Exachk User Guide

Exadata Configuration Audit Tool

Version 2.2.2.1

Table of Contents

Purpose

This document provides users of the exachk tool the information they need in order to run and maintain the tool.

exachk overview

exachk is designed to audit important configuration settings within an Oracle Exadata Database Machine. – The components examined are database servers, storage Servers, InfiniBand fabric, InfiniBand Switches, and Ethernet network. The tool audits configuration settings within the following categories:

- Hardware & firmware
- OS kernel parameters
- OS packages
- Many other OS configuration settings important to RAC.
- CRS/Grid Infrastructure
- RDBMS
- ASM
- Database and ASM initialization parameters
- Many other database configuration settings important to RAC.
- Maximum Availability Architecture (MAA) Scorecard
- 11.2.0.3 Database Upgrade Module with pre and post upgrade function

exachk also provides a listing of firmware, software versions, and patches for comparison to:

Database Machine and Exadata Storage Server 11g Release 2 (11.2) Supported Versions (Doc ID 888828.1)

Supported Platforms and Versions

For supported platforms and version information, please reference:

Oracle Exadata Database Machine exachk or HealthCheck (Doc ID 1070954.1)

Components

The exachk tool kit is provided by:

Oracle Exadata Database Machine exachk or HealthCheck (Doc ID 1070954.1)

The key components of the kit are the main code components (in exachk.zip):

- exachk – the main bash shell script
- collections.dat – a driver file used by the exachk script
- rules.dat – a driver file used by the exachk script

- "md5sums.txt" – provided for download verification.
- other miscellaneous files

And the documentation set:

- ExachkUserGuide.pdf – Main user documentation
- exachk_dbm_full_public.html– Sample exachk report
- exachk_dbm_pre-upgrade_public.html – Sample pre-upgrade report
- exachk_dbm_post-upgrade_public.html – S ample post-upgrade report
- ExachkBestPracticeChecks.xls – List of included checks

Features

1. The tool is NON-INTRUSIVE and does not change anything in the environment, except as follows:
   - SSH user equivalence for the RDBMS software owner is assumed to be configured among all the database server nodes being audited in order for it to execute commands on the remote database server nodes. If the tool determines that this user equivalence is not established it will offer to set it up either temporarily or permanently at the option of the user. If the user chooses to set up ssh user equivalence temporarily then the script will do so for the duration of the execution of the tool but then it will return the system to the state in which it found ssh user equivalence originally.
   - The tool creates a number of small output files into which the data needed is collected
   - The tool creates and executes some scripts dynamically in order to accomplish some of the data collection
   - The tool cleans up after itself any temporary files that are created and not needed as part of the collection.

2. The tool interrogates the system to determine the status of the Oracle stack components (i.e., Grid Infrastructure, RDBMS, Exadata, etc) and whether they are installed and/or running. Depending upon the status of each component, the tool runs the appropriate collections and audit checks. If due to local environmental configuration the tool is unable to properly determine the needed environmental information, please refer to the TROUBLESHOOTING section.

3. Watchdog daemon - The tool automatically runs a daemon in the background to monitor command execution progress. If for any reason one of the commands run by the tool should hang or take longer than anticipated, the monitor daemon kills the hung command after a configurable timeout so that main tool execution can progress. If that happens then the collection or command that was hung is skipped and a notation is made in the log. If the default timeout is too short please see the TROUBLESHOOTING section regarding RAT_TIMEOUT and RAT_ROOT_TIMEOUT.

4. If the tool's driver files are older than 90 days, the driver files are considered to be "stale" and the script will notify the user of a stale driver file. A new version of the tool and its driver files (kit) needs to be obtained from My Oracle Support (MOS) Note 1070954.1 since the tool is constantly being improved and new audit checks are constantly being added or revised.

5. When the tool completes its collection and analysis it produces an integrated HTML report whose name is synchronized to the exachk output directory (e.g., exachk_gsitst_111611_122257.html) and a .zip file which should be supplied to Oracle for further analysis if an SR needs to be logged. The HTML report contains

Benefit/Impact, Risk and Action/Repair information. In many cases it will also reference publicly available documents with additional information about the problem and how to resolve it.

6. The results of the audit checks can be optionally uploaded into database tables for reporting purposes. See below for more details on this subject.

7. In some cases customers may want to stage the tool on a shared filesystem so that it can be accessed from various systems but be maintained in a single location rather than being copied to each cluster on which it may be used. The default behavior of the tool is to create a subdirectory and its output files in the location where the tool is staged. If that staging area is a read only filesystem or if the user for any reason would like the output to be created elsewhere then there is an environment variable which can be used for that purpose. RAT_OUTPUT can be set to any valid writable location and the output will be created there.

When to Run Exachk

exachk should be executed after the initial Oracle Exadata Database Machine deployment, as part of the routine maintenance schedule (at least monthly), and before and after any system configuration change.

NOTE: Execute only one exachk in a cluster at a time. exachk exits with an error message if it finds another exachk script executing. The "minimal execution frequency" is the length of time it takes exachk to complete in a given environment. See also "Appendix A – troubleshooting scenarios", section "Another instance of exachk is running…".

Usage Considerations

It is recommended that the kit be staged and operated from a local filesystem on a single database server in order to provide the best performance possible.

For maximum usefulness execute exachk when the Grid Infrastructure and at least one database are up and running.

While exachk is a minimal impact tool, it is a best practice to execute it during times of least load on the system.

To avoid possible problems running the tool from terminal sessions on a network attached workstation or laptop, consider running the tool using VNC so that if there is a network interruption the tool will continue to process to completion.

If the execution of the tool should fail for some reason it can be re-run from the beginning but the tool is not "resumable" from the point of failure.

Guidelines for Running Exachk

If the oracle user exists on the system and all the Oracle components are installed or running (CRS, RDBMS, ASM), it is recommended to run the tool as the oracle (or RDBMS software install) user. The tool will need to

make some collections that require root privilege in which case it will display the following output (or similar), e.g.

```
7 of the included audit checks require root privileged data
collection.  If sudo is not configured or the root password is not
available, audit checks which require root privileged data collection
can be skipped.

1. Enter 1 if you will enter root password for each host when prompted
(once for each node of the cluster)
2. Enter 2 if you have sudo configured for oracle user to execute
/tmp/root_exachk.sh script
3. Enter 3 to skip the root privileged collections
4. Enter 4 to exit and work with the SA to configure sudo or arrange
for root access and run tool later

Please indicate your selection from one of the above options:-
```

If option1 is selected the tool will prompt for the root password once for each node of the cluster.

If option 2 is selected and sudo has been properly configured the root privileged collections will be performed under sudo control.

If option 3 is selected then all collections and audit checks that require "root" userid access will be skipped and those conditions will need to be checked manually by the customer.

It is recommended to run the tool as the database software owner (e.g., oracle). The user may run the tool as root or as the grid infrastructure software owner (e.g., grid) and it will collect the same data but then the database credentials will have to be supplied. Usually when run as oracle the customer will have OS authentication set up for the oracle database software owner and the database login credentials will not be needed. If the clusterware and database are installed and running it is best to run the tool as oracle (or whatever user owns the oracle database software installation. If for some reason you want to run the tool as another user then refer to VERIFYING DATABASE AUTHENTICATION in the TROUBLESHOOTING section for additional information on how to verify database authentication before running the tool.

2. The user should only use the driver files which are distributed with the tool kit and the driver files should not be edited by hand. A new version of the tool requires new driver files.

exachk Installation

Installation is straightforward, but there are some considerations.

Exachk must be executed by the owner of the oracle database or grid home.

In a non-role separated environment exachk is installed in one location and executed once, typically by the "oracle" userid. A typical example for such a configuration is that exachk is installed to "/home/oracle/exachk" and the directory and files are owned by the "oracle" userid.

NOTE: In later versions of the exadata software image, a version of exachk is included at this location: `/opt/oracle.SupportTools/exachk`. This exachk is primarily used at the end of the initial deployment process. There are several reasons why you should consider installing exachk at another location for regular maintenance use:

- The version at `/opt/oracle.SupportTools/exachk` may not be the most current version available from MOS note 1070954.1 due to timing differences in the release schedule of the exadata software image and updates to exachk.
- exachk is intended to be updated more frequently than exadata software updates are released, so it is a best practice to always check My Oracle Support note 1070954.1 periodically for new releases and before each exachk run.
- If you are maintaining some type of history archive, `/opt/oracle.SupportTools`/exachk could be overwritten by an upgrade or a bare metal restore operation.

In a role separated environment, exachk must be installed in multiple locations and run multiple times as the different owner userids. A typical example for such a configuration is that exachk is installed to "/home/oracle/exachk" and the directory and files are owned by the "oracle" userid, and also to "/home/gridowner/exachk" and the directory and files are owned by the "gridowner".

Please see "Appendix E – Multiple Database Support Scenarios" for additional information.

NOTE: exachk should not be installed as the "root" userid, as permission conflicts often interfere with an exachk run, and exachk is not to be executed from the "root" userid. exachk will exit if executed from the "root" userid.

These installation instructions are for a non-role separated environment. For a role separated environment, repeat steps 2) through 4) as many times as necessary, using as many userids as required, making the necessary substitutions.

1) Download the exachk bundle from My Oracle Support note 1070954.1 to your laptop and unzip it.
2) Transfer "exachk.zip" to a directory on the target Oracle Exadata Database Machine.
3) Unzip "exachk.zip"
4) Verify md5sums

exachk Execution

exachk command line arguments

```
$ ./exachk -h
Usage : ./exachk [-abvhpfmsuSo:c:t:]
        -a      All (Perform best practice check and recommended patch check)
        -b      Best Practice check only. No recommended patch check
        -h      Show usage
        -v      Show version
        -p      Patch check only
        -m      exclude checks for Maximum Availability Architecture scorecards(see
                user guide for more details)
        -u      Run exachk to check pre-upgrade or post-upgrade best practices for
                11.2.0.3 and 12.1.0.1
                -o pre or -o post is mandatory with -u option like
                    ./exachk -u -o pre
```

```
-f      Run Offline.Checks will be performed on data already collected from
        the customer system
-o      Argument to an option. if -o is followed by v,V,Verbose,VERBOSE or
        Verbose, it will print checks which passs on the screen
        if -o option is not specified,it will print only failures on
        screen. for eg: exachk -a -o v
-clusternodes
        Pass comma separated node names to run exachk only on selected
        nodes.
-localonly
        Run exachk only on local node.
-nopass
        Do not print PASS'ed checks in HTML report.
-noscore
        Do not print healthscore in HTML report.
-diff <Old Report> <New Report> [-outfile <Output HTML>]
        Diff two exachk reports. Pass directory name or zip file or html
        report file as <Old Report> & <New Report>
-c     Used only under the guidance of Oracle support or development to
       override default components
-d <start|stop|status>
       start      : Start the exachk daemon
       stop       : Stop the exachk daemon
       status     : Check if the exachk daemon is running
       nextautorun: print the next auto run time
-daemon
       Used to specify that run exachk only if daemon is running
-nodaemon
       Dont use exachk daemon to run command
-set "param1=value1;param2=value2.."
       Set exachk config parameter
       Supported parameters are:
         AUTORUN_INTERVAL <n[d|h]> : Automatic rerun interval
         in daemon mode.
         Set it zero to disable automatic rerun. Default is zero.
         AUTORUN_FLAGS <flags> : exachk flags to use for auto runs.
         Ex: exachk -set "AUTORUN_INTERVAL=12h;AUTORUN_FLAGS=-profile
         sysadmin"
             This will run sysadmin profile every 12 hours
             exachk -set "AUTORUN_INTERVAL=2d;AUTORUN_FLAGS=-profile
             sysadmin"
             This will run sysadmin profile once every 2 days.
         NOTIFICATION_EMAIL : Email address used for notifications by
         daemon if mail server is configured.
         PASSWORD_CHECK_INTERVAL <number of hours> : In daemon mode,
         interval to check change in password
-get <parameter | all>
       Print the value of parameter
-profile Pass specific profile.
         List of supported profiles:
         asm             asm Checks
         clusterware     clusterware checks
         dba             dba Checks
         maa             maa Checks
         storage         Storage Server Checks
         switch          Infiniband switch checks
         sysadmin        sysadmin checks
         virtual_infra   all OVS checks , all control VM checks, all NTP-
                         related checks, and stale VNICs check
```

```
                          (Exalogic Only)
          zfs             ZFS storage appliances checks
-cells
        Pass comma separated storage server names to run exachk only on
        selected storage servers.
-ibswitches
        Pass comma separated infiniband switch names to run exachk only on
        selected infiniband switches.
-zfsnodes
        Pass comma separated ZFS storage appliance names to run exachk only
        on selected storage appliances.
```

exachk Execution Phases

An exachk run has three phases:

1) Minimal Input (or usage of the daemon)
2) Data Collection
3) Analysis

When the exachk script is executed, it determines as much information as possible by directly querying the environment. However, not everything required to execute exachk can be learned directly from the system. During the "Minimal Input" phase there are a few input questions to confirm data retrieved from the system, provide a few execution choices, and to enter passwords.

During the "Data Collection" phase, the scripting collects the raw data based upon what is learned directly from the environment and the inputs collected earlier.

> NOTE: exachk version 2.2.0 introduced parallel data collection for the storage servers and InfiniBand switches as the default. exachk version 2.2.1 introduced parallel data collection for the database servers. If you wish to have exachk collect all (or some) data serially (the original pre-version 2.2.0 behavior), you may set the following environment variables:
>
> RAT_COMPUTE_RUNMODE - By default exachk will collect data for all database servers in parallel. If for some reason you wish to collect database server data in serial, set this variable to "`serial`". For example: "`export RAT_COMPUTE_RUNMODE=serial`".
>
> RAT_CELL_RUNMODE - By default exachk will collect data for all storage servers in parallel. If for some reason you wish to collect storage server data in serial, set this variable to "`serial`". For example: "`export RAT_CELL_RUNMODE=serial`".
>
> RAT_IBSWITCH_RUNMODE - By default exachk will collect data for all InfiniBand switches in parallel. If for some reason you wish to collect InfiniBand switch data in serial, set this variable to "`serial`". For example: "`export RAT_IBSWITCH_RUNMODE=serial`".

During the "Analysis" phase, exachk examines the raw data collected and makes findings based upon the exachk rule set.

Available environment variables to extend timeouts

Exachk has a "watchdog" process that monitors exachk execution and will kill commands that exceed default timeouts to prevent "hangs". Occasionally on a busy system, checks may be killed simply because the target of the check has not responded within the default timeout. These environment variables can be used to lengthen the default timeouts. The most common timeout environment variables are:

- RAT_TIMEOUT (default 90 seconds, non-root individual commands)
- RAT_ROOT_TIMEOUT (default 300 seconds, root userid command sets)
- RAT_PASSWORDCHEK_TIMEOUT (default 1 second, ssh login DNS handshake)

For additional timeout environment variables, see "Appendix A – Troubleshooting Scenarios".

Available options to limit scope

exachk provides several methods by which the scope of a given execution may be limited. The two general categories are:

- Interactive prompts before data collection phase
- Environment variables to set before execution

During the interactive prompt phase at the start of an exachk run, before the data collections begin, there are a number of choices that allow you to reduce the scope of the run. Examples are the database list, the prompt to skip the storage server check, and the prompt to skip the InfiniBand switch checks.

In addition to the interactive choices, there are a range of environment variables that can be set to limit the scope of the exachk run. For example, exachk normally checks all the storage servers contained in the cellip.ora file. However, you can set the environment variable "RAT_CELLS" to a space separated list of storage server names to check a subset of storage servers specified in the cellip.ora file.

For additional timeout environment variables, see "Appendix A – Troubleshooting Scenarios".

Use VNC Server

It is recommended to execute exachk from within a VNC to avoid exachk exiting and performing run cleanup when a network connection is lost.

Sample exachk Execution

Interactively

This section will present an overview of an exachk execution, using the full report including the MAA scorecard.

As the "oracle" userid log on to the target Oracle Exadata Database Machine and change working directory to the directory into which exachk was installed. In this example, the working directory is "`/home/oracle/exachk`".

Execute exachk with no command line arguments:

```
./exachk
```

If the environment variable “CRS_HOME” is not set, the first message and prompt is:

```
CRS stack is running and CRS_HOME is not set. Do you want to set CRS_HOME to
/u01/app/11.2.0/grid?[y/n][y]
```

Type “y” and press the return key, or just press the return key.

exachk checks for SSH configuration. If the environment has SSH for the “oracle” userid configured to the other database servers in the cluster, the next message is:

```
Checking ssh user equivalency settings on all nodes in cluster

Node randomdb02 is configured for ssh user equivalency for oracle user
```

If SSH is not configured for the “oracle” userid, the messaging is different, and you will be prompted later for how you wish to proceed.

exachk next determines the list of OCR registered databases and displays this message and prompt:

```
Searching for running databases . . . . .

. .
List of running databases registered in OCR
1. dbm
2. dss
3. All of above
4. None of above

Select databases from list for checking best practices. For multiple
databases, select 3 for All or comma separated number like 1,2 etc [1-4][3].1
```

In most cases, you will want to simply press the return key to evaluate all discovered databases. This example enters “1” to select only the “dbm” database.

exachk next queries the state of the Oracle software stack and reports its findings:

```
Searching out ORACLE_HOME for selected databases.

. . .


Checking Status of Oracle Software Stack - Clusterware, ASM, RDBMS

. . . . . .
--------------------------------------------------------------------------------------------
                                             Oracle Stack Status
--------------------------------------------------------------------------------------------
Host Name  CRS Installed  ASM HOME  RDBMS Installed  CRS UP  ASM UP  RDBMS UP  DB Instance Name
--------------------------------------------------------------------------------------------
randomdb01 Yes            Yes       Yes              Yes     Yes     Yes       dbm1
randomdb02 Yes            Yes       Yes              Yes     Yes     Yes       dbm2
--------------------------------------------------------------------------------------------
```

Execution continues without user intervention, and the following is typically presented:

```
root user equivalence is not setup between randomdb01 and STORAGE SERVER
randomcel01.

1. Enter 1 if you will enter root password for each STORAGE SERVER when
prompted.

2. Enter 2 to exit and configure root user equivalence manually and re-run
exachk.

3. Enter 3 to skip checking best practices on STORAGE SERVER.

Please indicate your selection from one of the above options[1-3][1]:-
```

In most environments, SSH is not configured for the “root” userid on the storage servers from the “oracle” userid on the database servers. There are several options here.

The most common answer is to select “1”, and exachk will prompt for the “root” userid password to store only in memory for the duration of the run and use with the expect command to log on to the storage servers.

The second option is to enter “2” to exit exachk at this point, configure SSH for the “root” userid on the storage servers from the “oracle” userid on the database server, and restart exachk.

The third option is to enter “3” to skip the storage server checks and continue the exachk run. This will result in the storage server findings being absent from the exachk report.

This example presses the return key, which enters “1” by default.

The next prompt is:

```
Is root password same on all STORAGE SERVER[y/n][y]
```

In most cases, enter “y” and press the return key, or simply press the return key. If each storage server has a unique “root” userid password, answer this prompt “n”, and you will be prompted for the password for each individual storage server.

The next prompt is:

```
Enter root password for STORAGE SERVER :-
```

Type in the common “root” userid password for the storage servers and press the return key.

exachk next verifies this password on the storage servers. Beginning with Exadata Storage Server Software version 11.2.3.1.0, if the password does not verify, exachk will exit after posting the message shown below:

```
The password entered for the root userid did not validate on 192.168.32.19

This userid may now be subject to a login delay on the specified node. Please
review the pam utility configuration, and allow the specified amount of login
delay time to elapse before retrying exachk. Please also check your pam
failed login counts for this userid against the permitted total, and clear if
required.

exachk is exiting.
```

If the password verifies, you will see the following prompt for the database servers:

```
101 of the included audit checks require root privileged data collection on
DATABASE SERVER. If sudo is not configured or the root password is not
available, audit checks which require root privileged data collection can be
skipped.


1. Enter 1 if you will enter root password for each on DATABASE SERVER host
when prompted

2. Enter 2 if you have sudo configured for oracle user to execute
root_exachk.sh script on DATABASE SERVER

3. Enter 3 to skip the root privileged collections on DATABASE SERVER

4. Enter 4 to exit and work with the SA to configure sudo on DATABASE SERVER
or to arrange for root access and run the tool later.

Please indicate your selection from one of the above options[1-4][1]:-
```

The most common option is to select “1” and provide the “root” userid password for the database servers, similar to the method discussed earlier for the storage servers.

If you already have sudo access from the “oracle” userid on the database servers to the “root” userid on the database servers, enter “2”.

The third option is to enter “3” to skip the database server checks and continue the exachk run. This will result in the database server findings being absent from the exachk report.

Enter “4” if you wish to exit the exachk run, and get sudo configured from the “oracle” userid on the database servers to the “root” userid on the database servers so that you can restart exachk and select option “2” at this prompt later.

This example presses the return key for the default action of “1”.

The next prompt is:

```
Is root password same on all compute nodes?[y/n][y]
```

In most cases, enter “y” and press the return key, or simply press the return key. If each database server has a unique “root” userid password, answer this prompt “n”, and you will be prompted for the password for each individual database server.

The next prompt is:

```
Enter root password on DATABASE SERVER:-
```

Type in the common “root” userid password for the database servers and press the return key.

exachk next verifies this password on the database servers. Beginning with Exadata Storage Server Software version 11.2.3.1.0, if the password does not verify, exachk will exit after posting the message shown below:

```
The password entered for the root userid did not validate on 192.168.32.19

This userid may now be subject to a login delay on the specified node. Please
review the pam utility configuration, and allow the specified amount of login
delay time to elapse before retrying exachk. Please also check your pam
failed login counts for this userid against the permitted total, and clear if
required.

exachk is exiting.
```

If the password verifies, you will see the following prompt for the InfiniBand switches:

```
9 of the included audit checks require nm2user privileged data collection on
INFINIBAND SWITCH.


1. Enter 1 if you will enter nm2user password for each INFINIBAND SWITCH when
prompted

2. Enter 2 to exit and to arrange for nm2user access and run the exachk
later.

3. Enter 3 to skip checking best practices on INFINIBAND SWITCH

Please indicate your selection from one of the above options[1-3][1]:-
```

The most common option is to select “1” and provide the “nm2user” userid password for the InfiniBand switches, similar to the method discussed earlier for the storage servers.

Enter “2” if you wish to exit the exachk run, and acquire the “nm2user” userid password for the InfiniBand switches.

Enter “3” to skip the InfiniBand switch checks and continue the exachk run. This will result in the InfiniBand switch findings being absent from the exachk report.

This example presses the return key for the default action of “1”.

The next prompt is:

```
Is nm2user password same on all INFINIBAND SWITCH ?[y/n][y]
```

In most cases, enter “y” and press the return key, or simply press the return key. If each InfiniBand switch has a unique “root” userid password, answer this prompt “n”, and you will be prompted for the password for each individual InfiniBand switch.

The next prompt is:

```
Enter nm2user password for INFINIBAND SWITCH:-
```

Type in the common “nm2user” userid password for the InfiniBand switches and press the return key.

exachk next verifies this password on the InfiniBand switches. If the password does not verify, the following message will be posted:

```
nm2user password for randomsw-ib1.us.oracle.com was incorrect. 2 retries
remaining.

Enter nm2user password for randomsw-ib1.us.oracle.com :-
```

Reenter the password, and exachk will try again. exachk will try a total of three times before it asks if you want to skip the storage servers and proceed, or exit the execution.

NOTE: exachk version 2.2.1 uses the "nm2user" userid for InfiniBand switch validation. If you wish to have exachk use the "root" userid for IB switch validation (the original pre-version 2.2.1 behavior), please set the RAT_IBSWITCH_USER environment variable. For example: "`export RAT_IBSWITCH_USER=root`".

If the password verifies, you will see the data collection process begin as shown below:

```
*** Checking Best Practice Recommendations (PASS/WARNING/FAIL) ***



Log file for collections and audit checks are at
/home/oracle/exachk_215/20120524/exachk_053012_102825/exachk.log

============================================================
                    Node name - randomdb01
============================================================
Collecting - ASM Diskgroup Attributes
Collecting - ASM initialization parameters
Collecting - Database Parameters for dbm database
Collecting - Database Undocumented Parameters for dbm database
Collecting - Clusterware and RDBMS software version
<output truncated for brevity>
```

Data collection will continue across the components of the machine, identifying each component by name and echoing back to the screen the checks that are being performed.

The collection process occurs on the first database server, and then it moves to the first storage server, as shown below:

```
Preparing to run root privileged commands on STORAGE SERVER randomcel01

root@192.168.32.19's password:
Collecting - Ambient Temperature on storage server
Collecting - Exadata software version on storage server
Collecting - Exadata software version on storage servers
Collecting - Exadata storage server system model number
<output truncated for brevity>
```

When data collection is complete for all storage servers, exachk moves on to the InfiniBand switches, as shown below:

```
Preparing to run root privileged commands on INFINIBAND SWITCH randomsw-
ib1.us.oracle.com.

root@randomsw-ib1.us.oracle.com's password:
Collecting - Hostname in /etc/hosts
Collecting - Infiniband Switch NTP configuration
Collecting - Infiniband subnet manager status
Collecting - Infiniband switch HCA status
<output truncated for brevity>
```

When data collection is complete for InfiniBand switches, exachk performs it's analysis phase on the local database server from which it was launched, as shown below:

```
Data collections completed. Checking best practices on randomdb01.
--------------------------------------------------------------------------------
---------


FAIL => A minimum of two controlfiles are not stored in high redundancy
diskgroups for dbm
INFO => Number of SCAN listeners is NOT equal to the recommended number of 3.
<output truncated for brevity>
```

At this time, exachk also performs analysis on the storage servers and InfiniBand switches, databases, and MAA Scorecard. When this activity is complete, exachk next gathers the data from the remaining database servers in the cluster:

```
============================================================
                    Node name - randomdb02
============================================================
Collecting - Clusterware and RDBMS software version
Collecting - Compute node PCI bus slot speed for infiniband HCAs
Collecting - Kernel parameters
<output truncated for brevity>
```

The data collection is followed by the analysis for each remaining database server, as shown below:

```
Data collections completed. Checking best practices on randomdb02.
--------------------------------------------------------------------------------
---------


FAIL => A minimum of two controlfiles are not stored in high redundancy
diskgroups for dbm
INFO => Number of SCAN listeners is NOT equal to the recommended number of 3.
<output truncated for brevity>
```

When all of the remaining database servers have been processed, exachk performs clusterwide checks and analysis, as shown below:

```
--------------------------------------------------------------------------------
                     CLUSTERWIDE CHECKS
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Typically, there is very little or no screen output following the clusterwide checks banner. The last screen output to appear is the file reference information, as shown below:

```
Detailed report (html) -
/home/oracle/exachk_215/20120524/exachk_dbm_053012_102825/exachk_dbm_053012_1
02825.html

UPLOAD(if required) -
/home/oracle/exachk_215/20120524/exachk_dbm_053012_102825.zip
```

Via exachk daemon

exachk version 2.2.2 introduces the daemon process functionality to permit non-interactive(batch or silent mode) execution on a regular interval. The exachk daemon can be configured to include storage servers and InfiniBand switches.

Before running exachk in daemon mode, you should set key parameters using the "-set" flag. More than one parameter can be set, delimited by a semi-colon. AUTORUN_INTERVAL can be specified in number of days or number of hours using <d/h>. See "./exachk –h" for more information. For example, to set the daemon to run every day, in verbose mode, specifying an email address for daemon notices, and to check for changed passwords every hour, execute the following command as the userid that will launch exachk in daemon mode (all on one line):

```
./exachk -set "AUTORUN_INTERVAL=1d;AUTORUN_FLAGS= -o
v;NOTIFICATION_EMAIL=firstname.lastname@company.com;PASSWORD_CHECK_INTERVAL=1
"
```

To see the current exachk daemon values, as the userid that launched the daemon, execute "`./exachk -get <parameter_name>`". For example, "`./exachk -get autorun_interval`" or "`./exachk -get all`". The parameters can be also be set or modified after the exachk daemon process has started.

> NOTE: It is highly recommended that you at least configure the "NOTIFICATION_EMAIL" and PASSWORD_CHECK_INTERVAL. If you do not have an email address configured, notifications will be written to the file "`exachk_daemon.log`" in the directory from which the daemon process was launched. Configuring the PASSWORD_CHECK_INTERVAL will help prevent an aborted run due to a password change.

After you have used the "-set" flag to configure the daemon, start the exachk daemon process on one of the compute nodes using "`./exachk -d start`".

exachk will present the standard interactive graphical user interface to collect the required information and start the daemon process. When the input collection process has completed, you should see output similar to:

```
Daemon is started with PID : 31333
```

The daemon now hibernates without making an exachk run and waits for an on demand request or the next scheduled auto-run time.

Once the exachk daemon is started, to initiate an exachk run manually on demand, simply execute "./exachk" as the user that started the daemon process, and in the same directory from which the exachk daemon process was launched. The output will be similar to:

```
[oracle@randomdb05 20130529]$ ./exachk
Sending commands to daemon (mypid 15747) args :
```

```
CRS stack is running and CRS_HOME is not set. Do you want to set CRS_HOME to
/u01/app/11.2.0.3/grid?[y/n][y]y

Checking ssh user equivalency settings on all nodes in cluster
```
<output truncated for brevity>

You will see the normal interactive interface and command feedback scroll past on your terminal, but you will not have the ability to respond to any of the prompts, as the daemon process is using its stored information to execute the run.

To query the exachk daemon to see when is your next auto-run is scheduled, use, as the userid that launched the daemon process, "`./exachk -d nextautorun`". Running on-demand using will not disturb scheduled auto run but you cannot run more than instance of exachk, at a time, just like interactive execution.

If daemon is running on the node where you run exachk, it will use daemon and will run without any interactive prompt. if user does not want to use daemon even its running, can say ./exachk -nodaemon and it will run in interactive mode. To force exachk to use daemon, use ./exachk -daemon and if daemon is not running, it will exit with proper message.

Daemon process will stop if:

- There is password validation for every node defined by PASSWORD_CHECK_INTERVAL parameter. If password is changed on any node, daemon will stop and will put entry in exachk_daemon.log as well as send an email to NOTIFICATION_EMAIL.
- Compute node where daemon is running goes down or restarts, user will have to restart exachk daemon.
- If exachk script has changed or replaced with new script since you started daemon, further on-demand as well as auto run will not succeed. You will have to restart daemon with new script for future run.

exachk daemon process started by one user can not be used to run exachk by other user like user1 started daemon then user2 cannot use exachk daemon to run exachk in non-interactive mode. In fact to use exachk daemon, you will have to be same user and will have to start on-demand run from same directory where you started daemon.

If the system configuration changed like you added more nodes (database server, storage servers or InfiniBand switches) or removed node, you will have to restart exachk daemon. Otherwise non-interactive run will have included newly added nodes.

You can check status of exachk daemon using the "./exachk -d status" command as the user that launched the daemon in the same directory from which the daemon was launched.

To start and stop the daemon, as the user that launched the daemon in the same directory from which the daemon was launched, use the ". /exachk -d <start|stop|status>" options.

exachk Report Structure

exachk produces an HTML report of findings, with the most important exceptions listed first by component. This report is contained within the zip file that is provided after each exachk run. The usual method is to bring

the zip file back to a desktop computer, unzip it, and then open the HTML report in your preferred browser. The HTML report appearance varies slightly by browser, depending upon your environment settings and browser preferences. If the report appearance is not quite as you might like, try a different browser.

These are the main sections of the report, and the list will vary depending upon the arguments that were passed when exachk was executed:

- Cluster Summary
- Findings Needing Attention
- MAA Scorecard
- Findings Passed
- Systemwide firmware and software versions
- Killed Processes
- Skipped Checks

"Cluster Summary" is a summarization of key data collected from the environment.

"Findings Needing Attention" contains FAIL, WARNING, ERROR, and INFO findings. It is divided into Database Server, Storage Server, InfiniBand Switch.

"MAA Scorecard" is a report of key Maximum Availability Architecture Best Practices.

"Findings Passed" contains PASS findings.

"Systemwide firmware and software versions" provides a listing of key component version levels.

"Killed Processes" provides a list of processes that were killed by the watchdog process.

"Skipped Checks" provides a list of checks that were not performed for some reason.

Within the report, each finding is reported once, and the affected components are listed. Each finding also presents a "View" link that will branch to the detail supporting the finding.

> NOTE: If the "Killed Processes" and "Skipped Checks" sections are in the report, the data set is not complete! These two items indicate that something exceeded a timer and was killed, or something went wrong with a check and it was skipped in the analysis phase. Please refer to the troubleshooting section for diagnostic and corrective action.

exachk Report Sample- Basic

The following is a sample "Cluster Summary" section of the report:

Cluster Summary

Cluster Name	random-cluster
OS Version	LINUX X86-64 OELRHEL 5 2.6.18-274.18.1.0.1.el5
CRS Home - Version	/u01/app/11.2.0/grid - 11.2.0.2.0
DB Home - Version - Names	/u01/app/oracle/product/11.2.0/dbhome_1 - 11.2.0.2.0 - dbm

Exadata Version	11.2.3.1.0
Number of nodes	9
Database Servers	2
Storage Servers	4
IB Switches	3
exachk Version	2.1.5_20120524
Collection	exachk_dbm_053012_102825.zip
Collection Date	30-May-2012 10:29:19

The underlined items on the right hand side may be expanded to see the details by clicking upon them. For example, clicking on the underlined "2" will expand to reveal the two database server names.

The following is a sample of the "Table of Contents" report section:

Table of Contents

The "Table of Contents" lists the major sections of the report that were generated by this execution. Clicking on an entry will transfer focus to that section of the report.

The contents of the "Table of Contents" will vary depending upon the command line switches used, any scope restrictions chosen, and whether or not the run was clean without any killed processes or skipped checks.

This report is a standard full run with MAA scorecard, killed processes and skipped checks. This report does not invoke the 11.2.0.3.0 upgrade module.

The following is a sample "Findings Needing Attention" report section, truncated for brevity:

Database Server

Status	Type	Message	Status On	Details
FAIL	OS Check	Database Server Physical Drive Configuration does not meet recommendation	All Database Servers	View

FAIL	OS Check	Verify-topology returned some errors or warning.	All Database Servers	View

In this section of the report, the findings that require attention are listed in priority order, with FAIL messages first.

Each row provides the “Status” of the check, the “Type” of the check which may be thought of as a region of the machine, the check “Message”, the “Status On” which indicates which component or components are associated with the check, and a “View” link that if clicked upon will move to the region of the report with the supporting detail for the finding.

In the next two screen captures, we’ll look at the detail for “Database Server Physical Drive Configuration does not meet recommendation”. To view the detail section, click on the “View” link at the far right of the check row in the exachk report.

The following is a sample of the first section of the detail provided by clicking on “View”:

Top

Verify Database Server Physical Drive Configuration

Success Factor	DBMACHINE X2-2 AND X2-8 AUDIT CHECKS
Recommendation	Benefit / Impact: For X2-2, there are 4 disk drives in a database server controlled by an LSI MegaRAID SAS 9261-8i disk controller. The disks are configured RAID-5 with 3 disks in the RAID set and 1 disk as a hot spare. There is 1 virtual drive created across the RAID set. Verifying the status of the database server RAID devices helps to avoid a possible performance impact, or an outage. For X2-8, there are 8 disk drives in a database server controlled by an LSI MegaRAID SAS 9261-8i disk controller. The disks are configured RAID-5 with 7 disks in the RAID set and 1 disk as a hot spare. There is 1 virtual drive created across the RAID set. Verifying the status of the database server RAID devices helps to avoid a possible performance impact, or an outage. The impact of validating the physical drives is minimal. The impact of corrective actions will vary depending on the specific issue uncovered, and may range from simple reconfiguration to an outage. Risk: Not verifying the physical drives increases the chance of a performance degradation or an outage. Action / Repair: To verify the database server physical drive configuration, use the following command: /opt/MegaRAID/MegaCli/MegaCli64 PDList -aALL | grep "Firmware

	state" The output for X2-2 will be similar to: Firmware state: Online, Spun Up Firmware state: Online, Spun Up Firmware state: Online, Spun Up Firmware state: Hotspare, Spun down There should be three lines of output showing a state of "Online, Spun Up", and one line showing a state of "Hotspare, Spun down". The ordering of the output lines is not significant and may vary based upon a given database server's physical drive replacement history. NOTE: Modified 03/21/12 Occasionally in normal operation, the "Hotspare" physical drive may be brought to a state of "Online, Spun Up". Thirty minutes (default) after the operation that brought the drive to "Online, Spun Up" has completed, the drive should spin down due to the powersaving feature. There is no harm for the drive to be "Online, Spun Up" if there are no other errors reported in the disk drive configuration checks. For additional information, please reference My Oracle Support note "Exadata: Hot Spares Not Spinning Down (Doc ID 1403613.1)"
Needs attention on	randomdb01, randomdb02
Passed on	-

In the first part of each of these detail sections, you will find an explanation of the “Recommendation”, the list of components that need attention, and the list of components that passed.

Each of these detail sections may contain specific instructions, references to MOS notes, or directions to open an SR with Oracle support.

There is also a “Top” link to return quickly to the top of the report.

The follow is a sample of the second portion of the detail provided by clicking on “View”:

Status on randomdb01: FAIL => Database Server Physical Drive Configuration does not meet recommendation
DATA FROM RANDOMDB01 FOR VERIFY DATABASE SERVER PHYSICAL DRIVE CONFIGURATION   Firmware state: Hotspare, Spun Up Firmware state: Online, Spun Up Firmware state: Online, Spun Up Firmware state: Online, Spun Up

Status on randomdb02: FAIL => Database Server Physical Drive Configuration does not meet recommendation

```
DATA FROM RANDOMDB02 FOR VERIFY DATABASE SERVER PHYSICAL DRIVE CONFIGURATION



Firmware state: Hotspare, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
Firmware state: Online, Spun Up
```

Top

In the second section of each of these detail sections, the raw data for each component is presented. If there is a large amount of raw data, there are "More" and "Less" links provided to expand or contract the amount of data presented.

There is also a "Top" link to return quickly to the top of the report.

The following is a sample of the first section of the "MAA Scorecard" section of the report:

MAA Scorecard

Outage Type	Status	Type	Message	Status On	Details
COMPUTER FAILURE PREVENTION BEST PRACTICES	PASS	**Description** Oracle RAC and Oracle Clusterware allow Oracle Database to run any packaged or custom application across a set of clustered servers. This capability provides the highest levels of availability and the most flexible scalability. If a clustered server fails, then Oracle Database continues running on the surviving servers. When more processing power is needed, you can add another server without interrupting access to data. For RAC and clusterware MAA best practices please consult chapter 6 and 7 of the HA Best Practices guide **Links:** • Chapter 6 - Configuring Oracle Database with Oracle Clusterware • Chapter 7 - Configuring Oracle Database with Oracle RAC			
	PASS	SQL Parameter Check	fast_start_mttr_target has been changed from default	All Instances	View

The "MAA Scorecard" provides an assessment of the current configuration against key MAA Exadata Best Practices.

"Outage Type" is the MAA outage classification or MAA best practice:

- COMPUTER FAILURE PREVENTION BEST PRACTICES
- STORAGE FAILURES PREVENTION BEST PRACTICES
- DATA CORRUPTION PREVENTION BEST PRACTICES
- LOGICAL CORRUPTION PREVENTION BEST PRACTICES
- DATABASE/CLUSTER/SITE FAILURE PREVENTION BEST PRACTICES
- NETWORK FAILURE PREVENTION BEST PRACTICES
- CLIENT FAILOVER OPERATIONAL BEST PRACTICES
- OPERATIONAL BEST PRACTICES
- SOFTWARE MAINTENANCE BEST PRACTICES
- CONSOLIDATION DATABASE PRACTICES

The "Status" column represents both the overall finding for an outage classification, and the individual check status or statuses that lead to the overall finding.

The "Type", "Message", "Status On", and "Details" columns correspond to the individual check columns discussed earlier.

Note that there is a "View" link provided to detailed data sections for each individual check.

When examining a system that does have a standby, exachk should be run on both the primary and standby environments. In a multi-database environment the database list can be restricted to just the primary and standby databases to help focus the exachk reports.

The following is a sample section of the "MAA Scorecard" section of the report that contains more than one check:

<table>
<tr><td rowspan="3">LOGICAL CORRUPTION PREVENTION BEST PRACTICES</td><td>FAIL</td><td colspan="4">Description
Oracle Flashback Technology enables fast logical failure repair. Oracle recommends that you use automatic undo management with sufficient space to attain your desired undo retention guarantee, enable Oracle Flashback Database, and allocate sufficient space and I/O bandwidth in the fast recovery area. Application monitoring is required for early detection. Effective and fast repair comes from leveraging and rehearsing the most common application specific logical failures and using the different flashback features effectively (e.g flashback query, flashback version query,flashback transaction query, flashback transaction, flashback drop, flashback table, and flashback database)

Links:
• HA Best Practices guide - 5.1.4 Enable Flashback Database</td></tr>
<tr><td>FAIL</td><td>SQL Check</td><td>Flashback is not configured</td><td>All Databases</td><td>View</td></tr>
<tr><td>PASS</td><td>SQL Parameter Check</td><td>Database parameter UNDO_RETENTION is not null</td><td>All Instances</td><td>View</td></tr>
</table>

In this example, one of the checks was “PASS” and one was “FAIL”, resulting in an overall “FAIL” for the “LOGICAL CORRUPTION PREVENTION BEST PRACTICES” segment of the MAA scorecard.

The following is an example of the software version mapping table found in the “SOFTWARE MAINTENANCE BEST PRACTICES” section of the MAA Scorecard:

Component		Host/Location	Found version	Recommended versions	Status
DATABASE SERVER	Database Home	randomadm01,randomadm02: /u01/app/oracle/product/11.2.0.3/dbhome_1	11.2.0.3.9	11.2.0.3.17	Older than recommended versions.
	Grid Infrastructure	randomadm01,randomadm02: /u01/app/11.2.0.3/grid	11.2.0.3.9	11.2.0.3.17	Older than recommended versions.
	Exadata	randomadm01,randomadm02	11.2.3.2.1	11.2.3.2.1	Version within recommended range.
STORAGE SERVER	Exadata	randomceladm01,randomceladm02,randomceladm03	11.2.3.2.1	11.2.3.2.1	Version within recommended range.
IB SWITCH	Firmware	randomsw-iba0,randomsw-ibb0,randomsw-ibs0	2.1.2-1	1.3.3-2	Version within recommended range.

In this section of the MAA Scorecard the installed software versions are checked for the following conditions:

- Noncurrent software
- Incompatible with feature usage

Noncurrent software is reported as out-of-date under the following conditions:

- Software is no longer in Error Correction Support. An example status message is the following:
  Current version out of Error Correction Support
- Software has been superseded by a recommended version for longer than 9 months. An example status message is the following:
  Older than recommended versions

Incompatible software is reported when a version installed does not meet the minimum requirement for a specific feature in use. An example status message is the following:

Write-back Flash Cache required minimum 11.2.0.3.9 not met

Software that passes all version checks reports the following status:

Version within recommended range

The following is a sample “Findings Passed” report section, truncated for brevity:

Findings Passed

Database Server

Status	Type	Message	Status On	Details
PASS	Patch Check	System is not exposed to Exadata Critical Issue DB11	All Homes	View
PASS	SQL Parameter Check	RECYCLEBIN is set to the recommended value	All Instances	View
PASS	OS Check	DNS Server ping time is in acceptable range	All Database Servers	View
PASS	OS Check	Database Server Disk Controller Configuration meets recommendation	All Database Servers	View

The "Findings Passed" section lists all the checks that were given a status of "PASS" based on the data collected by exachk.
This section contains the same basic data as the "Findings Needing Attention" section, and also includes a "View" link to the detailed data.

The "Findings Passed" section is also subdivided into "Database Server", "Storage Server", "InfiniBand Switch", and "Cluster Wide".

The following is a sample of the "Systemwide firmware and software versions" section of the report, truncated for brevity:

Systemwide firmware and software versions

Please compare these versions against Database Machine and Exadata Storage Server 11g Release 2 (11.2) Supported Versions (Doc ID 888828.1) in MyOracle Support

Database server randomdb01

Clusterware and RDBMS software version

```
randomdb01.CRS_ACTIVE_VERSION = 11.2.0.2.0
randomdb01.dbm.INSTANCE_VERSION = 112020
```

Clusterware home(/u01/app/11.2.0/grid) patch inventory

```
Patch  13396479     : applied on Tue Mar 06 06:24:33 MST 2012
Patch  13603787     : applied on Tue Mar 06 06:23:09 MST 2012
Patch  13603796     : applied on Tue Mar 06 06:24:50 MST 2012
Patch Description:  "Exadata Database Recommended Patch (CRS) : 11.2.0.2.15
(13396479) "
Patch Description:  "Exadata Database Recommended Patch (Database) :
11.2.0.2.15 (13603787)"
```

```
Patch Description:  "Exadata Database Recommended Patch (Diskmon) :
11.2.0.2.15 (13603796)"

Exadata Server software version
version:11.2.3.1.0.120304

Infiniband HCA firmware version
Firmware version: 2.7.8130

OpenFabrics Enterprise Distribution (OFED) Software version
1.5.1
1.5.1
1.5.1
```

The "Systemwide firmware and software versions" section is a listing of key component version levels that must be compared to MOS note 888828.1 for use in patch and upgrade planning.

The following is a sample of the "Killed Processes" report section truncated for brevity:

Killed Processes

exachk found that below commands were killed during the run, so some checks might have failed to execute properly. Refer to the troubleshooting section of the user guide to resolve the issues.

```
Fri Mar 09 08:44:43 2012 Stuck child pid 21573  of parent 21572
Fri Mar 09 08:44:43 2012 Stuck child command is oracleGSITST2
(DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq)))
Fri Mar 09 08:44:43 2012 killing stuck command
/u01/app/oracle/product/11.2.0.2/gsitst/bin/sqlplus -s   as sysdba .
Operating system process ID 21572
```

If a "Killed Processes" section is present, it indicates that one or more commands did not complete within either the default timeout for the command type or the extended timeout if the timeout environment variables were set.

NOTE: The presence of this section also indicates that the data set for the run is incomplete and therefore the report is incomplete!

Additional information to diagnose the reasons for a skipped check is provided in the exachk documentation set. Additional information about which process was killed is found in the "watchdog.log" file in the data directory for the run in question.

If the system was busy at the time of the exachk execution, the first corrective action to try is to extend the appropriate timeout environment variable for the class of command that timed out, or repeat the run at a less busy time.

The following is a sample of the "Skipped Checks" report section, truncated for brevity:

Skipped Checks

```
skipping Infiniband switch HOSTNAME configuration (checkid:-
9AD56124DDFE9FCCE040E50A1EC038A6) on randomsw-ib1 because
s_sysconfig_network_randomsw-ib1.out not found
skipping Infiniband Switch NTP configuration (checkid:-
9AD59DE0898D0513E040E50A1EC03EEA) on randomsw-ib1 because s_ntp_randomsw-
ib1.out not found
skipping Infiniband switch sminfo_polling_timeout configuration (checkid:-
9AD8CC2B50B63DEBE040E50A1EC0529A) on randomsw-ib1 because s_opensm_randomsw-
ib1.out not found
```

The final section of the report is a list of "Skipped Checks".

> NOTE: The presence of this section also indicates that the data set for the run is incomplete and therefore the report is incomplete!

Additional information to diagnose the reasons for a skipped check is provided in the troubleshooting section.

exachk Report Sample – 11.2.0.3 upgrade module "Pre" mode

This section discusses the exachk report produced by the 11.2.0.3 upgrade module, executed in "Pre-upgrade" mode.

The following is a sample "Cluster Summary" section of the report when the 11.2.0.3 upgrade module is executed in "Pre-upgrade" mode:

Cluster Summary

Cluster Name	random-cluster
OS Version	LINUX X86-64 OELRHEL 5 2.6.18-274.18.1.0.1.el5
CRS Home – Version	/u01/app/11.2.0/grid - 11.2.0.2.0
DB Home - Version - Names	/u01/app/oracle/product/11.2.0/dbhome_1 - 11.2.0.2.0 - dbm
Exadata Version	11.2.3.1.0
Target Version	11.2.0.3.0
Number of nodes	9
Database Servers	2
Storage Servers	4
IB Switches	3
Upgrade Mode	Pre-upgrade
exachk Version	2.1.4_20120313
Collection	exachk_dbm_031312_144758.zip
Collection Date	13-Mar-2012 14:48:51

The "Cluster Summary" content is basically the same as a standard exachk report, except that the "Upgrade Mode" row is included.

The following is a sample of the "Table of Contents" section of the report when the 11.2.0.3 upgrade module is executed in "Pre-upgrade" mode:

Table of Contents

The "Table of Contents" for the 11.2.0.3.0 upgrade module contains only the specific checks directly related to the upgrade. The 11.2.0.3 upgrade module does not perform a full exachk run, and a full exachk run does not include the 11.2.0.3 upgrade module.

The rest of the upgrade module report follows standard exachk report format and function conventions.

exachk Report Sample – 11.2.0.3 upgrade module "Post" mode

This section discusses the exachk report produced by the 11.2.0.3 upgrade module, executed in "Post-upgrade" mode.

The following is a sample "Cluster Summary" section of the report when the 11.2.0.3 upgrade module is executed in "Post-upgrade" mode:

Cluster Summary

Cluster Name	random-c-sol
OS Version	SOLARIS (X8664-BIT) 11 5.11
CRS Home - Version	/u01/app/11.2.0.3/grid - 11.2.0.3.0
DB Home - Version - Names	
Target Version	11.2.0.3.0
Number of nodes	2
Database Servers	2
Upgrade Mode	Post-upgrade
exachk Version	2.1.4_20120313
Collection	exachk_dbm_031312_144303.zip
Collection Date	13-Mar-2012 14:43:30

The "Cluster Summary" content is basically the same as a standard exachk report, except that the "Upgrade Mode" is included, as shown by the blue circle.

The following is a sample of the "Table of Contents" section of the report when the 11.2.0.3 upgrade module is executed in "Post-upgrade" mode:

Table of Contents

The "Table of Contents" for the 11.2.0.3.0 upgrade module contains only the specific checks directly related to the upgrade. The 11.2.0.3 upgrade module does not perform a full exachk run, and a full exachk run does not include the 11.2.0.3 upgrade module.

The "Table of Contents" varies for both the pre- and post- upgrade modes of execution.

The rest of the upgrade module report follows standard exachk report format and function conventions.

Automation

Exachk can be optionally run in "silent" or "non-interactive" mode in order to enable scheduling and automation.

There are required pre-requisite configuration steps in order to operate in silent mode.

NOTE: For scheduling and automation purposes the -s command line option is recommended

-s command line option (eg., $ ./exachk -s)

1. configure ssh user equivalence for rdbms software owner (eg., oracle) on execution database server to oracle user on all other database servers. To validate proper ssh user equivalence configuration, login as the RDBMS software owner (eg., oracle) and execute the following commands:
   - $ ssh -o NumberOfPasswordPrompts=0 -o StrictHostKeyChecking=no -l oracle dbServerName "echo \"oracle user equivalence is setup correctly\""
     - where oracle is the RDBMS software owner and dbServerName is the database server hostname. Repeat for each database server
     - If "Permission denied (publickey,gssapi-with-mic,password)." is returned then the ssh user equivalence is not properly configured
2. add the following line to the sudoers file on each database server using visudo command
   - oracle ALL=(root) NOPASSWD:/tmp/root_exachk.sh

if sudo configuration discussed for -s command line option cannot be provided then another option is to use the -S command line option with the following configuration

-S command line option (eg., $ ./exachk -S)

1. configure ssh user equivalence for rdbms software owner (eg., oracle) from execution database server to oracle user all other database servers (mandatory). To validate proper ssh user equivalence configuration login as the RDBMS software owner (eg., oracle) and execute the following commands:
    - $ ssh -o NumberOfPasswordPrompts=0 -o StrictHostKeyChecking=no -l oracle dbServerName "echo \"oracle user equivalence is setup correctly\""
        - where oracle is the RDBMS software owner and dbServerName is the database server hostname. Repeat for each database server
        - If "Permission denied (publickey,gssapi-with-mic,password)." is returned then the ssh user equivalence is not properly configured

NOTES:

1. With the -S option some checks will be skipped due to privileges limitations
    - no root privileged checks on database servers at all will be executed

2. In the current version of exachk regardless of option (-s or -S) NO Storage Server or Infiniband Switch checks will be performed.

Appendix A – Troubleshooting Scenarios

Runtime Command Timeouts

RAT_TIMEOUT - default 90 seconds, if the default timeout for any non-root privileged individual commands is not long enough then the watchdog daemon will kill that child process and the desired data will be missing. If that is happening the timeout can be lengthened by setting this environment variable in the script execution environment. eg export RAT_TIMEOUT=120

RAT_ROOT_TIMEOUT - default 300 seconds, the tool will execute a set of root privileged data collections once for each node in the cluster including storage servers and InfiniBand switches. If the default timeout for the set of root privileged data collections is not long enough then the watchdog daemon will kill that child process and the desired data will be missing for that node. If that is happening the timeout can be lengthened by setting this environment variable in the script execution environment. eg export RAT_ROOT_TIMEOUT=600

RAT_PASSWORDCHECK_TIMEOUT – default is 1 second. In some cases, during the SSH login handshake with the DNS server, if the delay in communication between the remote target and the DNS server is slow, the login or password validation operation may timeout. The symptoms may include a known good password failing the password validation, or other timeouts in the log. Lengthen this parameter in such cases. Example: export RAT_PASSWORDCHECK_TIMEOUT=10

NOTE: If any of these timeouts are being encountered it would be best to determine the cause of the delay and correct it. Run the tool during times of least load on the system. Missing data collections will limit the value of the tool.

exachk_error.log has errors

When examining the exachk_error.log for the tool some errors will most likely be listed. Some of those are expected errors and are not indicative of any problem. These errors are redirected and "absorbed" into the error.log to keep them from being reported to the screen and cluttering the display. So do not report any of the following errors to Support.

For instance, an error similar to the following may be reported numerous times (once for each Oracle software home for each node):

/bin/sh: /u01/app/11.2.0/grid/OPatch/opatch: Permission denied
chmod: changing permissions of `/u01/app/oracle_ebs/product/11.2.0.2/VIS_RAC/.patch_storage': Operation not permitted
OPatch could not open log file, logging will not be possible
Inventory load failed... OPatch cannot load inventory for the given Oracle Home.

Those errors occur in role separated environments when the tool which is run as the RDBMS software owner attempts to list the patch inventories of homes owned by other users (eg., grid, or other database home owners) using opatch. So when opatch is invoked to list the patch inventories for those other users it errors out because the current user does not have permissions on those other homes. In those cases the opatch error is ignored and the patch inventories for those homes are gathered by other means.

Additionally, errors similar to the following are ignorable:

./exachk: line [N]: [: : integer expression expected

The line number may change over time but this error just means we were expecting an integer return value and no value was found (ie, empty) and so the shell returns that error in trying to make the comparison. This error could be repeated many times for the same command, once for each node.

remote root Login Problems

If remote root login is not permitted over ssh the root privileged commands will not work in case of option 2 explained above. To verify oracle software owner (eg., oracle) the user should execute the following command manually from whichever node it's not working and make sure he gets output as follows. If remote root login is not working then the tool will not be able to check the remote nodes. Please engage the systems admins to correct this if only temporarily for running the tool.

How to verify expected output if remote root login over ssh is configured

$ ssh root@remotehostname "id"
root@remotehostname's password:
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)

If the remote root login can be configured edit the /etc/ssh/sshd_config file as follows:

PermitRootLogin to yes

then run the following command as root on all nodes of the cluster.

/etc/init.d/sshd restart

Local Environmental Issues

The utility attempts to derive all the data it needs from the environment (OS and OCR) however it might be possible at times that the tool doesn't work as expected due to local system variances and it is difficult to anticipate and test every possible scenario. Therefore support for a number of environment variables have been included to provide a way for the user to over-ride the default behavior of the utility or to give it the information it needs in order to work as expected. The list of variables and their usage is as follows:

RAT_INV_LOC - if the oraInst.loc file is not where expected, eg. /u01/app/oraInventory, the user may need to specify the exact location of the oraInventory directory

RAT_CRS_HOME - Set this variable if the utility cannot derive the correct CRS_HOME path. The user can tell if this variable is required if he/she knows that the clusterware is installed but the utility thinks it is not.

RAT_ORACLE_HOME - Set this variable if the utility cannot derive the correct ORACLE_HOME paths for the databases registered in the clusterware. The user will be able to determine if this variable is required if they know the database software is installed but the utility displays information to the effect that the software is not installed. The tool will perform best practice and recommended patch checks for all the databases running from the home specified in RAT_ORACLE_HOME.

RAT_ASM_HOME - if the utility cannot derive the correct ASM_HOME path from the clusterware. The user will be able to determine if this variable is required if they know the ASM software is installed in a separate home but the utility displays information to the effect that the software is not installed.

RAT_OS - if the utility improperly derives the platform needed. The utility will prompt the user that the data needed for the derived platform could NOT be found due to improperly detecting an unsupported platform.

RAT_DB - if the utility improperly derives an incorrect database version

RAT_DBNAMES - if the utility doesn't derive valid database names from the clusterware a space delimited list of databases can be specified and the tool will use that list instead of what it derives from the clusterware, eg., export RAT_DBNAMES="ORCL ORADB PROD". Only use double quotes if specifying more than one database. Note that if you configure RAT_DBNAMES as a subset of databases registered in the clusterware, and you want the patch inventories of ALL databases found registered in the clusterware to have their patch inventories checked for recommended patches then you should also configure RAT_DBHOMES.

RAT_DBHOMES - If RAT_DBNAMES is set then by default the recommended patch analysis will be limited to the homes for the list of databases specified in RAT_DBNAMES. If it is desirable to perform the recommended patch analysis for additional database homes than those specified in RAT_DBNAMES then specify the space delimited list of databases whose homes should be checked for recommended patches, eg., assume export RAT_DBNAMES="ORCL ORADB" but you also want the PROD database home, even if the PROD database is down, to be checked then export RAT_DBHOMES="ORCL ORADB PROD". In this way, best practices will be

checked for the ORCL and ORADB databases but the recommended patches will be checked for the homes of ORCL, ORADB and PROD. Only use double quotes if specifying more than one database.

RAT_SSHELL – overrides the default secure shell location in case ssh is not where expected (ie., /usr/bin/ssh). If ssh commands return the error ”-bash: /usr/bin/ssh -q: No such file or directory “ then it may be because ssh isn't located where expected and this variable can be used to redirect the tool to the proper location.

RAT_SCOPY - overrides the default secure copy location in case scp is not where expected (ie., /usr/bin/scp). If scp commands return the error ”/usr/bin/scp -q: No such file or directory “ then it may be because scp isn't located where expected and this variable can be used to redirect the tool to the proper location.

RAT_LOCALONLY – If set to “1” then exachk will only check the execution (local) database server node as well as all storage servers and Infiniband Switches. The user also has the option to skip all storage server and Infiniband switch checks by choosing option 3 when prompted for passwords. When RAT_LOCALONLY=1 and storage server and InfiniBand switch passwords are provided then only the non-local database server checks will be skipped. For example: `export RAT_LOCALONLY=1`

RAT_CLUSTERNODES - By default exachk will run on all database servers and a list is obtained from olsnodes but if the user wants to run on a subset of database servers, one can set RAT_CLUSTERNODES environment variable in the current shell. Values must be separated by a space and must be valid hostnames in the cluster. For example: `export RAT_CLUSTERNODES=”randomdb01 randomdb05”, or export RAT_CLUSTERNODES=randomdb01.`

RAT_CELLS - By default exachk will run on all storage servers and a list is obtained from cellip.ora but if the user wants to run on a subset of storage servers, one can set RAT_CELLS environment variable in the current shell. Values must be separated by a space and must be valid hostnames in the cluster.
For example: `export RAT_CELLS=”randomcel01 randomcel06”, or export RAT_CELLS=randomcel01.`

RAT_IBSWITCHES - By default exachk will run on all infiniband switches and a list is obtained from ibswitches command but if the user wants to run on subset of infiniband switches, one can set RAT_IBSWITCHES environment variable in the current shell. Values must be separated by a space and must be valid hostnames in cluster. For example: `export RAT_IBSWITCHES=”randomsw-ib1 randomsw-ib3”, or export RAT_CELLS=randomsw-ib2.`

Database login problems

VERIFYING DATABASE AUTHENTICATION - if you intend to run the tool as a user other than the database software installation owner (eg., root or grid) and if you experience problems connecting to the database then try the following steps:

- login as grid(OS) user on system.
- export ORACLE_HOME=<path of Oracle database home>
- export ORACLE_SID=<database SID>
- export PATH=$ORACLE_HOME/bin:$ORACLE_HOME/lib:$PATH
- add alias in $ORACLE_HOME/network/admin/tnsnames.ora for <database SID>.
- connect to database using $ORACLE_HOME/bin/sqlplus "sys@<SID> as sysdba" and enter password.

If this method of connecting to the database will not work then the tool will not be able to connect either. Consider running the tool as the Oracle database software installation owner.

"Another instance of exachk is running..."

"Another instance of exachk is running on randomdb01. Please allow it to finish on randomdb01 before you run it on another node."

See Executing Exachk Fails with 'Another instance of exachk is running on node1' (Doc ID 1325691.1)

Prompts in user profiles

Prompts in user profiles could lead to false positives or unexpectedly few collections. Make sure that in the user profiles for root, the RDBMS software owner user (eg., oracle) and the grid infrastructure software owner (eg., grid) there are no prompts in the profiles of those users (eg., to prompt user to select from a menu, etc.) as that can lead to unexpected timeouts that could lead to unexpected results. If any of those user profiles contain any prompts then please remove them or comment them temporarily and source the profile for the user running the tool to make the change take effect.

Error RC-001 - Unable to read driver files

When executing exachk as the "oracle" userid (or the home owner userid in a role-separated environment, exachk exits with the following:

```
Error RC-001 - Unable to read driver files. Please refer to the section for
this error code in "Appendix A - Troubleshooting Scenarios" of the "Exachk
User Guide".

Exiting .....
```

There are three cases that may cause this error message to appear.

1) There is no space available at a working directory location. This can be the temporary working directory (/tmp/.exachk) or the retained work directory in the directory where exachk was launched (default) or the alternate location specified by the environment variable "RAT_OUTPUT". The corrective action is to increase the available space or redirect "RAT_OUTPUT" to another location.

2) Not being able to write into or read out of the temporary working directory location.

   The classic example is to download and install exachk as the "root" userid into `/tmp/exachk`, and then try to run it as the "oracle" userid or home owner userid in a role separated environment). For example:

```
<after installation by "root" to /tmp/exachk>
[root@randomdb01 exachk]# pwd
/tmp/exachk
[root@randomdb01 exachk]# ls -la
total 14072
drwxr-xr-x  3 root root    4096 Jun  7 08:25 .
drwxrwxrwt 12 root root    4096 Jun  7 09:27 ..
drwxrwxr-x  2 root root    4096 May 24 16:50 .cgrep
-rw-rw-r--  1 root root 9099005 May 24 16:50 collections.dat
-rwxr-xr-x  1 root root  807865 May 24 16:50 exachk
-rw-r--r--  1 root root 1646483 Jun  7 08:24 exachk.zip
-rw-r--r--  1 root root    2591 May 24 16:50 readme.txt
-rw-rw-r--  1 root root 2799973 May 24 16:50 rules.dat
```

```
-rw-r--r--  1 root root     297 May 24 16:50 UserGuide.txt

<followed by doing the following as the "oracle" userid>
-bash-3.2$ cd /tmp/exachk
-bash-3.2$ ./exachk

Error RC-001 - Unable to read driver files. Please report this error to
your Oracle representative for action.

Exiting .....
```

The first corrective action is to follow all instructions to download the latest exachk version from MOS 1070954.1 to a "clean" directory and try executing exachk again.

3) Not being able to read the .cgrep file in the directory where exachk was installed. This could be due to a permissions issue or because the .cgrep file is not present. For example:

```
ls -la
total 19176
drwxr-xr-x 4 oracle oinstall     4096 Oct 29 15:06 .
drwxr-xr-x 6 oracle oinstall     4096 Oct 29 14:10 ..
drwxrwxr-x 2 oracle oinstall     4096 Oct 29 13:51 .cgrep
-rw-rw-r-- 1 oracle oinstall 12205953 Oct 29 13:51 collections.dat
-rwxr-xr-x 1 oracle oinstall   871152 Oct 29 13:51 exachk
drwxr-xr-x 3 oracle oinstall    28672 Oct 29 15:06
exachk_randomdb05_102912_141204
-rw-r--r-- 1 oracle oinstall   763898 Oct 29 14:25
exachk_randomdb05_102912_141204.zip
-rw-r--r-- 1 oracle oinstall  2305664 Oct 29 13:08 exachk.zip
-rw-r--r-- 1 oracle oinstall     2590 Oct 29 13:51 readme.txt
-rw-rw-r-- 1 oracle oinstall  3401690 Oct 29 13:51 rules.dat
-rw-r--r-- 1 oracle oinstall      296 Oct 29 13:51 UserGuide.txt
[oracle@randomdb05 20121029]$ mv .cgrep .dont_use_cgrep
[oracle@randomdb05 20121029]$ ./exachk

RC-001- Unable to read driver files.  Please refer to the section for
this error code in Appendix A - Troubleshooting Scenarios of the exachk
User Guide.

 exachk exiting .....
```

The first corrective action is to follow all instructions to download the latest exachk version from MOS 1070954.1 to a "clean" directory and try executing exachk again.

If the above corrective actions for the RC-xxx errors do not fix the issue, then follow the instructions in "Appendix B – How To Obtain Support".

Error RC-003 - no audit checks were found

In the process of identifying the environment characteristics, exachk constructs some environment variables that it then compares to the exachk rules database to determine what checks to execute. If one of these environment variables does not match a known profile in the rules database, then an error that starts with "error RC-003 - no audit checks were found…" will be displayed and exachk will exit.

The most common case occurs when an older version of exachk is used in an Oracle Exadata Database Machine environment with recently released components. This may occur because of a delay between the release of a new component or version and when exachk incorporates support for it.

For example, when older versions of exachk below 2.1.3_20111212 were executed on an Oracle Exadata Database Machine where 11.2.0.3.0 of the database was deployed, exachk exited with the following message:

```
Error RC-003 - No audit checks were found for LINUXX8664OELRHEL5_112030-.
Please refer to the section for this error code in "Appendix A -
Troubleshooting Scenarios" of the "Exachk User Guide".
```

In this example, the "_112030" indicates that the 11.2.0.3.0 oracle stack was installed on the system, and since the version of exachk used did not support 11.2.0.3.0 it could not find a known match in the exachk rules database.

The most common correction is to refer to MOS 1070954.1 to find the latest version and the list of supported components and versions that match the Oracle Exadata Database Machine environment.

Debug Linux "expect" command connections

exachk uses the "expect" utility to answer password prompts during the connection process to remote targets, both for password validation as well as executing root collections, without logging the actual connection process by default. There are two exachk environment variables that may be set to help debug remote target connection issues.

RAT_EXPECT_DEBUG - If this variable is set to "-d" (dash d, not underscore d), expect command tracing will be activated, and the trace information is written to standard output. For example, "`export RAT_EXPECT_DEBUG=-d`".

RAT_EXPECT_STRACE_DEBUG - If this variable is set to "strace", strace calls the expect command, and the trace information is written to standard output. For example, "`export RAT_EXPECT_STRACE_DEBUG=strace`".

By varying the combinations of these two variables, three levels of expect connection tracing are available.

NOTE: These two variables should only be set at the direction of Oracle support or development. They are typically used in combination with other variables and user interface options to restrict the amount of data collected during the tracing, and the "script" command to capture standard output. They should not be set for a full exachk run as that will generate a large amount of data, and if the "script" command is not used, the trace data will simply scroll by on the screen and be lost!

Preserve input working directory

RAT_NOCLEAN_DIR - If this variable is set to "1", the hidden directory ".input_*" generated during an exachk run will be preserved instead of removed when exachk exits. For example, "`export RAT_NOCLEAN_DIR=1`". Only set this variable when specifically requested by Oracle support or development in connection with diagnostic requests for an SR or Bug.

Appendix B – How To Obtain Support

If problems are encountered either at runtime or if there are questions about the content of the findings of the tool:

Refer to the Exachk Tool How To in the exachk bundle downloaded from Note 1070954.1
Review this document for Usage and Troubleshooting information
Finally if the problem is still not resolved then please log an SR with Oracle Support.

Appendix C – How Long Should It Take to Run exachk?

The time it takes to run the tool will vary based on the number of nodes in a cluster, CPU load, network latency, etc. but normally the entire process takes only a few minutes per node (ie., less than 5 minutes per node). This is just a general guideline but if it takes substantially more time than this then there may be some other problem that needs to be investigated. Experience in the field has been that it normally takes about an hour for a full rack system assuming 8 database servers, 14 storage servers and 3 infiniband switches. It normally takes about 15 minutes for a quarter rack system. In both cases those times include the tool environmental discovery phase and the entry of passwords. Adjust expectations accordingly for 1/2 racks, interconnected racks or very busy systems.

Appendix D – Handling of Passwords by exachk

The tool does not store or save any passwords, either OS or database. For root passwords, wherever the tool finds ssh user equivalence configured for root among nodes it will utilize that configuration. If no ssh user equivalence among nodes is found to be configured for root the user will be prompted for the root password. For each component (database servers, storage servers and Infiniband switches) the user will be asked if the root password is the same for all nodes of the same system component. If the user responds "yes" (the default) then the root password will be prompted for and validated once and that password will be used for all nodes of that system component. If the user responds that the root password is not the same for all nodes of the same system component then the tool will prompt for and validate the root password for each individual node of the same component type.

The tool leverages the Linux expect utility which is shipped by default as part of the OEL5 distribution for interactive password automation (see http://expect.sourceforge.org). In this way the passwords can be "gathered" at the beginning of the processing and expect will supply them when needed at the root password prompts so that the tool can continue without the need for further input from the user. Without expect the user would need to closely monitor tool execution and enter the passwords interactively as prompted (possibly 25 times for a full rack system).

In validating the root passwords the user will have three opportunities to type the correct password. If the user fails to type the correct password after three attempts the tool will move on to the next node and echo a message stating that the password was still incorrect and that the checks dependent upon data collected from that node will be skipped. At that point the user can either cancel tool execution and get the problem resolved or continue but with the understanding that valuable data may be missing from the report. It is better to resolve the problem and start over than to be missing data.

It is also possible that between the time that the root passwords are entered and validated and nodes for those passwords are reached that the passwords could have been changed. In that case a message will appear in the on-screen output stating that the password must have been changed and that the collections for that node will be skipped which means the checks for that node will also be skipped. The user can either allow the tool to continue to completion knowing that data and checks will be skipped or cancel tool execution (Control-C) and resolve the problem and try again. It is better to resolve the problem and start over than to be missing data.

In any case any checks that are skipped (for any reason) will be logged and the reports listed at the end of tool execution will list any checks that were skipped and on which nodes.

Appendix E – Multiple Database Support Scenarios

exachk is designed for multiple database support. The tool will present a list of running databases which are registered in the Grid Infrastructure. The user may choose one, all or enter a comma separated list of numbers which designate the databases listed. It is not necessary to stage the tool on multiple nodes in order to check database instances running on other nodes of the cluster.

All database logins are accomplished by the use of local bequeath connections and assume the existence of OS authentication in the database for the user executing the tool. In some configurations there could be multiple database homes all owned by the same OS user (eg., oracle) or in others there could be any number of database homes all owned by different OS users. In the former case, run the tool as "oracle". In the latter case, stage and run the tool as the OS user which owns the RDBMS home which has the largest number of database instances running from that home as that user will not be able to login into database instances running from homes which it does not own. In order to scan the other databases the tool needs to be staged and run under each database home user account.

Appendix F – Optionally Uploading Exachk Results and Patches to a Database for Reporting

If it would be useful to upload the results of the audit checks done by the tool or the list of installed patches into database tables for use as a source of data for reporting, that is supported and OPTIONAL.

In order to support this feature a number of environment variables need to be set in the execution environment and a table needs to be created to receive the data from the audit check results. The table can have any name that is meaningful to the customer and which is a supported table name in Oracle.

Results table specification (eg., auditcheck_result):

Note: Version 2.2.0 added several additional columns to this table. exachk users who have used the database reporting features prior to 2.2.0 MUST add these additional columns. The DDL to add these new columns is as follows:

```
SQL> alter table auditcheck_result add (
CHECK_ID VARCHAR2(40),
```

```
NEEDS_RUNNING VARCHAR2(100),
MODULES VARCHAR2(4000),
DATABASE_ROLE VARCHAR2(100),
CLUSTERWARE_VERSION VARCHAR2(100),
GLOBAL_NAME VARCHAR2(256));
```

Full DDL for the Results Table:

```
create table
  auditcheck_result
    (
    COLLECTION_DATE TIMESTAMP,
    CHECK_NAME VARCHAR2(256),
    PARAM_NAME VARCHAR2(256),
    STATUS VARCHAR2(256),
    STATUS_MESSAGE VARCHAR2(256),
    ACTUAL_VALUE VARCHAR2(256),
    RECOMMENDED_VALUE VARCHAR2(256),
    COMPARISON_OPERATOR VARCHAR2(256),
    HOSTNAME VARCHAR2(256),
    INSTANCE_NAME VARCHAR2(256),
    CHECK_TYPE VARCHAR2(256),
    DB_PLATFORM VARCHAR2(256),
    OS_DISTRO VARCHAR2(256),
    OS_KERNEL VARCHAR2(256),
    OS_VERSION NUMBER,
    DB_VERSION VARCHAR2(256),
    CLUSTER_NAME VARCHAR2(256),
    DB_NAME VARCHAR2(256),
    ERROR_TEXT VARCHAR2(256),
    CHECK_ID VARCHAR2(40),
    NEEDS_RUNNING VARCHAR2(100),
    MODULES VARCHAR2(4000),
    DATABASE_ROLE VARCHAR2(100),
    CLUSTERWARE_VERSION VARCHAR2(100),
    GLOBAL_NAME VARCHAR2(256)
);
```

Environment variables (with example settings):

export RAT_UPLOAD_CONNECT_STRING="(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = bonanza)(PORT = 1521)) (LOAD_BALANCE = yes) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))"

export RAT_UPLOAD_TABLE=auditcheck_result (should match the name of the table that is created for the purpose)

export RAT_UPLOAD_USER=auditcheck (schema owner of the table created for the purpose)

export RAT_UPLOAD_PASSWORD=auditcheck (password for the schema owner)

export RAT_UPLOAD_ORACLE_HOME=<path of database home> (optional, alternate home containing sqlplus that you want to use for connecting in case not the current $ORACLE_HOME as derived by the tool from the environment)

NOTE: use the fully qualified address (as in the example above) for the connect string rather than an alias from the tnsnames.ora file so that it is not necessary to rely on tnsnames.ora file name resolution on all the servers where the tool might be run. The double quotes should be included.

When the first four above environment variables are set in the execution environment the tool will assume that the intent is to upload the data into the tables and at the end of the process it will attempt to upload the data.

This process relies upon the environment being properly set, ie. the connect string must be reachable, the username and password must be correct and the table name must be correct. Otherwise, if the tool is unable to connect to the database a message to that effect will be written to the log. If the RAT_UPLOAD_ORACLE_HOME variable is set the tool will invoke sqlplus in that home rather than attempting to invoke sqlplus from the current $ORACLE_HOME derived by the tool from the clusterware.

If any of the first four environment variables are not set then the tool will not attempt to upload the data.

Appendix G – Optionally Excluding Audit Checks

There are two methods to exclude a check from an exachk report:

Before an exachk html report is generated

To exclude an audit check before the html report is generated, construct a text file in the same directory where the exachk script and driver files have been installed. For example:

```
[oracle@randomadm01 20130524c]$ ls -1
collections.dat
exachk
exachk.zip
excluded_check_ids.txt
readme.txt
rules.dat
UserGuide.txt
```

The “excluded_check_ids.txt” contains the check identification numbers for the checks to be skipped, one per line. Each check is assigned a unique check identification number that does not change once assigned. Some checks will require one check identification number to be fully skipped, and some will require two. If a check has both an “COLLECTION_NAME” and an “AUDIT CHECK NAME” in the “exachk.log”file, it will require two entries in “excluded_check_ids.txt”. If the check has only an “AUDIT CHECK NAME” in the “exachk.log”file, it will require only 1 entry in “excluded_check_ids.txt”.

To find the check identification numbers to exclude, search for the name of the check you wish to exclude from the html report in the “exachk.log” file. This needs to be done using an “exachk.log” file from a previous complete exachk run. In version 2.2.2, you will find the “exachk.log” file in the “log” subdirectory created

under the directory from the run. For example, if the run generated the subdirectory named "exachk_randomadm01_dbm_052413_181326", the "exachk.log" file will be at: "exachk_randomadm01_dbm_052413_181326/log/exachk.log".

To determine if a check can be excluded, and if it requires one or two check identification numbers, you can grep through the "exachk.log" file for the name of the check from the HTML report. For example, assume that you want to exclude the check named "Configure Storage Server alerts to be sent via email" from further HTML reports. Open the "exachk.log" file in an editor and search on the check name string. Each check has a block of text associated with it in the "exachk.log" file, usually followed by a line made of "-". The check identification number will be above the dashed line. For example:

```
OSCOLLECTCNT=141 OSCOLLECTSUM= 171 rootYesNoint=1 root_need_cell_ssh=0
REQUIRE_ROOT=106
OS DATA COLLECTION BY ROOT SENT TO
/home/oracle/vern_wagman/exachk_222/20130524c/.input_052413_181326/exachk_c
ells.sh
ROW = 172.0.0.0.0.0.0.0.0.0
PARAMETER OR PATH = UNSPECIFIED
COMMAND = cellcli -e "alter cell validate mail" > /dev/null 2>&1;echo $?
CHECK ID = 9B7A70E3DDE3D069E040E50A1EC01B25
COLLECTION_NAME = Configure Storage Server alerts to be sent via email

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

What is required is the alpha numeric text after the "=" sign in the line that contains "CHECK ID = ".

The first search returned the "COLLECTION_NAME". Repeat the search to see if there is an "AUDIT CHECK NAME". In this case, there is:

```
  SF = DBMACHINE X2-2 AND X2-8 AUDIT CHECKS
  CATEGORY = ORACLE
  SUBCATEGORY = CONFIGURATION
  IS_BRANCH = 0
  PARAMETER OR PATH = cell_email_alerts_enabled_obsolete
  COMMAND = OS OUT CHECK cell_email_alerts_enabled_obsolete  -eq  0
AUDIT_CHECK_COMPONENTS = X3-8:DBM:X2-2:X2-8:X3-2:AVM:SUPERCLUSTER:EIGHTH
AUDIT_CHECK_ID = 9B7C05C06FBC302BE040E50A1EC04E95
  COMMAND RESULT = 0
  OPERATOR = -eq
  COMPARISON VALUE = 0

ROW=377.0.0.0.0.0.0.0.0.0 command=OS OUT CHECK
cell_email_alerts_enabled_obsolete  -eq  0 actual value=0 opeartor=-eq
required value =0 execute once=0

PASS =>  Storage Server alerts are configured to be sent via email

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

The output tells you that this check has both a "COLLECTION_NAME" and an "AUDIT CHECK NAME" so it will require two check identification numbers in the "excluded_check_ids.txt" file. For example:

```
$ cat excluded_check_ids.txt
9B7A70E3DDE3D069E040E50A1EC01B25
9B7C05C06FBC302BE040E50A1EC04E95
```

To verify that the proper checks were skipped due to the presence of the "excluded_check_ids.txt", open the "exachk.log" file from a run produced after the "excluded_check_ids.txt" file was created, and search on the check identification number. You should see text similar to the following for each check identification number in the "excluded_check_ids.txt" file:

```
Skipping  (CHECK ID 9B7A70E3DDE3D069E040E50A1EC01B25) because its in exclude file
```

In the "log" subdirectory of the data directory produced by the run, you will also see the "excluded_check_ids.txt" file was included for reference:

```
$ ls -l
total 448
-rw-r--r-- 1 oracle oinstall   1209 May 28 13:26 exachk_error.log
-rw-r--r-- 1 oracle oinstall 435973 May 28 13:26 exachk.log
-rw-r--r-- 1 oracle oinstall     66 May 28 13:26 excluded_check_ids.txt
-rw-r--r-- 1 oracle oinstall   3233 May 28 13:17 randomadm02.slave.log
-rw-r--r-- 1 oracle oinstall   2020 May 28 13:26 watchdog.log
```

Note that the check identification number location varies within the block of text associated with each check, and that it may be named either "CHECK ID" or "AUDIT_CHECK_ID". For example:

```
SQL STEP 746.0.0.0.0.0.0.0.0.0
  SF = DBMACHINE X2-2 AND X2-8 AUDIT CHECKS
  CATEGORY = ORACLE
  SUBCATEGORY = CONFIGURATION
  IS_BRANCH = 0
  PARAMETER OR PATH = processes
  COMMAND = SQL PARAMETER processes  =  1024
AUDIT_CHECK_COMPONENTS = DBM:X2-2:X3-2:AVM:SUPERCLUSTER:EIGHTH
AUDIT_CHECK_ID = DCB1CEA9CF6875BEE04312C0E50A4571
  COMMAND RESULT = 1024
  OPERATOR = =
  COMPARISON VALUE = 1024

ROW=746.0.0.0.0.0.0.0.0.0 command=SQL PARAMETER processes  =  1024 actual
value=1024 opeartor== required value 1024 SOURCEFILENAME=v_parameter

PASS =>  Database parameter PROCESSES is set to recommended value on dbm1
instance

CHECK ID = DCB1CEA9CF6875BEE04312C0E50A4571
AUDIT CHECK NAME = processes
```

If the audit check block does not contain a check identification number line, then that check cannot be excluded. Only stand-alone audit checks or audit checks which are a step in a branch can be excluded. Branches and collections cannot be excluded.

Save the excluded_check_ids.txt file. On subsequent executions of the tool, before an audit check is run the tool will check the excluded_check_ids.txt file to see if that check has been excluded and skip it if it has. The

excluded_check_ids.txt file should be able to be carried forward for newer versions of the script or kits however newer kits may contain additional audit checks which were not in the older versions of the kit.

After an exachk html report is generated

The following method can be used to remove a check from an existing exachk html report.

Below the table of contents there is a “Remove finding from report” link as shown below:

Table of Contents

Remove finding from report

Click on the ““Remove finding from report” link and the format of the entire report changes as shown below:

Hide Remove Buttons

Removing findings in page does not change the original html file. Please use browsers save page button (or press Ctrl+S) to save the report.

Findings Needing Attention

FAIL, WARNING, ERROR and INFO findings should be evaluated. INFO status is considered a significant finding and details for those should be reviewed in light of your environment.

Database Server

Status	Type	Message	Status On	Details
[X]FAIL	OS Check	Database Server Physical Drive Configuration does not meet recommendation	All Database Servers	View
[X]FAIL	OS Check	Verify-topology returned some errors or warning.	All Database Servers	View

There is a new “Hide Remove Buttons” link, which when clicked, will return the report to the standard format. There is also a notice in red that you need to save the modified report to a new file, because exachk does not overwrite the original report.

And most importantly, “X” buttons appear next to each item on the report in the “Status” column.

Click on the“X” link for the “Database Server Physical Drive Configuration does not meet recommendation” check and the check and it’s detailed sections, will be removed from the report, as shown below:

Database Server

Status	Type	Message	Status On	Details
FAIL	OS Check	Verify-topology returned some errors or warning.	All Database Servers	View

Notice that the “Database Server Physical Drive Configuration does not meet recommendation” item is now gone from the report.

If this was the only change to be made, from here you would click on the “Hide Remove Buttons”, and then save the resulting file to a new name.

You can use the browser’s back button to “undo” a removal in error, or you can simply kill the browser session without saving to a new file to clear all changes.

Appendix H – Special Notes on USERIDs and Passwords

As a means of providing higher security when using the tool, passwords are not stored. The tool uses operating system or standard Oracle username and password authentication mechanisms.

If the user executing the tool has an account which is set up for OS authentication in Oracle then no username and password will be required for database log in. However, if the user is not set up with OS authentication for database access then the user will be prompted with the standard Oracle database authentication prompts.

Appendix I - Special Notes on Output Directory

To limit security vulnerabilities, the permissions of the tool output directory should be set as restrictive as possible. The output directory could contain sensitive configuration information and, when no other mechanism is available, temporary data collection files.

Appendix J - How to Upgrade Exachk

New versions of exachk will be released periodically. Check MOS Note 1070954.1 for new versions.

The recommended method for upgrading the tool would be to change the name of the old staging directory, create a new staging directory and unzip the new kit there and use the new staging directory and kit going forward, eg. if the staging directory is named exachkstage

```
$ mv exachkstage exachkstage_05172011 (a date)
$ mkdir exachkstage
$ mv exachk.zip exachkstage
$ unzip exachkstage/exachk.zip
```

Appendix K – Output File Maintenance

Whenever exachk is run it creates a subdirectory using a naming convention that begins with "exachk" and includes a date and time (eg., exachk_SIEBXL_072611_141001) and a .zip archive that contains the contents of the subdirectory (eg., exachk_SIEBXL_072611_141001.zip) at the same level on the filesystem as the tool itself. The total size of the subdirectory and .zip file is expected to be somewhat less than about 5M on the filesystem. The exact size may vary depending upon how many nodes and how many databases there are in the system. While it is expected that exachk will be run at times as described in the "When To Run Exachk" section over time the number of files will build up and the customer may want to perform maintenance and clean out older files and/or subdirectories.

Each customer may have different requirements and therefore it is incumbent upon the customer to define processes and procedures for implementing their own strategy for maintaining these subdirectories and files. Some customers may choose to archive the files to a different system. Some customers may want to delete the subdirectories and keep the .zip files. Still other customers might opt to delete both the older subdirectories and .zip files.

Oracle recommends that the customer implement cron jobs or other scheduling tools (eg., Oracle Enterprise Manager) to implement their own process and procedure for this task based on their individual requirements.

As an alternative to maintaining exachk data in operating system files, as part of your data retention strategy see Appendix F – Optionally Uploading Exachk Results and Patches to a Database for Reporting.

Appendix L – Maximum Availability Architecture Scorecard (MAA)

The MAA Scorecard is a set of Maximum Availability Architecture Best Practices and the findings related to them. The purpose is to give the customer a Scorecard for their preparedness for various kinds of faults that can occur in an Oracle Exadata Database Machine environment. The MAA Scorecard is presented by default in exachk because it is considered to be a very important feature. However, if it is desirable or necessary to suppress the MAA Scorecard that can be done by running exachk using the -m argument, eg

```
$ ./exachk -m
```

Appendix M – 11.2.0.3 upgrade module

This module assists with evaluating and preparing an Oracle Exadata Database Machine environment for upgrading to version 11.2.0.3 of the Oracle software. The pre-upgrade mode evaluates the environment and

makes recommendations to prepare the environment for the upgrade procedure. The post-upgrade mode evaluates the environment to confirm that key components are as expected after the upgrade procedure. The goal is to simplify and enhance the reliability of the upgrade experience.

NOTE: There are numerous documents which discuss various aspects of upgrading to Oracle RAC version 11.2.0.3. For example: Upgrade Companion, Upgrade Guide, Oracle Database Documentation, and Manual Upgrade Checklist. While the exachk upgrade module automates the checking of many best practices, patch pre-requisites, and configuration pre-requisites, it does not cover every possible combination. It is advised that customers thoroughly review the upgrade documents in the context of their own specific environment, as some concepts or individual items do not lend themselves easily to automation.

NOTE: As with any other exachk recommendation, the 11.2.0.3 upgrade module does not implement any of the recommendations. Recommendations must be manually implemented.

What's New By Version

Version 2.2.2.1:

Major New Functionality:

None

Checks added:

None

Checks removed:

None

NOTE: "Checks removed" does not typically indicate a loss of functionality, but that there is some other mechanism in base code that has taken over the purpose of this check, or a prior restriction has been lifted.

Issues Fixed By Version

Version 2.2.2.1

Bug Num	Fixed	Description
17256632	2.2.2.1	illegal octal digit '8' at -e line 1, at end of line
17206990	2.2.2.1	underscore "_" in grid owner name (a_grid) causes ASM checks to fail

Version 2.2.2:

Major New Functionality:

exachk daemon to support non-interactive execution on storage servers and IB switches
Ability to run –profile sysadmin under root userid
Software version recommendation matrix in MAA scorecard
Ability to run MAA scorecard stand alone
Identify hardware type of each storage server independently
Output directory restructure

Checks added:

Initialization parameter processes
Initialization parameter db_files=1024
Verify vm.min_free_kbytes=524288
Verify no asm corruption is reported
Verify subnet manager service not running on storage or db servers
Verify log transport services for enabled redo destinations are functional
“Verify data files are recoverable” to MAA scorecard
“Verify data files are recoverable (data guard)" to MAA scorecard
“Verify log_archive_max_processes parameter is optimally configured” to MAA scorecard
Verify storage server network configuration with ipconf

Checks removed:

None

NOTE: “Checks removed” does not typically indicate a loss of functionality, but that there is some other mechanism in base code that has taken over the purpose of this check, or a prior restriction has been lifted.

Issues Fixed By Version

Version 2.2.2

Bug Num	Fixed Description
16971269	exacheck does not upload output to database when run in daemon mode
16934205	"exadata storage server system model number" wrong in mixed x2-2 / x3-2
16920954	modify "verify electronic storage module (esm) lifetime is within specification"
16902904	add "verify log_archive_max_processes parameter is optimally configured"
16864328	exachk -m has maa scorecard (version: 2013/05/22)
16822355	./exachk -u -o pre when run in daemon mode hangs (2 hours)
16795936	add: initialization parameter processes
16795868	add: initialization parameter db_files=1024
16795740	add: verify vm.min_free_kbytes=524288
16795681	modify: verify exadata smart flash cache is created
16795675	modify: verify exadata smart flash log is created
16795505	add: verify no asm corruption is reported
16795289	add: verify subnet manager service not running on storage or db servers
16776890	exachk -profile switch has skipped checks (due to *.out not found)
16769762	bp ver installed does not match the bp ver registered - due to other $oh
16754221	exachk: local listener check raises false warning in multiple vip configuration
16693849	add "verify log transport services for enabled redo destinations are functional"
16682436	foreground the .exachk job stopped, that job goes away w/o updating client.pid
16682344	exachk daemon: ./exachk -a process lingers even after exachk is done
16682235	exachk should not terminate the exachk that is already running on xterm 2
16680382	./exachk -d stattt should have returned an error
16672596	add function to execute maa scorecard in stand alone mode
16666386	add "verify data files are recoverable" to maa scorecard
16666256	add check "verify data files are recoverable (data guard)" to maa scorecard
16575973	modify rationale for "exachkcfg autostart status" to match bp wiki
16563882	failed to completely exclude asrexacheck
16562790	add "verify storage server network configuration with ipconf"

16561752 exadata: exachk fail to copy xml files to remote node
16554523 the bundle patch version installed does not match the bundle patch version regis
16546921 modify documentation for "excluded_check_ids.txt" file
16520619 exachk issues with root password having special characters
16519731 exadata: exachk reporting a set of skipped checks
16448891 checkdiskfgmapping.sh griddisk suffix check should be case insensitive
16440031 sm_priority check has "is_spine = 0" in detail view
16320354 run ib switch checks while using silent mode option
16243437 identify storage server hardware types individually, rather than on rack basis
14534296 modify "verify infiniband subnet manager is running on an infiniband switch"
14525696 ada: improve exachk html report for jaws reader compatibility
13986761 exachk should be run regularly via crontab now that we deploy the exachk plugin
12666078 add capability to run exachk as the root user

COPYRIGHT NOTICE

TRADEMARK NOTICE

LEGAL NOTICES AND TERMS OF USE