Oracle Waveset to Oracle Identity Manager Migration Guidelines

A White Paper

February 2011

Contents

1. Introduction

After the acquisition of Sun Microsystems by Oracle Corporation, Oracle has announced that Oracle Identity Manager will be the strategic Identity Administration and Provisioning product moving forward, with Oracle Waveset (formerly Sun Identity Manager) going into 'sustain and converge' mode. All customers that have currently deployed Oracle Waveset are encouraged to migrate to Oracle Identity Manager.

However, Oracle understands that customers may not be able to undertake such a migration immediately. Project objectives and deadlines may force customers to postpone a migration till a more suitable time. In the meantime, these customers will continue to invest in their Waveset deployments, and are concerned about increasing their migration burden in doing so.

To that end, the objective of this whitepaper is to provide Oracle Waveset customers a high level guidance on how to continue to invest in their current Waveset deployment in a manner that is migration friendly. When Oracle releases the OW to OIM migration toolkit it will be accompanied by a detailed documentation on how each of the low level constructs in OW can be auto, partial or manually migrated to OIM.

As a general readiness guideline, customers are advised to upgrade their OW deployments to the 8.1.x version prior to migration or use the OW in-place upgrade scripts as an intermediate step during the migration process. This will allow OW customers to upgrade to *Identity Connector* framework based connectors thereby enabling them to leverage any new or updates to the connectors provided by Oracle.

2. References

- Oracle Waveset 8.0 documentation:
  http://download.oracle.com/docs/cd/E19225-01/index.html
- Oracle Identity Manager 11g documentation :
  http://download.oracle.com/docs/cd/E14571_01/im.htm#oim

3. Architecture Overview and Analysis

Both Oracle Waveset (OW) and Oracle Identity Manager (OIM) address a wide-range of enterprise level user provisioning and administration needs. This section provide a quick overview of the building blocks of each of these products, analyses and map each of the product components in OW and OIM and also provide some of the special migration considerations/guidelines for Waveset customers.

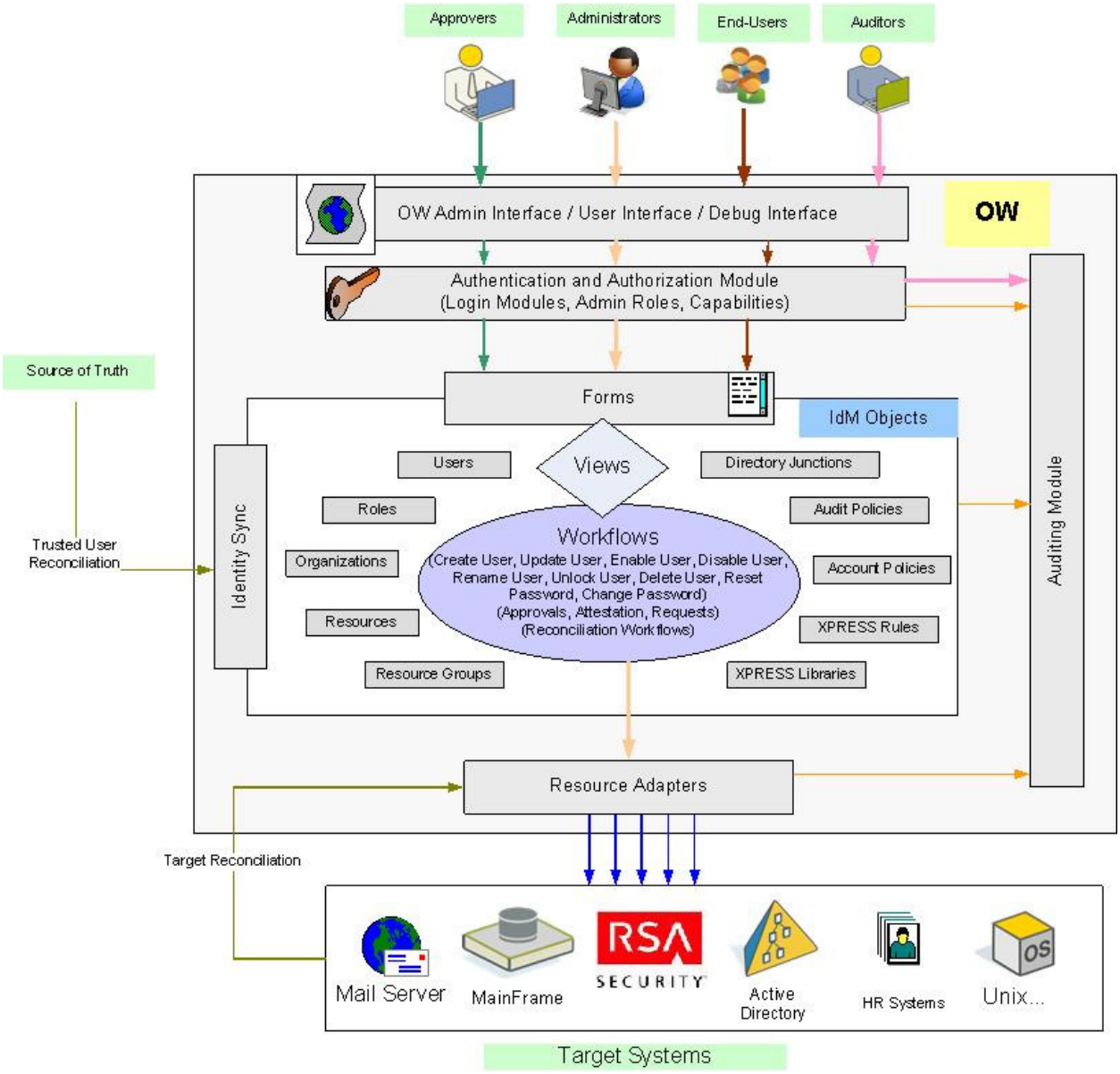

Figure 1: Oracle Waveset Component Architecture

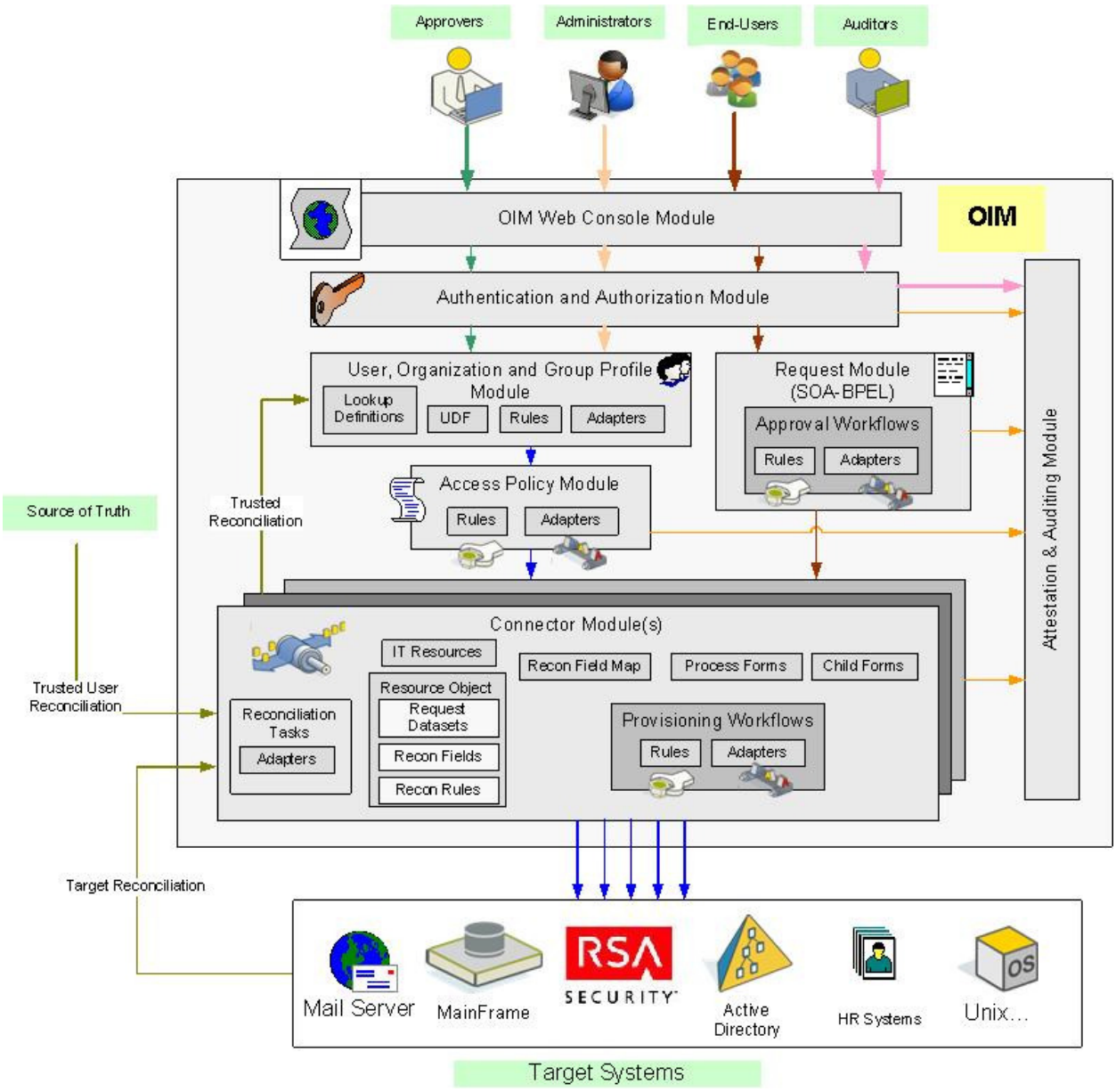

Figure 2: Oracle Identity Manager Component Architecture

3.1 User Interface

OW follows the MVC architecture for its various interfaces, Admin Interface, User Interface and Debug Interface (for troubleshooting and maintenance).

OIM follows Web 2.0 technology for its interfaces, Self Service Interface, Administrator console and Advanced Administrator console. It uses Oracle JDeveloper as the IDE tool for developing and deploying workflow objects etc.

Special Considerations

- As each product follows a completely different technology for its user interfaces, any customizations done on the Oracle Waveset web module would have to re-evaluated and if needed, implemented in OIM post migration.

3.2 Enterprise Identity Data Objects

a) Organization

In Waveset, Organizations enable logical and secure management of user accounts and administrators and are used to limit access to resources, applications, roles and other Waveset objects. The concept of Waveset organization directly maps to the OIM organization constructs with the field/data visibility controlled by OIM's Administrator Roles capabilities and enforced using Oracle Entitlement Server based fine grained authorization policies.

Special Considerations

- Attestation and Remediation Operations

  OW supports definition of organization-level forms for attestation or remediation operations. OIM supports these functions to be performed at a global level with the attestation policy having the capability of supporting scoping based on organization, users, roles and resources. Customers are advised to consider Oracle Identity Analytics (OIA), Oracle's strategic product for compliance and governance features, which can address all attestation and remediation operations needed.

- User Member Rules
  In OW, a user is statically associated with a single organization but user membership to an organization can be dynamically specified using a rule based assignment. OIM also allows a user to be statically associated with a single organization and uses the OIM roles concept with auto-membership rules to associate users dynamically to organizations.
- Default Organizations
  OW defines three default organizations ("Top", "All", "End-user") out of the box whereas OIM supports a hierarchy based static Organization assignment with "Xellerate Users" organization representing the default out of the box Organization. For new organization definition, OW customers are advised to limit the usage of "All" and "End-User" Organizations, instead define all capabilities within the "Top" organization.

b) Role

A role is an OW object that allows resource access rights to be grouped and efficiently assigned to users. The concept of an OW role maps directly to the concept of an OIM role.

Special Considerations

- Role Types
  In OW, roles are organized into four role types, Business Roles, IT Roles, Applications and Assets. OIM roles supports role hierarchy and nesting definition, role categories and the ability to define extended attributes on the role object all or any of these can be used to address the role type categorization in OW.
- Role-Resource Associations
  In OW, IT Roles/Application Roles can be associated with Resources and Resource Entitlements. This defines which resources and entitlements within a resource will get automatically provisioned to a user when they get assigned these roles. Entitlements can be specified either as "Text" value or "XPRESS Rule" and setting mechanism can be specified as "Default value", "Set to value", "Merge with value", etc.

  IT Roles/Application Roles feature of OW corresponds to the Access Policy construct in OIM. The entitlements for each of the resource in the access policy need to be pre-determined and specified during access policy definition. For this reason, customers are advised to make use of the "Text" value functionality when defining entitlements for a resource in the Role-Resource association definition.

- Contained Role Association Type

  In OW, the Contained Role association type can be set to either "Required", "Conditional" or "Optional". If the association type is set to "Conditional" an XPRESS rule defines when the role containment should occur. In OIM, as Roles definition needs a pre-determined list of access rights to be defined, customers are advised to make use of the "Required" association type to the maximum extent possible.
- Role Exclusions

  In OW, role exclusion allows a form of SoD around roles. OIM does not have any corresponding feature, and relies on the integration with OIA to provide this capability. If the role exclusion implies a resource exclusion, this could be modeled in the Access Policy using its "Deny" capability.
- Role Owners

  In OW, role owners have the responsibility to approve changes to the role definition. More than one user can be assigned as a role owner or the list of role owners can be evaluated using an XPRESS rule.

  Oracle's strategic product for Role management, OIA, has all (and additional) constructs that supports similar functionality. In OIM a single user can be designated statically as the role owner and multiple owners can be represented using additional user defined fields in the role object. Customers are advised to limit the usage of XPRESS rules to evaluate the list of role owners to the extent possible in order to have this construct a candidate for automated migration to OIM.
- Role Approvers

  In OW, more than one user can be specified as the approver for handling role assignment requests. It can also be specified using an XPRESS rule. In OIM, this list of approvers can be modeled as an OIM role (with auto-membership rules) which can be used in the creation of the role-assignment approval policy.

  XPRESS rules that support certain dynamic approver determination based on context may not map directly to the OIM role in the approval policy, and may therefore require definition or usage of an existing workflow composite with approver determination rules in OIM that accurately reflect the customer policies.

c) User

A user is an OW object that encapsulates a person of interest in the identity administration and provisioning engine. The concept of an OW user maps directly to the concept of an OIM user.

Special Considerations

- Organization Membership

  In OW, a user is statically associated with a single organization but user membership to an organization can be dynamically specified using a rule based assignment. OIM also allows a user to be statically associated with a single organization and uses the OIM roles concept with auto-membership rules to associate users dynamically to organizations.
- Resource Exclusions

  In OW, resource exclusion provides a way to specify resources that cannot/should not be provisioned at a user level. OIM addresses resource exclusion at the Access policy level that will get evaluated for each user belonging to the corresponding role during the policy evaluation.
- Admin Roles and Capabilities

  The OW User Admin Roles and Capabilities provides a way to define what an OW user is authorized to do within the system. OIM provides this feature through its embedded authorization engine (OES). Authorizations are defined at the Role level in OIM and hence customers are advised to avoid defining authorization policies on a per user basis in OIM.
- Controlled Organizations

  The Controlled Organizations attribute in OW is used to specify organizations that the user has rights to manage as an administrator. OIM addresses this functionality using the role and authorization policy constructs. Every organization in OIM will have an organization administrator role and any user added to this role will have administration capabilities on that organization.
- User Form and View User Form

  These forms allow OW to control what the organization administrator can view on a user in that organization. This capability maps to the Authorization Policies for User Management (with fine-grained attribute controls) construct in OIM. Customers are advised to avoid usage of Forms at User Level rather define authorization policies at a Role level as is done in OIM.

- Delegations

  The OW Delegation concept allows the user to delegate certain system level responsibilities to another user. This feature maps to the OIM Proxy feature. OW stores information about current, new and past proxies as does OIM.

  In OW the feature has some fine-grained capabilities that allow the user to select the type of "Work Items" (e.g. Role Approval, Organization Approval, etc) and assign a delegate for each of these Work Items. In OIM, a delegate/proxy user will have the responsibility to perform all approval functions of the original user and hence customers are advised to consider defining a single delegation for all Work Items, avoid defining overlapping delegation and avoid usage of the "Forward Approvals To" field in the User profile.
- Attestation and Remediation Operations

  OW supports definition of user-level forms for attestation or remediation operations. OIM supports these functions to be performed at a global level with the attestation policy having the capability of supporting scoping based on organization, users, roles and resources. Customers are advised to consider OIA, Oracle's strategic product for compliance and governance features, which can address all attestation and remediation operations needed.

d) Resource

The heart of a provisioning system is its ability to manage accounts on target systems, referred to as Resources in the conceptual architecture. Both OW and OIM have comprehensive capabilities to manage resources, with features that map to each other.

Special Considerations

- Identity Templates

  The Identity Template feature defines syntax for user accounts and is useful for hierarchical namespaces. This may be used while specifying how to auto-generate the value for account attributes (e.g. specifying the syntax of how to create the user DN for an AD user account). OIM provides similar capability with the use of pre-populate plug-ins that can be used to generate values for various account attributes.
- Resource Object versus Resource Instance Level Configurations

  OW supports the ability to configure a number of provisioning features per resource instance. This includes capabilities like Account Attributes, Account Features Configuration (individual connector features/operations like Create, Update,

Rename, Disable, Enable can be disabled and an action can be configured if such an operation is attempted for each resource instance), Identity System Parameters (Retry Configuration), Password Policy and Approvers.

In OIM, some of these configurations are defined at the resource object level, and so configurations are applicable to all resource instances associated with that resource object. If a customer needs the ability to define these configuration on a per resource instance basis, they should consider defining each of these resource instances as its own resource object instead of using the same (shared) resource object with multiple IT resources.

- Organization Scope
  OW allows the visibility of a resource instance to be scoped to a specific organization or a set of organizations. In OIM, resources (not instances) can be scoped at the Organization level rather than at a resource instance level. . If a customer needs the ability to scope resources at a per resource instance basis, they should consider defining each of these resource instances as its own resource object instead of using the same (shared) resource object with multiple IT resources.

3.3 Schema, Templates and Policy Objects

a) IDM Schema Configuration

User and Role extended, query-able, and summary attributes are defined in the IDM Schema Configuration object in OW. The OW User Extended Attributes directly maps to the OIM User Configuration and Role User Defined Fields objects.

Special Considerations

- Multi-Valued Attributes

  OW supports attributes to be specified as multi-valued for User, Role and Resource entitlement entities while OIM supports multi-valued attributes for Resource entitlements only. For existing multi-valued attributes in User and Role entities in OW, the OW to OIM Migration tools that will be provided by Oracle will have the capability of converting them to comma separated values and storing the value in a single text field. As part of the migration solution, Oracle will be able to provide samples that will address the customizations required for OIM LDAP synch, reconciliation and provisioning of these single text field attribute to the corresponding multi-valued attributes in the target systems.

b) Email Templates

OW and OIM use email templates to deliver information and requests for action to users and approvers. OIM uses the Notification Service to perform all notification-related operations including localization support.

Special Considerations

- Template Attributes

  OW has a pre-determined set of variables that are allowed in the Email body whereas OIM supports event sensitive variables to be defined during Email template definition. For example, request data and beneficiary data variables are available for Request based email templates. The migration tools will be able to migrate the Email templates except for the dynamic variables which can be configured in OIM once these templates are migrated to OIM.

c) Account and Account ID Policy

OW supports Identity System Account Policies (establish user, password and authentication policy options and constraints) and Resource password and Account ID policies (define length rules, character type rules and allowed words and attribute values).

OIM supports support username generation and validation as a standard feature. Customers have the flexibility to extend or create their customized plug-ins that defines the rules by which valid and unique usernames are generated and validated.

Special Considerations

- OW Account Policy Attributes

  Some of the OW Account Policy characteristics like Password provided by user/ generated, Reset option (permanent/temporary), Reset temporary password expires in (Days/Weeks/Months), Reset notification option (immediate, email, administrator), Password change or reset limit (Number of times in Days/Weeks/ Months) and Answer Quality Policy have no direct mapping with OIM constructs, though many of these can be achieved using custom plug-ins and scheduled tasks in OIM. Customers are advised to limit the use of Authentication Question Policies (All, Any, Next, Random, Round Robin) in OW as OIM currently supports static displays of all Challenge Q&A set at a system wide level.

- Account ID Policy Attributes

  Some of the Account ID Policy characteristics in OW like Account Lock expiry time for failed password and challenge question login, Max number of failed login attempts for password, Max number of failed login attempts for challenge question authentication and List of challenge questions are currently supported as a system-wide setting in OIM.

- Organization Scope

  OW allows the Account and Account ID policy to be scoped and specified at organization and resource levels. In OIM this can be achieved by extending the plug-ins available for Account and Account ID policy generation and validation.

d) Password Policy

Password policies establish limitations for passwords so that users provide strong passwords for authentication. The OW Password Policy object maps to the OIM Password Policy object. Both OIM and OW provide configurable password policy mechanisms that can be assigned at organization and resource level.

Special Considerations

- Password Policy Attributes

  Some of the OW Password Policy characteristics like Minimum number of character type rules that must pass, Character rule – Max Sequential, Character rule – Min Begin Alpha, Character rule – Min Begin Numeric, Character rule – Min Embedded Numeric, Character rule – Max Embedded Spaces, Character rule – Max Alpha, Character rule – Max Numeric, Character rule – Max Special, Character rule – Max Uppercase, Character rule – Max Lowercase, Max number of similar characters from previous passwords that cannot be reused and Must not contain words have no direct mapping with OIM though each of these additional characteristics can be enforced at the password validation stage by developing a custom plug-in. Customers are advised to limit the usage of these characteristics to the extent possible.

e) Reconciliation Policy

Reconciliation policies allow establishing a set of responses, by resource, for each Reconciliation task. Within a policy, it allows selection of the server to run reconciliation, determine how often and when reconciliation takes place, and set responses to each situation encountered during reconciliation. It can also be configured to detect changes made natively on the target systems to account attributes. OIM supports similar functionality using the Scheduled Task and Reconciliation Rule constructs.

Special Considerations

- Reconciliation Policy Attributes

  Some of the OW Reconciliation Policy characteristics like Account Confirmation Rule, Per-account workflow, Error Limit, Maximum natively removed accounts and Proxy Administrator to perform reconciliations have no direct mapping with OIM and hence customers are advised to limit the usage of these characteristics during Reconciliation policy definition.

3.4 Administration and Authorization Objects

a) Capabilities

Capabilities are groups of rights in the Waveset system. Capabilities represent administrative job responsibilities, such as resetting passwords or administering user accounts. Not all Waveset users need capabilities assigned. Only those users who will perform one or more administrative actions through Waveset will require capabilities. Capability definitions map to permissions/privileges present within OIM Authorization Policies.

Special Considerations

- Supported Capabilities

  Customers are advised to make use of the following User and Role Administration capabilities in OW as these have a direct mapping to OIM and can be automatically migrated to OIM. Create User, Update User, Bulk Update Users, Rename User, View User, Unlock User, Bulk Unlock User, Disable User, Enable User, Bulk Enable User, Bulk Disable User, Change Password Administrator, Reset Password Administrator, Password Administrator, De-provision User, Delete IDM User, Bulk Delete IDM User, Bulk Delete User, User Account Administrator, Account Administrator, Bulk User Account Administrator, Bulk Account Administrator, Change User Account Administrator, Change Account Administrator, Bulk Change User Account Administrator, Bulk Change Account Administrator, End User Administrator, Business Role Administrator, Role Administrator, View Business Role and View Role.

b) Admin Roles

Oracle Waveset admin roles allows to define a unique set of capabilities for each set of the organizations that are managed by an administrative user. An admin role is assigned capabilities and controlled organizations, which can then be assigned to an administrative user. Admin Roles in OW map to OIM roles and Authorization Policies.

Special Considerations

- Supported Capabilities

  Customers are advised to limit the use of "Controlled Organizations Rule", "Capabilities Rule", "Controlled Organizations User Form", "Assigners", "Objects to include or exclude" and "Assign to Users Rule" during creation of new Admin Roles as they don't have a direct mapping with OIM Constructs.

3.5 Business Logic and Process Data Objects

a) Workflows

OW provides a workflow engine that performs orchestration of various OW operations. In OW, Workflows mean any process by which work gets done. The workflow can be initiated via a form submit, an SPML call, a WF services API call, reconciliation, administrator driven activity etc.

OIM uses the human workflow process of Oracle SOA-BPEL suite for approval workflows and a kernel level orchestration layer in the form of event handlers and plug-ins to address all other provisioning workflow processing. It also does not rely on any proprietary scripting language for setup, configuration, or process modeling rather follows a standards based approach that is both configurable and customizable.

Since the two products differ completely in the way they execute workflows, it is evident that migration of these constructs from OW to OIM may not be completely migratable. To that effect, as part of the migration methodology, Oracle will provide industry wide commonly used request approval workflow composites like Manager Approval, Approval by Role, Entitlement or Resource Owner, Compliance Office Approval, Approval by a Role/Person in a specific Job Code and/or Department, Different Approval Paths based on criticality, risk or audit objective or role, resource or entitlement, Serial/parallel/voting based approvals, Escalation Channels etc., in addition to the out of the box workflow composites, to accelerate the migration process.

Special Considerations

Customers are advised to follow these general guidelines when defining additional workflows in OW

- Separate UI (Forms) from Workflows. Workflow wizards are specific to OW and may not be migratable.
- Separate Approval Tasks (or workflow sub tasks) from the overall workflow process
- OW Fork-Join logic that are request-approval based may be migrated to BPEL composites
- Consolidate Approval tasks in a single workflow (per scenario and not for the entire deployment)
- In case of bulk requests (multiple entitlements or multiple accounts in a single request), consider breaking them within the workflow.
- In case of uber workflows, consider using either a self-service request approach or a RBAC approach.

b) User Forms

A Waveset form is an object associated with a page that contains rules about how the browser should display user view attributes on that page. Forms can incorporate business logic and are often used to manipulate view data before it is presented to the user. Waveset forms map to OIM Process Forms and Request Data Sets.

Special Considerations

- Form Elements

  Some of the OW specific Form Elements like Title Width, Defun, Defvar, Fieldref, Include, Formref, Namespace and Form field elements like Options-Button, Options-Action, Options-Library and Disable are very OW specific and have no direct mapping with OIM constructs.
- Validation Logic

  The implementation technology of performing validation on each of the form elements differs in OW and OIM. In OIM, plug-in points are available to be implemented to perform such functions.

c) Task Templates

Waveset Task Templates are used to maintain a collection of task (workflow) launch parameters. Rather that requiring the user to enter those inputs every time the task is launched, the inputs can be encapsulated in a Task Template object and stored. Though OIM has no direct equivalent of Task Template feature, depending on the context, the attributes present in the Waveset Task Templates can map to OIM Provisioning Workflow or Request Approval Workflow.

Special Considerations

- The Oracle Pre-migration analysis tool can identify all task templates defined in the OW deployment and based on these customers can migrate the attributes in these task templates to the corresponding workflow composite in OIM.

3.6 Audit and Compliance Data Objects

a) Audit Policy

Waveset Audit Policies enable administrators to enforce preventive, detective and corrective types of internal controls. OIM enforces such policies by integrating with Oracle's compliance and governance product, OIA. Any such audit policies created in OW environment will need to be re-evaluated and implemented using the OIM-OIA integration libraries.

b) Access Scans

Waveset provides a process for conducting access reviews that enable managers or other responsible parties to review and verify user access privileges. Though this feature maps to OIM's Attestation function, customers are advised to consider usage of OIA which is Oracle's strategic product for all compliance requirements including attestation.

c) Report Definitions

Both OW and OIM products provide transactional and historical reports for compliance needs. OIM has corresponding reports for most of the report that OW supports as of today. OIM uses Oracle BI Publisher for reporting that provides a single reporting environment to author, manage, and deliver the reports.

d) Audit Logging

The purpose of Waveset auditing is to record Who did What to Which Waveset objects, and When did they do it. OW supports auditing Provisioner events, View Handler events, Session events and Workflow events. Some of the identity data captured by OIM includes user identity profile history, role membership history, user resource access, and fine-grained entitlement history. OIM also captures data generated by its workflow, policy, and reconciliation engines. By combining this data along with identity data, customers have all the required data to address any identity and access-related audit inquiry.

Special Considerations

- Audit Data

  OW stores audit data in two tables, waveset.log (stores most of the audit event details) and waveset.logattr (stores the IDs of the organizations to which each event belongs). OIM stores audit data in normalized format within UPA* tables within its database. As the two products follow different entity schema for data persistence, customers are advised to follow a co-existence strategy so that reports for audit data can be generated from both OW and OIM depending on the context.

3.7 Server Data Objects

a) Authentication Modules

OW uses pass-through authentication to grant user and administrator access through one or more different passwords. Waveset manages authentication through the implementation of Login applications (a collection of login module groups), Login module groups (an ordered set of login modules) and Login modules (set authentication for each assigned resource and specify one of several success requirements for authentication). OIM uses LoginMapper plug-in point to override the default mapping of JAAS user principal name to OIM username for SSO scenarios. This plug-in point can be used to address pass-through authentication features similar to OW for Administrator and User Interfaces. Authentication for other OW specific interfaces like Business Process Editor, Service Provider Interface and IVR interface have no direct correspondence to OIM authentication schemes.

b) OW Server Tasks

Waveset objects of the type TaskDefinition and RiskReportTask can be associated with a schedule and invoked to run periodically. OIM also provides a Scheduler service to provide the scheduling capabilities necessary for enterprise provisioning requirements. Though the Server tasks configuration has some direct mapping with OIM constructs, it is important to note that the implementation of business logic within these server tasks differ in technology (XPRESS scripts vs Java) requiring some re-implementation in OIM specific technology.

4. Conclusion

Though there are differences in the way OW and OIM addresses provisioning requirements, it is evident from the above analysis that most of these functions have corresponding or possibly better constructs in OIM. Oracle's migration solution will provide methodology, automation tools, assets (sample composites, event handlers etc) and detailed documentation to ease the migration of these constructs from OW to OIM. Customers can also benefit from additional proprietary assets that will be built on top of Oracle's migration toolkit by Oracle's migration go-to Partners. As an immediate step, customers are advised to make use of Oracle's Pre-Migration Analysis tool that can provide an insight into the complexities of their current OW environment and also enable them to plan for the various activities that will be required for the actual migration project. Based on these project planning metrics, customers can then decide to perform a immediate cutover or decide to follow an iterative migration process with co-existence strategies like having OIM for front office automation and OW for back office provisioning fulfillment or vice versa.