POC document

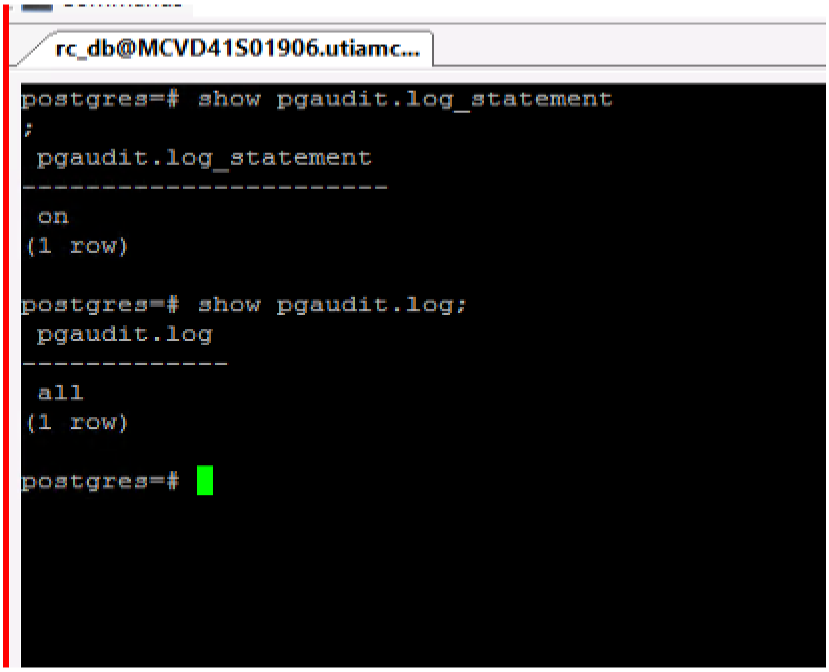
Configuring Audit in Postgres database

Prepared by: NTT DBA Team

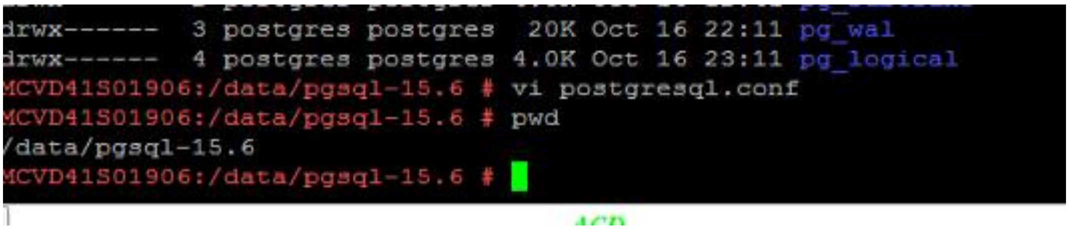
Date: 17 Oct 2024

Log path location:-

1. **Audit log loaction:- /data/pgsql-15.6/log**

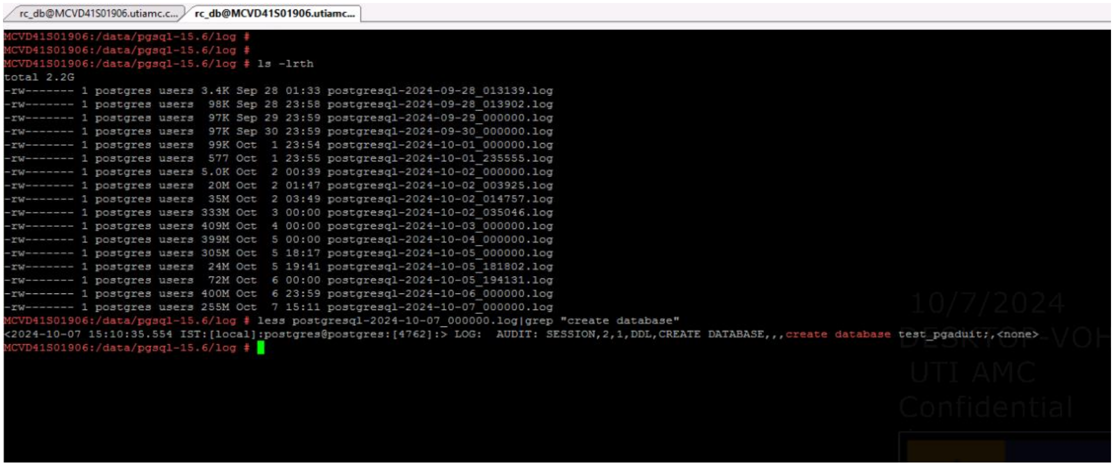


```
postgres=# show pgaudit.log_statement
;
 pgaudit.log_statement
-----------------------
 on
(1 row)

postgres=# show pgaudit.log;
 pgaudit.log
-------------
 all
(1 row)

postgres=#
```



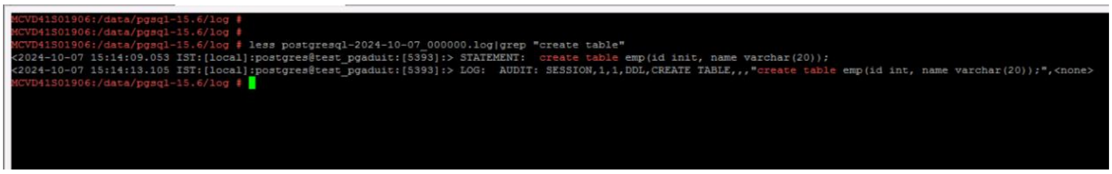
```
drwx------  3 postgres postgres  20K Oct 16 22:11 pg_wal
drwx------  4 postgres postgres 4.0K Oct 16 23:11 pg_logical
MCVD41S01906:/data/pgsql-15.6 # vi postgresql.conf
MCVD41S01906:/data/pgsql-15.6 # pwd
/data/pgsql-15.6
MCVD41S01906:/data/pgsql-15.6 #
```

2. **Create database:-**



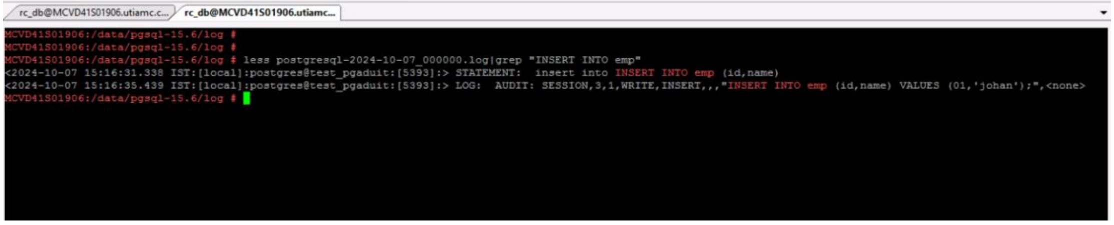
```
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log # ls -lrth
total 2.2G
-rw------- 1 postgres users 3.4K Sep 28 01:33 postgresql-2024-09-28_013139.log
-rw------- 1 postgres users  98K Sep 28 23:58 postgresql-2024-09-28_013902.log
-rw------- 1 postgres users  97K Sep 29 23:59 postgresql-2024-09-29_000000.log
-rw------- 1 postgres users  97K Sep 30 23:59 postgresql-2024-09-30_000000.log
-rw------- 1 postgres users  99K Oct  1 23:54 postgresql-2024-10-01_000000.log
-rw------- 1 postgres users  577 Oct  1 23:55 postgresql-2024-10-01_235555.log
-rw------- 1 postgres users 5.0K Oct  2 00:39 postgresql-2024-10-02_000000.log
-rw------- 1 postgres users  20M Oct  2 01:47 postgresql-2024-10-02_003925.log
-rw------- 1 postgres users  35M Oct  2 03:49 postgresql-2024-10-02_014757.log
-rw------- 1 postgres users 333M Oct  3 00:00 postgresql-2024-10-02_035046.log
-rw------- 1 postgres users 409M Oct  4 00:00 postgresql-2024-10-03_000000.log
-rw------- 1 postgres users 399M Oct  5 00:00 postgresql-2024-10-04_000000.log
-rw------- 1 postgres users 305M Oct  5 18:17 postgresql-2024-10-05_000000.log
-rw------- 1 postgres users  24M Oct  5 19:41 postgresql-2024-10-05_181802.log
-rw------- 1 postgres users  72M Oct  6 00:00 postgresql-2024-10-05_194131.log
-rw------- 1 postgres users 400M Oct  6 23:59 postgresql-2024-10-06_000000.log
-rw------- 1 postgres users 255M Oct  7 15:11 postgresql-2024-10-07_000000.log
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "create database"
<2024-10-07 15:10:35.554 IST:[local]:postgres@postgres:[4762]:> LOG:  AUDIT: SESSION,2,1,DDL,CREATE DATABASE,,,create database test_pgaduit;,<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

3. Create table:-



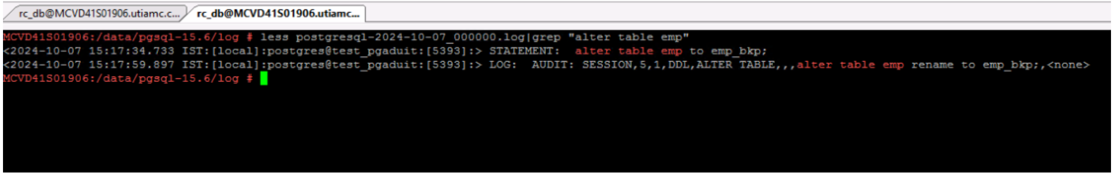
```
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "create table"
<2024-10-07 15:14:09.053 IST:[local]:postgres@test_pgaduit:[5393]:> STATEMENT:  create table emp(id init, name varchar(20));
<2024-10-07 15:14:13.105 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,1,1,DDL,CREATE TABLE,,,"create table emp(id int, name varchar(20));",<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

4. Insert :-



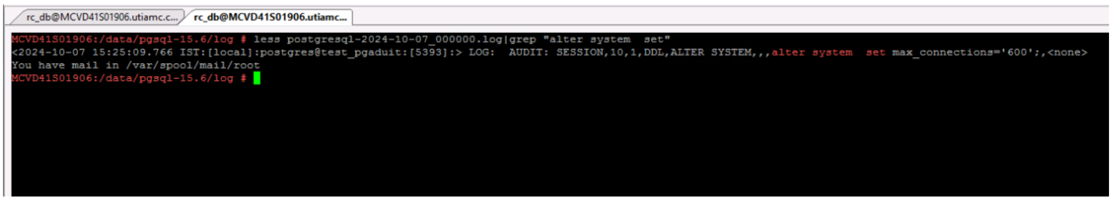
```
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "INSERT INTO emp"
<2024-10-07 15:16:31.338 IST:[local]:postgres@test_pgaduit:[5393]:> STATEMENT:  insert into INSERT INTO emp (id,name)
<2024-10-07 15:16:35.439 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,3,1,WRITE,INSERT,,,"INSERT INTO emp (id,name) VALUES (01,'johan');",<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

5. Alter table:-



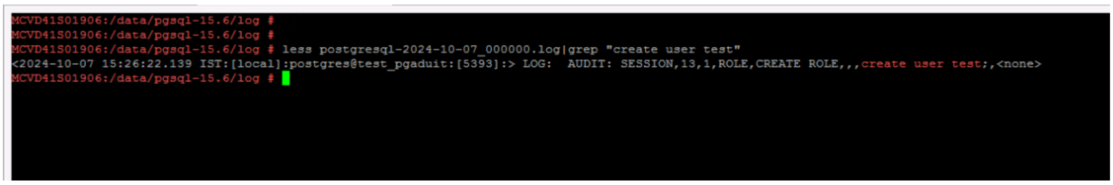
```
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "alter table emp"
<2024-10-07 15:17:34.733 IST:[local]:postgres@test_pgaduit:[5393]:> STATEMENT:  alter table emp to emp_bkp;
<2024-10-07 15:17:59.897 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,5,1,DDL,ALTER TABLE,,,alter table emp rename to emp_bkp;,<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

6. Change of parameter(like max_connection):-



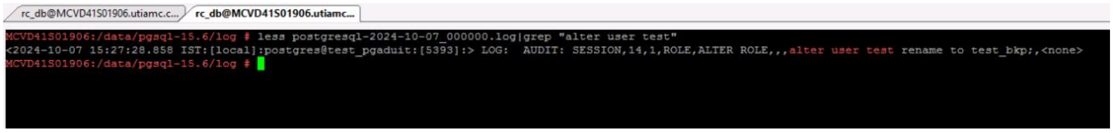
```
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "alter system  set"
<2024-10-07 15:25:09.766 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,10,1,DDL,ALTER SYSTEM,,,alter system  set max_connections='600';,<none>
You have mail in /var/spool/mail/root
MCVD41S01906:/data/pgsql-15.6/log #
```

7. Create user:-



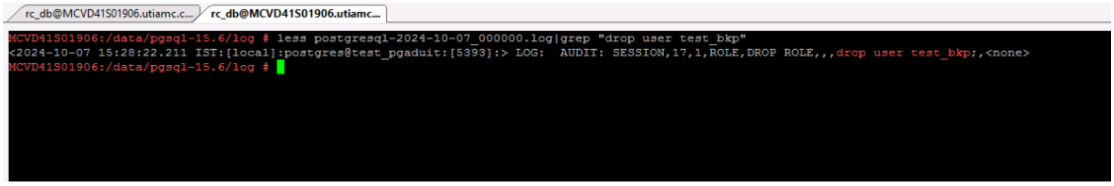
```
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log #
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "create user test"
<2024-10-07 15:26:22.139 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,13,1,ROLE,CREATE ROLE,,,create user test;,<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

8. Alter user:-



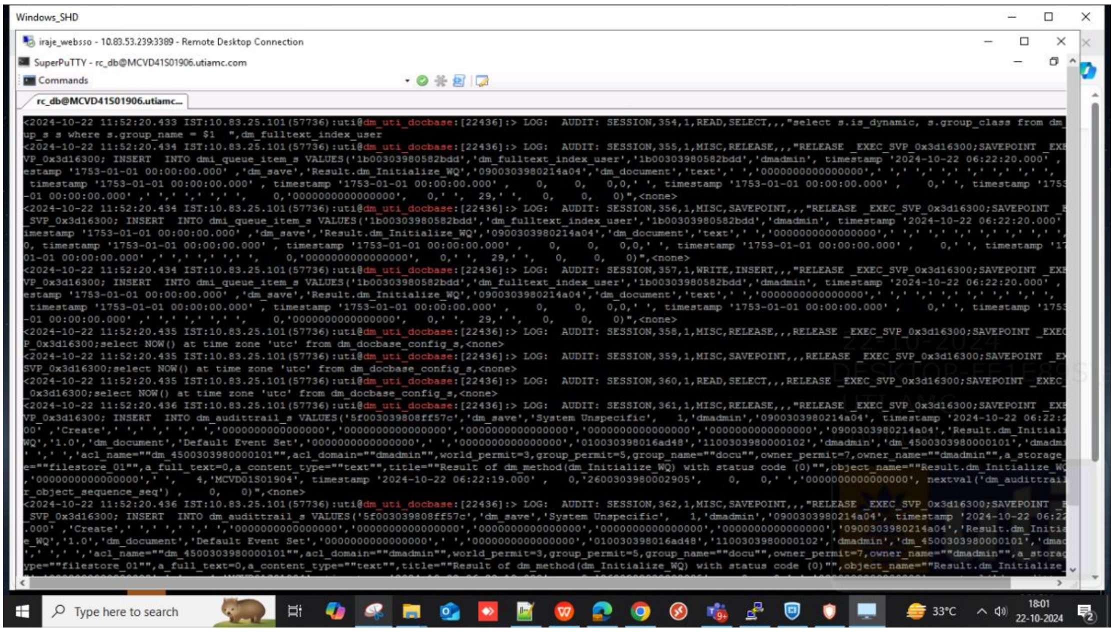
```
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "alter user test"
<2024-10-07 15:27:28.858 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,14,1,ROLE,ALTER ROLE,,,alter user test rename to test_bkp;,<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

9. Drop user:-



```
MCVD41S01906:/data/pgsql-15.6/log # less postgresql-2024-10-07_000000.log|grep "drop user test_bkp"
<2024-10-07 15:28:22.211 IST:[local]:postgres@test_pgaduit:[5393]:> LOG:  AUDIT: SESSION,17,1,ROLE,DROP ROLE,,,drop user test_bkp;,<none>
MCVD41S01906:/data/pgsql-15.6/log #
```

10. Sample Audit log from DMS UAT Database:



Windows_SHD
iraje_websso - 10.83.53.239:3389 - Remote Desktop Connection
SuperPuTTY - rc_db@MCVD41S01906.utiamc.com
Commands
rc_db@MCVD41S01906.utiamc...
Type here to search
33°C
18:01
22-10-2024

```
<2024-10-22 11:52:20.433 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,354,1,READ,SELECT,,,"select s.is_dynamic, s.group_class from dm_
up_s s where s.group_name = $1  ",dm_fulltext_index_user
<2024-10-22 11:52:20.434 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,355,1,MISC,RELEASE,,,"RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _EXE
VP_0x3d16300; INSERT  INTO dmi_queue_item_s VALUES('1b00303980582bdd','dm_fulltext_index_user','1b00303980582bdd','dmadmin', timestamp '2024-10-22 06:22:20.000' ,
estamp '1753-01-01 00:00:00.000' ,'dm_save','Result.dm_Initialize_WQ','0900303980214a04','dm_document','text',' ','0000000000000000',' ',' ',' ',' ',' ',' ',
 timestamp '1753-01-01 00:00:00.000' , timestamp '1753-01-01 00:00:00.000' ,    0,    0,   0,0,' ', timestamp '1753-01-01 00:00:00.000' ,    0,' ', timestamp '1753
-01 00:00:00.000' ,' ',' ',' ',' ',    0,'0000000000000000',   0,' ',  29,' ',   0,    0,   0)",<none>
<2024-10-22 11:52:20.434 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,356,1,MISC,SAVEPOINT,,,"RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _E
_SVP_0x3d16300; INSERT  INTO dmi_queue_item_s VALUES('1b00303980582bdd','dm_fulltext_index_user','1b00303980582bdd','dmadmin', timestamp '2024-10-22 06:22:20.000'
imestamp '1753-01-01 00:00:00.000' ,'dm_save','Result.dm_Initialize_WQ','0900303980214a04','dm_document','text',' ','0000000000000000',' ',' ',' ',' ',' ',' ',
0, timestamp '1753-01-01 00:00:00.000' , timestamp '1753-01-01 00:00:00.000' ,    0,    0,   0,0,' ', timestamp '1753-01-01 00:00:00.000' ,    0,' ', timestamp '17
01-01 00:00:00.000' ,' ',' ',' ',' ',    0,'0000000000000000',   0,' ',  29,' ',   0,    0,   0)",<none>
<2024-10-22 11:52:20.434 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,357,1,WRITE,INSERT,,,"RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _EXE
VP_0x3d16300; INSERT  INTO dmi_queue_item_s VALUES('1b00303980582bdd','dm_fulltext_index_user','1b00303980582bdd','dmadmin', timestamp '2024-10-22 06:22:20.000' ,
estamp '1753-01-01 00:00:00.000' ,'dm_save','Result.dm_Initialize_WQ','0900303980214a04','dm_document','text',' ','0000000000000000',' ',' ',' ',' ',' ',' ',
 timestamp '1753-01-01 00:00:00.000' , timestamp '1753-01-01 00:00:00.000' ,    0,    0,   0,0,' ', timestamp '1753-01-01 00:00:00.000' ,    0,' ', timestamp '1753
-01 00:00:00.000' ,' ',' ',' ',' ',    0,'0000000000000000',   0,' ',  29,' ',   0,    0,   0)",<none>
<2024-10-22 11:52:20.435 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,358,1,MISC,RELEASE,,,RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _EXEC
P_0x3d16300;select NOW() at time zone 'utc' from dm_docbase_config_s,<none>
<2024-10-22 11:52:20.435 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,359,1,MISC,SAVEPOINT,,,RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _EX
SVP_0x3d16300;select NOW() at time zone 'utc' from dm_docbase_config_s,<none>
<2024-10-22 11:52:20.435 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,360,1,READ,SELECT,,,RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _EXEC_
_0x3d16300;select NOW() at time zone 'utc' from dm_docbase_config_s,<none>
<2024-10-22 11:52:20.436 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,361,1,MISC,RELEASE,,,"RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _EXE
VP_0x3d16300; INSERT  INTO dm_audittrail_s VALUES('5f003039808ff57c','dm_save','System Unspecific',   1,'dmadmin','0900303980214a04', timestamp '2024-10-22 06:22:2
00' ,'Create',' ',' ',' ',' ','0000000000000000','0000000000000000','0000000000000000','0000000000000000','0000000000000000','0900303980214a04','Result.dm_Initiali
WQ','1.0','dm_document','Default Event Set','0000000000000000',' ','0000000000000000','010030398016ad48','1100303980000102','dmadmin','dm_450030398000010l','dmadmi
' ',' ','acl_name=""dm_4500303980000101"",acl_domain=""dmadmin"",world_permit=3,group_permit=5,group_name=""docu"",owner_permit=7,owner_name=""dmadmin"",a_storage_
e=""filestore_01"",a_full_text=0,a_content_type=""text"",title=""Result of dm_method(dm_Initialize_WQ) with status code (0)"",object_name=""Result.dm_Initialize_WQ
,'0000000000000000',' ',   4,'MCVD01S01904', timestamp '2024-10-22 06:22:19.000' ,   0,'2600303980002905',    0,    0,' ','0000000000000000', nextval('dm_audittrail
r_object_sequence_seq') ,    0,    0)",<none>
<2024-10-22 11:52:20.436 IST:10.83.25.101(57736):uti@dm_uti_docbase:[22436]:> LOG:  AUDIT: SESSION,362,1,MISC,SAVEPOINT,,,"RELEASE _EXEC_SVP_0x3d16300;SAVEPOINT _E
_SVP_0x3d16300; INSERT  INTO dm_audittrail_s VALUES('5f003039808ff57c','dm_save','System Unspecific',   1,'dmadmin','0900303980214a04', timestamp '2024-10-22 06:22
.000' ,'Create',' ',' ',' ',' ','0000000000000000','0000000000000000','0000000000000000','0000000000000000','0000000000000000','0900303980214a04','Result.dm_Initia
e_WQ','1.0','dm_document','Default Event Set','0000000000000000',' ','0000000000000000','010030398016ad48','1100303980000102','dmadmin','dm_4500303980000101','dmad
',' ',' ','acl_name=""dm_4500303980000101"",acl_domain=""dmadmin"",world_permit=3,group_permit=5,group_name=""docu"",owner_permit=7,owner_name=""dmadmin"",a_storag
ype=""filestore_01"",a_full_text=0,a_content_type=""text"",title=""Result of dm_method(dm_Initialize_WQ) with status code (0)"",object_name=""Result.dm_Initialize_
```