

Oracle Security

Spring 2018



Securing Database 18c with a Read Only Home

Dan Morgan

- One of the new features present in Oracle 18c in the read only Oracle home
- Why a read only home?
 - Prevents anyone from modifying files under \$ORACLE_HOME
 - /dbs (spfile)
 - /network/admin (sqlnet.ora, listener.ora, tnsnames.ora)
 - /rdbms/admin (source code for data dictionary objects, functions, packages, and procedures)
 - /sqlplus/admin (glogin.sql runs automatically with every SQL*Plus login)

```
2. Ora18Cloud
[oracle@oem13c2-demo-db18c oracle]$ ls
admin  audit  cfgtoollogs  checkpoints  diag  product
[oracle@oem13c2-demo-db18c oracle]$ cd product
[oracle@oem13c2-demo-db18c product]$ ls
18.0.0  apex  java  ords
[oracle@oem13c2-demo-db18c product]$ cd 18.0.0/
[oracle@oem13c2-demo-db18c 18.0.0]$ ls
dbhome_1
[oracle@oem13c2-demo-db18c 18.0.0]$ cd dbhome_1/
[oracle@oem13c2-demo-db18c dbhome_1]$ ls
addnode      clone  data      diagnostics  has      javavm  lib      nls      oracore    oss      precomp  relnotes  runInstaller  sqlj      ucp
apex         crs    dbjava    dm           hs      jdbc    log      odbc     oraInst.loc  oui     QOPatch  root.sh    schagent.conf  sqlpatch  usm
assistants  css    dbs       drdaas      install  jdk     md       olap     ord        owm     R        root.sh.bkup  sdk       sqlplus    utl
bin         ctx    deinstall dv           instantclient  jlib    mgw     OPatch  ordim     perl   racg    root.sh.old  slax      srvm       wwg
cfgtoollogs cv     demo      env.ora     inventory  ldap    network  opmn     ords      plsql  rdbms   root.sh.old.1  sqldeveloper  suptools  xdk
[oracle@oem13c2-demo-db18c dbhome_1]$
```



18c Read Only Oracle Home

By Franck Pachot | February 18, 2018 | Oracle | No Comments



This is the big new feature of Oracle 18c about database software installation. Something that was needed for decades for the ease of software deployment. [Piet de Visser](#) raised this to Oracle a long time ago, and we were talking about that recently when discussing this new excitement to deploy software in Docker containers. Docker containers are by definition immutable images. You need a Read Only Oracle Home, all the immutable files (configuration, logs, database) being in an external volume. Then, to upgrade the software, you just open this volume with an image of the new database version.

```
2. Ora18Cloud
[oracle@oem13c2-demo-db18c bin]$ pwd
/u01/app/oracle/product/18.0.0/dbhome_1/bin
[oracle@oem13c2-demo-db18c bin]$ ls -al rooh*
-rwxr-x--- 1 oracle oinstall 4631 Feb  8 08:45 roohctl
[oracle@oem13c2-demo-db18c bin]$
```

```
[oracle@oem13c2-demo-db18c bin]$ more roohctl
#!/bin/sh
#
# $Header: assistants/bin/roohctl.sh.pp /main/5 2017/09/05 01:53:02 jaikrish Exp $
#
# roohctl.sh
#
# Copyright (c) 2014, 2017, Oracle and/or its affiliates. All rights reserved.
#
# NAME
#   roohctl.sh - <one-line expansion of the name>
#
# DESCRIPTION
#   <short description of component this file declares/defines>
#
# NOTES
#   <other useful comments, qualifications, etc.>
#
# MODIFIED   (MM/DD/YY)
# mstalin    08/22/17 - 26495385 Could not get inventory location error
# mstalin    09/12/14 - Script file for roohctl
# mstalin    09/12/14 - Creation
#
#####
# Variables set by Oracle Universal Installer for dependent components.
#####
```

```
# Check if user is non-root

MYPLATFORM=`uname`

# make sure others can not read/write any files created
umask 27

# The environment variable $TWO_TASK cannot be set during the installation
unset TWO_TASK

# The environment variable $JAVA_HOME cannot be set during the installation
unset JAVA_HOME

# Basic error checking
case $OH in
  "") echo "*** ORACLE_HOME Not Set!"
      echo "    Set and export ORACLE_HOME, then re-run"
      echo "    ORACLE_HOME points to the main directory that"
      echo "    contains all Oracle products."
      exit 1;;
esac

#call platform_common script
. $ORACLE_HOME/bin/platform_common

# Check if user is non-root
if [ "$RUID" = "0" ]; then
    echo "roohctl cannot be run as root."
    exit 1;
fi

JRE_OPTIONS="${JRE_OPTIONS} -Dsun.java2d.font.DisableAlgorithmicStyles=true -DIGNORE_PREREQS=$IGNORE_PREREQS -mx128m $DEBUG_STRING"

# Set Classpath for ROOHCTL
CLASSPATH=$ROOHCTL_CLASSPATH:$ASSISTANTS_COMMON_CLASSPATH:$SHARE_CLASSPATH:$XMLPARSER_CLASSPATH:$GDK_CLASSPATH:$NETCFG_CLASSPATH:$SRVM_CLASSPATH:$INSTALLER_CLASSPATH

ARGUMENTS=""
NUMBER_OF_ARGUMENTS=$#
if [ $NUMBER_OF_ARGUMENTS -gt 0 ]; then
    ARGUMENTS=$*
fi
```



```
#####
# Run roohctl
exec $JRE_DIR/bin/java $JRE_OPTIONS -classpath $CLASSPATH oracle.assistants.roohctl.RoohCtl $ARGUMENTS
[oracle@oem13c2-demo-db18c bin]$ clear
[oracle@oem13c2-demo-db18c bin]$ pwd
/u01/app/oracle/product/18.0.0/dbhome_1/bin
[oracle@oem13c2-demo-db18c bin]$ ls -al rooh*
-rwxr-x--- 1 oracle oinstall 4631 Feb  8 08:45 roohctl
[oracle@oem13c2-demo-db18c bin]$ clear
[oracle@oem13c2-demo-db18c bin]$ more roohctl
#!/bin/sh
#
# $Header: assistants/bin/roohctl.sh.pp /main/5 2017/09/05 01:53:02 jaikrish Exp $
#
# roohctl.sh
#
# Copyright (c) 2014, 2017, Oracle and/or its affiliates. All rights reserved.
#
# NAME
#   roohctl.sh - <one-line expansion of the name>
#
# DESCRIPTION
#   <short description of component this file declares/defines>
#
# NOTES
#   <other useful comments, qualifications, etc.>
#
# MODIFIED   (MM/DD/YY)
# mstalin    08/22/17 - 26495385 Could not get inventory location error
# mstalin    09/12/14 - Script file for roohctl
# mstalin    09/12/14 - Creation
#
```

- With a Read Only Oracle Home we protect files that should be static upon install and minimize the footprint for attack to a very small number of files that must be dynamic
- To identify the new locations Oracle has created 2 new environment variables
 - Oracle Base Configuration (orabaseconfig) which exists primarily as a mapping to .ora and .dat files
 - Oracle Base Home (orabasehome) which is primarily intended as a mapping to /network/admin
- You enable a Read Only Oracle Home with `roohctl -enable` as shown below

```
[oracle@VM181 18c]$ roohctl -enable
Enabling Read-Only Oracle home.
Update orabasetab file to enable Read-Only Oracle home.
Orabasetab file has been updated successfully.
Create bootstrap directories for Read-Only Oracle home.
Bootstrap directories have been created successfully.
Bootstrap files have been processed successfully.
Read-Only Oracle home has been enabled successfully.
Check the log file /u01/app/oracle/cfgtoollogs/roohctl/roohctl-180217PM111551.log.
```

- In 12c, you can change your habits and replace all references to `${ORACLE_HOME}/dbs` with `$(oracle_base_config)/dbs` and `${ORACLE_HOME}` with `$(oracle_base_home)`. In 12c they will go to the same `ORACLE_HOME`. But you will be ready to enable ROOH in 18c

An IT Terrorist Attack (7:7)

- We need you to grab your keyboard and join us in the battle to protect your data, your database, your organization
- ROOH is a step in the right direction

