid object problems	`dbxdb`	Local-only
Oracle Data Guard problems	`dbdataguard`	Local-only
Alert log messages of `Corrupt block relative dba` problems	`dbblockcorruption`	Local-only
ASM / DBFS / DNFS / ACFS problems	`dnfs`	Local-only
Create / maintain partitioned / subpartitioned table / index problems	`dbpartition`	Local-only
Slow `Create` / `Alter` / `Drop` commands against partitioned table / index	`dbpartitionperf`	Local-only
SQL performance problems	`dbsqlperf`	Local-only
UNDO corruption problems	`dbundocorruption`	Local-only
Listener errors: `TNS-12516` / `TNS-12518` / `TNS-12519` / `TNS-12520`	`listener_services`	Local-only
Naming service errors: `ORA-12154` / `ORA-12514` / `ORA-12528`	`naming_services`	Local-only
Standard information for Oracle Database auditing	`dbaudit`	Local-only
Enterprise Manager tablespace usage metric problems	`emtbsmetrics`	Local-only (on Enterprise Manager Agent target)

Table 3-3 (Cont.) One Command Service Request Data Collections

Type of Problem	Available SRDCs	Collection Scope
Enterprise Manager general metrics page or threshold problems	`emmetricalert`	Local-only (on Enterprise Manager Agent target and repository database)
Enterprise Manager debug log collection Run `emdebugon`, reproduce the problem then run `emdebugoff`, which disables debug again and collects debug logs	`emdebugon` `emdebugoff`	Local-only (on Enterprise Manager Agent target and Oracle Management Service)

Enterprise Manager target discovery / add problems	`emcliadd`
	`emclusdisc`
	`emdbsys`
	`emgendisc`
	`emprocdisc`
		Local-only

Enterprise Manager OMS restart problems	`emrestartoms`	Local-only
Enterprise Manager Agent performance problems	`emagentperf`	Local-only
Enterprise Manager OMS Crash problems	`emomscrash`	Local-only
Enterprise Manager Java heap usage or performance problems	`emomsheap`	Local-only
Enterprise Manager OMS crash, restart or performance problems	`emomshungcpu`	Local-only
Oracle Exalogic full Exalogs data collection information	`esexalogic`	Local-only

For more information about SRDCs, run `tfactl diagcollect -srdc -help`.

What the SRDCs collect varies for each type, for example:

Table 3-4 SRDC collections

Command	What gets collected
`$ tfactl diagcollect -srdc ORA-04031`	• IPS package • Patch listing • AWR report • Memory information • RDA HCVE output
`$ tfactl diagcollect -srdc dbperf`	• ADDM report • AWR for good period and problem period • AWR Compare Period report • ASH report for good and problem period • OSWatcher • 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 prompts to enter event date/time and database name.

1. Oracle Trace File Analyzer scans the system to identify recent events in the system (up to 10).
2. Once the relevant event is chosen, Oracle Trace File Analyzer then proceeds with diagnostic collection.
3. Oracle Trace File Analyzer identifies all the required files.
4. Oracle Trace File Analyzer trims all the files where applicable.
5. Oracle Trace File Analyzer 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"
```

Example 3-2 Diagnostic Collection

```
$ tfactl diagcollect

Collecting data for the last 12 hours for all components...
Collecting data for all nodes

Collection Id : 20160616115923myserver69

Detailed Logging at :
/u01/app/tfa/repository/collection_Thu_Jun_16_11_59_23_PDT_2016_node_all/
diagcollect_20160616115923_myserver69.log
2016/06/16 11:59:27 PDT : Collection Name :
tfa_Thu_Jun_16_11_59_23_PDT_2016.zip
2016/06/16 11:59:28 PDT : Collecting diagnostics from hosts :
[myserver70, myserver71, myserver69]
2016/06/16 11:59:28 PDT : Scanning of files for Collection in progress...
2016/06/16 11:59:28 PDT : Collecting additional diagnostic information...
2016/06/16 11:59:33 PDT : Getting list of files satisfying time range
[06/15/2016 23:59:27 PDT, 06/16/2016 11:59:33 PDT]
2016/06/16 11:59:37 PDT : Collecting ADR incident files...
2016/06/16 12:00:32 PDT : Completed collection of additional diagnostic
information...
2016/06/16 12:00:39 PDT : Completed Local Collection
2016/06/16 12:00:40 PDT : Remote Collection in Progress...
.---------------------------------------.
|          Collection Summary           |
+------------+-----------+------+------+
| Host       | Status    | Size | Time |
+------------+-----------+------+------+
| myserver71 | Completed | 15MB |  64s |
| myserver70 | Completed | 14MB |  67s |
| myserver69 | Completed | 14MB |  71s |
'------------+-----------+------+------'

Logs are being collected to:
```

```
/u01/app/tfa/repository/collection_Thu_Jun_16_11_59_23_PDT_2016_node_all
/u01/app/tfa/repository/collection_Thu_Jun_16_11_59_23_PDT_2016_node_all/
myserver71.tfa_Thu_Jun_16_11_59_23_PDT_2016.zip
/u01/app/tfa/repository/collection_Thu_Jun_16_11_59_23_PDT_2016_node_all/
myserver69.tfa_Thu_Jun_16_11_59_23_PDT_2016.zip
/u01/app/tfa/repository/collection_Thu_Jun_16_11_59_23_PDT_2016_node_all/
myserver70.tfa_Thu_Jun_16_11_59_23_PDT_2016.zip
```

Example 3-3 One command SRDC

```
$ tfactl diagcollect –srdc ora600
Enter value for EVENT_TIME [YYYY-MM-DD HH24:MI:SS,<RETURN>=ALL] :
Enter value for DATABASE_NAME [<RETURN>=ALL] :

1. Jun/09/2016 09:56:47 : [rdb11204] ORA-00600: internal error code,
arguments: [], [], [], [], [], [], [], [], [], [], [], [] 2. May/19/2016 14:19:30 :
[rdb11204] ORA-00600: internal error code,
arguments: [], [], [], [], [], [], [], [], [], [], [], [] 3. May/13/2016 10:14:30 :
[rdb11204] ORA-00600: internal error code,
arguments: [], [], [], [], [], [], [], [], [], [], [], [] 4. May/13/2016 10:14:09 :
[rdb11204] ORA-00600: internal error code,
arguments: [], [], [], [], [], [], [], [], [], [], [], []

Please choose the event : 1-4 [1] 1
Selected value is : 1 ( Jun/09/2016 09:56:47 ) Collecting data for local node(s)
Scanning files
from Jun/09/2016 03:56:47 to Jun/09/2016 15:56:47

Collection Id : 20160616115820myserver69

Detailed Logging at :
/u01/app/tfa/repository/
srdc_ora600_collection_Thu_Jun_16_11_58_20_PDT_2016_node_local/
diagcollect_20160616115820_myserver69.log
2016/06/16 11:58:23 PDT : Collection Name :
tfa_srdc_ora600_Thu_Jun_16_11_58_20_PDT_2016.zip
2016/06/16 11:58:23 PDT : Scanning of files for Collection in progress...
2016/06/16 11:58:23 PDT : Collecting additional diagnostic information...
2016/06/16 11:58:28 PDT : Getting list of files satisfying time range
[06/09/2016 03:56:47 PDT, 06/09/2016 15:56:47 PDT]
2016/06/16 11:58:30 PDT : Collecting ADR incident files...
2016/06/16 11:59:02 PDT : Completed collection of additional diagnostic
information...
2016/06/16 11:59:06 PDT : Completed Local Collection
.----------------------------------------.
|           Collection Summary           |
+------------+-----------+-------+------+
| Host       | Status    | Size  | Time |
+------------+-----------+-------+------+
| myserver69 | Completed | 7.9MB |  43s |
'------------+-----------+-------+------'
```

> **Note:**
>
> For more information about how to diagnose and resolve ORA-00600 errors using Oracle Trace File Analyzer diagnostics, see ORA-600 (ORA-00600 Internal Error) Detection, Diagnosis & Resolution.

Related Topics

- ORA-600 (ORA-00600 Internal Error) Detection, Diagnosis & Resolution

3.7 Uploading Collections to Oracle Support

To enable collection uploads, configure Oracle Trace File Analyzer with your My Oracle Support user name and password.

For example:

```
tfactl setupmos
```

Oracle Trace File Analyzer stores your login details securely within an encrypted wallet. You can store only a single user's login details.

1. Run a diagnostic collection using the `-sr sr_number` option.

   ```
   tfactl diagcollect diagcollect options -sr sr_number
   ```

   At the end of collection, Oracle Trace File Analyzer automatically uploads all collections to your Service Request.

Oracle Trace File Analyzer can also upload any other file to your Service Request.

You can upload using the wallet, which was setup previously by `root` using `tfactl setupmos`.

```
tfactl upload -sr sr_number -wallet space-separated list of files to upload
```

You can also upload without the wallet. When uploading without the wallet `tfactl` prompts for the password.

```
tfactl upload -sr sr_number -user user_id space-separated list of files to upload
```

```
-bash-4.1# tfactl setupmos
Enter User Id: john.doe@oracle.com
Enter Password:
Wallet does not exist ... creating
Wallet created successfully
USER details added/updated in the wallet
PASSWORD details added/updated in the wallet
SUCCESS - CERTIMPORT - Successfully imported certificate
-bash-4.1# su - oradb


-bash-4.1$ /opt/oracle.tfa/tfa/myserver69/tfa_home/bin/tfactl diagcollect -srdc
ORA-00600 -sr 3-15985570811
Enter the time of the ORA-00600 [YYYY-MM-DD HH24:MI:SS,RETURN=ALL] :
Enter the Database Name [RETURN=ALL] :

1. Oct/23/2017 03:03:40 : [ogg11204] ORA-00600: internal error code, arguments:
[gc_test_error], [0], [0], [], [], [], [], [], [], [], [], []
2. Sep/26/2017 10:03:10 : [ogg11204] ORA-00600: internal error code, arguments: [],
[], [], [], [], [], [], [], [], [], []
3. Sep/26/2017 10:02:49 : [ogg11204] ORA-00600: internal error code, arguments: [],
[], [], [], [], [], [], [], [], [], []
4. Sep/26/2017 10:02:33 : [ogg11204] ORA-00600: internal error code, arguments: [],
[], [], [], [], [], [], [], [], [], []
5. Jan/09/2016 13:01:02 : [+ASM1] ORA-00600: internal error code, arguments:
[ksdhng:msg_checksum], [9070324609822233070], [15721744232659255108],
```

```
[0x7FFBDC07A9E8], [], [], [], [], [], [], [], []

Please choose the event : 1-5 [1] 1
Selected value is : 1 ( Oct/23/2017 03:03:40 )
Scripts to be run by this srdc: ipspack rdahcve1210 rdahcve1120 rdahcve1110
Components included in this srdc: OS CRS DATABASE NOCHMOS
Use of uninitialized value $db_home in length at /opt/oracle.tfa/tfa/myserver69/
tfa_home/bin/common/dbutil.pm line 186.
Collecting data for local node(s)
Scanning files from Oct/22/2017 21:03:40 to Oct/23/2017 09:03:40

Collection Id : 20180430080045myserver69

Detailed Logging at : /opt/oracle.tfa/tfa/repository/
srdc_ora600_collection_Mon_Apr_30_08_00_45_PDT_2018_node_local/
diagcollect_20180430080045_myserver69.log
2018/04/30 08:00:50 PDT : NOTE : Any file or directory name containing the
string .com will be renamed to replace .com with dotcom
2018/04/30 08:00:50 PDT : Collection Name :
tfa_srdc_ora600_Mon_Apr_30_08_00_45_PDT_2018.zip
2018/04/30 08:00:50 PDT : Scanning of files for Collection in progress...
2018/04/30 08:00:50 PDT : Collecting additional diagnostic information...
2018/04/30 08:01:15 PDT : Getting list of files satisfying time range [10/22/2017
21:03:40 PDT, 10/23/2017 09:03:40 PDT]
2018/04/30 08:01:34 PDT : Collecting ADR incident files...
2018/04/30 08:02:21 PDT : Completed collection of additional diagnostic
information...
2018/04/30 08:02:24 PDT : Completed Local Collection
2018/04/30 08:02:24 PDT : Uploading collection to SR - 3-15985570811
2018/04/30 08:02:27 PDT : Successfully uploaded collection to SR
.----------------------------------------.
|           Collection Summary           |
+------------+-----------+-------+------+
| Host       | Status    | Size  | Time |
+------------+-----------+-------+------+
| myserver69 | Completed | 559kB |  94s |
'------------+-----------+-------+------'

Logs are being collected to: /opt/oracle.tfa/tfa/repository/
srdc_ora600_collection_Mon_Apr_30_08_00_45_PDT_2018_node_local
/opt/oracle.tfa/tfa/repository/
srdc_ora600_collection_Mon_Apr_30_08_00_45_PDT_2018_node_local/
myserver69.tfa_srdc_ora600_Mon_Apr_30_08_00_45_PDT_2018.zip
```

3.8 Changing Oracle Grid Infrastructure Trace Levels

Enabling trace levels enables you to collect enough diagnostics to diagnose the cause of the problem.

Oracle Support asks you to enable certain trace levels when reproducing a problem.

Oracle Trace File Analyzer makes it easy to enable and then disable the correct 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.

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 3-5 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 CRS modules.
`lscomponents`	Lists all the components associated with the CRS module.
`lsres`	Lists all the discovered CRS resources.

Table 3-5 (Cont.) tfactl dbglevel Command Parameters

Parameter	Description
`getstate`	Displays the current trace or log levels for the CRS components or resources.
`module`	Specify the CRS 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 CRS components or resources.
`includetrace`	Adds or modifies a trace value for the CRS components.

WARNING:

Set the profiles only at the direction of Oracle Support.

4
REST Service

Learn to configure REST service, and use REST service APIs.

- Configuring REST Service Using ORDS
  Oracle Trace File Analyzer includes REST support allowing invocation and query over HTTPS.
- Configuring REST Service Using Apache Tomcat
  The Oracle Trace File Analyzer install includes a Web Application Resource (WAR) file to enable the REST service via Apache Tomcat.
- REST Service print API
  Learn to use the REST Service `print` API
- REST Service diagcollect API
  Learn to use the REST Service `diagcollect` API.
- REST Service download API
  Learn to use the REST Service `download` API.
- REST Service run API
  Learn to use REST Service `run` API.
- REST Service user API
  Learn to use REST Service `user` API.

4.1 Configuring REST Service Using ORDS

Oracle Trace File Analyzer includes REST support allowing invocation and query over HTTPS.

Syntax

To facilitate this REST support Oracle REST Data Services (ORDS) is included within the install.

```
tfactl rest [-status|-start|-stop|-upgrade|-uninstall] [-dir] [-port] [-user] [-
debug [-level]]
```

> **Note:**
>
> You can run the REST command only as `root` user.

Parameters

Table 4-1 REST Command Parameters

Parameter	Description
`-status`	Prints the current status.
`-start`	Starts Oracle Trace File Analyzer REST services if not already running.
`-stop`	Stops Oracle Trace File Analyzer REST services if running.
`-upgrade`	Checks if the configured ORDS API should be upgraded. If the ORDS API needs upgrading, then stops ORDS, upgrades the API, and then restarts ORDS.
`-uninstall`	Removes the Oracle Trace File Analyzer REST configuration.
`–dir`	The directory to use to store the Oracle Trace File Analyzer REST configuration details. Defaults to the users home directory.
`–port`	The port to run ORDS on. Defaults to 9090.
`-user`	The user to start ORDS as. Defaults to the GRID owner.
`–debug`	Enables debug.
`–level`	The level of debug to use, where available levels are: • 1 – FATAL • 2 – ERROR • 3 – WARNING • 4 – INFO (default) • 5 – DEBUG • 6 – TRACE

Once ORDS is running, you can invoke REST using the following APIs using requests of the form:

```
https://host:port/ords/api
```

For example:

```
https://host:port/ords/tfactl/print/status
```

REST Authentication

Oracle Trace File Analyzer REST uses first-party cookie-based authentication (basic authentication).

The Oracle Trace File Analyzer REST application is able to authenticate and authorize itself to the RESTful API using the same cookie session that the web application is using. The first party application has full access to the RESTful API.

During start-up Oracle Trace File Analyzer prompts you for the password for the `tfaadmin` and `tfarest` users.

- Use `tfarest` user for REST calls

- Use `tfaadmin` for making REST calls and to manage the REST service, for example, changing the logging level

```
# ./tfactl rest -start

Configuring TFA REST Services using ORDS :

This might take couple of minutes. Please be patient.

Adding Dependency Jars to ORDS

Adding users to ORDS :

Enter a password for user tfaadmin:
Confirm password for user tfaadmin:

Enter a password for user tfarest:
Confirm password for user tfarest:

Starting TFA REST Services

Successfully started TFA REST Services [PID : 32650]

URL : https://myserver:9090/ords/tfactl/print/status
```

Access the web service from a browser using the following URL:

`https://`*`host_name`*`:9090/ords/tfactl/print/status`

You are presented with a 401 message, which includes a **sign in** link. Click the link, sign in with `tfarest` credentials you just created, and you will be directed to REST output.

Alternatively, you can also specify the credentials in a `curl` command.

```
# curl -k --user tfarest:mypassword https://myserver:9090/ords/tfactl/print/status
[ {
  "status" : "CheckOK",
  "hostname" : "myserver",
  "pid" : 2430,
  "port" : 5000,
  "version" : "18.2.0.0.0",
  "buildId" : "18200020180501035221",
  "inventoryStatus" : "COMPLETE"
} ]
```

4.2 Configuring REST Service Using Apache Tomcat

The Oracle Trace File Analyzer install includes a Web Application Resource (WAR) file to enable the REST service via Apache Tomcat.

To enable the REST service using Apache Tomcat:

1. Deploy the WAR file located at `TFA_HOME/jlib/tfa.war` to your Tomcat server.
2. Change the `tfaadmin` user password.

   ```
   curl -k --user tfaadmin:tfaadmin -X POST "https://host/tfa/tfactl/user/update"
   '{ "password" : "some_new_password" }'
   ```

3. Change the `tfarest` user password.

```
curl -k --user tfarest:tfarest -X POST "https://host/tfa/tfactl/user/update"
'{ "password" : "some_new_password" }'
```

4. Add the Tomcat user to the Oracle Trace File Analyzer access list.

```
tfactl access add -user tomcat_user
```

4.3 REST Service print API

Learn to use the REST Service `print` API

- print
  Use GET requests to print the statuses of all hosts.
- hosts
  Use GET requests to print the list of hosts.
- actions
  Use GET requests to print the list of actions performed on all hosts.
- repository
  Use GET requests to print the repository details of all hosts.
- collections
  Use GET requests to print the details of all collections, or a specific collection.
- config
  Use GET requests to print the configuration details of all hosts.
- protocols
  Use GET requests to print the details of protocols of all hosts.
- directories
  Use GET requests to print the details of directories of all hosts.

4.3.1 print

Use GET requests to print the statuses of all hosts.

Syntax

```
/tfactl/print/status
```

Example 4-1 print

```
[ {
  "status" : "CheckOK",
  "hostname" : "myhost",
  "pid" : 73637,
  "port" : 9090,
  "version" : "18.1.0.0.0",
  "buildId" : "18100020180109014331",
  "inventoryStatus" : "COMPLETE"
} ]
```

4.3.2 hosts

Use GET requests to print the list of hosts.

Syntax

```
/tfactl/print/hosts
```

Example 4-2 hosts

```
[ {
  "hostname" : "myhost"
} ]
```

4.3.3 actions

Use GET requests to print the list of actions performed on all hosts.

Syntax

```
/tfactl/print/actions
```

Example 4-3 actions

```
[ {
  "actionName" : "Run inventory",
  "hostname" : "Requested in all nodes",
  "client" : "tfactl",
  "startTime" : "Jan 09 07:50:26 PST",
  "endTime" : "Jan 09 07:50:29 PST",
  "status" : "COMPLETE",
  "comments" : null
} ]
```

4.3.4 repository

Use GET requests to print the repository details of all hosts.

Syntax

```
/tfactl/print/repository
```

Example 4-4 repository

```
[ {
  "hostname" : "myhost",
  "directory" : "/scratch/smith/view_storage/smith_tfa_latest/oracle/log/tfa/
repository",
  "status" : "OPEN",
  "maxSizeMB" : 10240,
  "currentSizeMB" : 13,
  "freeSpaceMB" : 10227
} ]
```

4.3.5 collections

Use GET requests to print the details of all collections, or a specific collection.

Syntax

```
/tfactl/print/collections
/tfactl/print/collections/{collectionid}
```

Example 4-5 collections


```
[ {
  "id" : "20171010115528myhost",
  "type" : "Manual Collection",
  "requestUser" : "smith",
  "nodeList" : "[]",
  "masterHost" : "myhost",
  "startTime" : "Mon Oct 09 23:55:32 PDT 2017",
  "endTime" : "Tue Oct 10 11:55:32 PDT 2017",
  "tag" : "/scratch/smith/view_storage/smith_tfa_latest/oracle/log/tfa/repository/
tfa_11",
  "zipFileName" : "myhost.tfa_Tue_Oct_10_11_55_28_PDT_2017.zip",
  "componentList" : "[emagent, crsclient, oms, dbwlm,emplugins, cfgtools, afd, wls]",
  "zipFileSize" : 3055,
  "collectionTime" : 16,
  "events" : null
}]

[{
  "id" : "20171011044112myhost",
  "type" : "Manual Collection",
  "requestUser" : "smith",
  "nodeList" : "[]",
  "masterHost" : "myhost",
  "startTime" : "null",
  "endTime" : "Wed Oct 11 04:41:14 PDT 2017",
  "tag" : "/scratch/smith/view_storage/smith_tfa_latest/oracle/log/tfa/repository/
TFA_T1",
  "zipFileName" : "myhost.TFA_T1.zip",
  "componentList" : "[]",
  "zipFileSize" : 0,
  "collectionTime" : 0,
  "events" : null
}]
```


4.3.6 config

Use GET requests to print the configuration details of all hosts.

Syntax

```
/tfactl/print/config
```

Example 4-6 config


```
[ {
  "hostname" : "myhost",
  "tfaVersion" : "18.1.0.0.0",
  "javaVersion" : "1.8",
  "inventoryTraceLevel" : 1,
  "collectionTraceLevel" : 1,
  "scanTraceLevel" : 1,
  "otherTraceLevel" : 3,
  "currentSizeMB" : 13,
  "maxSizeMB" : 10240,
  "maxLogSize" : 50,
  "maxLogCount" : 10,
  "maxCoreFileSize" : 50,
  "maxCoreCollectionSize" : 500,
  "minSpaceForRTScan" : 500,
```

```
  "diskUsageMoninterInterval" : 60,
  "manageLogsAutoPurgeInterval" : 60,
  "manageLogsAutoPurgePolicyAge" : "30d",
  "minFileAgeToPurge" : 12,
  "language" : "en",
  "encoding" : "UTF-8",
  "country" : "US",
  "alertLogLevel" : "ALL",
  "userLogLevel" : "ALL",
  "baseLogPath" : "ERROR",
  "tfaIpsPoolSize" : 5,
  "autoPurge" : true,
  "publicIp" : false,
  "fireZipsInRT" : true,
  "rtscan" : true,
  "diskUsageMonOn" : true,
  "manageLogsAutoPurgeOn" : false,
  "trimmingOn" : true
} ]
```


4.3.7 protocols

Use GET requests to print the details of protocols of all hosts.

Syntax

```
/tfactl/print/protocols
```

Example 4-7 protocols


```
{
  "hostname" : "myhost",
  "available" : [ "TLSv1.2" ],
  "restricted" : [ "SSLv3", "SSLv2Hello", "TLSv1", "TLSv1.1" ]}
```


4.3.8 directories

Use GET requests to print the details of directories of all hosts.

Syntax

```
/tfactl/print/directories
```

Example 4-8 directories


```
[ {
  "hostname" : "myhost",
  "directory" : "/oem/app/oracle/product/emagent/agent_inst/install/logs",
  "components" : [ "EMPLUGINS" ],
  "permission" : "public",
  "owner" : "root",
  "collectionPolicy" : "exclusions",
  "collectAll" : false
}, {
  "hostname" : "myhost",
  "directory" : "/oem/app/oracle/product/emagent/agent_inst/sysman/log",
  "components" : [ "EMAGENT" ],
  "permission" : "public",
  "owner" : "root",
  "collectionPolicy" : "exclusions",
```

```
  "collectAll" : false
} ]
```

4.4 REST Service diagcollect API

Learn to use the REST Service `diagcollect` API.

- diagcollect
  Use POST requests to view collection details.

4.4.1 diagcollect

Use POST requests to view collection details.

Syntax

```
/tfactl/diagcollect
```

Returns

Oracle Trace File Analyzer default collection for last 12 hours for all components.

Or, Oracle Trace File Analyzer collection per JSON data as parameters specified.

Example 4-9 diagcollect–default collection

```
{
  "collectionId" : "20180111011121slc12ekf",
  "zipName" : "TFA_DEF_ZIP_20180111011121",
  "tagName" : "TFA_DEF_TAG_20180111011121"
}
```

Example 4-10 diagcollect–JSON data as Parameters

Input:

```
[{
  "components": "-database -asm -tns -crs -acfs -install -cfgtools -os",
  "timePeriod": "-since n[d|h] | -last n[d|h] | -for date |
        -from date -to date",
  "tagName": "crs_crash_collection",
  "nodeList": "node1,node2",
  "options": "-nocopy | -notrim | -silent | -nocores |
       -collectalldirs | -collectdir dir1,dir2..."
}]
```

Output:

```
[{
  "collectionId" : "20180111011121slc12ekf",
  "zipName" : "TFA_DEF_ZIP_20180111011121",
  "tagName" : "TFA_DEF_TAG_20180111011121"
}]
```

4.5 REST Service download API

Learn to use the REST Service `download` API.

- download
  Use GET requests to download collection ZIP file for a specific collection ID.

4.5.1 download

Use GET requests to download collection ZIP file for a specific collection ID.

Syntax

`/tfactl/download/{collectionid}`

Returns

Collection ZIP file for the collection ID specified.

Usage Notes

Specify the collection ID for which you want to download the collection ZIP file.

4.6 REST Service run API

Learn to use REST Service `run` API.

- alertsummary
  Use GET requests to run the `alertsummary` command.
- calog
  Use GET requests to run the `calog` command.
- changes
  Use GET requests to run the `changes` command.
- events
  Use GET requests to run the `events` command.
- history
  Use GET requests to run the `history` command.

4.6.1 alertsummary

Use GET requests to run the `alertsummary` command.

Syntax

`/tfactl/run/alertsummary`

Returns

Runs the `alertsummary` command and returns the alert summary.

Example 4-11 alertsummary

```
[ {
  "line" : "Output from host : myserver"
}, {
  "line" : "------------------------------"
}, {
  "line" : "Reading /scratch/app/oradb/diag/rdbms/apxcmupg/apxcmupg_2/trace/
alert_apxcmupg_2.log"
```

```
}, {
  "line" : "+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-"
}, {
  "line" : "--------------------------------------------------------------------------"
}, {
  "line" : "Oct 20 08:20:43 Database started"
}, {
  "line" : "--------------------------------------------------------------------------"
}, {
  "line" : "Nov 05 20:27:50 Database started"
},
....
....
```

4.6.2 calog

Use GET requests to run the `calog` command.

Syntax

`/tfactl/run/calog`

4.6.3 changes

Use GET requests to run the `changes` command.

Syntax

`/tfactl/run/changes`

Example 4-12 changes

```
[ {
  "line" : "Output from host : myserver"
}, {
  "line" : "-------------------------------"
}, {
  "line" : "[Jul/25/2018 03:45:15.325]: Parameter: fs.aio-nr: Value: 276224 =>
277760"
}, {
  "line" : "[Jul/25/2018 03:45:15.325]: Parameter: kernel.random.entropy_avail:
Value: 192 => 152"
}, {
  "line" : "[Jul/25/2018 03:45:15.325]: Parameter: kernel.random.uuid:
Value: 5eac06d7-560a-466d-a035-efe836fe0b57 => 3f329d9c-25d3-4057-ab00-17d031645490"
}, {
  "line" : "[Jul/25/2018 15:46:15.325]: Parameter: fs.aio-nr: Value: 277760 =>
279296"
},
....
....
```

4.6.4 events

Use GET requests to run the `events` command.

Syntax

`/tfactl/run/events`

Example 4-13 events

```
[ {
  "line" : "Output from host : myserver"
}, {
  "line" : "-----------------------------"
}, {
  "line" : "Event Summary:"
}, {
  "line" : "INFO    :0"
}, {
  "line" : "ERROR   :0"
}, {
  "line" : "WARNING :0"
}, {
  "line" : "Event Timeline:"
}, {
  "line" : "No Events Found"
} ]
```

4.6.5 history

Use GET requests to run the `history` command.

Syntax

```
/tfactl/run/history
```

4.7 REST Service user API

Learn to use REST Service `user` API.

- add
  Use POST requests to add users to Oracle Trace File Analyzer REST Services.
- delete
  Use POST requests to delete an Oracle Trace File Analyzer REST Services user.
- update
  Use POST requests to update the password of an Oracle Trace File Analyzer REST Services user.

4.7.1 add

Use POST requests to add users to Oracle Trace File Analyzer REST Services.

Syntax

```
/tfactl/user/add
```

Example 4-14 add

Input:

```
{
  "userName" : "test",
  "password" : "test"
}
```

Output:

```
{
  "status": "SUCCESS",
  "message": "Successfully added test to TFA REST Services"
}
```

4.7.2 delete

Use POST requests to delete an Oracle Trace File Analyzer REST Services user.

Syntax

```
/tfactl/user/delete
```

Example 4-15 delete

Input:

```
{
  "userName" : "test"
}
```

Output:

```
{
  "status": "SUCCESS",
  "message": "Successfully removed test from TFA REST Services"
}
```

4.7.3 update

Use POST requests to update the password of an Oracle Trace File Analyzer REST Services user.

Syntax

```
/tfactl/user/update
```

Example 4-16 update

Input:

```
{
  "password" : "test"
}
```

Output:

```
{
  "status": "SUCCESS",
  "message": "Successfully updated users's profile in TFA"
}
```

5

Maintaining Oracle Trace File Analyzer to the Latest Version

Oracle releases a new version of Oracle Trace File Analyzer approximately every three months.

Applying standard Release Update Revisions (RURs) automatically updates Oracle Trace File Analyzer. 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 Trace File Analyzer with Oracle Database support tools bundle from My Oracle Support note 1513912.1.

Upgrading is similar to first-time install. As `root`, use the `installTFA`*`platform`* script. If Oracle Trace File Analyzer 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.

```
$ ./installTFAplatform
```

If you are not able to install as `root`, then install Oracle Trace File Analyzer as Oracle home owner. Use the `-extractto` and `–javahome` options:

```
$ ./installTFAplatform -extractto dir -javahome jre_home
```

Related Topics

- Installing Oracle Trace File Analyzer on Microsoft Windows
- https://support.oracle.com/rs?type=doc&id=1513912.1

6
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 12 hours.
- 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
- Preventing 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.

6.1 Adjusting the Diagnostic Data Collection Period

Oracle Trace File Analyzer trims and collects any important logs updated in the past 12 hours.

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 6-1 Ways to Specify the Collection Period

Command	Description
`tfactl diagcollect -last` *n* `h|d`	Collects since the previous *n* hours or days.

`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"`

Table 6-1 (Cont.) Ways to Specify the Collection Period

Command	Description

`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"`

`tfactl diagcollect -for "yyyy-mm-dd"`	Collects for the specified date.
	Valid date formats:
	`"Mon/dd/yyyy"`
	`"yyyy-mm-dd"`

6.2 Collecting from Specific Nodes

To collect from specific nodes:

1. 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.

6.3 Collecting from Specific Components

To collect from specific components:

1. 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 CRS 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 6-2 Component Options

Component Option	Description
`-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 DBWLM logs.
`-tns`	Collects TNS logs.
`-rhp`	Collects RHP logs.
`-procinfo`	Collects `Gathers stack` and `fd` from `/proc` for all processes.
`-afd`	Collects AFD logs.
`-crs`	Collects CRS logs.
`-wls`	Collects WLS logs.
`-emagent`	Collects EMAGENT logs.
`-oms`	Collects OMS logs.
`-ocm`	Collects OCM logs.
`-emplugins`	Collects EMPLUGINS logs.
`-em`	Collects EM logs.
`-acfs`	Collects ACFS logs and data.
`-install`	Collects Oracle Installation related files.
`-cfgtools`	Collects CFGTOOLS logs.
`-os`	Collects operating system files such as `/var/log/messages`.
`-ashhtml`	Collects Generate ASH HTML Report.
`-ashtext`	Collects Generate ASH TEXT Report.
`-awrhtml`	Collects AWRHTML logs.

Related Topics

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

6.4 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 (12 hours 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 12 hours:

   ```
   tfactl diagcollect –collectdir dir1,dir2,...dirn
   ```

   For example:

   To trim and collect all CRS files updated in the last 12 hours 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.

6.5 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.

For example:

```
$ tfactl diagcollect -last 1h -tag MyTagName
Collecting data for all nodes
....
....

Logs are being collected to: /scratch/app/crsusr/tfa/repository/MyTagName
/scratch/app/crsusr/tfa/repository/MyTagName/
host_name.tfa_Mon_Aug_22_05_26_17_PDT_2016.zip
/scratch/app/crsusr/tfa/repository/MyTagName/
host_name.tfa_Mon_Aug_22_05_26_17_PDT_2016.zip
```

2. To rename the `zip` file:

```
-z zip name
```

For example:

```
$ tfactl diagcollect -last 1h -z MyCollectionName.zip
Collecting data for all nodes
....
....
Logs are being collected to: /scratch/app/crsusr/tfa/repository/
collection_Mon_Aug_22_05_13_41_PDT_2016_node_all
/scratch/app/crsusr/tfa/repository/
collection_Mon_Aug_22_05_13_41_PDT_2016_node_all/
myserver65.tfa_MyCollectionName.zip
/scratch/app/crsusr/tfa/repository/
collection_Mon_Aug_22_05_13_41_PDT_2016_node_all/
myserver66.tfa_MyCollectionName.zip
```

Related Topics

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

6.6 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.

6.7 Performing Silent Collection

1. 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.

6.8 Preventing Collecting Core Files

1. To prevent core files being included:

   ```
   -nocores
   ```

   For example:

   ```
   $ tfactl diagcollect -last 1d -nocores
   ```

Related Topics

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

6.9 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 6-3 tfactl ips Command Parameters

Command	Description
`tfactl ips`	Runs the IPS.

Table 6-3 (Cont.) tfactl ips Command Parameters

Command	Description
`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
   ```

Example 6-1 Show Incidents

```
$ tfactl ips show incidents

ADR Home = /scratch/app/crsusr/diag/clients/user_crsusr/host_622665046_106:

*********************************************************************
0 rows fetched

ADR Home = /scratch/app/crsusr/diag/afdboot/user_root/host_622665046_106:

*********************************************************************
0 rows fetched

ADR Home = /scratch/app/crsusr/diag/rdbms/_mgmtdb/-MGMTDB:

*********************************************************************
```

```
INCIDENT_ID PROBLEM_KEY CREATE_TIME

------------------- ------------------------------------------------------------
--------------------------------------

12913 ORA 700 [kskvmstatact: excessive swapping observed] 2016-06-30 14:05:48.491000
-07:00

12914 ORA 700 [kskvmstatact: excessive swapping observed] 2016-06-30 15:06:16.545000
-07:00

13161 ORA 445 2016-06-30 15:10:53.756000 -07:00

ADR Home = /scratch/app/crsusr/diag/asm/+asm/+ASM1:

*******************************************************************************

INCIDENT_ID PROBLEM_KEY CREATE_TIME

------------------- ------------------------------------------------------------
--------------------------------------

1177 ORA 445 2016-06-30 15:10:12.930000 -07:00

ADR Home = /scratch/app/crsusr/diag/asm/user_root/host_622665046_106:

*******************************************************************************
```

Example 6-2 Show Problems

```
$ tfactl ips show problems

ADR Home = /scratch/app/crsusr/diag/afdboot/user_root/host_622665046_106:

*******************************************************************************

0 rows fetched

ADR Home = /scratch/app/crsusr/diag/rdbms/_mgmtdb/-MGMTDB:

*******************************************************************************

PROBLEM_ID  PROBLEM_KEY LAST_INCIDENT LASTINC_TIME

------------------- ------------------------------------------------------------
--------------------

1 ORA 700 [kskvmstatact: excessive swapping observed] 12914 2016-06-30
15:06:16.545000 -07:00

2 ORA 445 13161  2016-06-30 15:10:53.756000 -07:00

ADR Home = /scratch/app/crsusr/diag/asm/+asm/+ASM1:

*******************************************************************************

PROBLEM_ID PROBLEM_KEY LAST_INCIDENT LASTINC_TIME

------------------- ------------------------------------------------------------
--------------------
```

```
1 ORA 445 1177 2016-06-30 15:10:12.930000 -07:00
```

Example 6-3 Show Packages

```
$ tfactl ips show package

            Multiple ADR homepaths were found for /scratch/app/crsusr, please select
one ...

            ( ) option[0] diag/asmtool/user_root/host_622665046_106
            ( ) option[1] diag/asmtool/user_crsusr/host_622665046_106
            ( ) option[2] diag/clients/user_root/host_622665046_106
            ( ) option[3] diag/clients/user_crsusr/host_622665046_106
            ( ) option[4] diag/afdboot/user_root/host_622665046_106
            ( ) option[5] diag/rdbms/_mgmtdb/-MGMTDB
                option[6] Done

            Pls select a homepath [6] ?5
            diag/rdbms/_mgmtdb/-MGMTDB was selected

               PACKAGE_ID             1
               PACKAGE_NAME           ORA700kge_20160731211334
               PACKAGE_DESCRIPTION
               DRIVING_PROBLEM        2
               DRIVING_PROBLEM_KEY    ORA 700 [kgerev1]
               DRIVING_INCIDENT       42605
               DRIVING_INCIDENT_TIME  2016-07-05 07:53:28.578000 -07:00
               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             2
               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
```

Example 6-4 IPS Collect

```
$ tfactl diagcollect -ips

Collecting data for the last 12 hours for this component ...
Collecting data for all nodes
Creating ips package in master node ...

Multiple ADR homepaths were found for /scratch/app/crsusr, please select one or
more...

( ) option[0] diag/asmtool/user_root/host_622665046_106
( ) option[1] diag/asmtool/user_crsusr/host_622665046_106
( ) option[2] diag/clients/user_root/host_622665046_106
```

```
( ) option[3] diag/clients/user_crsusr/host_622665046_106
( ) option[4] diag/afdboot/user_root/host_622665046_106
( ) option[5] diag/rdbms/_mgmtdb/-MGMTDB
    option[6] Done

Pls select a homepath [6] ?5
diag/rdbms/_mgmtdb/-MGMTDB was selected

Please select at least one ADR homepath.

Multiple ADR homepaths were found for /scratch/app/crsusr, please select one or
more...

( ) option[0] diag/asmtool/user_root/host_622665046_106
( ) option[1] diag/asmtool/user_crsusr/host_622665046_106
( ) option[2] diag/clients/user_root/host_622665046_106
( ) option[3] diag/clients/user_crsusr/host_622665046_106
( ) option[4] diag/afdboot/user_root/host_622665046_106
(*) option[5] diag/rdbms/_mgmtdb/-MGMTDB
    option[6] Done

Pls select a homepath [6] ?
Trying ADR basepath /scratch/app/crsusr
Trying to use ADR homepath diag/rdbms/_mgmtdb/-MGMTDB ...
Submitting request to generate package for ADR homepath /scratch/app/crsusr/diag/
rdbms/_mgmtdb/-MGMTDB
Master package completed for ADR homepath /scratch/app/crsusr/diag/rdbms/_mgmtdb/-
MGMTDB
Created package 15 based on time range 2016-08-21 15:58:00.000000 -07:00 to
2016-08-22 03:58:00.000000 -07:00,
correlation level basic
Remote package completed for ADR homepath(s) /diag/rdbms/_mgmtdb/-MGMTDB


Collection Id : 20160822035856myserver65

Detailed Logging at : /scratch/app/crsusr/tfa/repository/
collection_Mon_Aug_22_03_58_56_PDT_2016_node_all/
diagcollect_20160822035856_myserver65.log
2016/08/22 03:59:40 PDT : Collection Name : tfa_Mon_Aug_22_03_58_56_PDT_2016.zip
2016/08/22 03:59:40 PDT : Collecting diagnostics from hosts : [myserver65,
myserver66]
2016/08/22 03:59:40 PDT : Getting list of files satisfying time range [08/21/2016
15:59:40 PDT, 08/22/2016 03:59:40 PDT]
2016/08/22 03:59:40 PDT : Collecting additional diagnostic information...
2016/08/22 03:59:51 PDT : Completed collection of additional diagnostic
information...
2016/08/22 03:59:51 PDT : Completed Local Collection
2016/08/22 03:59:51 PDT : Remote Collection in Progress...
.----------------------------------------.
|           Collection Summary           |
+------------+-----------+-------+------+
| Host       | Status    | Size  | Time |
+------------+-----------+-------+------+
| myserver66 | Completed | 254kB |  16s |
| myserver65 | Completed | 492kB |  11s |
'------------+-----------+-------+------'

Logs are being collected to: /scratch/app/crsusr/tfa/repository/
collection_Mon_Aug_22_03_58_56_PDT_2016_node_all
/scratch/app/crsusr/tfa/repository/collection_Mon_Aug_22_03_58_56_PDT_2016_node_all/
```

```
myserver66.tfa_Mon_Aug_22_03_58_56_PDT_2016.zip
/scratch/app/crsusr/tfa/repository/collection_Mon_Aug_22_03_58_56_PDT_2016_node_all/
myserver65.tfa_Mon_Aug_22_03_58_56_PDT_2016.zip
```

Related Topics

- tfactl ips
  Use the `tfactl ips` command to collect Automatic Diagnostic Repository diagnostic data.

7

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.

7.1 Querying Oracle Trace File Analyzer Status and Configuration

Use the `print` command to query the status or configuration.

Table 7-1 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	1	Increases the level of verbosity. Possible values: • 1 • 2 • 3 • 4 A value of 1 results in the least amount of trace. A value of 4 results in the most amount of trace. Oracle recommends changing the trace level value only at the request of Oracle Support.
Automatic Purging	ON	Purges collections when: Free space in the repository falls below 1GB. 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.

Example 7-1 Print Configuration

```
$ tfactl print config
.------------------------------------------------------------------------.
|                            node1                                       |
+-----------------------------------------------------------+------------+
| Configuration Parameter                                   | Value      |
+-----------------------------------------------------------+------------+
```

```
| TFA Version                                                |12.2.1.0.0  |
| Java Version                                               | 1.8        |
| Public IP Network                                          | true       |
| 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          |
| Repository current size (MB)                               | 447        |
| Repository maximum size (MB)                               | 10240      |
| Max Size of TFA Log (MB)                                   | 50         |
| Max Number of TFA Logs                                     | 10         |
| Max Size of Core File (MB)                                 | 20         |
| Max Collection Size of Core Files (MB)                     | 200        |
| 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          |
'------------------------------------------------------------+------------'
```

Related Topics

- tfactl print
  Use the `tfactl print` command to print information from the Berkeley database.

7.2 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.

7.3 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

7.3.1 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:

   ```
   $ tfactl set repositorydir=/opt/mypath
   ```

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.

7.3.2 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 diagnostic collections from the Oracle Trace File Analyzer repository that are older than a specific time.
- tfactl print
  Use the `tfactl print` command to print information from the Berkeley database.

7.4 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 -nocores` to reduce the size of collections.

7.4.1 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 database.

7.4.2 Managing the Size of Collections

Use the Oracle Trace File Analyzer configuration options `trimfiles`, `maxcorefilesize`, `maxcorecollectionsize`, and `diagcollect -nocores` to reduce the size of collections.

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 20 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 200 MB):

```
tfactl set maxcorecollectionsize=n
```

   Oracle Trace File Analyzer skips collecting core files after `maxcorecollectionsize` is reached.

4. To prevent the collection of core files with diagnostic collections:

```
tfactl diagcollect -nocores
```

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.

7.5 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 install. Replace those certificates with one of the following:
   - Personal self-signed certificate
   - CA-signed certificate

7.6 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 stop

   tfactl start
   ```

7.7 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.

7.7.1 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
```

7.7.2 Configuring Self-Signed Certificates

Use `Java keytool` to replace self-signed SSL certificates with personal self-signed certificates.

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 server 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. Copy the keystores (`jks` files) to each node.
9. Configure Oracle Trace File Analyzer to use the new certificates:

```
$ tfactl set sslconfig
```

10. Restart the Oracle Trace File Analyzer process to start using new certificates:

```
$ tfactl stop
$ tfactl start
```

7.7.3 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

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 the CA root certificate from the signing authority into the Oracle Trace File Analyzer server certificate:

```
$ keytool -importcert -trustcacerts -alias inter -file caroot.cert -keystore
myserver.jks
```

10. Restrict the permissions on the keystores to `root read-only`:

```
$ chmod 400 myclient.jks myserver.jks
```

11. Copy the keystores (`jks` files) to each node.
12. Configure Oracle Trace File Analyzer to use the new certificates:

```
$ tfactl set sslconfig
```

13. Restart the Oracle Trace File Analyzer process to start using the new certificates.

```
$ tfactl stop
$ tfactl start
```

7.7.4 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`.

1. 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

7.8 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 7-2 tfactl diagnosetfa Command Parameters

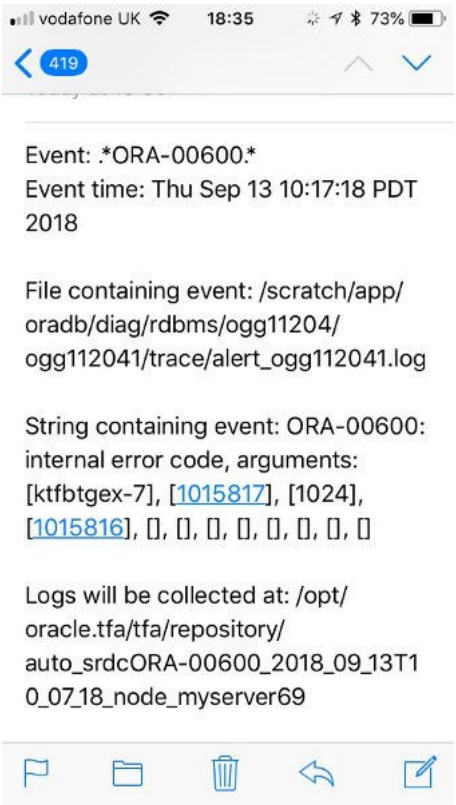
Parameter	Description
`smtp.host`	Specify the SMTP server host name.
`smtp.port`	Specify the SMTP server port.
`smtp.user`	Specify the SMTP user.
`smtp.password`	Specify password for the SMTP user.
`smtp.auth`	Set the Authentication flag to true or false.
`smtp.ssl`	Set the SSL flag to true or false.
`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 7-1 Email Notification



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.

Example 7-2 tfactl set smtp

```
# /u01/app/11.2.0.4/grid/bin/tfactl set 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 | true |
'---------------+-----------'

Enter the SMTP property you want to update : smtp.host
```

```
Enter value for smtp.host : myhost.domain.com

SMTP Property smtp.host updated with myhost.domain.com

Do you want to continue ? [Y]|N : N

#
```

8

Managing Oracle Database and Oracle Grid Infrastructure Diagnostic Data

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.

8.1 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.

8.2 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
   ```

8.3 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
   ```

9

Troubleshooting Oracle Trace File Analyzer

This section helps you diagnose and remediate Oracle Trace File Analyzer issues.

9.1 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.

9.2 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

9.3 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 install, 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
```

```
# ./installTFA-LINUX -perlhome /usr
```

9.4 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 | 12.1.2.6.0  | 12126020151019114604 | UPGRADED       |
| node2 | 12.1.2.6.0  | 12126020151019114604 | UPGRADED       |
'-------+-------------+----------------------+----------------'
```

If you see any differences as follows, then you must fix the issue.

```
.-------------------------------------------------------------.
| Host  | TFA Version | TFA Build ID          | Upgrade Status |
+-------+-------------+-----------------------+----------------+
| node1 | 12.1.2.6.0  | 12126020151019114604  | UPGRADED       |
| node2 | 12.1.2.3.0  | 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.

```
./installTFALite –local
```

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/server.jks
tfa_home/client.jks
tfa_home/internal/ssl.properties
```

9.5 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.

9.6 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.

9.7 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.

```
-bash-3.2$ /u01/app/12.1.0/grid/bin/tfactl diagcollect
Collecting data for the last 4 hours for this component...
Collecting data for all nodes
```

```
Repository Location in sales1 : /u01/app/oragrid/tfa/repository
2015/06/30 05:25:27 PDT : Collection Name : tfa_Tue_Jun_30_05_25_20_PDT_2015.zip
2015/06/30 05:25:27 PDT : Sending diagcollect request to host : sales2
2015/06/30 05:25:27 PDT : Sending diagcollect request to host : sales3
2015/06/30 05:25:27 PDT : Sending diagcollect request to host : sales4
2015/06/30 05:25:27 PDT : Scanning of files for Collection in progress...
....
....
....
2015/06/30 05:25:37 PDT : Remote Collection in Progress...
2015/06/30 05:25:57 PDT : sales3:Completed Collection
2015/06/30 05:26:07 PDT : sales2:Failed Unable to connect to Node sales2
2015/06/30 05:26:07 PDT : sales4:Failed Unable to connect to Node sales4
2015/06/30 05:26:07 PDT : Completed collection of zip files.
```

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.

9.8 OSWatcher Parameters are Different After a Reboot or Otherwise Unexpectedly Different

When Oracle Trace File Analyzer manages OSWatcher, after an install 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.

9.9 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`.

9.10 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.

9.11 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
   ```

9.12 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.

9.13 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 lsuser
/u01/app/12.1.0/grid/bin/tfactl access lsusers
.---------------------------------.
| TFA Users in myNode1            |
+-----------+-----------+---------+
| 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:

To enable non-privileged user access:

```
tfactl access enable
```

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.

9.14 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
   ```

3. Try starting the Oracle Trace File Analyzer daemon as `root`.

   ```
   # tfactl start
   ```

   If Oracle Trace File Analyzer still fails to start, then run `tfactl diagnosetfa -local`. Upload the resultant file to Oracle Support.

A

Oracle Trace File Analyzer Installer, Command-Line and Shell Options

The Trace File Analyzer control utility, TFACTL, is the command-line interface for Oracle Trace File Analyzer.

TFACTL provides a command-line and shell interface to Oracle Trace File Analyzer commands for:

- Administration
- Summary and analysis
- Diagnostic collection

The `tfactl` commands that you can run depends on your access level.

- You need `root` access or `sudo` access to `tfactl` to run administration commands.
- 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

  You gain access to summary, analysis, and diagnostic collection functionality by running the commands as an Oracle Database home owner or Oracle Grid Infrastructure home owner.

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:

```
tfactl
```

Once the shell starts enter commands as needed.

```
$ tfactl

tfactl>
```

Append the `-help` option to any of the `tfactl` commands to obtain command-specific help.

```
$ tfactl command -help
```

- Installing Oracle Trace File Analyzer
  Understand the options that you can supply to the Oracle Trace File Analyzer installer script to customize the installation.

- Running Administration Commands
  You need `root` access to `tfactl`, or `sudo` access to run all administration commands.
- Running 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 Diagnostic Collection Commands
  Run the diagnostic collection commands to collect diagnostic data.

A.1 Installing Oracle Trace File Analyzer

Understand the options that you can supply to the Oracle Trace File Analyzer installer script to customize the installation.

Without parameters the Oracle Trace File Analyzer installation script will take you through an interview process for installation.

The Oracle Trace File Analyzer installation script appends `/tfa` to `-tfabase` if it is not already there.

The Oracle Trace File Analyzer installation script writes the log to the `/tmp/tfa_install_`*`timestamp`*`.log` file, for example, `/tmp/tfa_install_9263_2018_09_25-07_55_52.log`.

Syntax

`installTFA-`*`platform`* `[[-local][-deferdiscovery][-tfabase` *`install dir`*`][-javahome` *`path to JRE`*`][-silent]|-extractto` *`extract dir`*`|-responsefile` *`response file`*`|-noorachk]`

Parameters

Table A-1 installTFA-<platform> Command Parameters

Parameter	Description
`-local`	Installs only on the local node.
`-deferdiscovery`	Discovers Oracle trace directories after installation completes.
`-tfabase`	Installs in the directory specified.
`-javahome`	Use this directory for the JRE. Do not use this option along with the `-extractto` option.
`-silent`	Use this option to not to ask any install questions.
`-extractto`	Extracts Oracle Trace File Analyzer into the directory specified (non-daemon mode).
`-tmploc`	Extracts the install archive into the temporary directory location specified (must exist).
`-debug`	Displays debug tracing and does not remove TFA_HOME on install failure.
`-perlhome`	Specify the custom location for Perl binaries.
`-responsefile`	Specify the response file to use to drive Oracle Trace File Analyzer setup parameters.

Table A-1 (Cont.) installTFA-<platform> Command Parameters

Parameter	Description
`-noorachk`	Specify the skip Oracle ORAchk autostart.

A.2 Running Administration Commands

You need `root` access to `tfactl`, or `sudo` access to run all administration commands.

Table A-2 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 allow 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.
- 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 stop any running Oracle Trace File Analyzer daemon and disable automatic restart.
- 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 host
  Use the `tfactl host` command to add hosts to, or remove hosts from the Oracle Trace File Analyzer configuration.
- tfactl print
  Use the `tfactl print` command to print information from the Berkeley database.
- tfactl rest
  Use the `tfactl rest` command to configure REST service.
- 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 setupmos
  Use the `tfactl setupmos` command to store My Oracle Support credentials in Oracle wallet.
- 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 status
  Use the `tfactl status` command to check the run status of Oracle Trace File Analyzer.
- 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 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 start` command to to uninstall Oracle Trace File Analyzer.
- tfactl upload
  Use the `tfactl upload` command to upload collections or files to a Service Request.

A.2.1 tfactl access

Use the `tfactl access` command to allow 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 and groups using the `tfactl access` command. Add or remove non-root users and groups 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.

Syntax

```
tfactl access command [options]
Commands:lsusers|add|remove|block|unblock|enable|disable|reset|removeall

tfactl access lsusers [ -local ]

tfactl access add -user user_name [ -local ]

tfactl access remove -user user_name [ -all ] [ -local ]

tfactl access block -user user_name [ -local ]

tfactl access unblock -user user_name [ -local ]

tfactl access enable [ -local ]

tfactl access disable [ -local ]

tfactl access reset

tfactl access removeall
```

Parameters

Table A-3 tfactl access Command Parameters

Parameter	Description
`lsusers`	Lists all the Oracle Trace File Analyzer users and groups.
`enable`	Enables Oracle Trace File Analyzer access for non-root users. Use the `-local` flag to change settings only on the local node.
`disable`	Disables 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 enabled later. Use the `-local` flag to change settings only on the local node.
`add`	Adds a user or a group to the Oracle Trace File Analyzer access list.
`remove`	Removes a user or a group 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 even though the user is a member of a group that is granted access to Oracle Trace File Analyzer.

Table A-3 (Cont.) tfactl access Command Parameters

Parameter	Description
`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`.
`reset`	Resets to the default access list that includes all Oracle Home owners and DBA groups.
`removeall`	Removes all Oracle Trace File Analyzer users and groups. Remove all users from the Oracle Trace File Analyzer access list including the default users and groups.

Example A-1 tfactl access

To list all the Oracle Trace File Analyzer users and groups.

```
$ tfactl access lsusers

.---------------------------------.
|     TFA Users in rws1270069     |
+-----------+-----------+---------+
| User Name | User Type | Status  |
+-----------+-----------+---------+
| oradb     | USER      | Allowed |
| oragrid   | USER      | Allowed |
'-----------+-----------+---------'
```

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 all members of a group, for example, *xyz* to the Oracle Trace File Analyzer access list and enable access to Oracle Trace File Analyzer on the localhost.

```
$ tfactl access add -group xyz -local
```

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 remove all Oracle Trace File Analyzer users and groups.

```
$ tfactl access removeall
```

A.2.2 tfactl availability

Use the `tfactl availability` command to enable or disable resources for Availability Score.

Syntax

```
tfactl enable -key key -value value  | -list

tfactl  disable -key key -value value [-for nd|D|h|H|m|M]  | -list [-for nd|D|h|H|m|
M]
```

Parameters

Table A-4 tfactl 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 A-5 tfactl 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..

Example A-2 tfactl enable

```
/scratch/app/11.2.0.4/grid/bin/tfactl availability enable -list
/scratch/app/11.2.0.4/grid/bin/tfactl availability enable -type server_disk -key
filesystem -value "/dev/xvdad1"
/scratch/app/11.2.0.4/grid/bin/tfactl availability enable -type server_network -key
interface -value eth1
```

Example A-3 tfactl disable

```
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -list
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -list -for 3d
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -list -for 15h
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -type server_disk -key
filesystem -value "/dev/xvdad1"
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -type server_network -key
interface -value eth1
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -type server_disk -key
filesystem -value "/dev/xvdad1" -for 3d
/scratch/app/11.2.0.4/grid/bin/tfactl availability disable -type server_network -key
interface -value eth1 -for 12h
```

A.2.3 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 A-6 tfactl diagnosetfa Command Parameters

Parameter	Description
`-repo` *repository*	Specify the repository directory for 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.

Example A-4 tfactl diagnosetfa

```
$ tfactl diagnosetfa -local

Running TFA Diagnostics...

Node List to collect TFA Diagnostics :
     1  myhost

Running TFA Diagnostics on myhost...

Wed Sep 12 00:12:18 2018 : Collecting TFA Process details...
Wed Sep 12 00:12:18 2018 : Collecting Details of TFA Files...
Wed Sep 12 00:12:19 2018 : Collecting CRS Status...
Wed Sep 12 00:12:19 2018 : Collecting GI Install Logs...
Wed Sep 12 00:19:15 2018 : Collecting TFA Install Logs...
Wed Sep 12 00:19:15 2018 : Collecting Disk Space...
Wed Sep 12 00:19:16 2018 : Collecting Top Output...
Wed Sep 12 00:19:16 2018 : Collecting TFA Status...
Wed Sep 12 00:19:19 2018 : Collecting JStack Output...
Wed Sep 12 00:19:31 2018 : Collecting TFA Logs...
Wed Sep 12 00:19:32 2018 : Collecting TFA BDB Stats...
Wed Sep 12 00:19:43 2018 : Zipping Collections...

Sleeping for 10 Seconds...

TFA Diagnostics are being collected to /tmp/tfadiagnostics_20180912_001217 :
/tmp/tfadiagnostics_20180912_001217/myhost.zip
```

A.2.4 tfactl disable

Use the `tfactl disable` command to stop any running Oracle Trace File Analyzer daemon and disable automatic restart.

Syntax

```
tfactl disable
```

A.2.5 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
```

A.2.6 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 database.

Example A-5 tfactl host

Specify a host name to add:

```
$ tfactl host add myhost
```

Specify a host name to remove:

```
$ tfactl host remove myhost
```

A.2.7 tfactl print

Use the `tfactl print` command to print information from the Berkeley database.

Syntax

```
tfactl print command [options]
Commands:status|components|config|directories|hosts|actions|repository|suspendedips|
protocols|smtp

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 hosts

tfactl print actions [ -status status ] [ -since nh|d ]

tfactl print repository

tfactl print suspendedips

tfactl print protocols

tfactl print smtp
```

Parameters

Table A-7 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.

Table A-7 (Cont.) tfactl print Command Parameters

Parameter	Description
`suspendedips`	Lists all paused Oracle Trace File Analyzer IPS collections.
`protocols`	Lists all available and restricted protocols.
`smtp`	Displays the SMTP server configuration

Options

Option	Description
`-status` *`status`*	Action status can be one or more of `COMPLETE`, `RUNNING`, `FAILED`, `REQUESTED` Specify a comma-separated list of statuses.
`-since` *`nh|d`*	Specify actions from past *n* days or *n* hours.

Example A-6 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 A-7 tfactl print protocols

```
tfactl print protocols

.-------------------------------------------------.
|                   rws1270069                    |
+-------------------------------------------------+
| Protocols                                       |
+-------------------------------------------------+
| Available : [TLSv1.2]                           |
| Restricted : [SSLv3, SSLv2Hello, TLSv1, TLSv1.1] |
'-------------------------------------------------'
```

Example A-8 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 A-9 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 A-10 tfactl print config

```
$ tfactl print config

.-------------------------------------------------------------------------------
.
|                                    rws1270069
|
+-------------------------------------------------------------------+------------
+
| Configuration Parameter                                           | Value
|
+-------------------------------------------------------------------+------------
+
| TFA Version                                                       | 18.3.0.0.0
|
| Java Version                                                      | 1.8
|
| Public IP Network                                                 | true
|
| 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
|
| Repository current size (MB)                                           | 588
|
| Repository maximum size (MB)                                           | 4724
|
| 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
|
| 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)                                            | 2592000
|
| TFA ISA Purge Mode                                                     | simple
|
'------------------------------------------------------------------------
+------------'
```

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.

A.2.8 tfactl rest

Use the `tfactl rest` command to configure REST service.

Syntax

```
tfactl rest
[-status|-start|-stop|-upgrade|-uninstall]
[-dir directory]
[-port port]
[-user user]
[-debug [-level debug_level 1-6]]
```

> **Note:**
>
> You can run the REST command only as `root` user.

Parameters

Table A-8 REST Command Parameters

Parameter	Description
`-status`	Prints the current status.
`-start`	Starts Oracle Trace File Analyzer REST services if not already running.
`-stop`	Stops Oracle Trace File Analyzer REST services if running.
`-upgrade`	Checks if the configured ORDS API should be upgraded. If the ORDS API needs upgrading, then stops ORDS, upgrades the API, and then restarts ORDS.
`-uninstall`	Removes the Oracle Trace File Analyzer REST configuration.

Table A-8 (Cont.) REST Command Parameters

Parameter	Description
`-dir`	The directory to use to store the Oracle Trace File Analyzer REST configuration details. Defaults to the users home directory.
`-port`	The port to run ORDS on. Defaults to 9090.
`-user`	The user to start ORDS as. Defaults to the GRID owner.
`-debug`	Enables debug.
`-level`	The level of debug to use, where available levels are: • 1 – FATAL • 2 – ERROR • 3 – WARNING • 4 – INFO (default) • 5 – DEBUG • 6 – TRACE

A.2.9 tfactl restrictprotocol

Use the `tfactl restrictprotocol` command to restrict certain protocols.

Syntax

```
tfactl restrictprotocol [-force] protocol
```

Example A-11 tfactl restrictprotocol

```
$ tfactl restrictprotocol TLSv1
```

A.2.10 tfactl sendmail

Use the `tfactl sendmail` command to send a test email to verify SMTP configuration.

Syntax

```
tfactl sendmail email_address
```

A.2.11 tfactl set

Use the `tfactl set` command to enable or disable, or modify various Oracle Trace File Analyzer functions.

Syntax

```
tfactl set
[ autodiagcollect=ON|OFF
| trimfiles=ON|OFF
| tracelevel=COLLECT|SCAN|INVENTORY|OTHER:1|2|3|4
| reposizeMB=n
| repositorydir=dir [-force]
```

```
| logsize=n [-local]
| logcount=n [-local]
| maxcorefilesize=n [-local]
| maxcorecollectionsize=n [-local] autopurge=ON|OFF
| publicip=ON|OFF
| minSpaceForRTScan=n
| rtscan=ON|OFF
| diskUsageMon=ON|OFF
| diskUsageMonInterval=n
| manageLogsAutoPurge=ON|OFF
| manageLogsAutoPurgeInterval=n
| manageLogsAutoPurgePolicyAge=d|h
| minagetopurge=n
| tfaIpsPoolSize=n
| tfaDbUtlPurgeAge=n
| tfaDbUtlPurgeMode=simple|resource ]
[-c]
```

Parameters

Table A-9 tfactl set Command Parameters

Parameter	Description
`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.
`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: 1 | 2 | 3 | 4`	You can set trace levels for certain operations, including `INVENTORY:n`, `SCAN:n`, `COLLECT:n`, `OTHER:n`. In this syntax, *n* is a number from 1 to 4 and `OTHER` includes all messages not relevant to the first three components. **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 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 is 50 MB). Use the `-local` parameter to apply the change only to the local node.
`logcount=n [-local]`	Sets the maximum number of logs of specified size that Oracle Trace File Analyzer retains (default is 10). Use the `-local` option to apply the change only to the local node.
`port=n`	Specify the Oracle Trace File Analyzer port.

Table A-9 (Cont.) tfactl set Command Parameters

Parameter	Description
`maxcorefilesize=n [-local]`	Sets the maximum size of the core files to the size specified in MB (default is 20 MB).
`maxcorecollectionsize=n`	Sets the maximum collection size of the core files to the size specified in MB (default is 200 MB).
`publicip=ON|OFF`	Allows Oracle Trace File Analyzer to run on public network.
`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 (default is 500).
`rtscan`	Specify to allow Oracle Trace File Analyzer to perform alert log scanning.
`diskUsageMon=ON|OFF`	Turns ON (default) or OFF monitoring disk usage and recording snapshots. Oracle Trace File Analyzer stores the snapshots under `tfa/repository/suptools/node/managelogs/usage_snapshot/`.
`diskUsageMonInterval=minutes`	Specify the time interval between snapshots (60 minutes by default).
`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 is 60 minutes).
`manageLogsAutoPurgePolicyAge=nd|h`	Age of logs to be purged (30 days by default).
`minagetopurge=n`	Set the minimum age, in hours, for a collection before Oracle Trace File Analyzer considers it for purging (default is 12 hours).
`autopurge`	When set to `ON`, enables automatic purging of collections when Oracle Trace File Analyzer observes less space in the repository (default is `ON`).
`tfaIpsPoolSize=n`	Sets the Oracle Trace File Analyzer IPS pool size.
`tfaDbUtlPurgeAge=n`	Sets the Oracle Trace File Analyzer ISA purge age (in seconds).
`tfaDbUtlPurgeMode=simple|resource`	Sets the Oracle Trace File Analyzer ISA purge mode (simple/resource).
`-c`	Propagates the settings to all nodes in the Oracle Trace File Analyzer configuration.

Example A-12 tfactl set

```
$ tfactl set autodiagcollect=ON reposizeMB=20480
$ tfactl set autodiagcollect=ON
$ tfactl set autopurge=ON
$ tfactl set tracelevel=INVENTORY:3
$ tfactl set reposizeMB=20480
$ tfactl set logsize=100
$ tfactl set port=5000
```

A.2.12 tfactl setupmos

Use the `tfactl setupmos` command to store My Oracle Support credentials in Oracle wallet.

Syntax

```
tfactl setupmos
```

A.2.13 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]
```

A.2.14 tfactl status

Use the `tfactl status` command to check the run status of Oracle Trace File Analyzer.

Syntax

```
tfactl status
```

Example A-13 tfactl status

```
$ /tfactl status

.-------------------------------------------------------------------------------
------------.
| Host       | Status of TFA | PID | Port | Version    | Build ID             |
Inventory Status |
+------------+---------------+-----+------+------------+----------------------
+------------------+
| rws1270069 | RUNNING       | 316 | 5000 | 18.3.0.0.0 | 18300020180828031750 |
COMPLETE         |
'------------+---------------+-----+------+------------+----------------------
+------------------'
```

A.2.15 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]
```

A.2.16 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 A-10 tfactl syncnodes Command Parameters

Parameter	Description
`-regenerate`	Regenerates Oracle Trace File Analyzer certificates.

A.2.17 tfactl uninstall

Use the `tfactl start` command to to uninstall Oracle Trace File Analyzer.

Syntax

Run the `uninstall` command as `root`, or install user

```
tfactl uninstall
```

A.2.18 tfactl upload

Use the `tfactl upload` command to upload collections or files to a Service Request.

Syntax

```
tfactl upload -sr SR# [ -user UserId | -wallet ] Files
```

Parameters

Table A-11 tfactl upload Command Parameters

Parameter	Description
`-sr` *`SR#`*	Specify the service request number to use for file upload.
`-user` *`userid`*	Specify the My Oracle Support user ID.
`-wallet`	Use this option for the `upload` command to use credentials from Oracle wallet.
`Files`	Specify a space-separated list of files that you want to upload.

A.3 Running 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 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 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.

A.3.1 tfactl analyze

Use the `tfactl analyze` command to obtain analysis of your system by parsing the database, 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 "MMM/DD/YYYY HH24:MI:SS"]
[-to "MMM/DD/YYYY HH24:MI:SS"]
[-for "MMM/DD/YYYY HH24:MI:SS"]
[-node all|local|n1,n2,...]
[-verbose]
[-o file]
[-examples]
```

Parameters

Table A-12 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.
`-from | -to | -for "MMM/DD/YYYY HH24:MI:SS"`	Specify a time interval, using the `-from` and `-to` parameters together, or a specific time using the `-for` parameter, that you want Oracle Trace File Analyzer to analyze.
`[-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.

Table A-12 (Cont.) tfactl analyze Command Parameters

Parameter	Description
`-o file`	Specify a file where Oracle Trace File Analyzer writes the output instead of displaying on the screen.
`[-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 A-13 tfactl analyze -type Parameter Arguments

Argument	Description

`error`	Error message patterns for 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`
	
	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:.*`

`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 A-14 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 A-15 oratop options

Argument	Description
`-d`	Real-time (RT) wait events (section 3. Default is Cumulative..
`-k`	FILE#:BLOCK#, section 4 It is (EVENT/LATCH).
`-m`	Specify `MODULE/ACTION` (section 4). Default is `USERNAME/PROGRAM`.
`-s`	Specify the SQL mode (section 4). Default is process mode.
`-c`	Specify the Oracle Database service mode. Default is connect string.
`-f`	Specify the detailed format (132 columns). Default is standard (80 columns).
`-b`	Specify the batch mode. Default is text-based user interface.
`-n`	Specify the maximum number of iterations.
`-i`	Specify the interval delay in seconds. Default is 5 seconds.

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 alert and system log files from the past two days for messages that contain the case-insensitive string "error".

- `$ tfactl analyze -comp os -for "Jul/01/2016 11" -search "."`

  Oracle Trace File Analyzer displays all system log messages for July 1, 2016 at 11 am.

- `$ tfactl analyze -search "/ORA-/c" -comp db -last 2d`

  Oracle Trace File Analyzer searches database alert logs for the case-sensitive string "ORA-" from the past two days.

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 collected from all alert logs and system messages from the past five hours.

- `$ tfactl analyze -comp os -last 1d`

  Oracle Trace File Analyzer displays a summary of events from system messages from the past day.

- `$ tfactl analyze -last 1h -type generic`

  Oracle Trace File Analyzer analyzes all generic messages from the last hour.

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 "2016-07-01" -to "2016-07-03"`

  Oracle Trace File Analyzer displays `OSWatcher` Slabinfo summary for specified time period.

A.3.2 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).

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
-bash-4.1# tfactl analyze
INFO: analyzing all (Alert and Unix System Logs) logs for the last 60 minutes...
Please wait...
INFO: analyzing host: myserver69

                     Report title: Analysis of Alert,System Logs
                Report date range: last ~1 hour(s)
         Report (default) time zone: UTC - Coordinated Universal Time
                Analysis started at: 26-Jul-2016 10:36:03 AM UTC
              Elapsed analysis time: 1 second(s).
                 Configuration file: /scratch/app/11.2.0.4/grid/tfa/myserver69/
tfa_home/ext/tnt/conf/tnt.prop
                Configuration group: all
                Total message count:         15,261, from 20-Nov-2015 02:06:21 AM
UTC to 26-Jul-2016 10:10:58 AM UTC
  Messages matching last ~1 hour(s):              1, from 26-Jul-2016 10:10:58 AM
UTC to 26-Jul-2016 10:10:58 AM UTC
        last ~1 hour(s) error count:              0
last ~1 hour(s) ignored error count:              0
 last ~1 hour(s) unique error count:              0

Message types for last ~1 hour(s)
   Occurrences percent  server name          type
   ----------- -------  -------------------- -----
             1  100.0%  myserver69           generic
   ----------- -------
             1  100.0%

Unique error messages for last ~1 hour(s)
   Occurrences percent  server name          error
   ----------- -------  -------------------- -----
   ----------- -------
             0  100.0%
```

A.3.3 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 ASM or CRS 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.

`-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

Example

```
$ tfactl events
Output from host : myserver69
------------------------------
Jul/25/2016 06:25:33 :
           [crs.myserver69] : [cssd(7513)]CRS-1603:CSSD on node myserver69 shutdown
by user.
Jul/25/2016 06:32:41 :
           [crs.myserver69] : [cssd(5794)]CRS-1601:CSSD Reconfiguration complete.
Active nodes are myserver69 myserver70 myserver71 .
Jul/25/2016 06:47:37 :
           [crs.myserver69] : [/scratch/app/11.2.0.4/grid/bin/scriptagent.bin(16233)]
CRS-5818:Aborted command 'start' for resource 'ora.oc4j'. Details at (:CRSAGF00113:)
{1:32892:193} in /scratch/app/11.2.0.4/grid/log/myserver69/agent/crsd/
scriptagent_oragrid/scriptagent_oragrid.log.
Jul/25/2016 06:24:43 :
           [db.apxcmupg.apxcmupg_1] : Instance terminated by USER, pid = 21581
Jul/25/2016 06:24:43 :
           [db.rdb11204.rdb112041] : Instance terminated by USER, pid = 18683
Jul/25/2016 06:24:44 :
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "FRA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "FRA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "FRA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "FRA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "FRA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "DATA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "DATA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "DATA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "DATA" does not exist or is not mounted
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15001: diskgroup "DATA" does not exist or is not mounted
Jul/25/2016 06:24:53 :
           [db.+ASM1] : ORA-15032: not all alterations performed
           [db.+ASM1] : ORA-15027: active use of diskgroup "VDATA" precludes its
dismount
Jul/25/2016 06:25:22 :
           [db.+ASM1] : Shutting down instance (immediate)
           [db.+ASM1] : Shutting down instance: further logons disabled

Summary :
=========
INFO    : 2
ERROR    : 26
WARNING    : 1
```

A.3.4 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 A-16 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.

A.3.5 tfactl run

Use the `tfactl run` command to run the requested action (can be inventory or scan or any support tool).

Syntax

```
tfactl run [inventory | scan | tool]
```

Parameters

Table A-17 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 A-18 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 CRS log / trace levels using profiles.

Table A-18 (Cont.) tfactl run Analysis Tools Parameters

Parameter	Description
`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 A-19 tfactl run Profiling Tools Parameters

Parameter	Description
`dbglevel`	Sets CRS log and trace levels using profiles.

A.3.6 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 A-20 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.

A.3.7 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] CRS 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
`-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

Example A-14 tfactl summary

```
$ tfactl summary
LOGFILE LOCATION : /opt/oracle.tfa/tfa/repository/suptools/myhost/summary/root/
20180912055547/log/summary_command_20180912055547_myhost_5136.log

  Component Specific Summary collection :
    - Collecting CRS details ... Done.
    - Collecting ASM details ... Done.
    - Collecting ACFS details ... Done.
    - Collecting DATABASE details ... Done.
```

```
    - Collecting PATCH details ... Done.
    - Collecting LISTENER details ... Done.
    - Collecting NETWORK details ... Done.
    - Collecting OS details ... Done.
    - Collecting TFA details ... Done.
    - Collecting SUMMARY details ... Done.

  Prepare Clusterwide Summary Overview ... Done
      cluster_status_summary

  COMPONENT   STATUS    DETAILS
+-----------+---------
+-------------------------------------------------------------------------------
-------------+
  CRS         OK        .-----------------------------------------------.
                        | CRS_SERVER_STATUS   : ONLINE                  |
                        | CRS_STATE           : ONLINE                  |
                        | CRS_INTEGRITY_CHECK : PASS                    |
                        | CRS_RESOURCE_STATUS : OFFLINE Resources Found |
                        '-----------------------------------------------'
  ASM         PROBLEM   .-------------------------------------------------------.
                        | ASM_DISK_SIZE_STATUS : WARNING - Available Size < 20% |
                        | ASM_BLOCK_STATUS     : PASS                           |
                        | ASM_CHAIN_STATUS     : PASS                           |
                        | ASM_INCIDENTS        : PASS                           |
                        | ASM_PROBLEMS         : FAIL                           |
                        '-------------------------------------------------------'
  ACFS        OFFLINE   .----------------------.
                        | ACFS_STATUS : OFFLINE |
                        '----------------------'

DATABASE              .-------------------------------------------------------------
------------------------------.
                        |
ORACLE_HOME_DETAILS                                                     |
ORACLE_HOME_NAME |

+-------------------------------------------------------------------------
+------------------+

| .-------------------------------------------------------------------. |
OraDb11g_home1   |
                        | | PROBLEMS | INCIDENTS | DB_BLOCKS | DATABASE_NAME |
STATUS | DB_CHAINS | |                 |
                        | +----------+-----------+-----------+---------------
+--------+-----------+ |                 |
                        | | PASS     | PASS      | PASS      | apxcmupg      |
OK     | PASS      | |                 |
                        | '----------+-----------+-----------+---------------
+--------+-----------' |                 |

'-------------------------------------------------------------------------
+------------------'
  PATCH       OK        .-----------------------------------------------.
                        | CRS_PATCH_CONSISTENCY_ACROSS_NODES      : OK |
                        | DATABASE_PATCH_CONSISTENCY_ACROSS_NODES : OK |
                        '-----------------------------------------------'
  LISTENER    OK        .----------------------.
                        | LISTNER_STATUS   : OK |
                        '----------------------'
  NETWORK     PROBLEM   .-----------------------------------.
```

```
                        | NODE_APPLICATION_CHECK : FAIL       |
                        | NODE_CONNECTIVITY : FAIL            |
                        | NTP_DAEMON_SLEW_OPTION_CHECK : FAIL |
                        '-------------------------------------'
  OS          OK        .----------------------.
                        | MEM_USAGE_STATUS : OK |
                        '----------------------'
  TFA         OK        .---------------------.
                        | TFA_STATUS : RUNNING |
                        '---------------------'
  SUMMARY     OK        .-----------------------------------.
                        | SUMMARY_EXECUTION_TIME : 0H:1M:42S |
                        '-----------------------------------'
+-----------+---------
+-------------------------------------------------------------------------------------
-------------+


       ### Entering in to SUMMARY Command-Line Interface ###

tfactl_summary>list

  Components : Select Component - select [component_number|component_name]
       1 => overview
       2 => crs_overview
       3 => asm_overview
       4 => acfs_overview
       5 => database_overview
       6 => patch_overview
       7 => listener_overview
       8 => network_overview
       9 => os_overview
       10 => tfa_overview
       11 => summary_overview

tfactl_summary>9

  IDLE_TIME   SWAP_USED   #CORES   HOSTNAME     MEM_USED   TASKS   LOAD   #PROCESSORS
+-----------+-----------+--------+------------+----------+-------+------
+-------------+
       78.7    8.11 %          1   myhost                    389   1.87             4
+-----------+-----------+--------+------------+----------+-------+------
+-------------+

tfactl_summary_osoverview>list

  Status Type: Select Status Type - select [status_type_number|status_type_name]
       1 => os_clusterwide_status
       2 => os_myhost

tfactl_summary_osoverview>1

  IDLE_TIME   SWAP_USED   #CORES   HOSTNAME     MEM_USED   TASKS   LOAD   #PROCESSORS
+-----------+-----------+--------+------------+----------+-------+------
+-------------+
       78.7    8.11 %          1   myhost                    389   1.87
4
+-----------+-----------+--------+------------+----------+-------+------
+-------------+
```

```
  Status Type: Select Status Type - select [status_type_number|status_type_name]
        1 => os_clusterwide_status
        2 => os_myhost

tfactl_summary_osoverview>back

  Components : Select Component - select [component_number|component_name]
        1 => overview
        2 => crs_overview
        3 => asm_overview
        4 => acfs_overview
        5 => database_overview
        6 => patch_overview
        7 => listener_overview
        8 => network_overview
        9 => os_overview
        10 => tfa_overview
        11 => summary_overview

tfactl_summary>help

  Following commands are supported in Summary Command-Line Interface
    l|list         => List Supported Components|Nodes|Databases|Tables
    number|select  => Select Component|Node|Database Listed in 'list'
    b|back         => UnSelect Component|Node|Database
    c|clear        => Clear Console
    q|quit         => Quit Summary Command-Line Interface
    ~              => Summary Command-Line Interface Home
    h|help         => Help

tfactl_summary>q

        ### Exited From SUMMARY Command-Line Interface ###

------------------------------------------------------------------------
REPOSITORY  : /opt/oracle.tfa/tfa/repository/suptools/myhost/summary/root/
20180912055547/myhost
------------------------------------------------------------------------
```

A.3.8 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 A-15 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.
```

A.4 Running Diagnostic Collection Commands

Run the diagnostic collection commands to collect diagnostic data.

- tfactl collection
  Use the `tfactl collection` command to stop a running Oracle Trace File Analyzer collection.
- 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 diagnostic collections from the Oracle Trace File Analyzer repository that are older than a specific time.

A.4.1 tfactl collection

Use the `tfactl collection` command to stop a running Oracle Trace File Analyzer collection.

Syntax

```
tfactl collection [stop collection_id]
```

You can only stop a collection using the `tfactl collection` command. You must provide a collection ID, which you can obtain by running the `tfactl print` command.

A.4.2 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 A-21 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.

Table A-21 (Cont.) tfactl dbglevel Command Parameters

Parameter	Description
`lsprofiles`	Lists all the available profiles.
`lsmodules`	Lists all the discovered CRS modules.
`lscomponents`	Lists all the components associated with the CRS module.
`lsres`	Lists all the discovered CRS resources.
`getstate`	Displays the current trace or log levels for the CRS components or resources.
`module`	Specify the CRS 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 CRS components or resources.
`includetrace`	Adds or modifies a trace value for the CRS components.

WARNING:

Set the profiles only at the direction of Oracle Support.

A.4.3 tfactl diagcollect

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

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

Prerequisites

Event-driven Support Service Request Data Collection (SRDC collections require components from the Oracle Trace File Analyzer Database Support Tools Bundle, which is available from My Oracle Support Note 1513912.2.

Syntax

```
tfactl diagcollect [[component_name1] [component_name2] ... [component_nameN] | [-
srdc srdc_profile] | [-defips]]
[-sr SR#]
[-node all|local|n1,n2,...]
[-tag tagname]
```

```
[-z filename]
[-last nh|d | -from time -to time | -for time]
[-nocopy]
[-notrim]
[-silent]
[-nocores]
[-collectalldirs]
[-collectdir dir1,dir2...]
[-examples]

Components:-ips|-database|-asm|-crsclient|-dbclient|-dbwlm|-tns|-rhp|-procinfo|-afd|-
crs|-cha|-wls|-emagent|-oms|-ocm|-emplugins|-em|-acfs
|-install|-cfgtools|-os|-ashhtml|-ashtext|-awrhtml|-awrtext
```

Parameters

Prefix each option with a minus sign (-).

Option	Description
`[[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 IPS Packages for ASM, CRS, and Oracle Databases in the default collection.
`[-sr SR#]`	Specify the Service Request number to which Oracle Trace File Analyzer automatically uploads all collections.
`-node all|local| n1,n2,...`	Specify a comma-delimited list of nodes from which to collect diagnostic information. Default is all.
`-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.
`-silent`	Specify this parameter to run diagnostic collection as a background process
`-nocores`	Specify this parameter to stop collecting core files when it would normally have 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.
`-examples`	Specify this parameter to view `diagcollect` usage examples.

Example A-16 tfactl diagcollect

```
$ tfactl diagcollect

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 : 20180912012618myhost

Detailed Logging at : /opt/oracle.tfa/tfa/repository/
collection_Wed_Sep_12_01_26_18_PDT_2018_node_all/
diagcollect_20180912012618_myhost.log
2018/09/12 01:26:23 PDT : NOTE : Any file or directory name containing the
string .com will be renamed to replace .com with dotcom
2018/09/12 01:26:23 PDT : Collection Name : tfa_Wed_Sep_12_01_26_18_PDT_2018.zip
2018/09/12 01:26:23 PDT : Collecting diagnostics from hosts : [myhost]
2018/09/12 01:26:23 PDT : Scanning of files for Collection in progress...
2018/09/12 01:26:23 PDT : Collecting additional diagnostic information...
2018/09/12 01:27:18 PDT : Getting list of files satisfying time range [09/11/2018
13:26:23 PDT, 09/12/2018 01:27:18 PDT]
2018/09/12 01:28:03 PDT : Collecting ADR incident files...
2018/09/12 01:28:28 PDT : Completed collection of additional diagnostic
information...
2018/09/12 01:28:38 PDT : Completed Local Collection
.-------------------------------------.
|          Collection Summary         |
+------------+-----------+------+------+
| Host       | Status    | Size | Time |
+------------+-----------+------+------+
| myhost     | Completed | 71MB | 135s |
'------------+-----------+------+------'

Logs are being collected to: /opt/oracle.tfa/tfa/repository/
collection_Wed_Sep_12_01_26_18_PDT_2018_node_all
/opt/oracle.tfa/tfa/repository/collection_Wed_Sep_12_01_26_18_PDT_2018_node_all/
myhost.tfa_Wed_Sep_12_01_26_18_PDT_2018.zip

$ tfactl diagcollect -for "2018-09-11 21:00:00"
Collecting data for all nodes
Scanning files for sep/11/2018 21:00:00

Collection Id : 20180912014217myhost

Detailed Logging at : /opt/oracle.tfa/tfa/repository/
collection_Wed_Sep_12_01_42_17_PDT_2018_node_all/
diagcollect_20180912014217_myhost.log
2018/09/12 01:42:21 PDT : NOTE : Any file or directory name containing the
string .com will be renamed to replace .com with dotcom
2018/09/12 01:42:21 PDT : Collection Name : tfa_Wed_Sep_12_01_42_17_PDT_2018.zip
2018/09/12 01:42:21 PDT : Collecting diagnostics from hosts : [myhost]
2018/09/12 01:42:21 PDT : Scanning of files for Collection in progress...
2018/09/12 01:42:21 PDT : Collecting additional diagnostic information...
2018/09/12 01:42:36 PDT : Getting list of files satisfying time range [09/11/2018
09:00:00 PDT, 09/12/2018 01:42:21 PDT]
2018/09/12 01:43:13 PDT : Collecting ADR incident files...
```

```
2018/09/12 01:44:00 PDT : Completed collection of additional diagnostic
information...
2018/09/12 01:44:06 PDT : Completed Local Collection
.--------------------------------------.
|          Collection Summary          |
+------------+-----------+------+------+
| Host       | Status    | Size | Time |
+------------+-----------+------+------+
| myhost     | Completed | 73MB | 105s |
'------------+-----------+------+------'

Logs are being collected to: /opt/oracle.tfa/tfa/repository/
collection_Wed_Sep_12_01_42_17_PDT_2018_node_all
/opt/oracle.tfa/tfa/repository/collection_Wed_Sep_12_01_42_17_PDT_2018_node_all/
myhost.tfa_Wed_Sep_12_01_42_17_PDT_2018.zip
```

The following command trims and zips all Oracle ASM logs from `myhost` updated between September 10, 2018 and September 11, 2018, and collects it on the initiating node:

```
$ tfactl diagcollect -asm -node myhost -from "2018-09-10 21:00:00" -to "2018-09-11
21:00:00"
Collecting data for myhost node(s)
Scanning files from sep/10/2018 21:00:00 to sep/11/2018 21:00:00

Collection Id : 20180912015138myhost

Detailed Logging at : /opt/oracle.tfa/tfa/repository/
collection_Wed_Sep_12_01_51_38_PDT_2018_node_myhost/
diagcollect_20180912015138_myhost.log
2018/09/12 01:51:43 PDT : NOTE : Any file or directory name containing the
string .com will be renamed to replace .com with dotcom
2018/09/12 01:51:43 PDT : Collection Name : tfa_Wed_Sep_12_01_51_38_PDT_2018.zip
2018/09/12 01:51:43 PDT : Collecting diagnostics from hosts : [myhost]
2018/09/12 01:51:43 PDT : Getting list of files satisfying time range [09/10/2018
21:00:00 PDT, 09/11/2018 21:00:00 PDT]
2018/09/12 01:51:43 PDT : Collecting additional diagnostic information...
2018/09/12 01:51:45 PDT : Collecting ADR incident files...
2018/09/12 01:52:16 PDT : Completed collection of additional diagnostic
information...
2018/09/12 01:52:20 PDT : Completed Local Collection
.--------------------------------------.
|           Collection Summary         |
+------------+-----------+-------+------+
| Host       | Status    | Size  | Time |
+------------+-----------+-------+------+
| myhost     | Completed | 818kB |  37s |
'------------+-----------+-------+------'

Logs are being collected to: /opt/oracle.tfa/tfa/repository/
collection_Wed_Sep_12_01_51_38_PDT_2018_node_myhost
/opt/oracle.tfa/tfa/repository/collection_Wed_Sep_12_01_51_38_PDT_2018_node_myhost/
myhost.tfa_Wed_Sep_12_01_51_38_PDT_2018.zip
```

Related Topics

- https://support.oracle.com/rs?type=doc&id=1513912.2

A.4.4 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 time]
-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.

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.
-database *database*	Specify the name of the database.

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
ORA-01555	Collects data for Oracle Database Snapshot too old error.

SRDC Profile	Description
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-29548	Provides Supporting Information for Oracle JVM Issues (My Oracle Support note 2175568.1).
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.
dbblockcorruption	Collects data for Alert Log Message `Corrupt block relative dba`.
dbdataguard	Collects data for Oracle Data Guard 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.

SRDC Profile	Description
`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.
`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)
`dbundocorruption`	Collects data for UNDO corruption problems.
`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.

SRDC Profile	Description
`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.
`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/rs?type=doc&id=2175568.1
- https://support.oracle.com/rs?type=doc&id=2045195.1
- https://support.oracle.com/rs?type=doc&id=1671509.1
- https://support.oracle.com/rs?type=doc&id=1905607.1

A.4.5 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]
```

For each of the three syntax models, you must specify a directory path where Oracle Trace File Analyzer stores collections.

Parameters

Table A-22 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 database 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 A-17 tfactl directory

The following command adds a directory:

```
# tfactl directory add /u01/app/grid/diag/asm/+ASM1/trace
```

The following command modifies a directory and makes 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
```

The following command removes a directory from all nodes in the cluster:

```
# tfactl directory remove /u01/app/grid/diag/asm/+ASM1/trace -node all
```

A.4.6 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 A-23 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.
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.

Table A-23 (Cont.) tfactl ips Command Parameters

Parameter	Description
`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.

A.4.6.1 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 A-24 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 A-18 tfactl ips ADD

```
$ tfactl ips add incident 22 package 12
```

A.4.6.2 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 A-25 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 A-19 tfactl ips ADD FILE

```
$ tfactl ips add file ADR_HOME/trace/mydb1_ora_13579.trc package 12
```

A.4.6.3 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 A-26 tfactl ips ADD NEW INCIDENTS Command Parameters

Parameter	Description
package_id	Specify the ID of the package to add the incidents to.

A.4.6.4 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 A-27 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.

A.4.6.5 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 A-28 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 A-20 tfactl ips COPY IN FILE

```
$ tfactl ips copy in file /tmp/key_file.txt to new_file.txt package 12 incident 62
```

A.4.6.6 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 A-29 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 A-21 tfactl ips COPY OUT FILE

```
$ tfactl ips copy out file ADR_HOME/trace/ora_26201 to /tmp/trace_26201.txt
```

A.4.6.7 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 A-30 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.

Table A-30 (Cont.) tfactl ips CREATE PACKAGE Command Parameters

Parameter	Description
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 A-22 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'
```

A.4.6.8 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 A-31 tfactl ips DELETE PACKAGE Command Parameters

Parameter	Description
package_id	Specify the ID of the package to delete.

Example A-23 tfactl ips DELETE PACKAGE

```
$ tfactl ips delete package 12
```

A.4.6.9 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 A-24 tfactl ips FINALIZE PACKAGE

```
$ tfactl ips finalize package 12
```

A.4.6.10 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 A-32 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 A-25 tfactl ips GENERATE PACKAGE

```
$ tfactl ips generate package 12 in /tmp
```

A.4.6.11 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 A-33 tfactl ips GET MANIFEST FROM FILE Command Parameters

Parameter	Description
file	Specify the external file with file name and full path.

Example A-26 tfactl ips GET MANIFEST

```
$ tfactl ips get manifest from file /tmp/IPSPKG_200704130121_COM_1.zip
```

A.4.6.12 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 A-34 tfactl ips GET METADATA Command Parameters

Parameter	Description
file	Specify the external file with file name and full path.

Example A-27 tfactl ips GET METADATA

```
$ tfactl ips get metadata from file /tmp/IPSPKG_200704130121_COM_1.zip
```

A.4.6.13 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 A-35 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 A-28 tfactl ips GET REMOTE KEYS

```
$ tfactl ips get remote keys file /tmp/key_file.txt package 12
```

A.4.6.14 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 A-36 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 A-29 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'
```

A.4.6.15 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 A-37 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 A-30 tfactl ips REMOVE

```
$ tfactl ips remove incident 22 package 12
```

A.4.6.16 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 A-38 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 A-31 tfactl ips REMOVE FILE

```
$ tfactl ips remove file ADR_HOME/trace/mydb1_ora_13579.trc package 12
```

A.4.6.17 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 A-39 tfactl ips SET CONFIGURATION Command Parameters

Parameter	Description
parameter_id	Specify the ID of the parameter to change.

Table A-39 (Cont.) tfactl ips SET CONFIGURATION Command Parameters

Parameter	Description
value	Specify the new value for the parameter.

Example A-32 tfactl ips SET CONFIGURATION

```
$ tfactl ips set configuration 6 2
```

A.4.6.18 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 A-33 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
```

A.4.6.19 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 A-34 tfactl ips SHOW FILES

```
$ tfactl ips show files package 12
```

A.4.6.20 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 A-35 tfactl ips SHOW INCIDENTS

```
$ tfactl ips show incidents package 12
```

A.4.6.21 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 A-36 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
```

A.4.6.22 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 A-37 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
```

A.4.6.23 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 A-40 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 A-38 tfactl ips UNPACK FILE

```
$ tfactl ips unpack file /tmp/IPSPKG_20061026010203_COM_1.zip into /tmp/newadr
```

A.4.6.24 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 A-41 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 A-39 tfactl ips UNPACK PACKAGE

```
$ tfactl ips unpack package IPSPKG_20061026010203 into /tmp/newadr
```

A.4.6.25 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 A-42 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 A-40 tfactl ips USE REMOTE KEYS

```
$ tfactl ips use remote keys file /tmp/key_file.txt package 12
```

A.4.7 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 A-43 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 A-44 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).

Example A-41 tfactl managelogs

```
$ tfactl managelogs -show usage -gi

Output from host : myhost
------------------------------

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

```
|                          Grid Infrastructure Usage                          |
+-------------------------------------------------------------+-----------+
| Location                                                    | Size      |
+-------------------------------------------------------------+-----------+
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/alert              | 2.51 MB   |
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/incident           | 4.00 KB   |
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/trace              | 8.82 MB   |
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/cdump              | 4.00 KB   |
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/hm                 | 4.00 KB   |
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/alert     | 83.32 MB  |
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/incident  | 4.00 KB   |
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/trace     | 516.38 MB |
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/cdump     | 4.00 KB   |
+-------------------------------------------------------------+-----------+
| Total                                                       | 611.05 MB |
'-------------------------------------------------------------+-----------'

$ tfactl managelogs -show variation  -older 2h -gi

Output from host : myhost
------------------------------
2018-09-12 21:16:40: INFO Checking space variation for 2 hours

2018-09-12 21:16:40: INFO Space is calculated in bytes [without round off]

2018-09-12 21:16:41: INFO Snapshot considered for size comparision was created at 12-
Sep-2018 18:55:29 PDT [2 hours ago].

.-------------------------------------------------------------------------------------
----.
|                              Grid Infrastructure
Variation                             |
+-------------------------------------------------------------+-----------
+-----------+
| Directory                                                   | Old Size  | New
Size  |
+-------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/trace     | 516.29 MB |
516.38 MB |
+-------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/incident  | 4.00 KB   | 4.00
KB   |
+-------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/cdump     | 4.00 KB   | 4.00
KB   |
+-------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/hm                 | 4.00 KB   | 4.00
KB   |
+-------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/trace              | 8.82 MB   | 8.82
MB   |
+-------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/alert              | 2.51 MB   | 2.51
MB   |
+-------------------------------------------------------------+-----------
```

```
+-----------+
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/incident              | 4.00 KB   | 4.00
KB   |
+--------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/tnslsnr/myhost/listener/alert        | 83.16 MB  | 83.33
MB  |
+--------------------------------------------------------------+-----------
+-----------+
| /scratch/app/oragrid/diag/asm/+asm/+ASM1/cdump                 | 4.00 KB   | 4.00
KB   |
'--------------------------------------------------------------+-----------
+-----------'
```

A.4.8 tfactl purge

Use the `tfactl purge` command to delete diagnostic collections from the Oracle Trace File Analyzer repository that are older than a specific time.

Syntax

```
tfactl purge -older n[h|d] [-force]
```

Example A-42 tfactl purge

To remove file(s) older than 30 days:

```
$ tfactl purge -older 30d
```

To remove file(s) older than 10 hours:

```
$ tfactl purge -older 10h
```

Index

P

R

S

T

U