

Oracle FMW SOA 11g R1: Using
Secure Files

*Oracle Maximum Availability Architecture White Paper
September 2012*

Maximum Availability Architecture

Oracle Best Practices For High Availability

ORACLE

Introduction 2

Secure Files features and their effect for Oracle FMW SOA Systems 2

Recommended Settings for SecureFiles in Oracle FMW SOA schemas 6

 Compression 6

 Deduplication..... 6

 Encryption 7

 Partitioning 7

 Adjusting PCTFREE 8

How to enable SecureFiles for the Oracle FMW SOA Schemas 8

 Requirements for using SecureFiles 8

 Changing the Oracle FMW SOA Schemas 9

Appendix A: Oracle FMW SOA EDG System used for the tests20

 Areas of comparison for the different settings.....21

 Empirical Method used for the analysis21

Appendix B: Metrics and Data from the tests performed.....23

 Comparison for COMPRESSION23

 Comparison for DEDUPLICATION23

 Comparison for ENCRYPTION.....24

 Comparison for PARTITIONED LOBS.....24

Appendix C: LOBs in the SOAINFRA schema.....25

References.....29

Introduction

Oracle Fusion Middleware Service Oriented Architecture (SOA) Suite is a database intensive middleware system with multiple components that store many different types of data in the Database. During a single invocation of a composite, multiple inserts and updates of unstructured data like documents, messages, faults and payloads may take place. The amount of data in the Oracle SOA Suite database grows very quickly and this rapid growth is especially relevant for such unstructured data as it may affect not only the manageability of the database, but also its performance. Audit Trails, Business Decision Rules, Sensors, EDN and multiple other objects in the Oracle FW SOA Schemas make intensive use of unstructured data in lobs, clobs and blobs. SecureFiles is a feature introduced in Oracle Database 11g that is specifically engineered to deliver high performance for this type of unstructured data. SecureFiles is designed as a superset of the ANSI standard for large objects (LOBs) which offers easy migration from old LOBs or BasicFiles and provides a new architecture that delivers substantially improved performance along with optimized storage for unstructured data inside the Oracle Database. This document provides some generic guidelines and examples for using Oracle FMW SOA with SecureFiles for the most common and relevant LOBs in the Oracle FMW SOA Infrastructure schemas (also referred to as “SOAINFRA schemas” in this paper). These guidelines are derived from a wide spectrum of performance and administration tests and are intended to provide a solution framework that will have different applicability depending on the type of Oracle FMW SOA system (i.e. the type of composites and payloads), the size of the Oracle FMW SOA Database and the type of usage/load it needs to sustain.

Secure Files features and their effect for Oracle FMW SOA Systems

Oracle Secure files, introduces many enhancements for improved performance, efficient storage and easier manageability. These are the most relevant ones in context of Oracle FMW SOA Suite:

Write-Gather Cache (WGC)

SecureFiles uses a new cache that buffers data typically up to 4MB during write operations before flushing or committing to the underlying storage layer. This buffering of in-flight data allows for large contiguous space allocation and large disk I/O and adapts very well to the common payloads and documents sizes used in Oracle FMW SOA Systems. Write performance is greatly improved due to reduced disk seek costs and for Oracle FMW SOA System this is perceived in improved average IO rates for the DB

Space Management

Space management for SecureFiles is optimized for unstructured data inside the Oracle Database. An intelligent space manager provides fast allocation of large, contiguous disk blocks and efficient deletion by automatically reclaiming freed space. Space is also pre-allocated based on heuristics of recent demand which ensures no stalling and, consequently, low impact on foreground performance. This is critical in Oracle FMW SOA systems that enable audit trail and business process that deal with large documents/payloads since both generate large-sized unstructured data. This effect, however, is very dependent on the type of instances (long vs. short living) on the data retention policies as well as on the type of documents that these instances deal with. SecureFiles segments require tablespaces managed with automatic segment space management (ASSM) (see the requirements section below)

Reduced Fragmentation

SecureFiles use a dynamic CHUNK (one or more Oracle blocks) size setting to maximize contiguous allocations on disk thus reducing fragmentation. This is important for Oracle FMW SOA Systems that deal with varying message sizes and payloads and have been modified not to use “in row” storage, however by default most of the Oracle FMW SOA LOBs are stored inline, hence this benefit is reduced just to a few segments with the default SOA schema structure.

No LOB Index Contention

SecureFiles do not use the LOB index to manage the inodes, which are data structures that map the logical offsets to the physical disk blocks. Instead, they use “private” meta-data blocks that are co-located with the data blocks in the LOB segment. This design reduces considerably LOB index contention waits which is a very common cause of performance degradation in Oracle FMW SOA Suite systems.

No High water mark contention

High Water mark contention (“enq: HW – contention” wait events in AWR reports) is present in practically every Oracle FMW SOA system using Mediator and BPEL composites (both Mediator Payloads and CUBE_SCOPE data are stored as LOBS). With SecureFiles, reclamation of space is done in the background and all the space belonging to a freed SecureFiles is reclaimed at once. This reduces the high water mark contention during space reclaims that typically affects those SOA Systems that use the default settings for LOB’s storage.

Easier Manageability

SecureFiles implement intelligent space and memory management algorithms and consequently require lesser

number of user-tuned parameters. Specifically, FREEPOOLS, FREELISTS, FREELIST GROUPS & PCTVERSION no longer need to be specified and are ignored for SecureFiles. Given all the different LOBs that are present in the SOA schemas, this reduces dramatically the number of DBA tuning adjustments.

Besides the above the following “configurable” features are available with SecureFiles that are especially relevant in Oracle FMW SOA Systems:

De-duplication

SecureFiles store only one copy of identical secure file data. This is very important for SOA systems since the same document-payload may be used in multiple composite instances thus generating unnecessary read and write overhead. Deduplication simplifies storage management and also results in significantly better performance, especially for copy operations.

Compression

SecureFiles automatically detects if data is compressible and compresses it using industry standard compression algorithms. Compression not only saves storage but also improves performance by reducing I/O, buffer cache requirements, redo generation and encryption overhead. Given the high data growth rates typically experienced in Oracle FMW SOA Databases, this can be key aspect for advising SecureFiles (especially for those business processes that deal with large payloads of unstructured data)

Encryption

In 11g, Oracle has extended the encryption capability to SecureFiles and uses the Transparent Data Encryption (TDE) syntax. For sensitive Oracle FMW SOA business processes that include private and regulated data, encryption may be a key driver for SecureFiles adoption. Encryption with SecureFiles is performed at the block level. Column-level and tablespace-level encryption for SecureFiles must not be turned on at the same time as they may cause considerable CPU overhead and make each other unnecessary.

All these configurable features’ provide benefits that have been confirmed by multiple stress tests of Oracle FMW SOA (refer to Appendix A and B for details on the system used, the methodology for the comparisons and the tests performed). The following table shows a few metrics resulting from the tests performed where the increased performance and reduced space requirements are demonstrated. Observe also the minimum impact in the Database’s nodes CPUs (the tests were performed using a RAC database) that the use of SecureFiles introduces.

TABLE 1. EFFECT OF USING SECURE FILES (LOW COMPRESSION) FOR LOBS IN THE SOAINFRA SCHEMA

SOA INFRA SCHEMAS	SOA (FOD) THROUGHPUT (MPS)	SOA DB IDLE CPU %	AVERAGE PHYSICAL IO DURING STRESS TEST	SPACE USED BY SOA SEGMENTS (MB)
LOBS ON BASIC FILES	12.44	81.37	705.94	17645.6
LOBS ON SECURED FILES	14.99	80.13	739.36	16,956.7

In the following excerpt from an Automatic Workload Repository (AWR) report, the top 10 wait events are compared for 2 stress tests: one using BasicFiles and another one using SecureFiles with LOW compression. Observe the significant reduction in most events. Observe the reduction in most wait events:

Wait Events

- Ordered by absolute value of 'Diff' column of '% of DB time' descending (idle events last)

Event	Wait Class	% of DB time			# Waits/sec (Elapsed Time)			Total Wait Time (sec)		
		1st	2nd	Diff	1st	2nd	%Diff	1st	2nd	%Diff
log file sync	Commit	31.40	26.29	-5.11	760.36	768.57	1.08	259,209.91	199,020.66	-23.22
gc buffer busy acquire	Cluster	20.46	24.75	4.29	1,049.76	1,225.85	16.77	168,865.45	187,328.24	10.93
gc buffer busy release	Cluster	9.85	7.22	-2.62	160.20	114.31	-28.65	81,269.13	54,684.71	-32.71
gc current block busy	Cluster	11.61	10.83	-0.78	377.18	382.00	1.28	95,849.88	81,974.69	-14.48
gc cr block busy	Cluster	7.00	7.65	0.66	329.53	362.53	10.01	57,774.98	57,936.48	0.28
gc cr block 2-way	Cluster	3.01	3.61	0.60	1,527.31	1,661.22	8.77	24,835.73	27,313.73	9.98
gc current block 2-way	Cluster	1.85	2.43	0.58	894.36	1,084.38	21.25	15,230.67	18,358.49	20.54
enq: TX - index contention	Concurrency	2.62	2.12	-0.50	77.05	61.33	-20.40	21,619.81	16,051.44	-25.76
cursor bin \$ wait on x	Concurrency	0.01	0.41	0.40	0.03	0.03	0.00	4.336	3,111.35	7,079.62
enq: HW - contention	Configuration	0.40	0.01	-0.39	13.56	0.67	-95.06	3,270.80	45.09	-98.62

IMPROVED IO

REDUCED LOB INDEX CONTENTION

IMPROVED gc PERF.

REDUCED HIGH W. CONTENTION

Image 1: AWR Wait Event comparison for a stressed SOA system using Basic Files for LOBs (1st) and SecureFiles (2nd)

Recommended Settings for SecureFiles in Oracle FMW SOA schemas

Compression

SecureFiles provides different degrees of compressions (HIGH | MEDIUM | LOW). **The applicability of each will require a specific analysis of tradeoffs for each Oracle FMW SOA system.** Database Administrators will have to analyze the performance impact of using greater compression (time consumed in performing the compression or latency) vs. the space savings. SecureFiles compression is orthogonal to table and index compression. It needs to be noted that a considerable amount of unstructured data used by an Oracle FMW SOA Business Process may be transient (it is used during runtime but can be removed/purged from the SOAINFRA tables when a process is completed); hence LOBs that are used during a business process will have a limited impact on the final space consumed by the SOA infra segments in the mid/long term unless auditing/regulation requires long periods of persistence for the information. Different audit levels will also generate different amount of unstructured data. For SOA systems that make intensive use of BPEL and Mediator composites, the CUBE_SCOPE.SCOPE_BIN and MEDIATOR_CASE_DETAIL.AUDIT_TRAIL LOBs (for audit-enabled systems) are the ones with the greatest impact in the system's storage. Oracle recommends using LOW compression for this type of systems. The reason is that the space gains are not too relevant for SOA with higher compression settings. Also, the system's performance improves and the CPU impact on the DB nodes is lower than when using HIGH or MEDIUM compression. See Appendix B for specific metrics and data gathered in stress tests with each type of compression. It needs to be noted that the default compression mode for LOBS on SecureFiles (i.e. if no qualifier is specified in the compress statement) is MEDIUM, hence turning to LOW requires adding the pertaining modifier to the ALTER statement. Refer to section "How to change to secure files" for more details on how to modify the SOAINFRA schemas to use SecureFiles for LOBs with different compression settings.

Deduplication

Oracle recommends enabling DEDUPLICATION for Oracle FMW SOA Systems using SecureFiles. This may not only eliminate redundant copies of data in a transparent way for Oracle FMW SOA Suite (which is beneficial for space-saving reasons) but it improves the system's performance (Refer to appendix B for metrics from the FOD stress tests with and without DEDUPLICATION). In a SOA System where the same information (payloads, attachments etc) may be duplicated in Service Engines, DEDUPLICATION may improve CPU and IO. However these improvements will not be dramatic as duplicate detection happens within a LOB segment. The final effect in an Oracle FMW SOA System using SecureFiles will be affected also

by partitioning. This is because duplicate detections do not span across partitions of SecureFiles columns. Since the effect of partitioning is even more beneficial (see Section “Partitioning LOBS on Secure Files”) than the gains provided by DEDUPLICATION, the effect of DEDUPLICATION is slightly reduced. In any case and since DEDUPLICATION does not introduce much overhead in the Oracle FMW SOA Database, it is still recommended.

Encryption

The drivers for adopting ENCRYPTION in the SecureFiles used by Oracle FMW SOA are obviously more related to the security sensitiveness of the business process involved than to technical aspects. The great advantage for Oracle FMW SOA is that no changes are required at the application level to use this encryption. Since there is a CPU and performance impact when using encryption (See Appendix B for specific metrics and data gathered in stress tests) Oracle recommends using it only when the strict security requirements apply to the pertaining Oracle FMW SOA LOBs. It is estimated that the overhead associated with encrypting or decrypting a common attribute can be around 5% in CPU and that for each 9 bytes of required storage Transparent Data Encryption will require an additional 7 bytes. Refer to the Oracle® Database Advanced Security Administrator's Guide (see References) for details on expected overhead and encryption details. The great benefit of using SecureFiles in this area is that it provides a fine control of the specific data that needs to be encrypted (just like column encryption) and may improve performance as compared to encrypting entire tables. See Appendix C for a rough rating of the sensitiveness of the LOBs present in the SOAINFRA schemas **(whether encryption should be used or not for each one of them will depend on each business case)**.

Partitioning

Most Oracle FMW SOA Suite systems are advised to use partitioning to improve both database manageability and performance. For SOAINFRA LOBs this is especially relevant because some of them typically cause high “buffer busy” and “gc busy” waits specially when using SecureFiles. The fact that most of the SecureFiles advanced features can be enabled at partition level, provides also fine control and better administration of storage (for example it may be decided to compress LOBs in specific date ranges only). It is highly recommended to partition the TABLES with LOBs on SecureFiles to distribute DML. LOBs are supported in RANGE-partitioned, LIST-partitioned, and HASH-partitioned tables. However the SOA schemas have been instrumented with partition keys to take advantage of the Oracle database RANGE partitioning and this should be the type of partitioning used. The following picture compares the top 10 wait events in the DB when the CUBE_SCOPE table (which holds one of the most critical LOBs in an Oracle FMW SOA FOD deployment

SCOPE_BIN)is partitioned, with a system not using partitioning (both tests using LOW compression)

Wait Events

- Ordered by absolute value of 'Diff' column of '% of DB time' descending (idle events last)

Event	Wait Class	% of DB time			# Waits/sec (Elapsed Time)			Total Wait Time (sec)			Avg Wait Time (ms)		
		1st	2nd	Diff	1st	2nd	%Diff	1st	2nd	%Diff	1st	2nd	%Diff
log file sync	Commit	12.99	27.09	14.10	978.27	1,099.59	12.40	59,405.22	56,945.21	-4.14	9.00	8.22	-8.67
gc buffer busy acquire	Cluster	20.73	10.86	-9.86	1,151.06	575.51	-50.00	94,777.75	22,838.11	-75.90	13.33	7.73	-42.01
buffer busy waits	Concurrency	4.13	0.35	-3.78	331.00	85.11	-74.29	18,870.59	730.18	-96.13	9.89	2.10	-78.77
log file parallel write	System I/O	3.49	5.75	2.26	844.38	737.97	-12.60	15,959.59	12,080.31	-24.31	3.08	2.96	-3.90
rdbms ipc reply	Other	2.74	4.64	1.90	1,833.95	1,884.37	15.33	12,526.67	9,753.73	-22.14	1.20	0.98	-18.33
gc buffer busy release	Cluster	4.59	2.83	-1.76	96.43	33.12	-65.65	20,988.67	5,946.13	-71.67	37.74	30.37	-19.53
gc current grant busy	Cluster	3.30	1.63	-1.67	543.85	174.53	-67.91	15,087.40	3,431.29	-77.26	4.39	3.71	-15.49
DFS lock handle	Other	2.66	4.09	1.43	446.16	497.53	11.51	12,162.95	8,605.86	-29.25	4.41	3.52	-20.18
gc current block 2-way	Cluster	7.93	6.66	-1.27	2,042.65	1,006.79	-50.71	36,270.88	14,000.61	-61.40	2.89	2.63	-9.00
gc cr block 2-way	Cluster	6.96	8.09	1.13	1,879.99	1,275.28	-32.17	31,830.64	17,012.77	-46.55	2.77	2.53	-8.66
gc current block busy	Cluster	11.48	10.42	-1.05	526.66	271.43	-48.46	52,486.83	21,916.46	-58.24	16.15	15.07	-6.69
enq: TX - contention	Other	0.86	0.01	-0.85	19.57	0.27	-98.62	3,925.58	13.23	-99.66	32.13	11.09	-65.48
enq: TX - index contention	Concurrency	1.70	0.94	-0.77	61.74	27.74	-55.07	7,790.18	1,969.14	-74.72	19.97	13.30	-33.40

Image 2: Comparison of wait events for a stress test using SecureFiles for LOBS without Partitioning (1st) and using SecureFiles for LOBS with range partitioning (2nd)

Refer to section “How to change to secure files” for an example of partitioned SOINFRA TABLE using a RANGE.

Adjusting PCTFREE

Multiple SOAINFRA update statements that use LOBS are significantly affected by buffer busy waits. This waits may even increase when using SecureFiles. In most cases it is recommended to rebuild these LOBS with higher values for PCTFREE. Since this has storage implications it is advised to analyze the requirements and available storage in each specific SOA system, but in general a slightly higher PCTFREE than the default one (10) for the most critical LOBs in the SOAINFRA schemas will be beneficial. For example: With an increase of PCTFREE from 10 to 20 for the BIN LOB in the CUBE_SCOPE table buffer busy waits were reduced by more than 75% in multiple Oracle FMW SOA stress tests.

How to enable SecureFiles for the Oracle FMW SOA Schemas

Requirements for using SecureFiles

Oracle SecureFiles are available starting Oracle Database 11g R1. SecureFiles segments require tablespaces managed with automatic segment space management (ASSM). This means that LOB creation on SecureFiles will fail if ASSM is not enabled. However the SOAINFRA tablespace is created by default with ASSM enabled

and with the default configuration nothings needs to be changed in this area in order to enable SecureFiles:

```
SQL> select segment_space_management from dba_tablespaces where tablespace_name='SOAINFRA';
AUTO
```

The *db_securefile* system parameter controls the SecureFiles usage policy. This parameter can be modified dynamically. The following options can be used for using SecureFiles:

- **PERMITTED:** allows SecureFiles to be created (This is the default setting for *db_securefile*. The default storage method uses BasicFiles)
- **FORCE:** create all (new) LOBs as SecureFiles
- **ALWAYS:** try to create LOBs as SecureFiles, but fall back to BasicFiles if not possible (if ASSM is disabled)

Other values for the *db_securefile* parameter are:

- **IGNORE:** ignore attempts to create SecureFiles
- **NEVER:** disallow new SecureFiles creations

Changing the Oracle FMW SOA Schemas

Using SecureFiles for new systems

Oracle recommends enabling SecureFiles when the SOA schemas are being created. For this, the Oracle FMW Repository Creation Utility (RCU) needs to be used just in the same way as it is used for BasicFiles, with the only change that the *db_securefile* parameters needs to be set to **ALWAYS** (provided that ASSM is used by all SOAINFRA tablespaces) or **FORCE** before executing RCU. As explained in previous sections SecureFiles uses **MEDIUM** compression with no **DEDUPLICATION** or **ENCRYPTION** by default, so once the RCU operation is completed additional steps are required to change these settings. The following script can be used to modify all tablespaces so that **LOW** compression and **DEDUPLICATION** (without **ENCRYPTION**) is used for all the LOBs in the SOAINFRA schema (assuming a prefix “PROD” for the schemas)

```

spool on;
spool /tmp/reportLOBs.log;
set lin 300;
SET SERVEROUTPUT ON SIZE 100000
  BEGIN
    FOR t IN (select table_name, column_name, securefile, owner from dba_lobs where securefile='YES' and owner like
'PROD_SOAINFRA') LOOP
      EXECUTE IMMEDIATE
        'alter table ' || t.owner || '.' || t.table_name || ' modify lob(' || t.column_name || ') (deduplicate)';
      EXECUTE IMMEDIATE
        'alter table ' || t.owner || '.' || t.table_name || ' modify lob(' || t.column_name || ') (compress LOW)';
    END LOOP;
  END;
/
column column_name format a25;
column table_name format a25;
select table_name, column_name, securefile, retention, encrypt, compression, deduplication from dba_lobs where
securefile='YES' and owner like 'PROD_SOAINFRA';
spool off;
/

```

After executing the script, verify the /tmp/reportLOBs.log file and check the appropriate change in each LOB.

Using Secure Files for existing/running systems

For Oracle FMW SOA systems that have been running for some time and that did not enable SecureFiles when the SOAINFRA schemas were created, Oracle recommends using Online Redefinition to migrate BasicFiles to SecureFiles. The redefinition can be done at the table or partition level. Using Online Redefinition allows the tables or partitions to remain online and can be done in parallel. The drawback of using online redefinition is that 1) additional storage equal to the entire table or partition and all its LOB segments must be available and 2) global indexes must be rebuilt. The following example provides the migration of the CUBE_SCOPE table using Online Redefinition. The example not only moves the SCOPE_BIN column to SecureFiles and increases

```
---Create Interim Table
--Constraints are copied by the redefinition
CREATE TABLE PROD_SOAINFRA.CUBE_SCOPE_RD
  ("CIKEY" NUMBER(*,0),
   "BINARY_FORMAT" NUMBER(*,0),
   "MODIFY_DATE" TIMESTAMP (6),
   "SCOPE_BIN" BLOB,
   "CI_PARTITION_DATE" TIMESTAMP (6)
 )
SEGMENT CREATION DEFERRED
PCTFREE 20 PCTUSED 1 INITRANS 1 MAXTRANS 255 NOCOMPRESS LOGGING
STORAGE( FREELISTS 6)
LOB ("SCOPE_BIN") STORE AS SECUREFILE (
  TABLESPACE "PROD_SOAINFRA" ENABLE STORAGE IN ROW CHUNK 8192
  CACHE NOCOMPRESS KEEP_DUPLICATES
  STORAGE( INITIAL 16384 NEXT 16384))
PARTITION BY RANGE (CI_PARTITION_DATE)
  (PARTITION part1 VALUES LESS THAN (TO_date('25-Jul-2012 00:30', 'dd-mon-
yyyy hh24:mi')) ,
  PARTITION part2 VALUES LESS THAN (TO_date('25-Aug-2012 00:30', 'dd-mon-
yyyy hh24:mi')),
  PARTITION part3 VALUES LESS THAN (TO_date('25-Sep-2012 00:30', 'dd-mon-
yyyy hh24:mi'))
  )
TABLESPACE "PROD_SOAINFRA";
```

```
--Perform Redefinition
--Define Column Mappings
DECLARE
    col_mapping VARCHAR2(1000);
BEGIN
    col_mapping := 'CIKEY CIKEY , ' || 'BINARY_FORMAT BINARY_FORMAT , ' || 'MODIFY_DATE
MODIFY_DATE, ' || 'SCOPE_BIN SCOPE_BIN, ' || 'CI_PARTITION_DATE CI_PARTITION_DATE';

--Start redef.
    DBMS_REDEFINITION.START_REDEF_TABLE (uname => 'PROD_SOAINFRA',orig_table =>
'CUBE_SCOPE',int_table => 'CUBE_SCOPE_RD',col_mapping =>col_mapping);
END;
/
--Redefine copying constraints etc
DECLARE
    error_count pls_integer := 0;
BEGIN
    DBMS_REDEFINITION.COPY_TABLE_DEPENDENTS('PROD_SOAINFRA', 'CUBE_SCOPE',
'CUBE_SCOPE_RD', 1, TRUE,TRUE,TRUE,FALSE, error_count);
    DBMS_OUTPUT.PUT_LINE('errors := ' || TO_CHAR(error_count));
END;
/

EXEC DBMS_REDEFINITION.FINISH_REDEF_TABLE('PROD_SOAINFRA', 'CUBE_SCOPE', 'CUBE_SCOPE_RD');

--Drop the interim table
DROP TABLE PROD_SOAINFRA.CUBE_SCOPE_RD;
```

As explained in the **Oracle® Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite** (see References) when implementing partial partitioning of the SOAINFRA schema (i.e. restrict partitioning to specific tables with a high growth rate) specific rules apply. In order to partition a dependent table, its master table must be partitioned as well. (Refer to the Oracle® Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite for a list of dependencies and range keys). Additionally the COMPOSITE_INSTANCE table always needs to be partitioned when the Audit Level property is set to Development or Production for any of the composites. This implies that the example above (CUBE_SCOPE table) requires also the appropriate redefinition of the COMPOSITE_INSTANCE table and the CUBE_INSTANCE table (which is the CUBE_SCOPE's master) with the exact same ranges. The statements bellow provide the required table partitions for these tables (to match the example above) without using online redefinition statements for simplicity:

```
CREATE TABLE "PROD_SOAINFRA"."COMPOSITE_INSTANCE"  
( "ECID" VARCHAR2(100),  
  "ID" NUMBER(*,0),  
  "PARENT_ID" VARCHAR2(100),  
  "CONVERSATION_ID" VARCHAR2(100),  
  "COMPOSITE_DN" VARCHAR2(500),  
  "SOURCE_NAME" VARCHAR2(100),  
  "SOURCE_TYPE" VARCHAR2(200),  
  "SOURCE_ACTION_TYPE" VARCHAR2(10),  
  "SOURCE_ACTION_NAME" VARCHAR2(500),  
  "BATCH_ID" VARCHAR2(100),  
  "BATCH_INDEX" NUMBER(*,0),  
  "BUSINESS_STATUS" NVARCHAR2(100),  
  "INDEX1" VARCHAR2(100),  
  "INDEX2" VARCHAR2(100),  
  "INDEX3" VARCHAR2(100),  
  "INDEX4" VARCHAR2(100),  
  "INDEX5" VARCHAR2(100),  
  "INDEX6" VARCHAR2(100),  
  "TITLE" NVARCHAR2(100),  
  --Continues
```

```

"TAGS" VARCHAR2(2000),
"TEST_RUN_NAME" VARCHAR2(100),
"TEST_RUN_ID" VARCHAR2(100),
"TEST_SUITE" VARCHAR2(100),
"TEST_CASE" VARCHAR2(100),
"STATE" NUMBER(3,0),
    "LIVE_INSTANCES" NUMBER(3,0),
"STATE_COUNT" NUMBER,
"HAS_ASSOC" CHAR(1),
"VERSION" NUMBER(*,0),
"PARTITION_DATE" TIMESTAMP (6) DEFAULT systimestamp,
"TENANT_ID" NUMBER(18,0) DEFAULT -1,
"CREATED_BY" VARCHAR2(100),
"CREATED_TIME" TIMESTAMP (6) NOT NULL ENABLE,
"UPDATED_BY" VARCHAR2(100),
"UPDATED_TIME" TIMESTAMP (6)
) SEGMENT CREATION DEFERRED
PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255 NOCOMPRESS LOGGING PARTITION BY
RANGE (CREATED_TIME)
    (PARTITION part1 VALUES LESS THAN (TO_date('25-Jul-2012 00:30', 'dd-mon-yyyy hh24:mi')),
    PARTITION part2 VALUES LESS THAN (TO_date('25-Aug-2012 00:30', 'dd-mon-yyyy hh24:mi')),
    PARTITION part3 VALUES LESS THAN (TO_date('25-Sep-2012 00:30', 'dd-mon-yyyy hh24:mi')))
) TABLESPACE "PROD_SOAINFRA";

```

```

CREATE TABLE "PROD_SOAINFRA"."CUBE_INSTANCE"
( "CIKEY" NUMBER(*,0) NOT NULL ENABLE,
  "CREATION_DATE" TIMESTAMP (6) NOT NULL ENABLE,
  "CREATOR" VARCHAR2(100),
  "MODIFY_DATE" TIMESTAMP (6),
  "MODIFIER" VARCHAR2(100),
--Continues....

```

```
"STATE" NUMBER(*,0),
"PRIORITY" NUMBER(*,0),
"TITLE" NVARCHAR2(200),
"STATUS" NVARCHAR2(100),
"STAGE" VARCHAR2(100),
"CONVERSATION_ID" VARCHAR2(256),
"ROOT_ID" VARCHAR2(100),
"PARENT_ID" VARCHAR2(100),
"SCOPE_REVISION" NUMBER(*,0),
"SCOPE_CSIZE" NUMBER(*,0),
"SCOPE_USIZE" NUMBER(*,0),
"PROCESS_TYPE" NUMBER(*,0),
"METADATA" NVARCHAR2(1000),
"EXT_STRING1" VARCHAR2(100),
"EXT_STRING2" VARCHAR2(100),
"EXT_INT1" NUMBER(*,0),
"TEST_RUN_ID" VARCHAR2(100),
"TEST_RUN_NAME" VARCHAR2(100),
"TEST_CASE" VARCHAR2(100),
"TEST_SUITE" VARCHAR2(100),
"ECID" VARCHAR2(100),
"CMPST_ID" VARCHAR2(100),
    "OUTCOME" VARCHAR2(100),
"TRACKING_LEVEL" VARCHAR2(16),
"AT_COUNT_ID" NUMBER(*,0),
"AT_EVENT_ID" NUMBER(*,0),
"AT_DETAIL_ID" NUMBER(*,0),
"VERSION" NUMBER(*,0),
"AG_ROOT_ID" VARCHAR2(100),
"AG_MILESTONE_PATH" VARCHAR2(100),
```

--Continues

```

"CACHE_VERSION" NUMBER(*,0),
  "PARENT_REF_ID" VARCHAR2(150),
  "COMPONENTTYPE" VARCHAR2(10) NOT NULL ENABLE,
  "NOTM" NUMBER(*,0),
  "COMPOSITE_NAME" VARCHAR2(500) NOT NULL ENABLE,
  "DOMAIN_NAME" VARCHAR2(50),
  "COMPONENT_NAME" VARCHAR2(300) NOT NULL ENABLE,
  "COMPOSITE_LABEL" VARCHAR2(50),
  "COMPOSITE_REVISION" VARCHAR2(50) NOT NULL ENABLE,
  "CREATE_CLUSTER_NODE_ID" VARCHAR2(100),
  "LAST_CLUSTER_NODE_ID" VARCHAR2(100),
  "CPST_INST_CREATED_TIME" TIMESTAMP (6) DEFAULT systimestamp,
  "TENANT_ID" NUMBER(18,0) DEFAULT -1,
  CONSTRAINT "CI_PK" PRIMARY KEY ("CIKEY")
  USING INDEX REVERSE PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS
  TABLESPACE "PROD_SOAINFRA" ENABLE
) SEGMENT CREATION DEFERRED PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
NOCOMPRESS LOGGING
STORAGE( FREELISTS 20) PARTITION BY RANGE (CPST_INST_CREATED_TIME)
  (PARTITION part1 VALUES LESS THAN (TO_date('25-Jul-2012 00:30', 'dd-mon-yyyy hh24:mi')),
  PARTITION part2 VALUES LESS THAN (TO_date('25-Aug-2012 00:30', 'dd-mon-yyyy hh24:mi')),
  PARTITION part3 VALUES LESS THAN (TO_date('25-Sep-2012 00:30', 'dd-mon-yyyy hh24:mi'))
) TABLESPACE "PROD_SOAINFRA";

```

Enabling Encryption

LOBs can be encrypted only with SecureFiles and on a per-column basis, i.e. partitioned LOBs have either all partitions encrypted or not encrypted. As explained in previous sections SecureFiles LOBs are encrypted using the Transparent Data Encryptions (TDE) feature available in Oracle since Oracle 10g R2. TDE is simple to adopt because users or applications do not need to manage the encryption and decryption of data, it is handled by the database. The encryption keys are stored in a location (wallet) external to the database. This location defaults to `$ORACLE_BASE/admin/$ORACLE_SID` or can be specified in `sqlnet.ora` file using parameter `WALLET_LOCATION`. To enable encryption for specific SecureFiles LOBs follow these steps.

1. Set your `ORACLE_BASE` variable to point to the appropriate directory:

For example:

```
PROMPT> export ORACLE_BASE=/u01/app/orcl
```

2. Create the wallet directory (otherwise encryption enabling commands will fail with `ORA-28368: cannot auto-create wallet error`):

```
PROMPT >mkdir $ORACLE_BASE/$ORACLE_SID/wallet
```

3. Start SQL Plus as `sysdba` (or user with `ALTER SYSTEM` privileges) and create an encrypted wallet by using the “`ALTER SYSTEM set encryption`” command:

```
SQL> ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "my_password";
```

4. Before performing any encryption or decryption operation it is required to make sure that the Oracle wallet is open. Use the following command to open the wallet containing the master encryption key:

```
SQL> ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY "my_password";
```

5. Use the `alter table modify lob(lob) (encrypt)` statement to encrypt the specific SecureFiles LOB. For example:

```
SQL> ALTER TABLE PROD_SOAINFRA.CUBE_SCOPE modify lob(SCOPE_BIN) (ENCRYPT);
```

(TDE enables you to specify a non default encryption algorithm. You can choose from one of the following algorithms: 3DES168, AES128, AES192 (default), AES256. To enable a different algorithm from default use

“ENCRYPT USING ALGORITHM_NAME” instead of just “ENCRYPT”

The encryption statement will error out if the DATA TYPE used by the column is of type “ANYDATA” (and there are a few columns using it in the SOAINFRA schema). It will also fail if the COLUMN is already encrypted. To encrypt all SOAINFRA LOBS using the default algorithm, the following script can be used:

```

spool on;
spool /tmp/reportEncyprtion.log;
SET SERVEROUTPUT ON SIZE 100000
DECLARE
  DT VARCHAR(30);
BEGIN
  FOR t IN (select table_name, column_name, securefile, owner from dba_lobs where securefile='YES' and
owner like 'PROD_SOAINFRA%') LOOP
    BEGIN
      select distinct tD.data_type into DT from all_tab_columns tD where tD.TABLE_NAME =
t.table_name and tD.COLUMN_NAME=t.column_name;
      dbms_output.put_line('Datatype: ');
      dbms_output.put_line(DT);
      IF ( DT not like 'ANYDATA') THEN
        dbms_output.put_line(DT);
        EXECUTE IMMEDIATE
        'alter table ' || t.owner || '.' || t.table_name || ' modify lob(' || t.column_name || ') (ENCRYPT)';
      END IF;
    EXCEPTION
      when others THEN
        dbms_output.put_line('Error performing encryption ... ');
    END;
  END LOOP;
END;
/
column column_name format a25;
column table_name format a25;
select table_name, column_name, securefile, retention, encrypt, compression, deduplication from
dba_lobs where securefile='YES' and owner like 'PROD_SOAINFRA%';
spool off;
/

```

After the script completes, check the `/tmp/reportEncyprtion.log` file to verify that the pertaining LOBs have been encrypted:

TABLE_NAME	COLUMN_NAME	SEC	RETENTION	ENCR	COMPRES	DEDUPLICATION
WFRULEDICTIONARY	DICTIONARY	YES		YES	LOW	LOB
WFROUTINGSLIP	ROUTINGSLIP	YES		YES	LOW	LOB
WFMESAGEATTRIBUTE	BLOBVALUE	YES		YES	LOW	LOB
WFHEADERPROPS	PROPERTIES	YES		YES	LOW	LOB
WFEVIDENCE	PLAINTEXT	YES		YES	LOW	LOB
...						

Appendix A: Oracle FMW SOA EDG System used for the tests

To mimic a realistic system for the tests, 2 Middle Tier SOA cluster front ended with OHS and an F5 LBR using a two node Oracle 11g R2 RAC was used for verifying the behavior of Oracle FMW SOA with SecureFiles. The topology was set up using **Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite 11g Release 1 (11.1.1.6)**. The Fusion Order Demo (FOD) example was deployed to the SOA cluster (refer to the **Oracle® Fusion Middleware Developer's Guide for Oracle SOA Suite 11g Release 1 (11.1.1.6)** for details on this Oracle FMW SOA suite example). Oracle Application Testing Suite (ATS) was used to stress the system. An Oracle Load Testing (OLT) Controller was set up in a Windows node and an Oracle ATS agent was deployed in a Linux server to stress the system. Twenty virtual users were configured to trigger the FOD order processing web service. Figure 1 shows the topology used for tests:

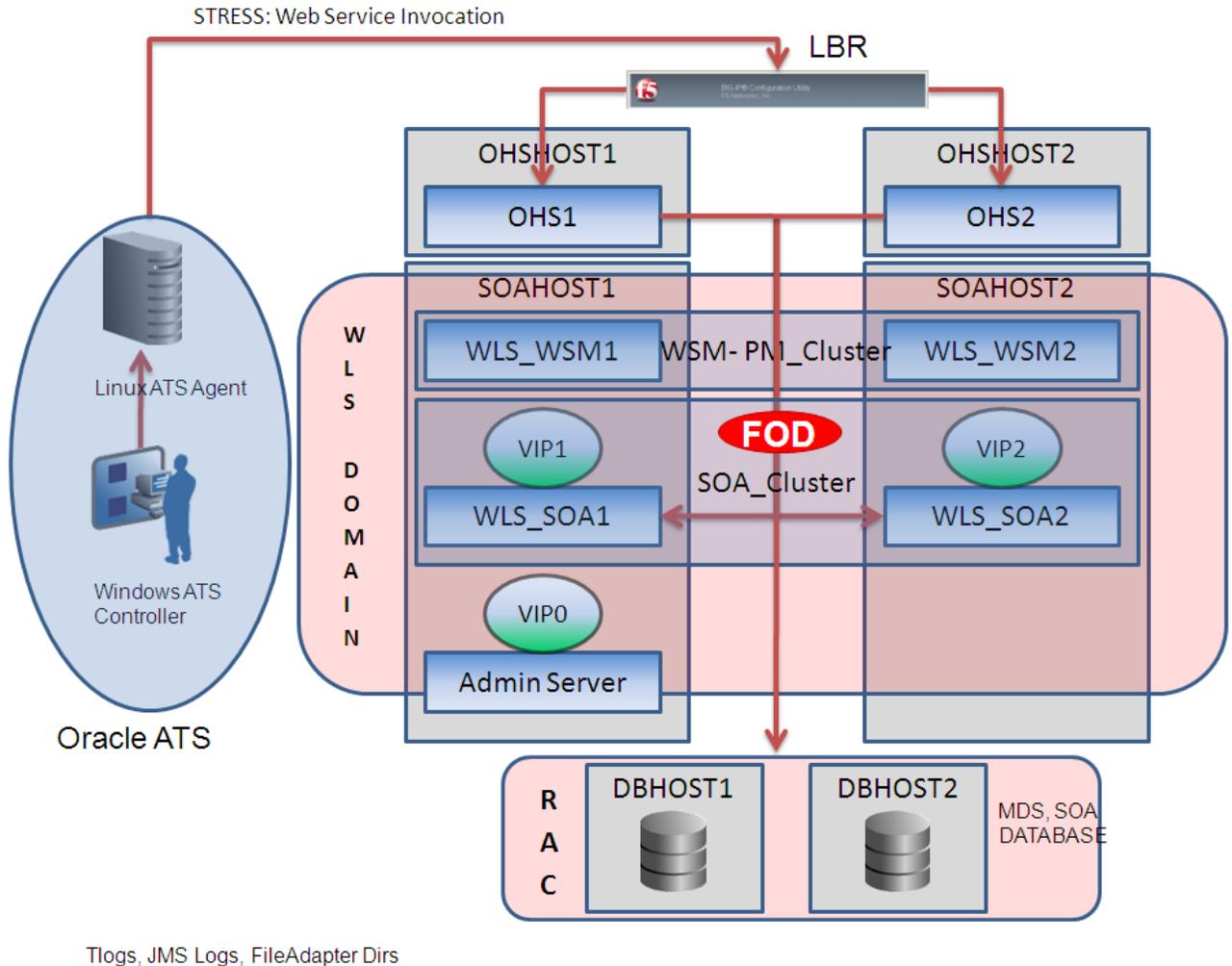


Image 3: Topology used for the tests

Each invocation by a virtual user involved 3 different composites, with multiple Oracle Mediator, Oracle BPEL

and JMS and File adapter invocations. Each tests executed 10000 iterations per virtual user. At the end of the test, JMX Metrics from the WLS Servers, OS Metrics from the DB and Middle Tier nodes as well as Oracle DB Automatic Workload Repository (AWR) reports and Oracle DB ADDM information were used to analyze the performance of the system. All the comparisons were executed with the exact same pool min and max capacity as well as with the exact same periods for XA retry intervals and retry duration.

It needs to be noted that the Oracle FMW Fusion order Demo uses very specific payloads (XML Documents and AUDIT information generated) that obviously will differ from the ones used by each customer's Oracle FMW SOA Suite production system. However, given the different types of components that it involves, it was chosen as highly representative of different real cases. For the tests, AUDIT was set to the default "Production" level: with this, composite instance tracking is collected, but Mediator engine will not collect payload details and BPEL engine will not collect payload details for assign activities (payload details for other BPEL activities are collected). This is the optimal level recommended for most normal production systems.

Areas of comparison for the different settings

The aspects that were compared in all cases are the following:

- DB Impact & Resource Consumption: Determine the wait events, overhead in CPU, Average Physical reads and writes per second, Average number of sessions per test, Memory and SQLNet overhead that may be caused in the Database Nodes when a specific settings is used. Comparison of top 10 wait events in AWR reports
- Final (post stress test) storage occupied, top 5 LOBs' average sizes.
- Middle Tier messages per second, thread throughput, transaction throughput, CPU overhead and average transaction latency

Empirical Method used for the analysis

Each metrics/result shown in this document was obtained as the average of AT LEAST 5 different tests repeated with the same settings. For the performance tests, results with more than 30% deviation from average were discarded and repeated. The "JMS message throughput" (the most relevant information from the performance behavior perspective since it involves full end to end behavior) was obtained as an average from the total 200,000 iterations that the 20 virtual users performed on the system. Hence, the performance values are an average of more than 1,000,000 invocations. Furthermore, for each test the thread throughput and transaction throughput was calculated as an average of the results for the two servers in the SOA Cluster. Each test was always run after a full SOAINFRA and MDS schema recreation for which the exact same data files

size and autoextend settings were configured (i.e. all relevant datafiles were laid out “fresh” on storage before each test) JMS messages, Files produced by the File Adapter and transaction logs were cleaned up for each tests and a full re-deployment of the composites involved was performed. The metrics obtained are valid in the context of each individual comparison. I.e. conditions may have varied from the comparison of YES/NO DEDUPLICATION vs. the comparison of YES/NO ENCRYPTION (thus the different throughputs for the same setting in different sections) but remained immutable during each group of tests for a feature. For the comparison of two different settings, the different settings were alternated to eliminate temporary effects affecting just one of the tests (i.e. for verifications of LOW COMPRESSION vs. MEDIUM COMPRESSION, we first run a test for LOW, then for MEDIUM, then for LOW, then for MEDIUM and so forth).

TEST	TYPE	DURATION	JMS Messages SOA1	JMS Messages SOA2	TOTAL JMS	JMS THROUGHPUT
90	B FILE TLOG 2s NEW VMS Incr	13225	91745	85387	177132	13.39
91	B FILE TLOG 2s NEW VMS Incr	13651	94409	85967	180376	13.21
92	B FILE TLOG 2s NEW VMS Incr	14587	96081	89248	185329	12.71
93	B FILE TLOG 2s NEW VMS Incr	13225	94336	84743	179079	13.54
94	B FILE TLOG 2s NEW VMS Incr	13584	82230	78443	160673	11.83
95	B FILE TLOG 2s NEW VMS Incr	13591	77066	70259	147325	10.84
96	B FILE TLOG 2s NEW VMS Incr	13640	83132	76671	159803	11.72
109	B FILE TLOG 2s NEW VMS Incr	13205	83952	76694	160646	12.17
118	B FILE TLOG 2s NEW VMS Incr	13099	84626	73288	157914	12.06
125	B FILE TLOG 2s NEW VMS Incr	11884	99945	99897	199842	16.82
128	B FILE TLOG 2s NEW VMS Incr	11064	99799	100073	199872	18.07
98	SECURE FILES NO COMPRESS	12509	73291	68087	141378	11.30
99	SECURE FILES NO COMPRESS	12834	65433	62704	128137	9.98
110	SECURE FILES NO COMPRESS	12266	71906	65375	137281	11.19
122	SECURE FILES NO COMPRESS	11821	84907	81883	166790	14.11
130	SECURE FILES NO COMPRESS	11555	98248	96469	194717	16.85
100	SECURE FILES COMPRESSMED	13266	73684	70047	143731	10.83
111	SECURE FILES COMPRESSMED	12219	57408	54930	112338	9.19
112	SECURE FILES COMPRESSMED	12379	71802	67583	139385	11.26
101	SECURE FILES COMPRESSLOW	12474	69183	65337	134520	10.78
108	SECURE FILES COMPRESSLOW	12736	69006	65096	134102	10.53
113	SECURE FILES COMPRESSLOW	12578	70099	68379	138478	11.01
126	SECURE FILES COMPRESSLOV	12236	96130	92813	188943	15.44
131	_netbk_SECURE FILES COMPR	11440	99428	100087	199515	17.44
103	SECURE FILES LOB PARTCOMP	13231	81925	75014	156939	11.86
104	SECURE FILES LOB PARTCOMP	13237	97871	93735	191606	14.48

Image 4: Example of averages calculated from repeated tests for the same settings

In summary, the number of verifications exceeded 75 different tests of more than 3 hour each. This reduced the chance of obtaining unreliable or variant results dramatically.

Appendix B: Metrics and Data from the tests performed

Comparison for COMPRESSION

The following table reflects the throughput, storage and physical IO for different COMPRESSION settings

TABLE 1. EFFECT OF DIFFERENT COMPRESSIONS ON SOA LOBS WHEN USING SECURE FILES					
COMPRESSION SETTING FOR LOBS ON SECURE FILES	SOA (FOD) THROUGHPUT (MPS)	SOA DB IDLE CPU %	AVERAGE PHYSICAL IO DURING STRESS TEST	SPACE USED BY SOA SEGMENTS	SOAINFRA LOBS AVERAGE SIZE
LOW	18.02	82.92	832.94	16844.45	310.05
MEDIUM	17.27	79.47	902.34	17207.90	311.01
HIGH	14.61	70.16	940.99	18962.60	302.98

The space savings for FOD composite are not high when using higher compressions. It is true that LOB size is reduced, but since multiple LOBs are transient the final total space used in the SOAINFRA Tablespaces may not reflect big space gains. Additionally there is an increased throughput when using LOW compression.

However in all cases the differences are not too high. Although in most cases using COMPRESSION LOW may be the best approach, different type of composites may have a different behavior. Oracle recommends verifying each system to obtain the more suitable configuration in each case.

Comparison for DEDUPLICATION

The following table reflects the throughput, storage and physical IO for an Oracle FMW SOA FOD system using DEDUPLICATION (LOW COMPRESSION) and a system without DEDUPLICATION (also using LOW COMPRESSION)

TABLE 3 EFFECT OF DEDUPLICATION ON SOA LOBS WHEN USING SECURE FILES				
DEDUPLICATION SETTING FOR LOBS ON SECURE FILES	SOA (FOD) THROUGHPUT (MPS)	SOA DB IDLE CPU %	AVERAGE PHYSICAL IO DURING STRESS TEST	SPACE USED BY SOA SEGMENTS (MB)
ENABLED	18.02	82.92	832.94	16844.45
DISABLED	17.95	80.94	910.41	16963.60

Observe that the performance improvements are not huge and neither are the final space differences. This is mainly because for BPEL/Mediator composites (and in the specific FOD's case) most of the final space used by SOAINFRA LOBs is allocated to XML_DOCUMENTS (where duplicates are uncommon) and a lot of duplicated data is transient. The impact of enabling DEDUPLICATION in the Database system resources is dismissible (CPU, MEM).

Comparison for ENCRYPTION

The following table reflects the throughput, storage and physical IO for an Oracle FMW SOA FOD system using ENCRYPTION (LOW COMPRESION) and a system without ENCRYPTION (also using LOW COMPRESION)

TABLE 4 EFFECT OF ENCRYPTION ON SOA LOBS WHEN USING SECURE FILES					
ENCRYPTION SETTING FOR LOBS ON SECURE FILES	SOA (FOD) THROUGHPUT (MPS)	SOA DB IDLE CPU %	AVERGAE PHYSICAL IO DURING STRESS TEST	SPACE USED BY SOA SEGMENTS (MB)	SOAINFRA LOBS AVERAGE SIZE
ENABLED	16.68	80.29	866.01	17705.50	309.65
DISABLED	18.00	82.92	846.30	16844.45	310.96

Observe the slight increase in CPU utilization (3.3%) and the increased final space allocated (consistent with the expected generic overhead introduced by TDE (around 5%). Notice also the decreased throughput of the system.

Comparison for PARTITIONED LOBS

The following table reflects the throughput, IDEL CPU and physical IO for an Oracle FMW SOA FOD system using a partitioned CUBE_SCOPE table and a system without any partitions:

TABLE 5. EFFECT OF PARTITIONING ON SOA LOBS WHEN USING SECURE FILES			
PARTITIONING	SOA (FOD) THROUGHPUT (MPS)	SOA DB IDLE CPU %	AVERGAE PHYSICAL IO DURING STRESS TEST
DISABLED	10.77	78.28	761.84
ENABLED	13.70	81.50	739.36

In the tests, using partitioning increased the systems throughput in almost 30%

Appendix C: LOBs in the SOAINFRA schema

TABLE 1. SOAINFRA SCHEMAS LOBS AND THEIR SECURITY-SENSITIVE ROUGH RATING

TABLE	LOB COLUMN	SECURITY SENSITIVENESS
BPM_CUBE_ACTIVITY_INSTANCE	ERRORMESSAGE	LOW
BPM_CUBE_ACTIVITY	SOURCECODE	MEDIUM
BPM_CASE_DATA	DATA	MEDIUM
BPM_AUDIT_QUERY	AUDIT_COMMENT	MEDIUM
BPM_ACTIVITY_INSTANCE	ERRORMESSAGE	LOW
BPM_ACTIVITY	SOURCECODE	MEDIUM
SOAQTZ_TRIGGERS	JOB_DATA	MEDIUM
BPM_CUBE_PROCESS	DEPLOYMENTINFO	MEDIUM
BPM_CUBE_AUDITINSTANCE	BUSINESSINDICATORS	HIGH
B2B_WIRE_MESSAGE	ERROR_TEXT_CLOB	MEDIUM
B2B_WIRE_MESSAGE	ERROR_DESCRIPTION_CLOB	MEDIUM
B2B_TRANSPORT_MANAGER	STATS	MEDIUM
B2B_EXT_BUSINESS_MESSAGE	PROTOCOL_WORK_AREA	LOW
B2B_EXT_BUSINESS_MESSAGE	ERROR_TEXT_CLOB	LOW
B2B_EXT_BUSINESS_MESSAGE	ERROR_DESCRIPTION_CLOB	LOW
B2B_EXT_BUSINESS_MESSAGE	ERROR_DETAIL_CLOB	LOW
MDS_LARGE_ATTRIBUTES	ATT_LONG_VALUE	LOW
MDS_METADATA_DOCS	MD_CONTENTS	LOW
MDS_STREAMED_DOCS	SD_CONTENTS	MEDIUM
WFRULEDICTIONARY	DICTIONARY	MEDIUM
WFROUTINGSLIP	ROUTINGSLIP	MEDIUM

TABLE 1. SOINFRA SCHEMAS LOBS AND THEIR SECURITY-SENSITIVE ROUGH RATING

TABLE	LOB COLUMN	SECURITY SENSITIVENESS
WFMESSEGEATTRIBUTE	BLOBVALUE	MEDIUM
WFHEADERPROPS	PROPERTIES	MEDIUM
WFEVIDENCE	SIGNATURE	HIGH
WFEVIDENCE	PLAINTEXT	HIGH
WFCERTIFICATEREVOKED	VALIDATIONDATA	HIGH
WFCERTIFICATE	CERTIFICATE	HIGH(*)
WFATTACHMENT	CONTENT	HIGH
BPELNOTIFICATION	MESSAGE	HIGH
PC_TASKPAYLOAD	PAYLOAD	MEDIUM
PC_TASKATTACHMENT	CONTENT	HIGH
XML_DOCUMENT	DOCUMENT	HIGH
TEST_INSTANCE	RESULTS	LOW
REJECTED_MSG_NATIVE_PAYLOAD	PAYLOAD	HIGH
REJECTED_MESSAGE	ERROR_MESSAGE	LOW
REJECTED_MESSAGE	STACK_TRACE	LOW
REFERENCE_INSTANCE	ERROR_MESSAGE	LOW
REFERENCE_INSTANCE	STACK_TRACE	LOW
COMPOSITE_INSTANCE_FAULT	ERROR_MESSAGE	LOW
COMPOSITE_INSTANCE_FAULT	STACK_TRACE	LOW
ATTACHMENT	ATTACHMENT	HIGH
EDN_LOG_MESSAGES	MSG	LOW
EDN_EVENT_ERROR_STORE	PAYLOAD	HIGH

TABLE 1. SOINFRA SCHEMAS LOBS AND THEIR SECURITY-SENSITIVE ROUGH RATING

TABLE	LOB COLUMN	SECURITY SENSITIVENESS
BPM_PML_HS	METADATA_CHANGE	HIGH
BPM_PML_HS	CHANGES	MEDIUM
WLI_QS_REPORT_DATA	DATA_VALUE	HIGH
MEDIATOR_PAYLOAD	BIN	HIGH
MEDIATOR_CASE_INSTANCE	FAULT_OBJ	LOW
MEDIATOR_CASE_DETAIL	AUDIT_TRAIL	MEDIUM
MEDIATOR_AUDIT_DOCUMENT	DOCUMENT	HIGH
WFUSERTASKVIEW	DEFINITION	MEDIUM
BPM_USERAPPLICATIONDATA	APPLICATIONDATA	MEDIUM
BPM_PRESENTATION	DEFINITION	MEDIUM
B2B_BAM_QTAB	"USER_DATA"."HEADER"."PROPERTIES"	HIGH
B2B_BAM_QTAB	"USER_DATA"."TEXT_LOB"	HIGH
B2B_BAM_QTAB	USER_PROP	HIGH
VARIABLE_SENSOR_VALUES	BLOB_VALUE	MEDIUM
VARIABLE_SENSOR_VALUES	CLOB_VALUE	MEDIUM
FAULT_SENSOR_VALUES	MESSAGE	MEDIUM
COMPOSITE_SENSOR_VALUE	CLOB_VALUE	MEDIUM
COMPOSITE_SENSOR_VALUE	BLOB_VALUE	MEDIUM
ACTIVITY_SENSOR_VALUES	ERROR_MESSAGE	LOW
BRDECISIONUNITOFWORK	UOW_DATA	MEDIUM
BRDECISIONINSTANCE	DECISION_TRACE	HIGH
BRDECISIONFAULT	MESSAGE	MEDIUM

TABLE 1. SOINFRA SCHEMAS LOBS AND THEIR SECURITY-SENSITIVE ROUGH RATING

TABLE	LOB COLUMN	SECURITY SENSITIVENESS
CUBE_SCOPE	SCOPE_BIN	MEDIUM
AUDIT_DETAILS	BIN	HIGH
EDN_OAOO_DELIVERY_TABLE	SYS_NC00032\$(*)	MEDIUM
EDN_OAOO_DELIVERY_TABLE	USER_PROP	HIGH
EDN_EVENT_QUEUE_TABLE	SYS_NC00032(*)	MEDIUM
EDN_EVENT_QUEUE_TABLE	USER_PROP	HIGH
TASK_NOTIFICATION_Q_T	"USER_DATA"."HEADER"."PROPERTIES"	MEDIUM
TASK_NOTIFICATION_Q_T	"USER_DATA"."TEXT_LOB"	HIGH
TASK_NOTIFICATION_Q_T	USER_PROP	HIGH
B2B_APP_MESSAGE	APP_MESSAGE_PROPS	MEDIUM
B2B_APP_MESSAGE	ERROR_TEXT_CLOB	LOW
B2B_APP_MESSAGE	ERROR_DESCRIPTION_CLOB	LOW
B2B_DATA_STORAGE	CLOB_VALUE	MEDIUM
B2B_DATA_STORAGE	BLOB_VALUE	MEDIUM
AG_INSTANCE	MILESTONE_STATE	MEDIUM
BPM_PROJECTSHAREDATA	VALUEBLOB	MEDIUM
SOAQTZ_JOB_DETAILS	JOB_DATA	MEDIUM
SOAQTZ_CALENDARS	CALENDAR	MEDIUM
SOAQTZ_BLOB_TRIGGERS	BLOB_DATA	LOW
WI_FAULT	MESSAGE	MEDIUM
TEST_DETAILS	TEST_RESULT	LOW
TEST_DEFINITIONS	DEFINITION	LOW

References

1. *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*
http://docs.oracle.com/cd/E23943_01/core.1111/e12036/toc.htm
2. *Oracle® Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*
http://docs.oracle.com/cd/E23943_01/admin.1111/e10226/toc.htm
3. *Oracle® Fusion Middleware Developer's Guide for Oracle SOA Suite 11g Release 1 (11.1.1.6)*
http://docs.oracle.com/cd/E23943_01/dev.1111/e10224/fod_hi_level_fod.htm#CIHGDIII
4. *Oracle® Database SecureFiles and Large Objects Developer's Guide 11g Release 2 (11.2)*
http://docs.oracle.com/cd/E11882_01/appdev.112/e18294/toc.htm
5. *Oracle® Real Application Clusters Administration and Deployment Guide*
http://download.oracle.com/docs/cd/B28359_01/rac.111/b28254/toc.htm
6. *Oracle® Database Advanced Security Administrator's Guide*
http://docs.oracle.com/cd/B28359_01/network.111/b28530/toc.htm



Oracle FMW SOA 11g R1: Secure Files
Analysis

September 2012

Author: Fermin Castro

Contributing Authors:

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2009, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.