ORACLE
FUSION MIDDLEWARE
IDENTITY AND ACCESS
MANAGEMENT SUITE

Migration Best Practices for Oracle Access Manager 10gR3 deployments

ORACLE WHITE PAPER | MARCH 2015

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.

Table of Contents

Introduction

Oracle recognized the need for comprehensive access management and has delivered a solution that addresses the broadest set of access management capabilities ranging from Web Single Sign On, Identity Federation and Security Token Services to Mobile Security, Social Identity and Fraud Prevention under a single umbrella. Oracle's truly unique Oracle Access Management 11gR2 platform provides comprehensive and internet scale Access Management in a single product, with innovative new services and simplified deployment and management.

Oracle Access Management Oracle Access Management 11gR2 (referred to as simply Oracle Access Management 11gR2) is a service component and the foundation of Oracle Access Management that provides the core functionality of web single sign-on, authentication, authorization, centralized policy administration and agent management, real-time session management and auditing.

Oracle Access Management 11gR2 provides the following benefits:

- Centralized policy management and auditing reduces cost and improves compliance.
- Support for access management in a heterogeneous environment reduces total cost of ownership and accelerates deployment.
- Flexible and powerful policy model allows organizations to meet complex access management needs.
- Scalable deployment model supports most demanding, internet scale deployments.
- Extensible architecture enables easy customization to meet organization specific requirements.

Existing OAM10g customers should consider migrating to Oracle Access Management 11gR2 to leverage the benefits described above and take advantage of the platform approach of Oracle Access Management 11gR2 to address new requirements beyond Web-SSO like mobile access, fraud prevention, web services security, cloud-based solution etc. Finally, OAM 10g customers should migrate to the 11g platform before 10g premium support ends.

This document describes the capabilities of Oracle Access Management 11gR2 that facilitate OAM10g customers to move to the new platform, the various migration strategies they can adopt and the best practices they should follow to ensure a smooth and successful migration.

Oracle Access Management 11gR2 maps only to the access management features of OAM 10g (OAM Access 10g) and this document refers to the migration of access policies and configuration from OAM 10g to Oracle Access Management 11gR2. The identity administration features of OAM 10g (OAM Identity 10g) including user self-service and self-registration, workflow functionality, dynamic group management, and delegated identity administration is provided through Oracle Identity Manager 11g, a component of the Oracle Identity Governance Suite.

Capabilities to support migration

While existing OAM10g customers would like to move to the new 11g platform to leverage the new benefits it provides, they will need a clear migration path that will ensure a smooth transition with minimal impact on their end users. Oracle Access Management 11gR2 provides the following three key capabilities to ease the migration.

- **Agent Compatibility.** Oracle Access Management 11gR2 provides Agent Compatibility in order to allow enterprises currently on OAM10g to continue using their existing 10g web-gates while upgrading their server infrastructure to the new 11gR2 platform. A Protocol Compatibility Framework allows the Access Manager server to communicate with 10g WebGates the same way it communicates with the new 11g WebGates. This capability is especially important for OAM10g customers with large deployments since they can focus on upgrading their server infrastructure first and adopt a more phased approach for replacing their existing 10g WebGates with new 11g WebGates over time.

- **Migration Utility.** In order to reduce the manual effort of migration, Oracle Access Management 11gR2 provides a WLST (WebLogic Scripting Tool) command line utility that enables the migration of policies and configuration from the existing OAM10g server to the new Oracle Access Management 11gR2 server. The artifacts that get migrated include Data Sources, Authentication Schemes, Resource Types, Host Identifiers, Agents and Policy Domains. It also brings over any delegated administration rights for specific Policy Domains. This migration utility takes, as an input, a property file containing the details of the policy and configuration store of the existing OAM10g server along with other migration parameters and then maps the OAM10g policy artifacts to the new 11gR2 policy model, reporting any incompatibilities that would need manual intervention in an Excel-based report. This utility can also be run in an assessment mode to analyze the incompatibilities and decide the appropriate course of action to resolve them.

- **Server Co-existence Support.**. In case of very large deployments with thousands of WebGates and applications spread across the enterprise, it may not be advisable to do the server migration at one go. To ensure zero down time migration, Oracle supports OAM10g and Oracle Access Management 11gR2 server co-existence to enable customers to gradually migrate from 10g servers to 11g over time. With server co-existence, both 10g and 11g servers can be live in production at the same time protecting different sets of applications while providing SSO across all applications.

Migration Strategy

Leveraging the above capabilities, customers can plan their migration strategy based on the overall size of the deployment. Typically, customers with small to medium deployments should consider doing a complete migration of the servers in one shot though they can replace 10g WebGates with 11g WebGates over a period of time. Large deployments should consider a phased incremental approach for the server migration as well with the 10g and 11g servers co-existing during the migration.

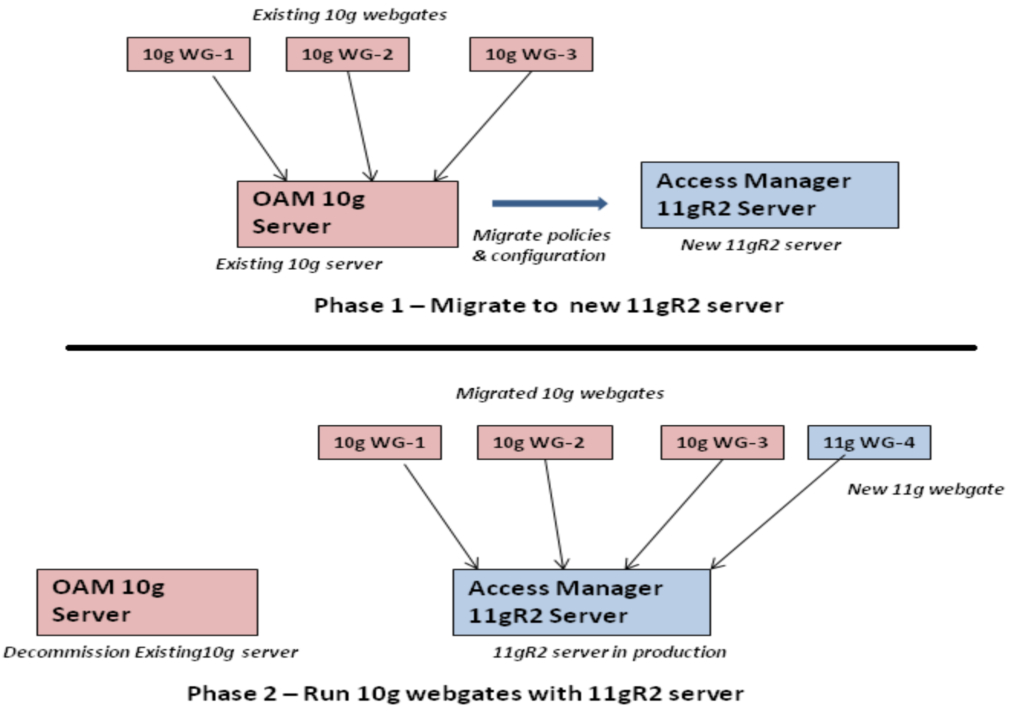

Existing 10g webgates
10g WG-1
10g WG-2
10g WG-3
OAM 10g Server
Existing 10g server
Migrate policies & configuration
Access Manager 11gR2 Server
New 11gR2 server
Phase 1 – Migrate to new 11gR2 server
Migrated 10g webgates
10g WG-1
10g WG-2
10g WG-3
11g WG-4
New 11g webgate
OAM 10g Server
Decommission Existing10g server
Access Manager 11gR2 Server
11gR2 server in production
Phase 2 – Run 10g webgates with 11gR2 server

Figure 1. Migration from OAM10g to 11gR2 without server co-existence

Figure 1 above depicts how an organization would migrate from their current OAM10g platform to the new Oracle Access Management 11gR2 platform without using server co-existence mode. Using migration utilities, organizations will do a complete migration of policies and configuration from the existing OAM10g server to the new Oracle Access Management 11gR2 server in Phase 1. Once migrated, the existing OAM10g server will be decommissioned while the migrated 10g WebGates will start working with the new Oracle Access Management 11gR2 server during Phase 2. Any new applications deployed during this phase can start using a new 11g WebGate that will communicate with the Oracle Access Management 11gR2 server.

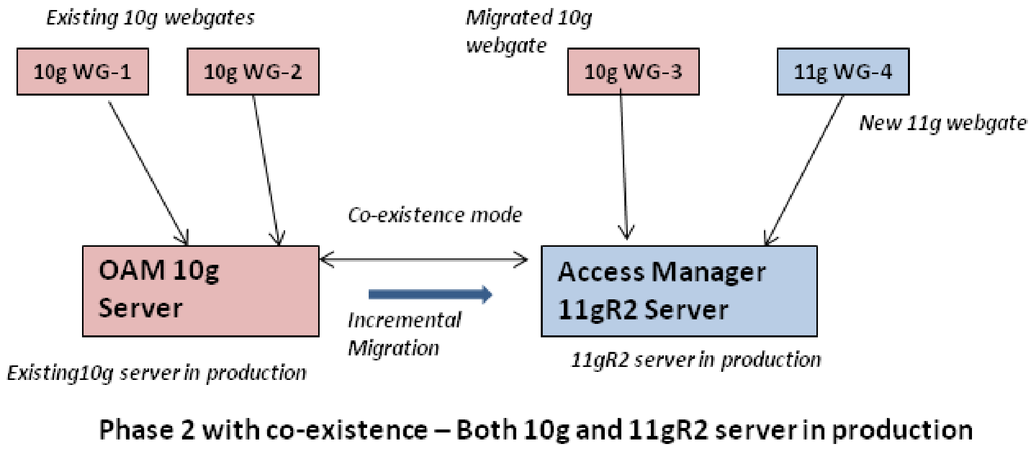

Existing 10g webgates
10g WG-1
10g WG-2
Migrated 10g webgate
10g WG-3
11g WG-4
New 11g webgate
Co-existence mode
OAM 10g Server
Access Manager 11gR2 Server
Incremental Migration
Existing10g server in production
11gR2 server in production
Phase 2 with co-existence – Both 10g and 11gR2 server in production

Figure 2. Difference in Phase 2 by introducing server co-existence.

Figure 2 above shows how Phase 2 would differ in case an organization chooses to do the server migration over time and therefore configures the existing OAM10g server and the new Oracle Access Management 11gR2 server in a server co-existence mode. In this case, the migration of policies and configuration from OAM10g server to the new Oracle Access Management 11gR2 server will happen in increments. At any point in time, some of the 10g WebGates will continue to work with the existing OAM10g server whereas the migrated 10g WebGates along with any new 11g WebGates will start working with the Oracle Access Management 11gR2 server. This phase will continue till all the 10g WebGates have been migrated to the Oracle Access Management 11gR2 server and the OAM10g server can be eventually decommissioned.

While the migration utility provides a simple way to move policies from 10g to the 11g platform, it may not necessarily be the optimal solution for very small deployments where the number of WebGates and policies are low (less than 20). In such cases, customers can choose to manually recreate policies in the 11g server and register either existing 10g WebGates or new 11g WebGates against it.

Migration Best Practices

Following are some recommended best practices to ensure a smooth migration from OAM10g to Oracle Access Management 11gR2.

Familiarize with Oracle Access Management 11gR2

The admin user interface and navigation as well as a number of artifact names in the 11gR2 platform are significantly different from the 10g platform. It is highly recommended that customers planning to migrate to the new 11gR2 platform invest time to acquaint themselves with new terminology and user interface. Administrators should go through the 11gR2 product documentation to familiarize themselves with concepts and terminology in 11gR2 and how this maps to their existing 10g nomenclature. For example, Policy Domain in 10g is referred to as Application Domain in 11g or the Policy Manager in 10g maps to the Oracle Access Management console in 11g and so on.

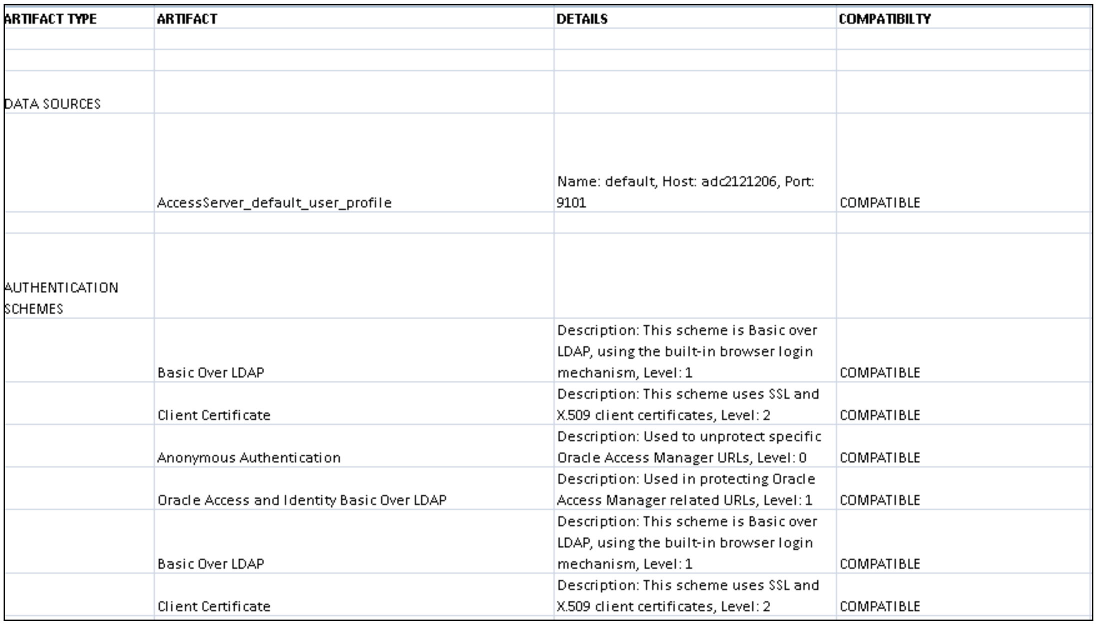
Similarly, policy administrators should also learn how the 11g policy model maps to the 10g policy model and be aware of the key differences between the two. For example, OAM 10g default behavior allowed access when a resource was not protected by a rule or policy that explicitly denied access. Oracle Access Management 11gR2 default behavior is to deny access when a resource is not protected by a policy that explicitly allows access.

Understanding these differences and familiarizing oneself with the 11g interface and policy model before starting on the migration would go a long way in ensuring a smooth migration.

Run Migration in Assessment Mode

The migration tool can be run in an assessment or preview mode where it goes through the 10g policy and configuration store and creates a preview report on all the artifacts to be migrated. The Excel-based report provides details on every artifact, whether it is fully compatible, partially compatible or incompatible with the 11g policy model and what manual action, if any, will be required post-migration. For example, authentication schemes containing custom authentication plugins or WebGate profile names greater than 255 characters in length are considered incompatible and cannot be migrated. Similarly, if the host name variation is in the incorrect format or the port value is non-numeric, it is considered to be partially compatible needing some manual intervention after migration. Figure 3 below depicts a screenshot of the excel-based preview report.

Running the tool in an assessment mode can provide customers with a lot of useful insight on what manual effort, if any, will be required for the migration and an approximate idea of how long the actual migration would take. It is recommended that OAM10g customers should first run the tool in assessment mode and use the generated report for creating a migration plan. Administrators can also decide whether they want to fix these incompatibilities in the 10g policy store itself before running the actual migration or whether they would prefer to manually create or edit these artifacts in the 11g store after migration. The migration tool can be run any number of times in the assessment mode, allowing administrators to make the fixes in the 10g policy store over time.



ARTIFACT TYPE	ARTIFACT	DETAILS	COMPATIBILTY
DATA SOURCES			
	AccessServer_default_user_profile	Name: default, Host: adc2121206, Port: 9101	COMPATIBLE
AUTHENTICATION SCHEMES			
	Basic Over LDAP	Description: This scheme is Basic over LDAP, using the built-in browser login mechanism, Level: 1	COMPATIBLE
	Client Certificate	Description: This scheme uses SSL and X.509 client certificates, Level: 2	COMPATIBLE
	Anonymous Authentication	Description: Used to unprotect specific Oracle Access Manager URLs, Level: 0	COMPATIBLE
	Oracle Access and Identity Basic Over LDAP	Description: Used in protecting Oracle Access Manager related URLs, Level: 1	COMPATIBLE
	Basic Over LDAP	Description: This scheme is Basic over LDAP, using the built-in browser login mechanism, Level: 1	COMPATIBLE
	Client Certificate	Description: This scheme uses SSL and X.509 client certificates, Level: 2	COMPATIBLE

Figure 3. Excel-based Assessment Report generated by migration tool.

Pre-Migration Tasks

There are a few steps administrators should pay close attention to before running the actual migration. Migration for large deployments with thousands of policy artifacts will need sufficient memory for processing. The Java heap size for the WebLogic Administration Server should be increased as needed prior to running the migration. Also, the size of the log file should be increased to ensure the migration logs are not lost during rotation of the log files.

As a part of the migration parameters specified as input, administrators need to specify the agent_mode_to_override parameter which indicates what mode will the agents be migrated – Open, Simple, Cert or retain the existing mode. It is important to decide this prior to the migration to avoid inconsistencies or manual reconfiguration after the migration.

Like any software migration process, it is recommended to take adequate back-ups of the source and target environments to restore in case of unforeseen failures.

Leverage Incremental Migration and Co-existence Support

In case of very large deployments with thousands of WebGates and applications spread across the enterprise, it may not be advisable to do the server migration at one go. In such cases, customers can choose to perform the migration in increments over a period of time. As part of the migration parameters specified as input, administrators can specify the migration mode as Incremental and provide an include or exclude file which will contain the list of agents and policy domains that they specifically want to include or exclude in that particular increment. Administrators can leverage the assessment report generated earlier to create these include or exclude files instead of manually creating them to minimize human errors. This approach helps customers to perform migration in a phased approach over time. For example, a deployment with 1000 applications can choose to do the migration in 10 increments of 100 applications over a period of 6 months. The migration can be run in incremental mode any number of times while it can be run in complete mode only once at the end.

Customers that choose to perform their migration in increments will need to configure their OAM10g and Oracle Access Management 11gR2 servers in co-existence mode till they complete the migration so end users can have a seamless SSO experience as they navigate between applications protected by the two sets of servers.

Customers with very large deployments can thus take advantage of the incremental mode of migration and co-existence support to mitigate the risk of a single “big-bang” migration.

Post-Migration Tasks

The migration takes care of copying the artifacts from the 10g policy store to the 11g policy store. But there are a few steps needed at the end of every migration run to actually associate the migrated WebGates to the Oracle Access Management 11gR2 server. This can be done by creating a new server profile through OAM 10g Access System console with the hostname and port details of the Oracle Access Management 11gR2 server instance and propagate this information to the migrated web gates. The webserver hosting the migrated WebGate will need to be restarted for the change to take effect immediately.

Needless to say, the most critical post-migration task is to verify whether the migration has been performed correctly. Administrators should also login to the admin console and visually verify whether all artifacts have gotten migrated properly and check the log files for any errors or warnings. They should plan to test various migrated policies and verify whether runtime behavior is as expected. The Access Tester utility that ships with 11gR2 can be leveraged for this testing.

Server Co-existence

Co-existence Topology

As explained in the previous section, customers with large deployments that choose to perform their migration in increments will need to configure their OAM10g and Oracle Access Management 11gR2 servers in co-existence mode till they complete the migration.

Starting Patch Set2 (11.1.2.2), Oracle Access Management 11gR2 supports a co-existence model with OAM10g, where both of them are able to work off the same ObSSOCookie and provide an SSO experience for end users as they navigate between applications protected by the two servers. The SSO session can start from either an OAM10g protected application or a 11gR2 protected application and depending on this, the end user would get either the 10g login page or the 11gR2 credential collector. There is no restriction on the type of Authentication Scheme used to protect the applications. Applications protected by Oracle Access Management 11gR2 can be sitting behind a 10g WebGate or 11g WebGate.

Figure 4 below depicts such a topology where Resource A is protected by a 11g WebGate and Resource C is protected by a 10g WebGate, both talking to a Oracle Access Management 11gR2 server and Resource B is protected by a 10g WebGate talking to a an OAM10g server. The end user can start his SSO session by accessing any one of these resources and then navigating to the others. A DCC WebGate plays the key role of encrypting/decrypting the ObSSOCookie that can also be understood by the OAM10g server.

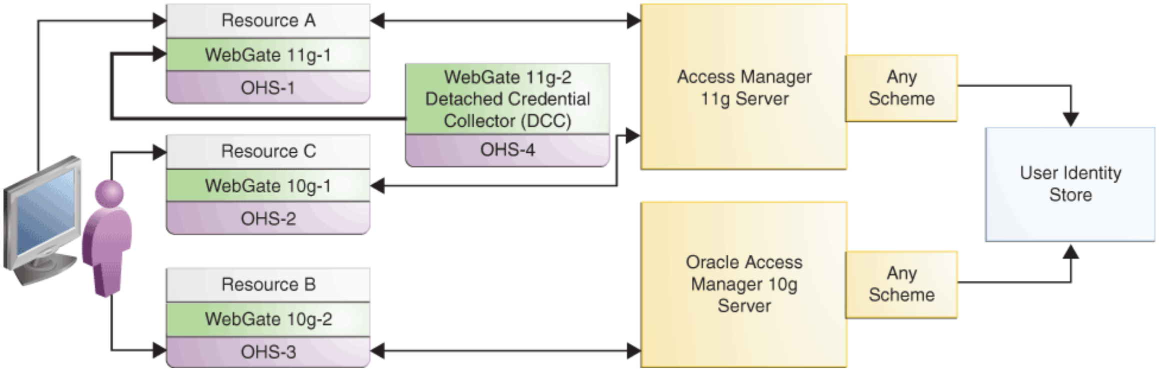


Figure 4. Topology for Co-existence between OAM10g and Oracle Access Management 11gR2

Co-existence Limitations

Following are some of the limitations of a server co-existence deployment

- Since Server co-existence works on the basis of 10g ObSSOCookie , certain 11g server side session capabilities do not apply. Only a single unified session is created in 11g.
- Maximum session limit for a user cannot be imposed and administrators cannot purge a user’s sessions. As long as user has a valid ObSSOCookie, he will be able to stay authenticated.
- Authentication level and Idle time out for a session are driven by values in the ObSSOCookie not the 11g server.
- Multi-data center (MDC) deployments are supported while on co-existence, but session data cannot be retrieved from one data center to the other.

Conclusion

Oracle’s new, innovative Oracle Access Management 11gR2 platform is the most complete and scalable access management solutions in the market and customers on existing OAM10g platforms should strongly consider migrating to the new 11g platform to take advantage of the various benefits it has to offer. Oracle Access Management 11gR2 also provides a clear migration path consisting of agent compatibility, migration utility and server co-existence support which enables customers to have a smooth and successful migration.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Hardware and Software, **Engineered to Work Together**

MIGRATION BEST PRACTICES FOR ORACLE ACCESS MANAGER 10GR3 DEPLOYMENTS
March 2015
Author: Venu Shastri
Contributing Authors: Svetlana Kolomeskaya, Forest Yin