Backup and Restore for Avaya Speech Analytics

Release 2.0.2
November 2015

Contents

1. **Overview** 3

About this document 3

Intended Audience 3

About Speech Analytics 3

Related Documents 3

2. **About Speech Analytics Backup and Restore Procedures** 4

3. **AASA Regular Operation** 4

Performing the Backup 4

Setting NFS Server 4

Setting up the NFS Mount Point for Backups 5

Activating the Backup Feature 6

Checking the Backup at Oracle RMAN 17

Restoring the AASA Backup in regular operation 17

4. **AASA in Disaster Recovery** 18

Performing the Backup 18

Performing the Restore of the Backup 23

Overview

About this document

Avaya Speech Analytics is part of the Avaya Aura ® Performance Analytics suite of software. All software from this suite runs on top of the Avaya Aura ® Performance Center environment. This document explains how to administer Speech Analytics.

Intended Audience

This document is meant for contact center staff that performs administrative and quality improvement roles, such as:

- Contact center administrators
- Contact center business intelligence and reporting staff

About Speech Analytics

Avaya Speech Analytics is a search and analytics solution based on phonetic technology. Data analysts and executives use Speech Analytics to rapidly and efficiently analyze sets of call recordings for quality monitoring, compliance and business intelligence. Speech Analytics is based on phonetic technology and provides speaker independent search and analytics, which is not limited to a pre-defined dictionary of keywords or terms, providing greater flexibility, significantly increased performance, and reduced total cost of ownership.

Related Documents

This document is part of the Speech Analytics documentation set that also includes the following documents:

- *Avaya Speech Analytics Reporting*
- *Implementing Avaya Speech Analytics*
- *Administering Avaya Speech Analytics*

You can download the documents from http://support.avaya.com.

About Speech Analytics Backup and Restore Procedures

The AASA backup and restore procedures are divided in 2 main scenarios:

1. Regular operation: when backups are taken regularly and, for any reason, data needs to be restored while AASA is operating normally.
2. Disaster Recovery: when the AASA has been re-installed and data backup collected prior the reinstallation needs to be restored in a fresh environment.

In each of the scenarios above, both the data backup and restoring procedures use distinguished methods. In the next chapters, this document will describe the steps required for backing up and restoring the AASA data on each of scenarios above.

AASA Regular Operation

Performing the Backup

These are the steps required for backing up the AASA while it is under normal operation.

Setting NFS Server

Prerequisites

A NFS server is required for backup purposes.

This backup procedure assumes that the AASA Server host has the NFS service installed and that there is enough space available for backup storage.

The NFS server host must not be the AAPC/AASA server.

Procedure

1. Create a directory in a partition with enough space available.

   # mk <nfs_dir>

2. Edit exports file

   # vi /etc/exports

3. Add the following line

   <nfs_dir> <APC Server IP>(rw,sync,no_root_squash)

   Save the file

4. Restart the NFS service

   # service nfs restart

Setting up the NFS Mount Point for Backups

Prerequisites

An NFS mount point must be set on the All-In-One host. Setting an NFS mount point for backups can be a difficult procedure. If you need assistance, contact Avaya Support personnel.

NOTE: The backup procedure requires that a NFS mount point is set up for backups.

Procedure

1. Configure the network drive for NFS mount and log on to the host that the network drive resides. Follow the instructions the host OS vendor provides to make the network drive ready for NFS mount. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

2. Create a Mount point

   # mkdir MountPoint

   The MountPoint variable is a path from the host to the backup location on the network drive or storage array. For example, you can name the mount point /backup.

3. Edit fstab

   # vi /etc/fstab

   Add the following line

   <NFS Server IP>:RemotePath MountPoint nfs rw,rsize=32768,wsize=32768,timeo=14,intr

   Save the file.

4. Mount the new file system

 # cd /

 # mount -a

5. Check that the fs is created.

   # df —h

6. For testing purposes, copy a dummy file into the MountPoint and verify that the file is copied to the NFS server and vice versa.

Activating the Backup Feature

Before starting the backup process you must to copy the “db_backup.sh” script below to “/avaya/Oracle/” folder and make sure it has the proper permissions to be executed.

The Backup script

Below you can find the contents of “db_backup.sh” script

```
#!/bin/bash
################################################################################
# Copyright (c) 2008, Avaya. All rights reserved.
#
# NAME:  db_backup.sh
#
# DESCRIPTION:
#    Perform a full or an incremental database backup.
#    Incremental backups can be either level 0 or level 1
#    A level 1 incremental backup can be either of the following types:
#    1) A differential backup, which backs up all blocks changed after the most
#       recent incremental backup at level 1 or 0
#    2) A cumulative backup, which backs up all blocks changed after the most
recent
#       incremental backup at level 0
#    Incremental backups are differential by default. Only use differential
#    incremental backups to save space.
#
# ORA-27054 ERROR may happen when running RMAN with NFS
# see metalink Note:424785.1
# One workaround is using following nfs options for Linux
# rw,bg,hard,nointr,rsize=32768,wsize=32768,tcp,vers=3,timeo=600,actimeo=0
# e.g.
# mount -o
rw,bg,hard,nointr,rsize=32768,wsize=32768,tcp,vers=3,timeo=600,actimeo=0
# nfs_server:/backup/data /u02/backup
#
# Arguments:
#    -t [db|log] -i [0|1]
```

```
#
# Installed:
#    /avaya/Oracle/db_backup.sh
#
# Usage:
#    db_backup.sh [-t db [-i 0|1] | log]
#
# MODIFICATIONS:
#
# DATE        WHO    DESCRIPTION
# 02/22/2008  hgl    created
# 03/17/2010  jfk    remove destination option in favor of fast recovery area
# 03/17/2010  jfk    added option for backup type of db-database log-archivelogs
# 04/01/2010  jfk    modified logging and environment variables
# 03/15/2011  hgl    added compression
# 04/28/2011  bart   fixed fail detection of RMAN execution;
#                    fixed possible permission issue with write of DBID, INITORA
# 02/07/2012  skwest added data guard
# 04/18/2012  skwest add GLBL_PSWD
# 05/23/2012  skwest wi01001615 fix PGM issue, add check for VARLOGFILEDIR
# 06/20/2012  skwest removed delete input from DG backups per Oracle
Recommendation
#                    change /u01/avaya to /avaya so links work.
# 07/05/2012  skwest added 2 special lines for archivelog deletion per Oracle
#                    wi01016595/SR 3-5833438821
# 07/05/2012  skwest wi01001166 add check/create for /var/log/Avaya...CCR...
################################################################################
#-------------------------------------------------------------------------------
# setup
#-------------------------------------------------------------------------------
if [ "${ENVDIR}" = "" ]
then
  ENVDIR=/avaya/Avaya_IQ/services/env
  export ENVDIR
fi

. ${ENVDIR}/OSENV.sh
. ${ENVDIR}/APPENV.sh
. ${ENVDIR}/ORAENV.sh

if [ "${PGM}" = "" ]
then
   PGM=db_backup
   LOGFILE=/avaya/Avaya_IQ/services/log/${PGM}.log
   VARLOGDIR=/var/log/Avaya/CCR/backup
   VARLOGFILE=/var/log/Avaya/CCR/backup/${PGM}.log
fi

if [ ! -d /var/log/Avaya ]; then
   mkdir -p /var/log/Avaya > /dev/null 2>&1
   chmod 766 /var/log/Avaya
fi

if [ ! -d /var/log/Avaya/CCR ]; then
   mkdir -p /var/log/Avaya/CCR > /dev/null 2>&1
```

```
   chmod 766 /var/log/Avaya/CCR
fi

if [ ! -d $VARLOGDIR ]; then
   mkdir -p $VARLOGDIR > /dev/null 2>&1
   chmod 766 $VARLOGDIR
fi


# manage local backup logfile
# audit logfiles: /var/log/Avaya/CCR/backup/db_backup.sh ($VARLOGFILE)
${TAIL} -40000 ${LOGFILE} > ${TMPDIR}/${PGM}_tmp.log
${MV} ${TMPDIR}/${PGM}_tmp.log ${LOGFILE}

GLBL_PSWD="`cat /avaya/LICENSE/.tkpph | gpg --batch --passphrase-fd 0 -d
/avaya/LICENSE/.tkp 2> /dev/null`"


#-------------------------------------------------------------------------------
db_backupDate=`${DATE}`
trapID=18231
start_time=`${DATE} "+%Y:%m:%d:%H:%M:%S"`
keyword="Full Backup"

trap 'clean_exit 2' 1 2 3 15

ARG=$@

log_action()
{
 # make sure start_time is correct for db_diag log parsing
 if [ "$@" = "Backup.Start." ]; then
    action_time=$start_time
 else
    action_time=`${DATE} "+%Y:%m:%d:%H:%M:%S"`
 fi

 echo -e "${err}:${trapID}:${PGM}:${PGM}:${action_time}:${keyword}. $@" >>
${LOGFILE}
 echo -e "${err}:${trapID}:${PGM}:${PGM}:${action_time}:${keyword}. $@" >>
${VARLOGFILE}
}

clean_exit()
{
    if [ $1 -ne 3 ]; then
        rm -f $LOCKFILE
    fi
    if [ $1 -ne 0 ]; then
        if [ $1 -eq 2 ]; then
            echo "Caught signal(2) to exit. Exiting..."
            echo -e "This may take a while, please wait..."
            err="001"
            log_action "Caught signal(2) to exit.Exit."
            # waiting RMAN finishes
```

```
            TIMEOUT=180
            count=0
            rt=0
            while [ $rt -eq 0 -a $count -lt $TIMEOUT ]
            do
                echo -e ".\c"
                sleep 2
                count=`expr $count + 1`
                ps -ef | grep -v grep | grep "rman target" > /dev/null 2>&1
                rt=$?
            done
            echo ""
        fi
    fi
    log_action "Backup.End."
    exit $1
}

# wi00880538 - fix potential permission issue for oracle write to these files
${RM} ${TMPDIR}/DBID
${RM} ${TMPDIR}/INITORA
${RM} ${TMPDIR}/control01.ctl.bkup

#skwest added 2 additional backup controlfiles per best 11g practices
${CAT} ${DETECTDIR}/REQSQLHEAD                                          >
${TMPDIR}/dbid.sql
${ECHO} "SELECT 'dbid:'||dbid FROM V\$DATABASE;"                       >>
${TMPDIR}/dbid.sql
${ECHO} "SELECT 'scn:'||dbms_flashback.get_system_change_number"       >>
${TMPDIR}/dbid.sql
${ECHO} "  FROM dual;"                                                  >>
${TMPDIR}/dbid.sql
${ECHO} "exit;"                                                        >>
${TMPDIR}/dbid.sql
${CAT} ${DETECTDIR}/REQSQLHEAD                                          >
${TMPDIR}/init.sql
${ECHO} "CREATE pfile='${TMPDIR}/INITORA' FROM SPFILE;"                >>
${TMPDIR}/init.sql
${ECHO} "ALTER DATABASE BACKUP CONTROLFILE TO TRACE;"                   >>
${TMPDIR}/init.sql
${ECHO} "ALTER DATABASE BACKUP CONTROLFILE TO '${TMPDIR}/control01.ctl.bkup';"
>> ${TMPDIR}/init.sql
${ECHO} "exit;"                                                        >>
${TMPDIR}/init.sql
su - oracle -c "sqlplus -s ${ORACLE_LOGIN} @${TMPDIR}/dbid.sql         >
${TMPDIR}/DBID"
su - oracle -c "sqlplus -s ${ORACLE_LOGIN} @${TMPDIR}/init.sql"
BKUPDIR=`cat ${ENVDIR}/Backup_Location`


${CP} ${TMPDIR}/DBID ${ENVDIR}/DBID
${CP} ${ENVDIR}/DBID ${BKUPDIR}/DBID
${CP} ${TMPDIR}/INITORA ${ENVDIR}/INITORA
${CP} ${ENVDIR}/INITORA ${BKUPDIR}/INITORA
${CP} ${TMPDIR}/control01.ctl.bkup ${ENVDIR}/control01.ctl.bkup
```

```
${CP} ${ENVDIR}/control01.ctl.bkup ${BKUPDIR}/control01.ctl.bkup

${CP} /avaya/Avaya_IQ/services/env/Full_Database_Backup.currentcron
${BKUPDIR}/Full_Database_Backup
${CP} /avaya/Avaya_IQ/services/env/Incremental_Database_Backup.currentcron
${BKUPDIR}/Incremental_Database_Backup
${CP} /avaya/Avaya_IQ/services/env/Archive_Log_Backup.currentcron
${BKUPDIR}/Archive_Log_Backup
${CP} /avaya/Avaya_IQ/services/env/Detection_Monitor.currentcron
${BKUPDIR}/Detection_Monitor
   chmod 644 /etc/cron.d/Full_Database_Backup
   chmod 644 /etc/cron.d/Incremental_Database_Backup
   chmod 644 /etc/cron.d/Archive_Log_Backup
   chmod 644 /etc/cron.d/Detection_Monitor
   touch /etc/cron.d/Full_Database_Backup
   touch /etc/cron.d/Incremental_Database_Backup
   touch /etc/cron.d/Archive_Log_Backup
   touch /etc/cron.d/Detection_Monitor
   touch /etc/cron.d
   touch /etc/crontab


err="000"

uid=`id | cut -d '=' -f 2 | cut -d '(' -f 1`
if [ $uid -ne 0 ]; then
    echo "You must login as root to run database backup. Exiting..."
    err="001"
    log_action "You must login as root to run database backup.Exit."
    exit 1
fi

if [ $# -ne 0 -a $# -ne 1 -a $# -ne 2 -a $# -ne 3 -a $# -ne 4 ]; then
    echo "Invalid call to backup, (usage is $0 [-t db [-i 0|1] | log])"
    err="001"
    log_action "Invalid call to backup, (usage is $0 [-t db [-i 0|1] |
log]).Exit."
    clean_exit 1
fi

while getopts 'i:t:' option
do
    case $option in
    t)
        case $OPTARG in
        db)
            backupType=$OPTARG
        ;;
        log)
            keyword="Archive Log Backup"
            backupType=$OPTARG
        ;;
        *)
            echo "Invalid backup type given (must be db or log)."
            err="001"
```

```
            log_action "Invalid backup type given (must be db or log).Exit."
            clean_exit 1
        ;;
        esac
    ;;
    i)
        case $OPTARG in
        0)
       keyword="Full Backup"
            level=$OPTARG
        ;;
        1)
       keyword="Incremental Backup"
            level=$OPTARG
        ;;
        *)
            echo "Invalid incremental backup level value given (must be 0 or 1)"
            err="001"
            log_action "Invalid incremental backup level value given (must be 0 or
1).Exit."
            clean_exit 1
        ;;
        esac
    ;;
    \?)
        err="001"
        echo "Invalid backup call (must be $0 [-t db [-i 0|1] | log])."
        log_action "Invalid backup call (must be $0 [-t db [-i 0|1] | log]).Exit."
        clean_exit 1
    ;;
    esac
done

if [ -f $LOCKFILE ]; then
    ps -ef | grep rman | grep EOF > /dev/null 2>&1
    if [ $? -eq 0 ]; then
        echo "Backup is already running."
        err="001"
        log_action "Backup is already running.Exit."
        clean_exit 3
    fi
else
    touch $LOCKFILE
fi

if [ -z $backupType ]; then
    backupType="db"
fi

#skwest added filesperset 1 based on 11g restore recommendations
#skwest changed DELETE ALL INPUT to DELETE INPUT so it will only delete files in 1
location
if [ "$backupType" = "db" ]; then
    if [ $level -eq 0 ]; then
         trapID=18231
```

```
         keyword="Full Backup"
         log_action "Backup.Start."
         log_action "Performing a full database backup ($0 $ARG).dbBackup."
         bkup_cmd="BACKUP AS COMPRESSED BACKUPSET filesperset 4 DATABASE PLUS
ARCHIVELOG FILESPERSET 20"
     else
         trapID=18232
         keyword="Incremental Backup"
         log_action "Backup.Start."
         log_action "Performing an incremental level $level database backup ($0
$ARG).dbBackup."
         bkup_cmd="BACKUP AS COMPRESSED BACKUPSET INCREMENTAL LEVEL $level
filesperset 10 DATABASE PLUS ARCHIVELOG FILESPERSET 20"
     fi
fi

if [ "$backupType" = "log" ]; then
    trapID=18233
    keyword="Archive Log Backup"
    log_action "Backup.Start."
    log_action "Performing a backup of archive logs ($0 $ARG).logBackup."
    bkup_cmd="BACKUP AS COMPRESSED BACKUPSET archivelog all not backed up 1 times"
fi

IS_DataGuard=FALSE
PrimaryStandBy=FALSE
# Is Data Guard Installed?
if [ -f /avaya/Oracle/dataGuardInstalled.txt ]; then
   if [ -n "`grep Primary /avaya/Oracle/dataGuardInstalled.txt`" ]; then
       IS_DataGuard=TRUE
       PrimaryStandBy=Primary
   elif [ -n "`grep StandBy /avaya/Oracle/dataGuardInstalled.txt`" ]; then
       IS_DataGuard=TRUE
       PrimaryStandBy=StandBy
   fi
fi

echo -e "Check Data Guard just finished.\n"
echo -e "DataGuardInstalled:$IS_DataGuard"

err="000"
echo "Backup ($0) may take a while to finish."
echo -e "Please see ${VARLOGFILE} for progress.\n"

if [ ! -d $VARLOGDIR ]; then
    mkdir -p $VARLOGDIR
fi

${ECHO} "${db_backupDate}:${PGM}:${keyword}.Started."                          >>
${CUSTAUDITLOG}

# Some features are not available for Standard Edition One
# cannot allocate multiple channels
# parallelism require Enterprise Edition
# cannot enable block change tracking which improves incremental backup
```

```
#
# RMAN commands:
# BACKUP DATABASE PLUS ARCHIVELOG;
# BACKUP CURRENT CONTROLFILE;
# BACKUP INCREMENTAL LEVEL 1 CUMULATIVE DATABASE PLUS ARCHIVELOG;
# BACKUP INCREMENTAL LEVEL 1 DIFFERENTIAL DATABASE PLUS ARCHIVELOG;
# DELETE NOPROMPT BACKUP OF DATABASE COMPLETED BEFORE 'SYSDATE-7';
# CROSSCHECK BACKUP;
# CROSSCHECK ARCHIVELOG ALL;
# DELETE NOPROMPT OBSOLETE;
# DELETE NOPROMPT EXPIRED BACKUP;
# LIST BACKUP;
# LIST ARCHIVELOG ALL;
# DELETE ARCHIVELOG ALL COMPLETED BEFORE 'SYSDATE-5';
# DELETE ALL INPUT
#

if [ "$IS_DataGuard" == "FALSE" ] ; then
  # Configure Backup DB
  echo "Regular backup"
  # non-data guard can use delete input
  newbkup_cmd=$bkup_cmd" DELETE INPUT"
  su - oracle -c "
  rman target / << !EOF
  set echo on;
  RUN {
    CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 7 DAYS;
    CONFIGURE CONTROLFILE AUTOBACKUP ON;
    CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK CLEAR;
    CONFIGURE CHANNEL DEVICE TYPE DISK CLEAR;
    ALLOCATE CHANNEL ch1 TYPE DISK;
    CROSSCHECK ARCHIVELOG ALL;
    CROSSCHECK BACKUP;
    $newbkup_cmd;
    DELETE NOPROMPT OBSOLETE;
    DELETE NOPROMPT EXPIRED BACKUP;
    DELETE NOPROMPT EXPIRED ARCHIVELOG ALL;
    RELEASE CHANNEL ch1;
  }
  EXIT;
  !EOF" > ${TMPDIR}/${PGM}.log 2>&1
else
  #skwest DG backup
    echo "Data Guard backup"
    # password required for resync, oracle ORA-17628 [ID 1327156.1]
    su - oracle -c "
    rman target sys/${GLBL_PSWD} << !EOF
    connect catalog rmancat/${GLBL_PSWD}@avayaiqh
    set echo on;
    RUN
    {
      allocate channel d1 type disk;
      CROSSCHECK ARCHIVELOG ALL;
      CROSSCHECK BACKUP;
      $bkup_cmd;
```

```
      BACKUP (CURRENT CONTROLFILE);
      DELETE NOPROMPT OBSOLETE;
      DELETE NOPROMPT EXPIRED BACKUP;
      DELETE NOPROMPT EXPIRED ARCHIVELOG ALL;
      release channel d1;
    }
    RESYNC CATALOG FROM DB_UNIQUE_NAME ALL;
    EXIT;
    !EOF" > ${TMPDIR}/${PGM}.log 2>&1

    if [[ "$PrimaryStandBy" == "StandBy" && "$backupType" != "log" ]]; then
      # backup the recovery catalog database
      echo "starting recovery catalog backup, database is not in archivelog mode,
hot backup" ${TMPDIR}/${PGM}.log 2>&1
      ${RM} ${TMPDIR}/DBIDRecovery
      ${RM} ${TMPDIR}/INITORARecovery
      ${RM} ${TMPDIR}/control01.ctl.bkup.recovery

      su - oracle -c "
         ORACLE_SID=avayaiqh
         sqlplus / as sysdba << !EOF
           CREATE pfile='${TMPDIR}/INITORARecovery' FROM SPFILE;
           ALTER DATABASE BACKUP CONTROLFILE TO
'${TMPDIR}/control01.ctl.bkup.recovery';
           EXIT;
       !EOF" >> ${TMPDIR}/${PGM}.log 2>&1
       cat /avaya/Avaya_IQ/services/detect/REQSQLHEAD      >  /tmp/dbidR.sql
       echo "SELECT 'dbid:'||dbid FROM V\$DATABASE;"           >> /tmp/dbidR.sql
       echo "SELECT 'scn:'||current_scn from v\$database;"     >> /tmp/dbidR.sql
       echo "exit;"                                            >> /tmp/dbidR.sql
       su - oracle -c "sqlplus -s sys/${GLBL_PSWD}@avayaiqh as sysdba
@/tmp/dbidR.sql    > ${TMPDIR}/DBIDRecovery"

       cp -f ${TMPDIR}/DBIDRecovery ${ENVDIR}/DBIDRecovery
       cp -f ${TMPDIR}/INITORARecovery ${ENVDIR}/INITORARecovery
       cp -f ${TMPDIR}/control01.ctl.bkup.recovery
${ENVDIR}/control01.ctl.bkup.recovery
       cp -f ${TMPDIR}/DBIDRecovery ${BKUPDIR}/DBIDRecovery
       cp -f ${TMPDIR}/INITORARecovery ${BKUPDIR}/INITORARecovery
       cp -f ${TMPDIR}/control01.ctl.bkup.recovery
${BKUPDIR}/control01.ctl.bkup.recovery

      su - oracle -c "
      ORACLE_SID=avayaiqh
      rman target / << !EOF
      set echo on;
      RUN {
        shutdown immediate;
        startup nomount;
        alter database mount;
        CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 7 DAYS;
        CONFIGURE CONTROLFILE AUTOBACKUP ON;
        CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK CLEAR;
        CONFIGURE CHANNEL DEVICE TYPE DISK CLEAR;
        ALLOCATE CHANNEL ch1 TYPE DISK;
```

```
        CROSSCHECK BACKUP;
        BACKUP AS COMPRESSED BACKUPSET DATABASE;
        DELETE NOPROMPT OBSOLETE;
        DELETE NOPROMPT EXPIRED BACKUP;
        RELEASE CHANNEL ch1;
        alter database open;
      }
      EXIT;
      SET ORACLE_SID=avayaiq
      !EOF" >> ${TMPDIR}/${PGM}.log 2>&1
    fi
fi


# 00880534 - fix rman execution status determination
rman_ret=$?

cat  ${TMPDIR}/${PGM}.log >> ${LOGFILE}
cat  ${TMPDIR}/${PGM}.log >> ${VARLOGFILE}
${RM} ${TMPDIR}/${PGM}.log


if [ ${rman_ret} -eq 0 ]; then
    echo -e "$0 $ARG successfully finished.\n"
    log_action "Backup finished successfully.Exit.start time: $start_time"
    ${ECHO} "${db_backupDate}:${PGM}:${keyword}.Finished Successfully.Completed."
>> ${CUSTAUDITLOG}
    clean_exit 0
else
    err="001"
    echo -e "$0 $ARG did not successfully finished.\n"
    log_action "Backup did not finish successfully.Exit. $start_time"
    ${ECHO} "${db_backupDate}:${PGM}:${keyword}.Did Not Finish
Successfully.Completed." >> ${CUSTAUDITLOG}

    # backup failure may cause archived logs space full
    # cleanup archived logs otherwise oracle will not function
    rm -rf /u01/app/oracle/archivelog/*
    su - oracle -c "
        rman target / << !EOF
        RUN {
        CROSSCHECK ARCHIVELOG ALL;
        DELETE NOPROMPT EXPIRED ARCHIVELOG ALL;
        }
        EXIT;
    !EOF"

    clean_exit 1
fi
```

Procedure

1. Log on to the AASA host as root or a root-level user.

2. To activate the database backup, execute the following command:

   # sh /avaya/bin/config_db_backup.sh

   The "config_db_backup.sh" script will call the "db_backup.sh" script for setting up the backup.

3. When prompted, select an option to configure the database backup and perform the following:
   a) Enter the location of the backup file system (Mount Point).
   b) Select the start day of the week.
   c) Enter the time of day when you want the backups to run.
   d) Select OK.

4. After the backup has been executed for the first time, please check that:
   a) The following files should be created

      Archive_Log_Backup
      control01.ctl.bkup
      DBID
      Detection_Monitor
      Full_Database_Backup
      Incremental_Database_Backup
      INITORA

   b) The following directories should be created

      <nfs dir>/AVAYAIQ
      <nfs dir>/AVAYAIQ/autobackup
      <nfs dir>/AVAYAIQ/backupset

   c) Inside the above "autobackup" and "backupset" directories there will be other directories named with the respective timestamps and these directories will contain .bkp files inside.

Checking the Backup at Oracle RMAN

As soon as the above backup procedure is completed, the Oracle RMAN can be used to verify that the backup has been created successfully. Below you can find the steps required for connecting to RMAN and check the backup.

Procedure

1. Change current user to “oracle” user:

   # su - oracle

2. Start Oracle RMAN:

   # rman target /

3. Check the backup by giving this command on RMAN prompt:

   RMAN> LIST BACKUP;

Restoring the AASA Backup in regular operation

In order to the restore a backup like the one done in the previous chapter, please follow the steps listed in the procedure below.

Procedure

1. Change current user to oracle:

   # su - oracle

2. Start Oracle RMAN:

   # rman target /

3. On RMAN prompt, execute the following commands to restore the backup. This restoration process may take several minutes depending on the amount of data being restored.

   RMAN> SET ECHO ON;
   RMAN> STARTUP FORCE MOUNT;
   RMAN> RESTORE DATABASE;
   RMAN> RECOVER DATABASE;

RMAN> ALTER DATABASE OPEN;
RMAN> SHUTDOWN IMMEDIATE;
RMAN> STARTUP;
RMAN> EXIT;

AASA in Disaster Recovery

Performing the Backup

The AASA demands that, in a Disaster Recovery scenario, a regular backup is taken using Oracle Data Pump Export Utility. It is up to the customer to define how frequent the backup must be done so the Data Export can be set up accordingly.

Depending on the amount of Speech Analytics data that is stored in Oracle Database, it is recommended that backup is done at least on weekly basis.

The Data Pump Export Utility will be invoked by a "cron" job that will be executed according to the frequency defined by customer.

In order to configure the backup the following prerequisites needs to be satisfied so the backup can be properly exported.

Prerequisites

These are the required steps that need to be followed before taking any backup in the Disaster Recovery scenario. This procedure must be followed only once after the AASA server is reinstalled.

1. Change user to oracle:

   # su - oracle

2. Connect to Oracle´s SQLPLUS as "sysdba":

   # sqlplus / as sysdba

3. At SQL prompt, grant "exp_full_database" permission to the "avayadw" user:

   SQL> grant exp_full_database to avayadw;

4. Exit from SQLPLUS

   SQL> exit;

Procedure

The backup can be taken by executing the EXPDP command like in the example below:

 # expdp avayadw/AvayaIQ07@avayaiq DIRECTORY=DATA_PUMP_DIR COMPRESSION=all DUMPFILE=export-avayadw-compress.dmp LOGFILE=export-aasa-compress.log FULL=Y

Where:

- ”AvayaIQ07” refers to the password of the “avayadw” user at the Oracle Database and this value may be different depending on the password chosen for “avayadw” at the AASA installation.
- DUMPFILE is the name of the backup file.
- DATA_PUMP_DIR is the directory where the backup file will be saved to. By default it is the “/u01/app/oracle/admin/avayaiq/dpdump/” folder.
- LOGFILE is the name of log file generated during the execution of the “expdp” command. This log is created in the “/u01/app/oracle/admin/avayaiq/dpdump/” folder.
- COMPRESSION determines that that the backup file should be compressed so some space is saved during the backup.
- FULL indicates that this is a complete backup

Once the backup file is created, it must be copied to an NFS directory so the backup is saved in an external server, other than the AASA server. Since this is a backup for a Disaster Recovery situation, it is desirable that the backup file is stored in another server where it can be restored from.

The “expdp” command should be executed through the following “AASA_backup.sh” script that will be executed by a cron job in a frequency that should be determined by the customer needs.

AASA_backup.sh Script

This script creates the backup file using the “expdp” Oracle utility and once the backups are created, they are moved to an NFS folder. It also deletes the backups and its respective logs that are older than 7 days. This cleanup procedure can be changed to adjust to costumer´s needs by changing the parameter “mtime” in the script.

```
#!/bin/bash
################################################################################
# Copyright (c) 2008, Avaya. All rights reserved.
#
# NAME:  AASA_backup.sh
#
# DESCRIPTION:
#  Perform backup of AASA data
#  This Script uses the Oracle Data Pump Export Utility to generate a dump file
```

```
#  containing data from all the tables used by AASA. This dump file can be used in
#  AASA data recovery when required.
#
#  This script creates a dump file at the default directory
u01/app/oracle/admin/avayaiq/dpdump/
#  and once the dump is created, it is moved to another folder which preferably
#  should be a NFS folder.
#
# INSTALLED:
#   /avaya/Oracle/AASA_backup.sh
#
# USAGE:
#   This script preferably should be executed by a cron job, so it can run at
#   a frequency determined by the customer. Like in the crontab example below
where
#  the backup is taken at 1:59 AM every Sunday:
#
#        59 1 * * 0 /bin/sh /avaya/Oracle/AASA_backup.sh
#
#  This script can also be executed manually by running the following command
#        sh /avaya/Oracle/AASA_backup.sh
#
################################################################################


ORACLE_HOME="/u01/app/oracle/product/11.2.0/db_1"
dump_file="/u01/app/oracle/admin/avayaiq/dpdump/export-aasa-*.dmp"
dump_log="/u01/app/oracle/admin/avayaiq/dpdump/export-aasa-*.log"
nfs_directory="/tmp/nfs_backup"

if [ "${PGM}" = "" ]
then
   PGM=i
   VARLOGDIR=/var/log/Avaya/CCR/backup
   VARLOGFILE=/var/log/Avaya/CCR/backup/${PGM}.log
fi

if [ ! -d /var/log/Avaya ]; then
   mkdir -p /var/log/Avaya > /dev/null 2>&1
   chmod 766 /var/log/Avaya
fi

if [ ! -d /var/log/Avaya/CCR ]; then
   mkdir -p /var/log/Avaya/CCR > /dev/null 2>&1
   chmod 766 /var/log/Avaya/CCR
fi

if [ ! -d /var/log/Avaya/CCR/backup ]; then
   mkdir -p /var/log/Avaya/CCR/backup > /dev/null 2>&1
   chmod 766 /var/log/Avaya/CCR/backup
fi

if [ ! -d $VARLOGDIR ]; then
   mkdir -p $VARLOGDIR > /dev/null 2>&1
   chmod 766 $VARLOGDIR
```

```
fi


log_action()
{
   echo -e "`date "+%F %T %Z"`: ${1}" >>${VARLOGFILE}
   if [ $? -ne 0 ]; then
      echo "Line ${LINENO}: Cannot write to ${VARLOGFILE}" >> ${VARLOGFILE}
   fi
}

echo "AASA Backup Script Starting"
log_action "AASA Backup Script Starting"

# If a NFS directory does not exist yet, create it.
if [ ! -d "$nfs_directory" ]; then
   echo "Creating the $nfs_directory that will store the dump file."
   log_action "Creating the $nfs_directory that will store the dump file."
   mkdir $nfs_directory
fi

# Taking the Backup using Oracle expdp
echo "Executing the AASA expdp backup command."
log_action "Executing the expdp backup command."

su - oracle -c "$ORACLE_HOME/bin/expdp avayadw/AvayaIQ07@avayaiq
DIRECTORY=DATA_PUMP_DIR COMPRESSION=all DUMPFILE=export-aasa-$(date
+%Y%m%d%H%M).dmp LOGFILE=export-aasa-$(date +%Y%m%d%H%M).log FULL=Y"

# Moving dump files
echo "Moving dump files to $nfs_directory"
log_action "Moving dump files to $nfs_directory"
mv -u $dump_file $nfs_directory

# Moving log files
echo "Moving dump log files to $nfs_directory"
log_action "Moving dump log files to $nfs_directory"
mv -u $dump_log $nfs_directory

# Granting Permission to dump files
chmod -R 775 $dump_file

# Removing 7 days old dump files
echo "Deleting old dump and log files from the $nfs_directory directory"
log_action "Deleting old dump and log files from the $nfs_directory directory"
find $nfs_directory/export-aasa* -mtime +6 -exec rm {} \;

# Backup Script Finished
echo "AASA Backup Completed."
log_action "AASA Backup Completed.\n"
```

Configuring the cron job for the AASA backup

1. Log on to the AASA host as root.

2. Copy the "AASA_backup.sh" to the "/avaya/Oracle" folder.

3. Add the "execute" attribute to the "AASA_backup.sh" script.

 # chmod +x /avaya/Oracle/AASA_backup.sh

4. Open the crontab for edition:

 # crontab -e

5. Add the following entry to the crontab:

**** * * * * /bin/sh /avaya/Oracle/AASA_backup.sh***

And set the cron execution frequency following the table below:

```
# The first five crontab fields are integer patterns that specify the following:
#     minute (0-59),
#     hour (0-23),
#     day of the month (1-31),
#     month of the year (1-12),
#     day of the week (0-6 with 0=Sunday).
```

Verifying the backup execution

After the backup script is executed according to the time scheduled in the cron table, the log files can be checked to validate that the backup was taken properly. There are the 2 main logs where the backup execution can be checked:

1. The "export-aasa-<timestamp>.log" that is the log file that contain the output of the "expdp" backup command. This file is created initially at the "/u01/app/oracle/admin/avayaiq/dpdump" folder and then it is moved to an NFS folder (that needs to be configured in the script) by the "AASA_backup.sh" script.

2. The "AASA_backup.log" that is the log file that contains the output of all the commands executed in the "AASA_backup.sh" script. This file is created at the "/var/log/Avaya/CCR/backup" folder.

Performing the Restore of the Backup

In order to have the AASA backup restored in a new AASA installation the following procedure must be followed:

Procedure

1. Log on to the AASA host as root or a root-level user.

2. Copy the backup file to the "/u01/app/oracle/admin/avayaiq/dpdump/" folder. This is the .dmp file that was generated after running the above backup procedure.

   # cp export-aasa-<timestamp>.dmp /u01/app/oracle/admin/avayaiq/dpdump/

3. Change the file permissions of the backup file:

   # chmod 775 /u01/app/oracle/admin/avayaiq/dpdump/export-aasa-<timestamp>.dmp

4. Change current user to “oracle” user:

   # su - oracle

5. Connect to Oracle´s SQLPLUS as “sysdba”:

   # sqlplus / as sysdba

6. Grant “create directory” permission to “avayadw” user:

   SQL> grant create any directory to avayadw;

7. Exit from SQLPLUS prompt:

   SQL> exit;

8. Restore the backup by running the following command. Please note that the DUMPFILE parameter must match the file name that has been copied to the "/u01/app/oracle/admin/avayaiq/dpdump/" folder.

   # impdp avayadw/AvayaIQ07@avayaiq DIRECTORY=DATA_PUMP_DIR DUMPFILE=export-aasa-<timestamp>.dmp LOGFILE=import_aasa_dump.log

TABLE_EXISTS_ACTION=REPLACE DATA_OPTIONS=SKIP_CONSTRAINT_ERRORS TABLES=STGETLAPPLPARAMETER,STGETLBATCH,STGETLCONNPARAMETER,STGETLCONNECTION,STGETLJOB,STGETLJOBRUN,STGETLMESSAGELOG,STGETLPROCESS,STGETLSOURCEAPPLICATION,DW_ACCOUNT,DW_AGENT,DW_CLASSIFICATION,DW_CONTACTDIRECTION,DW_DEVICEGROUP,DW_DIMDATE,DW_DIMDURATION,DW_DIMINTERVAL,DW_EXITREASON,DW_PROCESS,DW_QUEUE,DW_ROUTINGPOINT,DW_SOURCE,DM_SOURCE,DM_TENANTGROUP,DM_DIMTENANT,DM_CLASSIFICATION,DM_CONTACTDIRECTION,DM_DEVICEGROUP,DM_DIMAGENT,DM_DIMACCOUNT,DM_DIMAGENTGROUP,DM_DIMAGENTGROUPBRIDGE,DM_DIMAGENTTENANTBRIDGE,DM_DIMDATE,DM_DIMDURATION,DM_DIMINTERVAL,DM_DIMQUEUEGROUP,DM_QUEUE,DM_DIMQUEUEGROUPBRIDGE,DM_DIMROUTINGPOINTGROUP,DM_ROUTINGPOINT,DM_DIMROUTINGPOINTGROUPBRIDGE,DM_EXITREASON,DM_PROCESS,CFG_AASA_DBCHANGELOGLOCK,CFG_AASA_DBCHANGELOG,DM_AU_FCTROOTCAUSE,DM_AU_FCTUPLOAD,CFG_AU_TABLELIST,CFG_AASA_SCHEDULE,ETLJOBMSG_T,DM_AU_DIMDATE,DM_AU_DIMTIME,DM_AU_DIMAGENT,DM_AU_DIMBUSINESSIMPACT,DM_AU_DIMCOMPONENT,DM_AU_DIMDRIVER,DM_AU_DIMFEEDBACKCLASS,DM_AU_DIMFEEDBACKITEM,DM_AU_DIMNONMINEABLE,DM_AU_DIMOUTCOMECLASS,DM_AU_DIMOUTCOME,DM_AU_DIMPROFILE,DM_AU_DIMROOTCAUSECLASS,DM_AU_DIMROOTCAUSEREASON,DM_AU_DIMTEAM,DM_AU_DIMTIMEMEASURE,DM_AU_DIMPROFILETOCOMPONENT,DM_AU_DIMDATASET,DM_AU_DIMDIRECTION,STG_AU_TMPFCALLHANDLINGTIME,STG_AU_TMPFCALL,STG_AU_TMPFFEEDBACK,STG_AU_TMPFROOTCAUSE,STG_AU_TMPDAGENT,STG_AU_TMPDBUSINESSIMPACT,STG_AU_TMPDCOMPONENT,STG_AU_TMPDDRIVER,STG_AU_TMPDFEEDBACKCLASS,STG_AU_TMPDFEEDBACKITEM,STG_AU_TMPDNONMINEABLE,STG_AU_TMPDOUTCOMECLASS,STG_AU_TMPDOUTCOME,STG_AU_TMPDPROFILE,STG_AU_TMPDROOTCAUSECLASS,STG_AU_TMPDROOTCAUSEREASON,STG_AU_TMPDTEAM,STG_AU_TMPDTIMEMEASURE,STG_AU_TMPDDATASET,STG_AU_TMPFCALLPROFILE,STG_AU_TMPFCOMPONENT,DM_AU_FCTCALL,DM_AU_FCTCOMPONENT,DM_AU_FCTFEEDBACK,DM_AU_FCTCALLHANDLINGTIME;

Where:

- ”AvayaIQ07” refers to the password of the “avayadw” user at the Oracle Database and this value may be different depending on the password chosen for “avayadw” at the AASA installation.
- DUMPFILE is the name of the backup file.
- DATA_PUMP_DIR is the directory where the backup file will be saved to. By default it is the “/u01/app/oracle/admin/avayaiq/dpdump/” folder.
- LOGFILE is the log file that will be created for the backup restoring. In the command above the log file is called “import_aasa_dump.log” and it is always created at “/u01/app/oracle/admin/avayaiq/dpdump/” folder in the execution of the impdp command.

- TABLES is the reference to all the tables used by the Speech Analytics application

9. Check the “impdp” command output or the “import_aasa_dump.log” to verify that the data has been properly restored in the AASA tables. The following output is an example of a successful data restoring. The error message highlighted below is normal for this kind of procedure and it can be ignored.

```
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/TABLE
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/TABLE_DATA
. . imported "AVAYADW"."DM_DIMDATE"                      715.6 KB   25933 rows
. . imported "AVAYADW"."DW_DIMDATE"                      715.6 KB   25933 rows
. . imported "AVAYADW"."DM_DIMDURATION"                  80.39 KB   10191 rows
. . imported "AVAYADW"."DM_DIMINTERVAL"                  6.070 KB      97 rows
. . imported "AVAYADW"."DM_DIMTENANT"                    5.375 KB       1 rows
:
:
. . imported "AVAYADW"."STGETLBATCH"                         0 KB       0 rows
. . imported "AVAYADW"."STGETLCONNECTION"                    0 KB       0 rows
. . imported "AVAYADW"."STGETLCONNPARAMETER"                 0 KB       0 rows
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/INDEX/INDEX
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/CONSTRAINT/CONSTRAINT
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/INDEX/STATISTICS/INDEX_STATISTICS
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/CONSTRAINT/REF_CONSTRAINT
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/STATISTICS/TABLE_STATISTICS
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/TRIGGER
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/POST_INSTANCE/PROCACT_INSTANCE
ORA-39083: Object type PROCACT_INSTANCE failed to create with error:
ORA-00942: table or view does not exist
Failing sql is:
BEGIN
SYS.DBMS_AQ_IMP_INTERNAL.IMPORT_QUEUE_TABLE('ETLJOBMSG_T',1,25192573,2,0,0,'',
SYS.DBMS_AQ_IMP_INTERNAL.DBVER_10i, '00:00');COMMIT; END;
Processing object type DATABASE_EXPORT/SCHEMA/TABLE/POST_INSTANCE/PROCDEPOBJ
Job "AVAYADW"."SYS_IMPORT_TABLE_01" completed with 1 error(s) at 07:02:58
```