ORACLE

FUSION MIDDLEWARE
IDENTITY MANAGEMENT

An Oracle White Paper
August, 2013

Extreme Scalability with Oracle Access Management Products

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

1 Executive Overview

With increasing requirements for high scalability and performance in the field of Identity Management, Oracle has recently conducted a large scale benchmark test on its Oracle Identity Management (IDM) suite of products. Oracle Access Manager (OAM) and Oracle Adaptive Access Manager (OAAM) were tested to serve extreme loads with 250 million (250M) users seeded in the Oracle Internet Directory (OID) and Oracle Database. Mid-tiers were deployed on Oracle Exalogic Elastic Cloud Software (EECS) and Database on Oracle Exadata hardware. The results on the Exalogic/Exadata enhanced systems are as follows.

OAM Authentication Benchmark

- Scale Out - OAM can support 7.7M, 12.5M, and 16.4M Logins per hour with one, two, and three EL nodes respectively
- Scale Up - OAM shows a perfect linear scale up in 4, 8, and 16 core testing.

OAAM Authentication Benchmark

- Scale Out - OAAM supports up to ~12M transactions per hour with one EL node, and up to ~20M transactions per hour with two EL nodes.

2 Introduction

A large scale benchmark test on the Oracle IDM suite of products was executed by Oracle PSR team. The goal of this Benchmark Test was to demonstrate the ability of the IDM products OAM and OAAM to support extreme loads when deployed on Exalogic(EL) and Exadata(ED) hardware. More specifically, the test:

- Demonstrates that Oracle IDM products support the operational requirement with a user base of 250M or more.
- Identifies the scalability characteristics for Oracle Access Manager and Oracle Adaptive Access Manager on EL and ED.
- Identifies the optimal settings for each tier (OS, Middleware and Database).
- Identifies the optimal settings for each component (Oracle Traffic Director, Oracle Http Server, Java Virtual Machine, OAM, OAAM, Oracle Internet Directory and Oracle Database).
- Identifies areas in which optimizations will help to support extreme loads across all these components.

This paper highlights that ability of OAM and OAAM to deliver high performance under large workloads with linear scalability by adding CPUs (scale up) and Nodes (scale-out). It begins with a description of the products involved in the tests and deployment details. The paper concludes by reporting the performance achieved, the extreme scalability and performance offered when the user base is over 250M users.

3 Oracle Products In The Benchmark Test

The following Oracle products are included in the Benchmark Test.

- About Oracle Access Manager
- About Oracle Adaptive Access Manager
- About Oracle Exalogic
- About Oracle Exadata Database Machine

3.1 About Oracle Access Manager

Oracle Access Manager uniquely offers access control services to provide centralized authentication, policy-based authorizations, and auditing. By protecting resources at the point of access and delegating authentication and authorization decisions to a central authority, OAM helps secure web, J2EE and enterprise applications while reducing cost, complexity, and administrative burdens. OAM is state-of-the-art software for access control, providing an integrated standards-based solution that delivers authentication, web single sign-on, access policy creation and enforcement, delegated administration, reporting, and auditing. Because of its unique functionality, OAM is established as the leading solution for web access management.

3.2 About Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) provides an innovative, comprehensive feature set to help organizations prevent fraud and misuse. Strengthening standard authentication mechanisms, innovative risk-based challenge methods, intuitive policy administration and integration across the Identity and Access Management Suite and with third party products makes OAAM uniquely flexible and effective. OAAM provides real-time evaluation of multiple data types and batch risk analytics to combat fraud and misuse across multiple channels of access. OAAM makes exposing sensitive data, transactions and business processes to consumers, remote employees or partners via your intranet and extranet safer.

3.3 About Oracle Exalogic

Oracle Exalogic is an integrated hardware and software system designed to provide a complete platform for a wide range of application types and widely varied workloads. Exalogic is intended for large-scale, performance-sensitive, mission-critical application deployments. It combines Oracle Fusion Middleware software and industry-standard Sun hardware to enable a high degree of isolation between concurrently deployed applications, which have varied security, reliability, and performance requirements. Exalogic enables customers to develop a single environment that can support end-to-end consolidation of their entire applications portfolio. Exalogic is designed to fully leverage an internal InfiniBand fabric that connects all of the processing, storage, memory and external network interfaces within an Exalogic machine to form a single, large computing device. Each Exalogic machine is connected to the customer's data center networks via 10 GbE (traffic) and GbE (management) interfaces.

3.4 About Oracle Exadata Database Machine

The Oracle Exadata & Database Machines are engineered to be the highest performance and most available platform for running the Oracle Database. Built using industry-standard hardware from Sun, and intelligent database and storage software from Oracle, the Exadata Database Machine delivers extreme performance for all types of database workloads including Online Transaction Processing (OLTP), Data Warehousing (DW) and consolidation of mixed workloads. Simple and fast to implement, the Exadata Database Machine is ready to tackle your largest and most important database applications and often run them 10x faster, or more.

4 Benchmark Test Deployment Details

The main hardware components of an Exalogic (X3-2) machine ¼ rack are:

- Eight Compute Nodes (Intel® Xeon® CPU E5-2690; 2x8 core @ 2.90GHz; 256GB RAM)
- Total 128 Compute Cores
- Total 2TB Compute Node Memory
- One ZFS Storage 7320 Clustered Configuration
- High-Speed InfiniBand Internal Network
- 42RU Rack Exposure

The main hardware components of an Exadata(X3-2) machine ¼ rack are:

- Two Compute Nodes (Intel® Xeon® CPU E5-2690; 2x8 core @ 2.90GHz; 256GB RAM)
- Total 512GB Memory
- Disk Controller HBA with 512MB Battery Backed Write Cache

- 4 x 300 GB 10,000 RPM Disks
- 2 x QDR (40Gb/s) Ports
- 2 x 10 Gb Ethernet Ports based on the Intel 82599 10GbE Controller
- 3 x Exadata Storage Servers X 3-2 with 36 CPU cores for SQL processing, 12 x PCI
- flash card with 4.8 TB Exadata Smart Flash Cache and, 36 x 600 GB 15,000 RPM
- High Performance disks or 3 TB High Capacity disks

The software components deployed on the Application Server include:

- OS: Oracle Linux Server release 5.8 (Tikanga)
- Exalogic Elastic Cloud Software (EECS) 2.0.4.0.0
- Exalogic Optimized WebLogic Server 10.3.6.0
- JRockit jdk1.6.0_37-R28.2.5-4.1.0
- Oracle Traffic Director (OTD) 11.1.1.7.0
- Oracle Http Server (OHS) 11.1.1.7
- OAM 11.1.2.1
- OAAM 11.1.2.1
- Oracle Internet Directory (OID) 11.1.1.7

The software components deployed on the Database Server include:

- OS: Enterprise Linux Server release 5.8 (Tikanga)
- DB Version: Oracle Enterprise Edition 11.2.0.3.0

The components were deployed as follows:

- OAM and OAAM servers were deployed on Exalogic nodes.
- The OAM and OAAM database was deployed on Exadata.
- OID was deployed on Exalogic node and the OID Database on Exadata.
- OHS/WebGate components were deployed on Exalogic nodes.
- OTD as load balancers were deployed on Exalogic nodes.
- Load Runner Controller was on a Windows machine.
- Load Generators were on support machines.

5 Test Scenarios and Results

The following sections contain information on the configurations, test scenarios and their results.

5.1 Benchmark Configurations

The Exalogic/Exadata deployments have all of the Oracle Exalogic Elastic Cloud Software (EECS) enhancements configured and enabled. The EECS software enhancements are licensed and cannot be used on non-Exalogic hardware. In this paper, we refer to the Exalogic and Exadata systems as Exa. More details can be found in

Section 7, "Appendix: Tuning the Test Environment."

5.2 Oracle Access Manager Test Case Overview

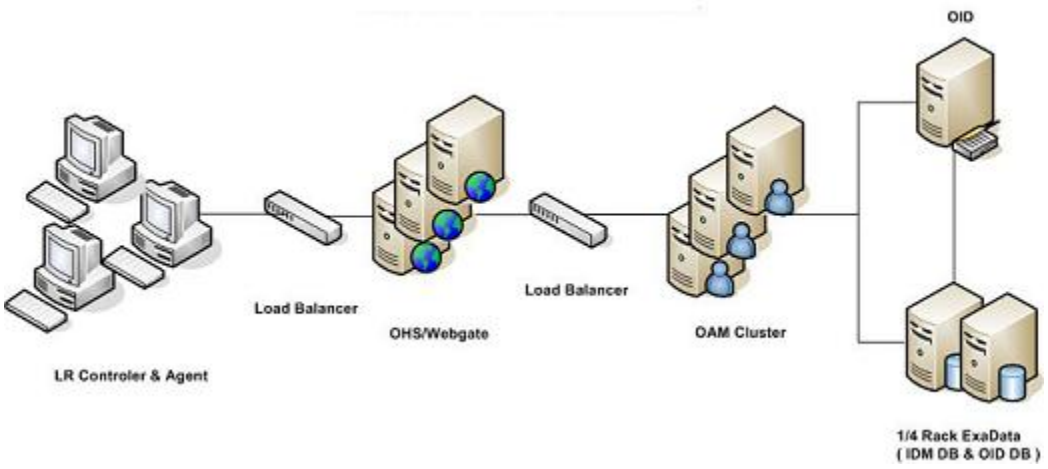
Oracle Access Manager offers access control services to provide centralized authentication, policy-based authorizations, and auditing. Different sets of OAM authentication tests were run to showcase OAM scale up and scale out characteristics on the Exa platform. To demonstrate the linear scale out, one, two and three server tests were run. To demonstrate the linear scale up, controlled tests with 4, 8, 16 physical cores as well as 32 logical cores (16 physical cores with hyper-threading) were run on a single server.

The OAM authentication test case involves a user navigating to a website URL protected by OAM. The WebGate plug-in in the Web Server will intercept the request and check with the OAM server to see if the user has been authenticated and has a valid session. If not, the OAM Server will redirect the user to an OAM login page where a username and password can be submitted. The OAM server then evaluates the authentication policy, and authenticates against the LDAP directory. Once the user is authenticated, a user session is created and authorization policies are checked to see if the user is allowed access to the protected resource. If authorized, the user will be redirected to the requested page.

OAM 11g uses Coherence-based session management. In other words, session data is stored (and persisted) on the server side in a distributed coherence cache. OAM sessions represent state that is associated with the user's login and resource access, which is utilized to manage the user's access to OAM protected resources. Some of the information that is managed includes authorization and authentication events during user access.

Figure 1-1 illustrates the OAM Benchmark topology for 250 million users.

Figure 1-1 OAM Benchmark Topology for 250 Million Users



5.3 Oracle Access Manager Test Results and Analysis

By default, OAM 11g uses Coherence session management. Besides the strong functional improvements and enhancements, OAM showed very solid performance, linear scale up vertically, and linear scale out horizontally. The Exa platform was able to support 7.7 M, 12.5M and 16.4M OAM logins/hour with one, two and three EL nodes respectively. The following sections contain more detailed results.

- OAM Authentication Benchmark Results (Scale Out)
- OAM Authentication Benchmark Results (Scale Up)

5.3.1 OAM Authentication Benchmark Results (Scale Out)

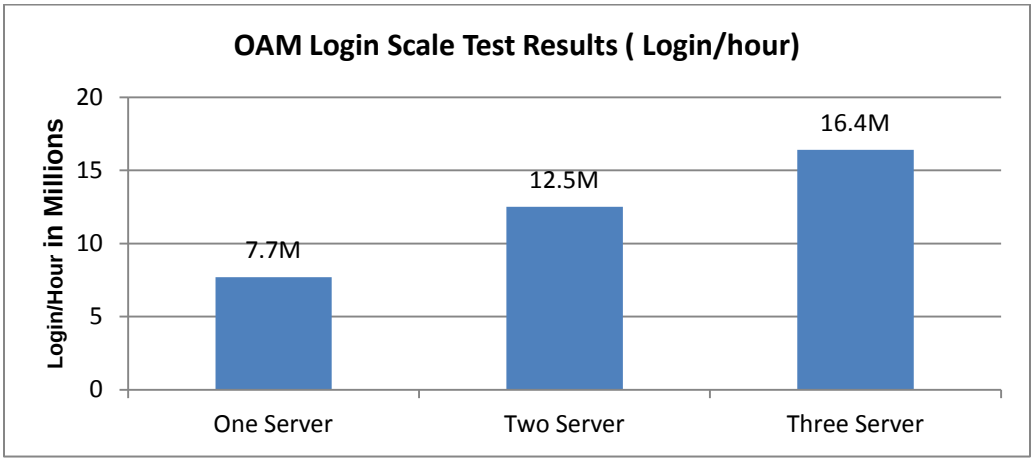
Table 1-2 documents the results of the OAM Authentication Benchmark Tests (Scale Out).

Table 1-2 OAM Authentication Benchmark Results

Test #	EL Nodes	OAM Servers	Login/sec	Login/hour	Login RT (seconds)
1	1	1	2151	7.7M	0.037
2	2	2	3475	12.5M	0.042
3	3	3	4562	16.4M	0.043

Figure 1-2 illustrates the Login/hour results based on the number of servers.

Figure 1-2 OAM Login Scale Test Results (Login/hour)



5.3.3 OAM Authentication Benchmark Results (Scale Up)

Table 1-3 documents the results of the OAM Authentication Benchmark Tests (Scale Up).

Table 1-3 OAM Authentication Benchmark Linear Scale Factors

# Core	TPS	CPU %	TPS/CPU	Scale Factor
4 Core	420	96	4.38	1.0
8 core	900	100	9.00	2.0
16 core	1700	96	17.71	4.0
32 core*	2200	86	25.58	5.8

* - 16 Physical cores with hyper-threading to 32 Logical cores

Figure 1-3 illustrates the OAM Linear Scale Up for 4 Core machines.

Figure 1-3 OAM Linear Scale Up 4 Cores

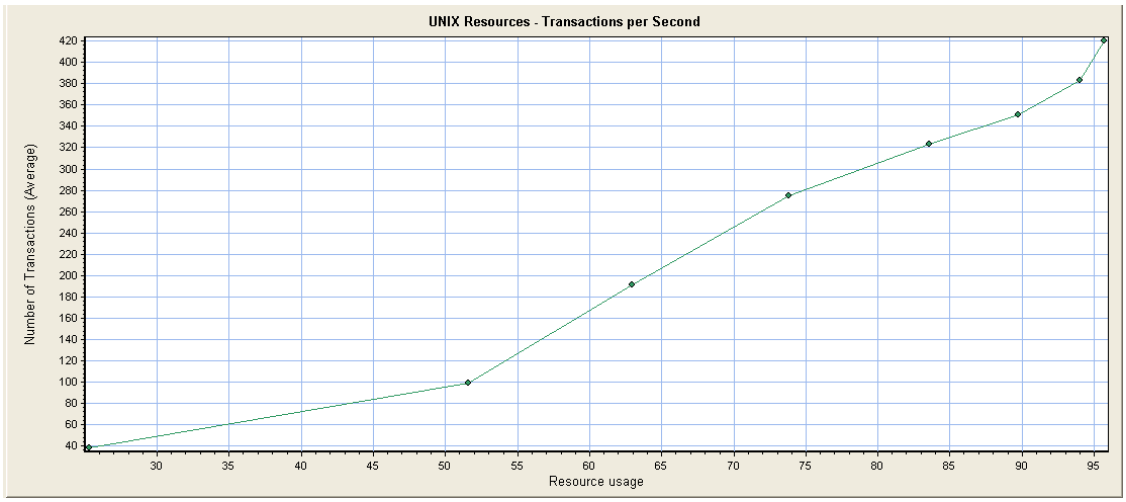


Figure 1-4 illustrates the OAM Linear Scale Up for 8 Core machines.

Figure 1-4 OAM Linear Scale Up 8 Cores

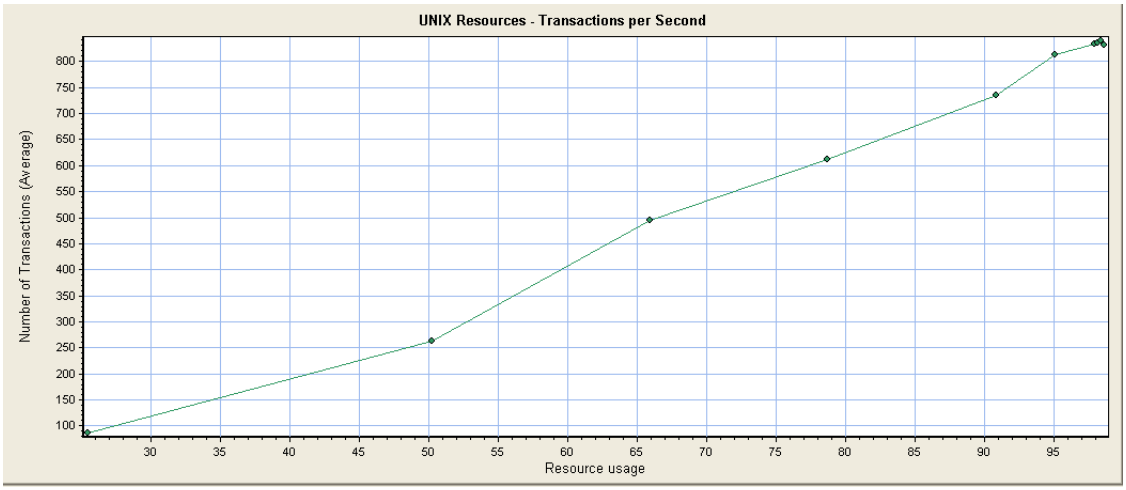


Figure 1-5 illustrates the OAM Linear Scale Up for 16 Core machines.

Figure 1-5 OAM Linear Scale Up 16 Cores

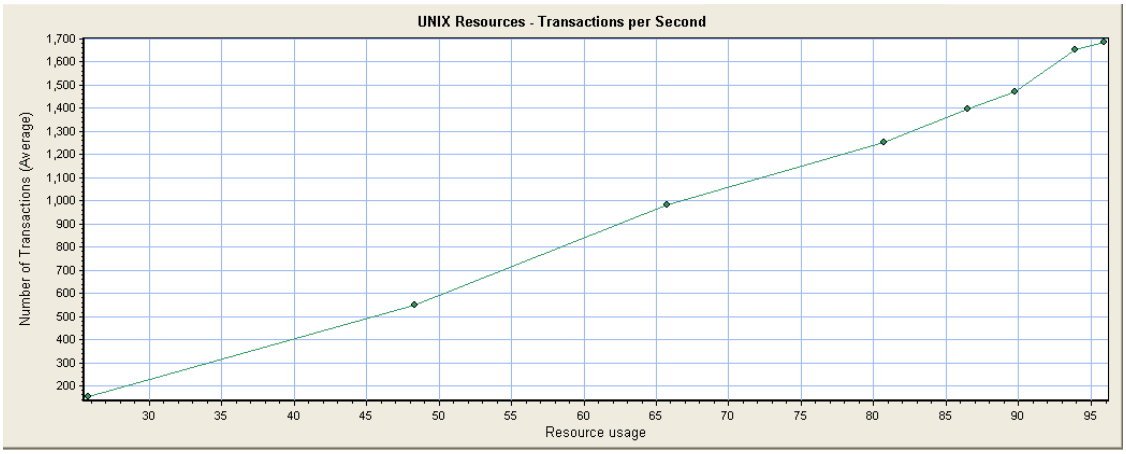


Figure 1-6 illustrates the OAM Linear Scale Up for 32 Core machines (with hyper-threading).

Figure 1-6 OAM Linear Scale Up 32 Cores (with Hyper-Threading)

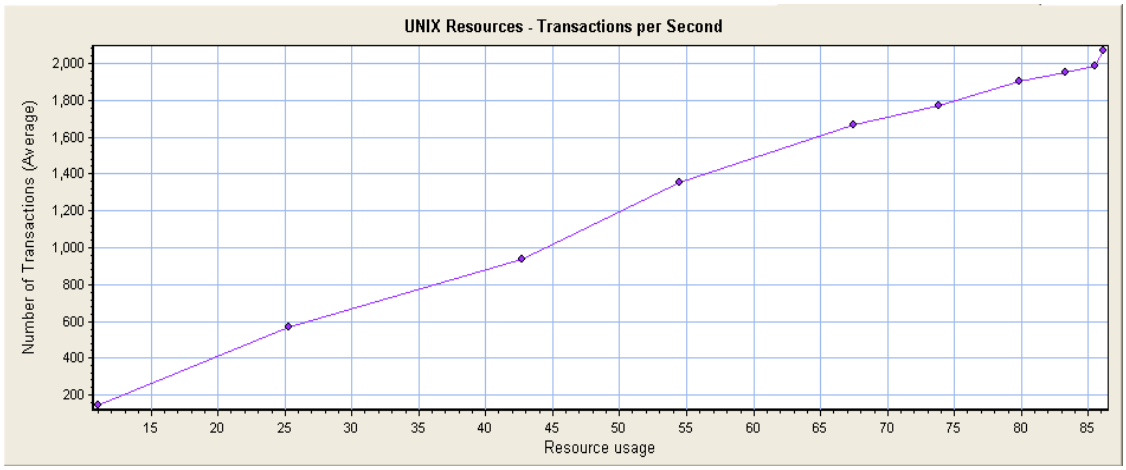
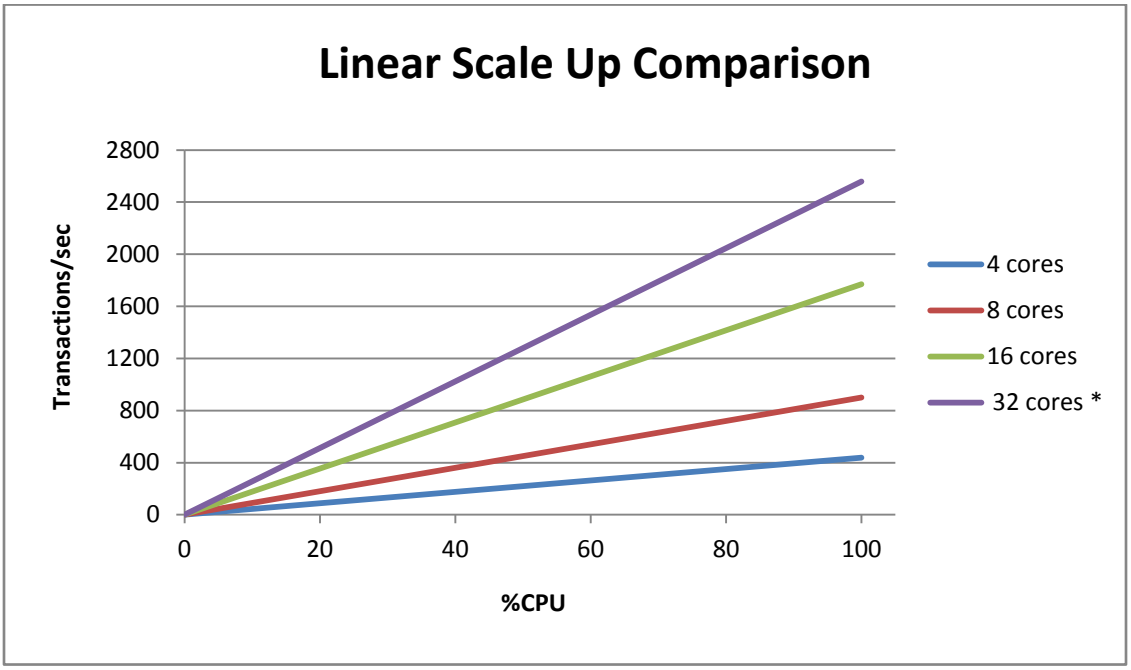


Figure 1-7 illustrates the comparison of the OAM Linear Scale Up test results.

Figure 1-7 OAM Linear Scale Up Core Comparison



5.4 Oracle Adaptive Access Manager Test Case Overview

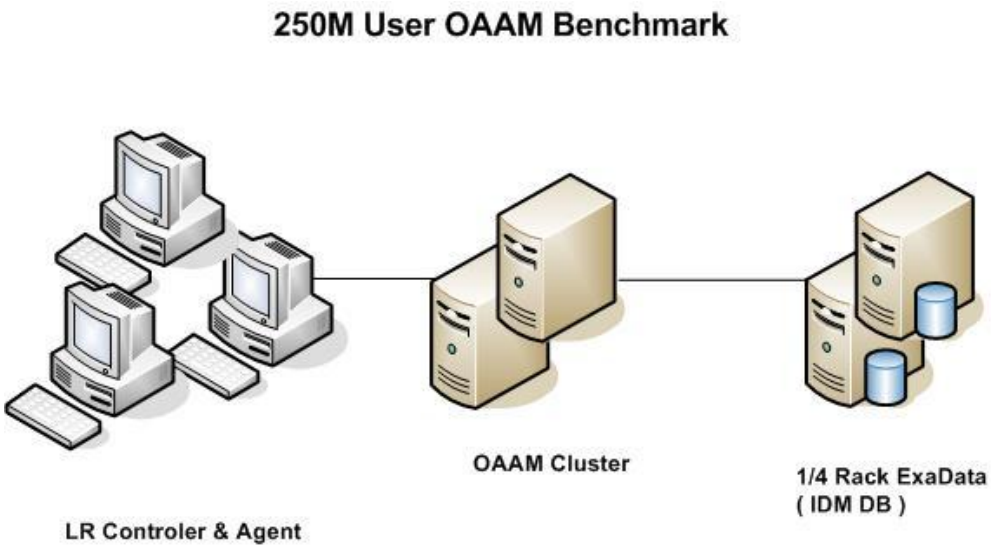
Oracle Adaptive Access Manager helps organizations prevent fraud and misuse by strengthening existing authentication flows, evaluating the risk of events as they happen and providing risk-based interdiction mechanisms such as multi-factor out-of-band authentication. It provides real-time and batch risk analytics across multiple channels of access, automates reviews of access and transaction events, and offers intuitive policy administration and standardized integrations with the Identity and Access Management Suite components.

Different sets of OAAM authentication tests were run to showcase OAAM scale up and scale out characteristics on Exa platform. To demonstrate the linear scale out, one and two server tests were run. Tests were also run with one OAAM server and two OAAM servers in the same EL node.

The OAAM test case involves a user navigating to the index page of a website URL protected by the application. Redirection to the OAAM login page offers the user a Username field in which the appropriate user ID is entered and submitted. OAAM identifies the device, creates a User Session, evaluates the Authentication policy, and displays a password page with a personalized or non-personalized AuthentiPad. The user enters the password, submits the page and OAAM evaluates the Post Authentication policy. After successful validation, the user is redirected to the application's JSP.

Figure 1-8 illustrates the OAAM Benchmark topology for 250 million users.

Figure 1-8 OAAM Benchmark Topology for 250 Million Users



The OAAM fraud protection rules are common across all transaction checkpoints. Table 1-4 lists the OAAM pre-authentication fraud protection rules. Table 1-5 (immediately following) lists the OAAM post-authentication fraud protection rules.

Table 1-4 OAAM Pre-Authentication Fraud Protection Rules

S.NO.	Rule Name	Description
1	Blacklisted users	This rule will trigger if a user has previously been blacklisted.
2	Blacklisted Counties	This rule will trigger if a country has been blacklisted in the past.
3	Blacklisted ISP's	This rule will trigger if a login is attempted from an ISP that was previously blacklisted.
4	Blacklisted devices	This rule will trigger if the device used has been blacklisted in the past.
5	WEBZIP used	This rule will trigger if there is a login attempt using the WEBZIP browser. The WEBZIP browser is often utilized by fraudsters to record a website in preparation for a phishing exercise. For this reason it is too risky to allow the use of WEBZIP.
6	Blacklisted IP's	This rule will trigger if an IP address has been blacklisted previously.

Table 1-5 OAAM Post Authentication Fraud Protection Rules

S.NO.	RuleName	Description
1	Active Anonymizer	This rule checks to see if the IP being used has been confirmed as an anonymizer in the last six months by Quova.
2	Risky countries	This rule will trigger if a country has previously been watch listed by the security team.
3	Suspect Anonymizer	This rule checks to see if the IP being used has been confirmed as an anonymizer in the last two years but not in the last six months by Quova.
4	Unknown Anonymizer	No positive test results are currently available. The initial anonymizer assignment is based upon other sources and has not yet been verified by Quova. If no positive test results are obtained, this address is removed from the list.
5	Dormant Device	If a device has not been used in thirty days and then more than two users login from it within twenty four hours this rule will trigger.
6	Device With Many Failures	If there are more than four unsuccessful login attempts from a device within eight hours this rule will trigger.
7	Maximum Devices Per User	If a user logs in using more than 2 devices within eight hours this rule will trigger.
8	Device Maximum Velocity	This rule will trigger if a device appears to have traveled faster than jet speed since it's last login in the last 20 hours.
9	Risky Connection Type	This rule will trigger if a connection type has previously been watch listed by the security team.
10	User Blocked Recently	If a user has been blocked more than twice within the last eight hours this rule will trigger.
11	Dormant IP	If an IP is not from a mobile connection and has not been used in thirty days and then more than one user logs in from it within twenty four hours this rule will trigger.
12	Surge Of Users From IP	If an IP is not from a mobile connection or one used by AOL and more than three users log in within five minutes this rule will trigger.
13	Private Anonymizer	IP addresses with this designation allegedly contain anonymous proxies that are not publicly accessible. As such they cannot be routinely tested with automated tools. These addresses typically belong to commercial ventures that sell anonymity services to the public. Addresses with this designation are derived from ownership information or obtained from trusted, high confidence sources.
14	Maximum Users Per Device	If more than four users log in using a device within thirty days this rule will trigger.
15	Risky Device	This rule will trigger if a device has previously been watch listed by the security team.
16	Risky IP	This rule will trigger if an IP has previously been watch listed by the security team.

The information in Table 1-6 was seeded into the database before testing began.

Table 1-6 OAAM Benchmark Test Data Generation

Test Item	Number of records	Comments/Description
Number of Users	250 million	
Number of Devices	~100 million	Each user may have 3 devices (home, office, mobile)

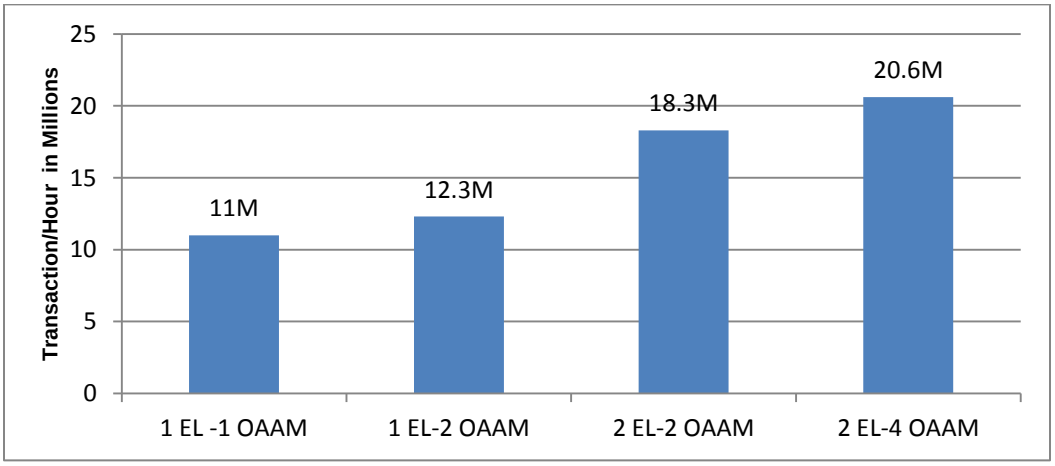
5.5 Oracle Adaptive Access Manager Test Results and Analysis

Besides providing an innovative, comprehensive feature set to help organizations prevent fraud and misuse, OAAM shows very robust performance. It can support ~12M transactions per hour with one EL node, and ~20M transactions per hour with two EL nodes. The results shown in Table 1-7 were obtained by running OAAM Servers on each EL node. Figure 1-10 illustrates these numbers in a linear scale.

Table 1-7 OAAM Throughput vs Number of Servers

EL Nodes	OAAM Servers	Transactions/sec	Transactions/hour
1	1	3031	11M
1	2	3423	12.3M
2	2	5073	18.3M
2	4	5735	20.6M

Figure 1-9 OAAM Throughput vs Number of Servers Linear Scale



6 Conclusion

The OAM & OAAM Scale Up & Scale Out benchmark tests showcased the extreme scalability and performance over a huge user base of over 250 million users. It illustrated the linear scalability characteristics for OAM and OAAM on EL and ED, and also identified the optimal settings for each tier and component (OTD, OHS, JVM, OAM, OAAM & OID).

7 Appendix: Tuning the Test Environment

The following sections document details of all tunings implemented in the test environment. Unless noted, these tunings are general and should apply to most deployments.

- OS Tuning
- OHS Tuning
- JVM and WLS Tuning
- OAM Tuning
- OAAM Tuning
- OID/OIDDB Tuning
- Exadata Database Tuning
- Enabling Exalogic-Specific Enhancements in Oracle WebLogic Server

For more specific information on tuning the Oracle products in this section, see the *Oracle Fusion Middleware Performance and Tuning Guide* at

http://docs.oracle.com/cd/E27559_01/doc.1112/e28552/toc.htm.

7.1 OS Tuning

The following Linux parameters were set in `sysctl.conf`.

- fs.file-max - 524288
- Shmall - 4294967296
- Shmax - 68719476736

The following semaphore limits were also set in `sysctl.conf`.

- max number of arrays = 128
- max semaphores per array = 5010
- max semaphores system wide = 641280

- max ops per semop call = 5010
- semaphore max value = 32767

These changes will take effect after running the following command.

```
sudo /sbin/sysctl -p /etc/sysctl.conf
```

The following changes in the `/etc/security/limits.conf` file require a reboot of the server.

```
#*          soft       nofile         8192    This change after reboot proved vital for the fix.
#*          hard      nofile         8192
*             soft         nofile         150000
*             hard        nofile         150000
```

7.2 OHS Tuning

Make the following changes in the `httpd.conf` file.

- MaxKeepAliveRequests 0
- Timeout 300
- KeepAliveTimeout 10

Make the following changes in the httpd.conf file under `<IfModule mpm_worker_module>`.

- StartServers 2
- ServerLimit 10
- ThreadLimit 250
- MaxClients 1500
- MinSpareThreads 200
- MaxSpareThreads 200
- ThreadsPerChild 250
- MaxRequestsPerChild 0
- AcceptMutex fcntl
- LockFile "/exl_installations/locks/http_lock_7777"

7.3 General Tuning for JVM & WLS

- JAVA_OPTIONS="-Xms12G -Xmx12G -Xns6G {JAVA_OPTIONS}"
- JAVA_PROPERTIES="-XXaggressive -XX:-UseLargePagesForHeap -XgcPrio:throughput -XXgcthreads:8 -Xverbose:gc=debug -Xverboselog:

$DOMAIN_HOME/tmp/${SERVER_NAME}_GC.log -Djbo.dofailover=false -Dweblogic.threadpool.MinPoolSize=100 ${JAVA_PROPERTIES}

Set level='ERROR' in the Logging.xml file for all log handlers and loggers and setup large pages by running the following commands in order.

- Switch to root
- echo 10000 > /proc/sys/vm/nr_hugepages
- mount -t hugetlbfs nodev /mnt/hugepages
- chmod 777 /mnt/hugepages

7.4 OAM Tuning

WebGate tunings can be set by logging into the Oracle Access Management 11g Administration Console and searching for (then selecting) the specific agent. Navigate to the search screen from the System Configuration tab to Access Manager Settings -> ssoAgents -> OAM agents. The following section lists the default setting => tuned setting.

- Max Connections: 1 => 20
- Serverlist -> (for each server)-> max num of connections : 1 => 2
- Cache Pragma header = no-cache => //Delete
- Cache Control Header = no cache => //Delete
- LDAP Min Connection Pool : 0 => 50
- LDAP Max Connection Pool : 0 => 200

Set the following Access Manager tunings.

- Increase OAM Max MessageBean pool size: 100 =>1000
- DeletedSessionReaperSettings : 100 => 500
- SessionStoreSettings : 100 => 500
- -DMaxRandomPoolSize=1000
- -DMaxCipherPoolSize=1000

Set the following Access Manager Coherence tunings.

- NW Tuning:

  sudo /sbin/sysctl -w net.core.rmem_max= 16777216

  sudo /sbin/sysctl -w net.core.wmem_max= 16777216

- In oam-config.xml:

<Setting Name="ThreadCount" Type="htf:map">

<Setting Name="Key"

Type="xsd:string">oam.coherence.distributed.threads</Setting>

<Setting Name="Value" Type="xsd:integer">16</Setting

7.5 OAAM Tuning

Set the following properties in Oaam_admin_properties.

- oaam.oam.oamclient.timeout = 30000
- oaam.oam.oamclient.periodForWatcher = 1806000
- oaam.oam.oamclient.initDelayForWatcher = 60000
- oaam.oam.oamclient.minConInPool =10
- oaam.uio.oam.num_of_connections = 300
- vcrypt.tracker.rulelog.detailed.minMillis=5000
- bharosa.uio.default.password.auth.provider.classname=com.bharosa.uio.manager.auth.DummyAuth Manager
- bharosa.uio.default.password.auth.provider.classname=20
- vcrypt.tracker.rules.trace.workerCount=10
- vcrypt.tracker.rule.cookiePatternCheck.workerCount = 20
- vcrypt.tracker.dbmgr.postcommit.workerCount=20
- bharosa.tracker.loadbalanced = true

Set the following autolearning properties to false.

- vcrypt.tracker.autolearning.enabled=false
- vcrypt.tracker.autolearning.use.auth.status.for.analysis =false

Set the following autolearning data collection properties to false.

- bharosa.trackernodehistory.enable=false
- tracker.wf.createHourlyEntries=false
- tracker.wf.createDailyEntries=false
- vcrypt.tracker.autolearning.update.entity.profile.for.auth.patterns=false

7.6 OID/OIDDB Tuning

The following configurations were set for OID.

- dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory

  orclecachemaxentries: 100000000

  orclecachemaxsize: 214748364800

  orclmatchdnenabled: 0

  orclskiprefinsql: 1

- dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry

  orclserverprocs: 16

  orclmaxcc: 4

  orclgeneratechangelog: 0

- OID Database Tuning

  sga_max_size: 48G

  sga_target: 48G

  pga_aggregate_target: 1g

  processes: 1024

- OID tablespace usage

  OLTS_ATTRSTORE: 227GB

  OLTS_CT_STORE: 346GB

  OLTS_DEFAULT: 43GB

7.7 Exadata Database Tuning

The following configurations were set for the Exadata Database.

- OAAAM1.__db_cache_size=14461960192
- OAAAM1.__java_pool_size=33554432
- OAAAM1.__large_pool_size=201326592
- OAAAM1.__pga_aggregate_target=16GB
- OAAAM1.__sga_target=77GB
- OAAAM1.__shared_io_pool_size=0
- OAAAM1.__shared_pool_size=2181038080
- OAAAM1.__streams_pool_size=0

- OAAAM1.__streams_pool_size=67108864
- *._awr_disabled_flush_tables='wrh$_tempstatxs'
- *._b_tree_bitmap_plans=FALSE
- *._file_size_increase_increment=2143289344
- *._kill_diagnostics_timeout=140
- *._lm_rcvr_hang_allow_time=140
- *.audit_file_dest='/u01/app/oracle/admin/OAAAM/adump'
- *.audit_sys_operations=FALSE
- *.audit_trail='NONE'
- *.cluster_database=true
- *.compatible='11.2.0.3.0'
- *.control_files='+LYVDATA/oaaam/controlfile/current.298.779489829'
- *.db_block_checking='OFF'
- *.db_block_checksum='typical'
- *.db_block_size=8192
- *.db_create_file_dest='+LYVDATA'
- *.db_domain=''
- *.db_files=2000
- *.db_lost_write_protect='typical'
- *.db_name='OAAAM'
- *.db_recovery_file_dest='+LYVRECO'
- *.db_recovery_file_dest_size=4718592000000
- *.diagnostic_dest='/u01/app/oracle'
- *.global_names=TRUE
- *.log_buffer=134217728
- *.nls_sort='BINARY'
- *.open_cursors=1500
- *.os_authent_prefix=''
- *.parallel_adaptive_multi_user=FALSE
- *.parallel_execution_message_size=16384

- *.parallel_max_servers=128
- *.parallel_min_servers=32
- *.pga_aggregate_target=8589934592
- *.plsql_code_type='NATIVE'
- *.pre_page_sga=false
- *.processes=2500
- *.recyclebin='OFF'
- *.remote_listener='exa4-scan:1521'
- *.remote_login_passwordfile='exclusive'
- *.session_cached_cursors=1500
- sessions=1131

7.8 Exalogic-Specific Tunings

The following sections contain Exalogic-specific enhancements and other configurations set in the test deployment.

- Enabling Domain-level Enhancements
- Enabling Cluster-level Session Replication Enhancements
- Additional Exalogic Specific Configurations

7.8.1 Enabling Domain-level Enhancements

The Enable Exalogic Optimizations setting enables all of the individual features described in Table 1-8 collectively. The Startup Option column (located in http://docs.oracle.com/cd/E18476_01/doc.220/e18479/optimization.htm#BABICIJG) indicates how to independently enable and disable each feature.

Table 1-8 Features Enabled By The Domain-Level Flag

Feature	Description
Scattered Reads	Increased efficiency during I/O in environments with high network throughput
Gathered Writes	Increased efficiency during I/O in environments with high network throughput
Lazy De-serialization	Increased efficiency with session replication
Self Tuning Thread Pool Optimization	Increased efficiency of the self tuning thread pool by aligning it with the Exalogic's processor architecture threading capabilities

7.8.2 Enabling Cluster-level Session Replication Enhancements

The following session replication enhancements were enabled for Managed Servers in a WebLogic cluster. For details, see http://docs.oracle.com/cd/E18476_01/doc.220/e18479/optimization.htm#BABBHGCF.

- Configure multiple replication channels
- Enable SDP Protocol
- Enable One Way RMI for Replication option

7.8.3 Additional Exalogic Specific Configurations

The following links contain information on additional Exalogic specific configurations

set in the test deployment.

- Configuring Grid Link Data Source for Dept1_Cluster1

  http://docs.oracle.com/cd/E18476_01/doc.220/e18479/optimization.htm#BABIHEDI

- Configuring SDP-Enabled JDBC Drivers for Dept1_Cluster1

  http://docs.oracle.com/cd/E18476_01/doc.220/e18479/optimization.htm#BABHBJGG

- Configuring SDP InfiniBand Listener for Exalogic Connections

  http://docs.oracle.com/cd/E18476_01/doc.220/e18479/optimization.htm#CJHGIIHG

Extreme Scalability with Oracle Access Management Products
August 2013
Author: PSR Team
Contributing Authors: IDM Dev Team, IDM PM Team

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

Hardware and Software, Engineered to Work Together