ORACLE

Deep Dive into Oracle Access Management 12.2.1.4.0 Performance

An Oracle White Paper, 1st Edition

March 10, 2021 | Version 1.0

TABLE OF CONTENTS

PURPOSE STATEMENT

This document discusses performance recommendations and sizing for Oracle Access Manager (OAM) as part of Oracle Identity Management (IDM) Suite, Release 12.2.1.4.0.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. 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 in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

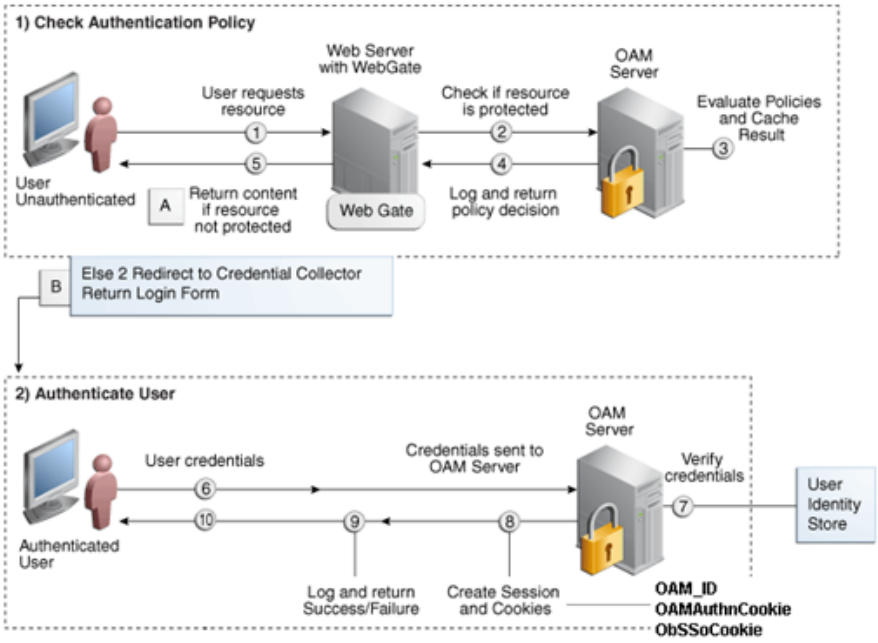
INTRODUCTION

With increasing requirements for high scalability and performance in the field of Identity Management, Oracle has conducted scalability benchmarks for Oracle Access Manager (OAM) as part of Oracle Identity Management (IDM) Release 12.2.1.4.0, 2021 12c PS4 January BP. The environments for OAM scalability benchmarks were deployed on virtual Compute and DBaaS shapes in Oracle Cloud Infrastructure (OCI). The objective was to measure OAM user authentication flow scalability for up to 150 thousand (150K) users, seeded in Oracle Unified Directory (OUD), measure the load for one and two OAM cluster nodes, provide the tuning recommendations and project the scalability for higher number of OAM users.

ORACLE ACCESS MANAGER TEST CASE OVERVIEW

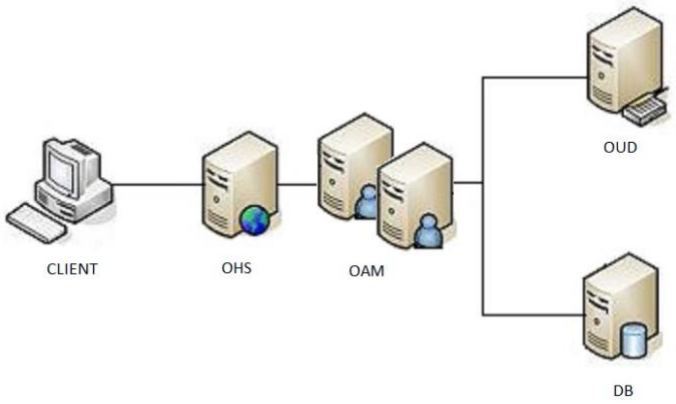
Oracle Access Manager offers access control services to provide centralized authentication, policy-based authorizations, and auditing. To measure the performance and scalability, several OAM authentication tests were executed to show OAM scaling up on a single node and scaling out for two nodes in OCI virtual compute shapes.

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 OUD 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 12c uses database for server-side session management. In other words, session data is stored (and persisted) on the database server side. 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. The users are defined under a single hierarchical group, which gives access to the protected resources by simple LDAP authentication. Refer to the sequence diagram below, depicting the described flow.



Topology

Refer to the schematic picture below, describing the test configuration with all required OAM tiers, collocated in the same network segment to eliminate network latencies in the scalability runs.



Hardware Configuration

Depending on the number of concurrent users OAM configurations can be categorized as small, medium and large sized implementations. This section covers recommended hardware shapes, offered in Oracle Cloud Infrastructure (OCI) for each size to accommodate for the concurrent load and projects for the future growth. The OAM customers can use the OCI shape specifications as the guidance for deploying comparable on-premise OAM configurations. Refer to the following link for more details on OCI compute shapes: https://docs.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm

Table 1-1: OAM single compute node recommended configurations

Configuration	Small	Medium	Large
Concurrent OAM Users	**Up to 25,000**	**25,000-50,000**	**50,000 and higher**
OCI shape for OAM (one node)	Standard2.4	Standard2.8	Standard2.16
OCI shape RAM, Gb	60	120	240
OCI shape OCPUs	4	8	16

Table 1-2: OAM Oracle RDBMS configuration

Configuration	Small	Medium	Large
OAM DB	Standard2.4	Standard2.4 - 2.8	Standard2.8 - 2.16
OCI shape RAM, Gb	60	60 - 120	120 - 240
OCI shape OCPUs	4	4 – 8	8 - 16

Table 1-3: OUD compute node configuration

Configuration	Small	Medium	Large
OUD Compute	Standard2.4	Standard2.4 - 2.8	Standard2.4 - 2.16
OCI shape RAM, Gb	60	60 - 120	60 – 120
OCI shape OCPUs	4	4 – 8	4 – 16

Table 1-4: OHS compute node configuration

Configuration	Small	Medium	Large
OHS Compute	Standard2.4	Standard2.4 - 2.8	Standard2.8 - 2.16
OCI shape RAM, Gb	60	60 - 120	120 - 240
OCI shape OCPUs	4	4 – 8	8 - 16

Important!

- OAM compute sizing specifications apply to a single node only. You can deploy another OAM compute node, using the same shape / specifications to scale-out and run as an OAM cluster. CPU %utilization reflects the OAM workload, when it reaches 50-60%, you may have to plan for scaling out the cluster by adding another OAM node.
- OAM database can handle user authentication load from more than one OAM node, so the recommended specifications apply to a single database instance. You will have to closely monitor the database load when you add more OAM Compute nodes and enable more concurrent users in your environments. Use of Oracle Database Real Application Cluster (RAC) is recommended to provide better load balancing and OAM database scale-out for large configurations.
- OUD compute single node can sustain higher concurrent load, so you can use smaller shapes for Small and Medium configurations. Large configuration extends to high-end workload, so it has the wider range for its compute specifications.
- OHS compute node can handle the load from more than one OAM node. You can consider deploying more than one OHS node to ensure load balancing in OAM environments.

OAM AUTHENTICATION BENCHMARK RESULTS

This chapter provides the results of OAM load using authentication scenario, described earlier, for Small, Medium and Large sample configurations. OUD has been seeded with 200K users for all configurations.

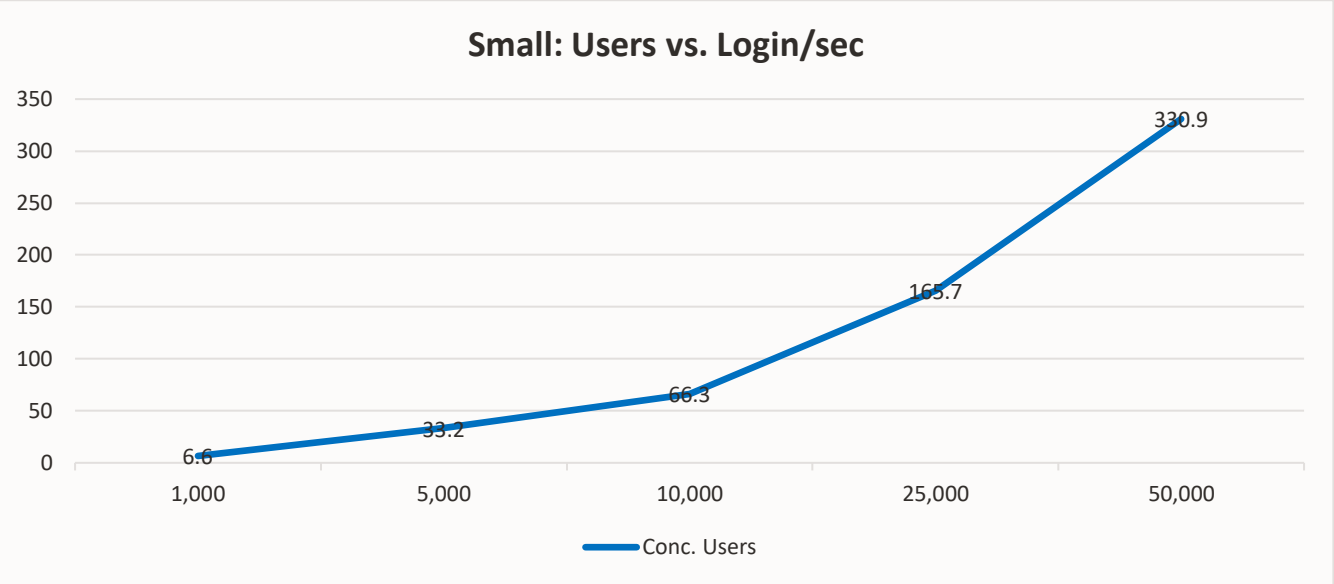
‘Small’ Configuration Benchmarks

The ‘Small’ configuration used Standard2.4 shapes for all its tiers, OAM, database, OUD and OHS.

Table 2-1: Small Configuration Benchmarks

Conc. Users	Login / hour	Login / sec	Avg RT, sec	90% RT, sec	OUD CPU Usage %	OAM DB CPU Usage %	OHS CPU Usage %	OAM1 CPU Usage %	OAM2 CPU Usage %
1,000	23.8K	6.6	0.019	0.023	0.8	4.2	1.1	3.1	-
5,000	119.5K	33.2	0.019	0.024	1.1	6.2	3.1	11.3	-
10,000	238.7K	66.3	0.023	0.030	1.7	12.6	6.1	22.2	-
25,000	596.5K	165.7	0.038	0.059	3.2	31.7	14.2	59.8	-
50,000	1.191M	330.9	0.056	0.063	5.9	55.2	29.2	55.2	60.7

Figure 2-1: No. of Users to TPS for a one and two OAM 'Small' configurations



The following are the observations from the user authentication scalability benchmarks for one and two OAM cluster nodes for 'Small' configuration:

- OAM has demonstrated near-linear scalability for the number of transactions per second (TPS) with the number of users for one and two OAM nodes.
- The average response time has been consistent in the range of 0.03-0.04 seconds for a single node, but went up to 0.056 sec for two OAM nodes with the doubled load in the system.
- The CPU % utilization rebalanced to 55% and 60% for OAM1 and OAM2, when the 2nd OAM node was added to the system and the workload increased to 50,000 concurrent users.

- OAM DB (single instance) CPU utilization has reached ~55% for 2 OAM nodes, and sustained the load for 'Small' configuration.
- OHS and OUD have not manifested any noticeable resource spikes and handled the system load for all tried scenarios.

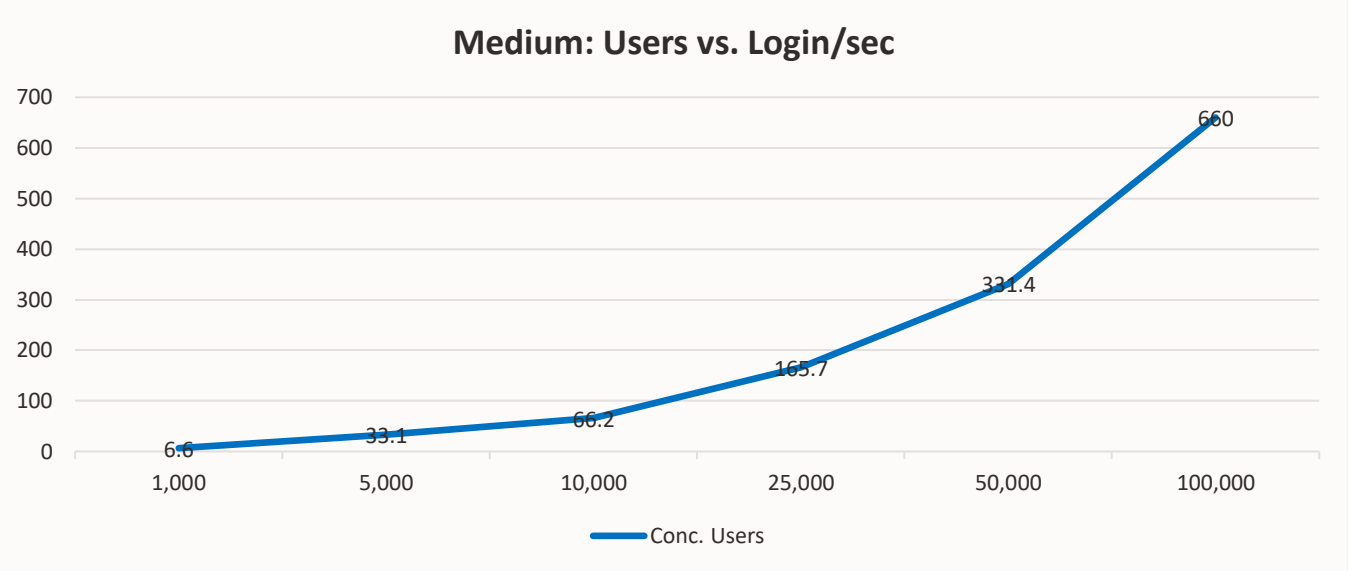
'Medium' Configuration Benchmarks

The 'Medium' configuration used Standard2.8 shapes for all its tiers, OAM, database, OUD and OHS.

Table 2-2: Medium Configuration Benchmarks

Conc. Users	Login / hour	Login / sec	Avg Response, sec	90% Response, sec	OUD CPU Usage %	OAM DB CPU Usage %	OHS CPU Usage %	OAM1 CPU Usage %	OAM2 CPU Usage %
1,000	23.8K	6.6	0.019	0.023	0.4	2.1	0.5	1.6	-
5,000	119.2K	33.1	0.019	0.024	0.6	3.1	1.2	4.1	-
10,000	238.3K	66.2	0.023	0.030	0.8	6.6	3.0	11.1	-
25,000	596.5K	165.7	0.030	0.042	1.6	12.9	6.2	22.3	-
50,000	1.193M	331.4	0.039	0.053	2.9	24.0	13.2	60.8	-
100,000	2.376M	660.0	0.253	0.622	5.1	54.1	59.6	65.5	63.8

Figure 2-2: No. of Users to TPS for a one and two OAM 'Medium' configurations



The following are the observations from the user authentication scalability benchmarks for one and two OAM cluster nodes for 'Medium' configuration:

- OAM has demonstrated near-linear scalability for the number of transactions per second (TPS) with the number of users for one and two OAM nodes.

- The average response time has been consistent in the range of 0.04-0.05 seconds but went up to 0.25 sec for two OAM nodes with the doubled load in the system.
- The CPU % utilization rebalanced to ~66% and ~64% for OAM1 and OAM2, when the 2nd OAM node was added to the system and the workload increased to 100,000 concurrent users.
- OHS Compute node CPU utilization has reached ~54% for 2 OAM nodes, and sustained the load for 'Medium' configuration.
- OUD and OAM DB have not manifested any noticeable resource spikes and handled the system load for all tried scenarios.

'Large' Configuration Benchmarks

The 'Large' configuration used Standard2.16 shapes for all its tiers, OAM, database, OUD and OHS.

Table 2-3: Large Configuration Benchmarks

Conc. Users	Login / hour	Login / sec	Avg Response, sec	90% Response, sec	OUD CPU Usage %	OAM DB CPU Usage %	OHS CPU Usage %	OAM1 CPU Usage %	OAM2 CPU Usage %
1,000	23.8K	6.6	0.019	0.023	0.1	1.2	1.0	0.8	-
5,000	119.5K	33.2	0.020	0.024	0.3	1.4	2.0	2.2	-
10,000	238.7K	66.3	0.021	0.028	0.4	2.3	3.1	4.4	-
25,000	594.7K	165.2	0.027	0.034	0.8	5.8	7.7	11.3	-
50,000	1.193M	331.6	0.032	0.040	1.1	11.6	9.6	25.9	-
75,000	1.789M	497.1	0.039	0.049	2.0	16.2	10.9	45.3	-
100,000	2.381M	661.4	0.131	0.475	2.9	25.1	14.0	63.0	-
150,000	3.370M	936.2	0.263	0.648	3.0	25.3	29.9	48.4	48.5

The following are the observations from the user authentication scalability benchmarks for one and two OAM cluster nodes for 'Medium' configuration:

- OAM has demonstrated near-linear scalability for the number of transactions per second (TPS) with the number of users for one and two OAM nodes.
- The average response time has been consistent in the range of 0.02-0.04 seconds but went up to 0.26 sec for two OAM nodes with the higher load in the system.
- The CPU % utilization rebalanced to 48% and 48% for OAM1 and OAM2, when the 2nd OAM node was added to the system and the workload increased by 50,000 concurrent users.
- OUD, OHS and OAM DB have not manifested any noticeable resource spikes and handled the system load for all tried scenarios.

Figure 2-3: No. of Users to TPS for a one and two OAM 'Large' configurations

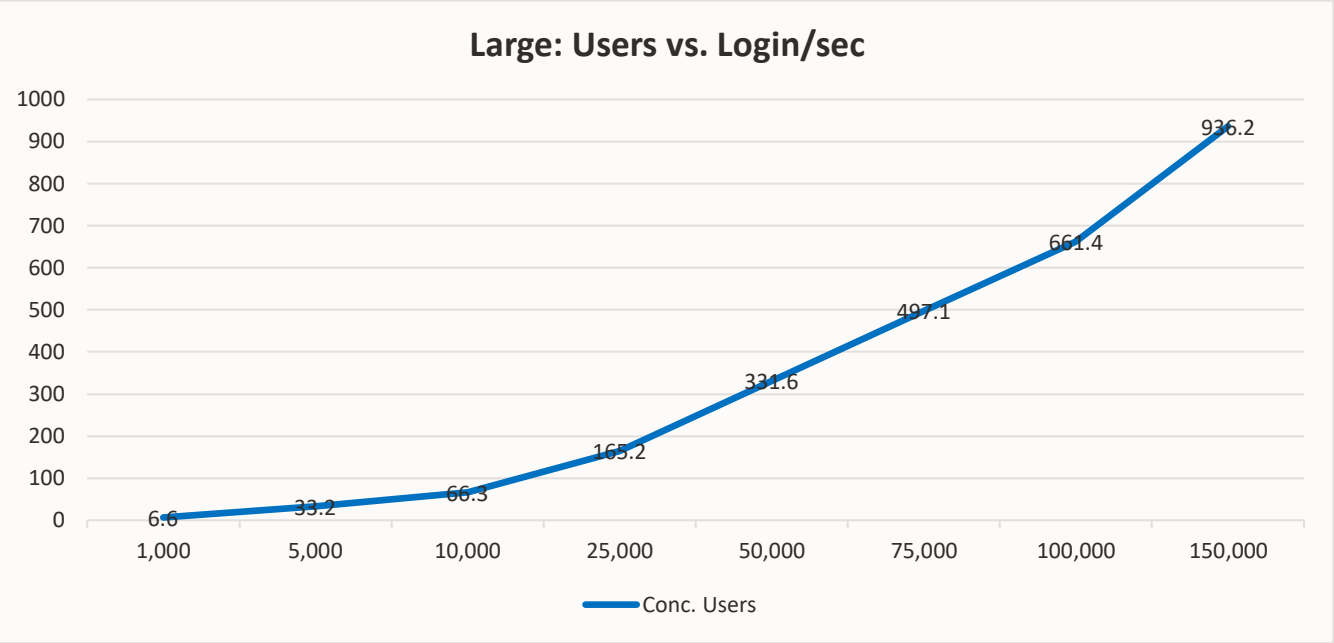
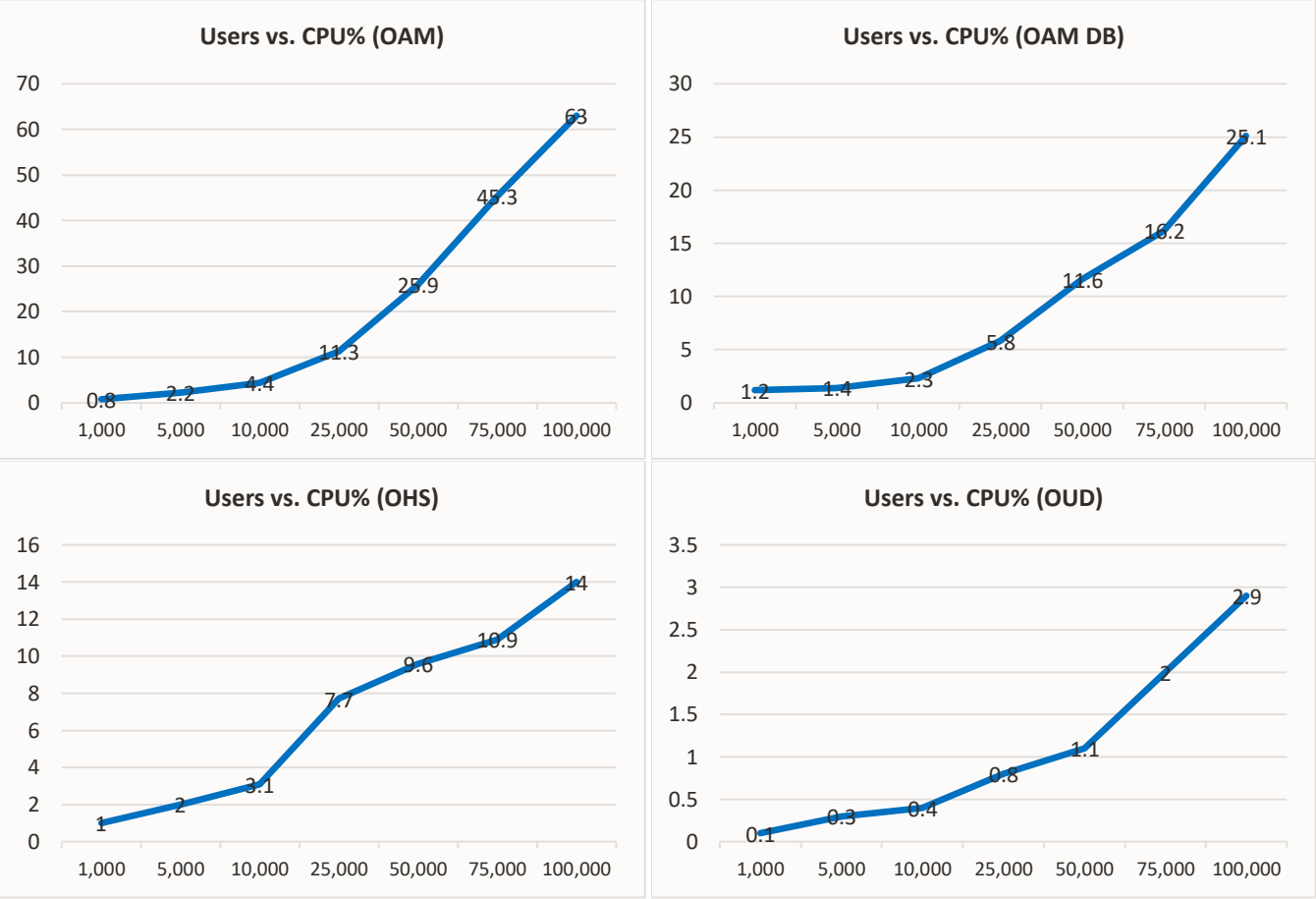


Figure 2-4: CPU% Utilization to No. of Users for a single OAM 'Large' configuration



PERFORMANCE TUNING

The performance tuning recommendations are common for all configurations. Shape specific recommendations are referenced explicitly throughout the section.

Webgate /Agent Side Performance Tuning

Webserver Tuning:

1. Set Max Connection to 50 for all managed OAM servers: OAM Console → Application Security → Agents → Server list → Primary Server List → Max Connections =50.
2. Validate the session properties: OAM Console → Configuration → Settings → Common Settings → Session Lifetime (minutes) = 5, Idle Timeout = 15, Max. session per user = 0.

Webgate Tuning:

1. Check that Webgate Max Connections is equal or higher than the sum of all managed servers' Max Connections.

OUD Tuning:

1. Set your 'User Identify Store' Connection pool size: OAM Console → Configuration → User Identity Stores → Select your created Identity store and click Edit → Connection Details → Min and Max Pool Size = 150.

OAM server Side Tuning

Host Tuning

Update the configuration file /etc/security/limits.conf:

```
*          hard    nofile      500000
*          soft    nofile      500000
root       hard    nofile      500000
root       soft    nofile      500000
*          hard    nproc       500000
*          soft    nproc       500000
```

Weblogic Tuning

OAM JVM Tuning

Edit the file $DOMAIN_HOME/bin/setDomainEnv.sh for all OAM servers:

```
if [ "${SERVER_NAME}" = "oam_server1" ] ; then
JAVA_PROPERTIES="${JAVA_PROPERTIES} -server -Xms8192m -Xmx8192m -XX:+UseParallelGC -
XX:+AggressiveHeap -XX:+DisableExplicitGC -DWLSAGENT_DISABLED=true -
XX:ReservedCodeCacheSize=1024m -XX:+PrintGCDetails -XX:+PrintGCTimeStamps -
Xloggc:${DOMAIN_HOME}/tmp/GC.log -XX:+UnlockCommercialFeatures -XX:+FlightRecorder -
Djava.security.egd=file:/dev/./urandom -Dweblogic.ProductionModeEnabled=true -
Dweblogic.Chunksize=8192 -DMaxRandomPoolSize=1000 -DMaxCipherPoolSize=1000 -
```

```
DMinRandomPoolSize=1000 -Dweblogic.threadpool.MinPoolSize=300 -
Dweblogic.utils.io.chunkpoolsize=8192"
export JAVA_PROPERTIES
fi
```

OAMDS DataSource Tuning

Update oamDS connection pool settings.

- Login to the WebLogic Server Console, click 'Lock & Edit'.
- Navigate to Domain Structure → Expand Data Sources → Data Sources → oamDS → Settings for oamDS → Configuration → Connection Pool.
- Update the values for Initial Capacity, Minimum Capacity to 100 and Maximum Capacity to 800
- Click OK and 'Activate Changes'.

Work Manager Tuning

OAPOverRestWM tuning

Add Minimum Thread constraint to worker manager "OAPOverRestWM"

- Login to the WebLogic Server Console, click 'Lock & Edit'.
- Navigate to Domain Structure → Deployments → Expand 'oam_server' → click click /iam/access/binding → Configuration → Workload → wm/OAPOverRestWM
- Click 'New' under 'Application Scoped Work Managed Components', select 'Minimum Threads Constraint' under 'Create a New Work Manager Component', click 'Next'.
- Set Count=400 under 'Minimum Threads Constraint Properties' and click Finish.
- Update the 'Path' In 'Save Deployment Plan' to the default path of your Plan.xml.
- Click OK and 'Activate Changes'.

Max Thread/CapacityConstraint Tuning

Remove Max Thread Constraint and Capacity Constraint:

- Repeat the same navigation steps as above.
- Under 'Application Scoped Work Managed Components' select the check box for Capacity and MaxThreadsCount. Click Delete.
- In the 'Delete Work Manage Components' screen, click OK to delete.
- Click on 'Release Configuration' and then Log Out.

OHS Server Tuning

Connect to your OHS Server take a backup and edit its configuration file:
file $ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/httpd.conf:

```
MaxKeepAliveRequests 0
Timeout 300
KeepAliveTimeout 10
```

Under <IfModule mpm_worker_module>:

```
StartServers              2
ThreadLimit             250
MaxClients             1500
```

```
MinSpareThreads         200
MaxSpareThreads         200
ThreadsPerChild         250
MaxRequestWorkers       400
MaxConnectionsPerChild    0
MaxRequestsPerChild       0
Mutex fcntl:${ORACLE_INSTANCE}/servers/${COMPONENT_NAME}/logs
```

Database Tuning

The database memory settings for pga_aggregate_target and sga_target should be set not to exceed 60% of available physical RAM on OAM DB tier.

Refer to the configuration parameters below:

```
fast_start_mttr_target  = 3600
session_cached_cursors  = 1500
sessions =7552
Processes = 5000
audit_trail = DB,EXTENDED
nls_sort = BINARY
db_securefile = ALWAYS
plsql_code_type = NATIVE SCOPE
"_b_tree_bitmap_plans" = FALSE
_active_session_legacy_behavior" = TRUE
_optimizer_batch_table_access_by_rowid" = FALSE
pga_aggregate_target =5G  #5Gb for Small, 20Gb (and higher) for Large configuration
sga_target =          10G #10Gb for Small, 40Gb (and higher) for Large configuration
```

CONCLUSION

This document consolidates the best practices and recommendations for sizing Oracle Access Manager 12.2.1.4.0 to ensure best performance and scalability.

GLOSSARY

- IDM – Oracle Identity Management
- OAM – Oracle Access Manager
- OCI – Oracle Cloud Infrastructure
- OHS – Oracle HTTP Server
- OUD – Oracle Unified Directory
- RAC – Oracle Real Application Cluster
- RT – Response Time
- TPS – transactions per second

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Deep Dive into Oracle Access Management 12.2.1.4.0 Performance
March 10, 2021
Contributing Authors: Pavel Buynitsky, Vijay Mangalgi, Sravya Madduri, Muthukumar Karunanidhi