/Modernize IAM accelerators for OAM11G and OUD11G

OAM11G and OUD11G Migration - ForgeRock Solution Guide

Table of Contents

Introduction **4**

Glossary 4

OAM 11G Architecture - TBC 5

ForgeRock AM Based SSO Toolkit for OAM11G **6**

Target Customer Deployment 6

High Level Reference Architecture 6

Scope Definition 7

Extensible Framework for Bidirectional SSO 8

Migration Accelerators Package 9

External Libraries Needed for Rebuilding the Code 9

Solution Design 11

Migration Authentication Tree 11

Scenarios 12

Scenario 1 - The user has a valid legacy OAM11G SSO token in the browser, and accesses the authentication tree 12

Scenario 2 - The user accesses the authentication tree, with no legacy OAM11G SSO token in the browser, after previously he accessed Scenario 1 - was created with no password 12

Scenario 3 - The user is not migrated, does not have a valid legacy OAM11G SSO token, and accesses the authentication tree 13

Scenario 4 - This scenario is triggered when the user has a valid legacy OAM11G SSO token in the browser and is already migrated 14

Scenario 5 - This is the standard scenario triggered when the user is already migrated, and a Data Store Decision node authenticates the user successfully 14

Secret Stores 15

The passwords used in the toolkit authentication tree nodes must be saved in secret stores for security reasons. 15

ForgeRock Bulk User Migration Toolkit for OUD **16**

Target Customer Deployment 16

High Level Reference Architecture 16

Scope Definition 17

Identity Management Bulk Reconciliation Process 17

Bulk Migration Toolkit Package 17

Solution Design 18

IDM Managed User Object Definition 18

IDM Group Managed Object Definition 19

User mappings: OUD -> ForgeRock IDM mappings -> ForgeRock DS 20

Group mappings: OUD11G -> ForgeRock IDM mappings -> ForgeRock DS 20

/ Author	/ Action	/ Date	/ Version
Andrei Dumitru	Draft - Template	2020-01-27	0.1

1 Introduction

The purpose of this document is to provide guidance for customers and partners to accelerate migration projects from OAM11G to the ForgeRock Identity Platform.

The target audience for this document is technical staff (enterprise architect, solution architect, integration architect) with a general understanding of identity and access management systems.

1.1 Glossary

The following terms and abbreviations are used in this guide:

Term	Description
AM	ForgeRock Access Management
SSO	single sign-on
IG	ForgeRock Identity Gateway
RP	reverse proxy
OAM	Oracle Access Manager
API	application programmable interface
OUD	Oracle Unified Directory
OIDC	OpenID Connect
RS	resource server
PEP	policy enforcement point
PDP	policy definition point
TLS	transport layer security
REST	representational state transfer

1.2 OAM 11G Architecture

The following typical legacy solution architecture is a baseline for the Modernize IAM Accelerators:

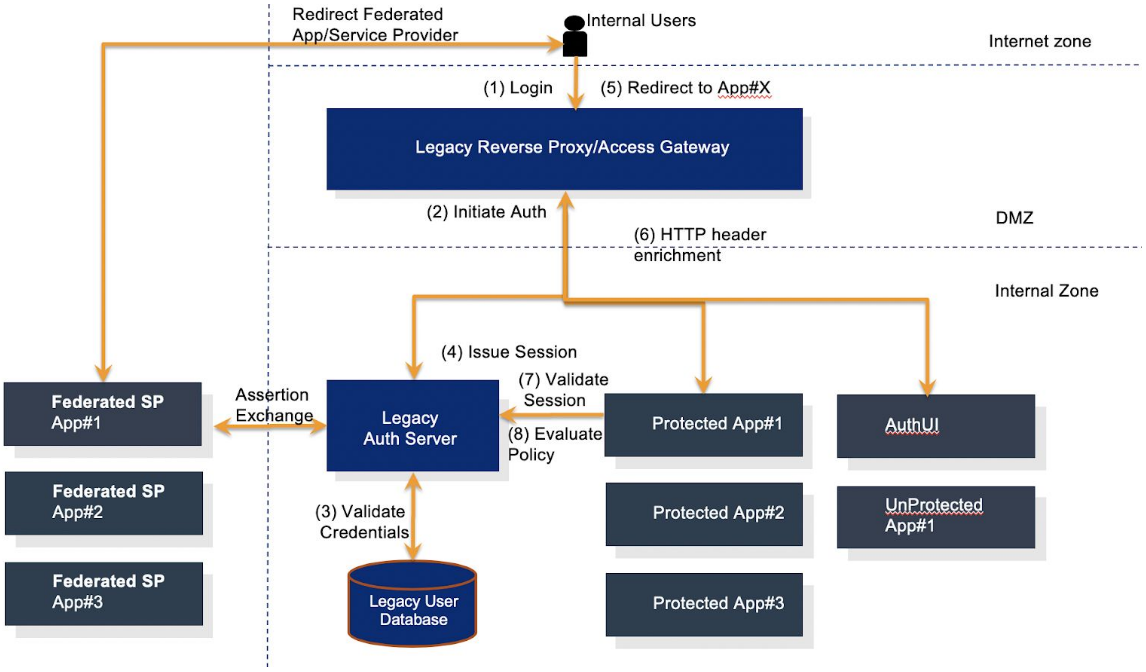

Figure 1 - Legacy OAM11G Deployment

System	Role
OAM11G	Validates authentication and authorization requests
Legacy reverse proxy	Unified point of entry inside the domain (WebGate)
OUD11G	Oracle Universal Directory user store
Protected apps	Existing applications integrated with OAM11G
Auth UI	Legacy UI pages for authentication (login, logout)
Unprotected apps	Existing applications not protected by OAM11G

2 ForgeRock AM Based SSO Toolkit for OAM11G

2.1 Target Customer Deployment

The ForgeRock AM-based SSO Toolkit accelerates migration activities in customer scenarios where the following assumptions are met:

- OAM11G deployment with OAM Access Client SDK setup is available
- A username & password authentication scheme is used in OAM
- The userstore is LDAP-based
- The user profile API (/userinfo) is available

The toolkit implementation has been tested against OAM 11G R2 PS3 and OUD 11G R2 PS3.

2.2 High Level Reference Architecture

The reference architecture for the AM-based SSO Toolkit consists of:

- ForgeRock Access Manager
- ForgeRock Directory Server
- ForgeRock Identity Manager
- OAM 11G Runtime with standard configuration based on OUD 11G
- OAM 11G Access Client SDK

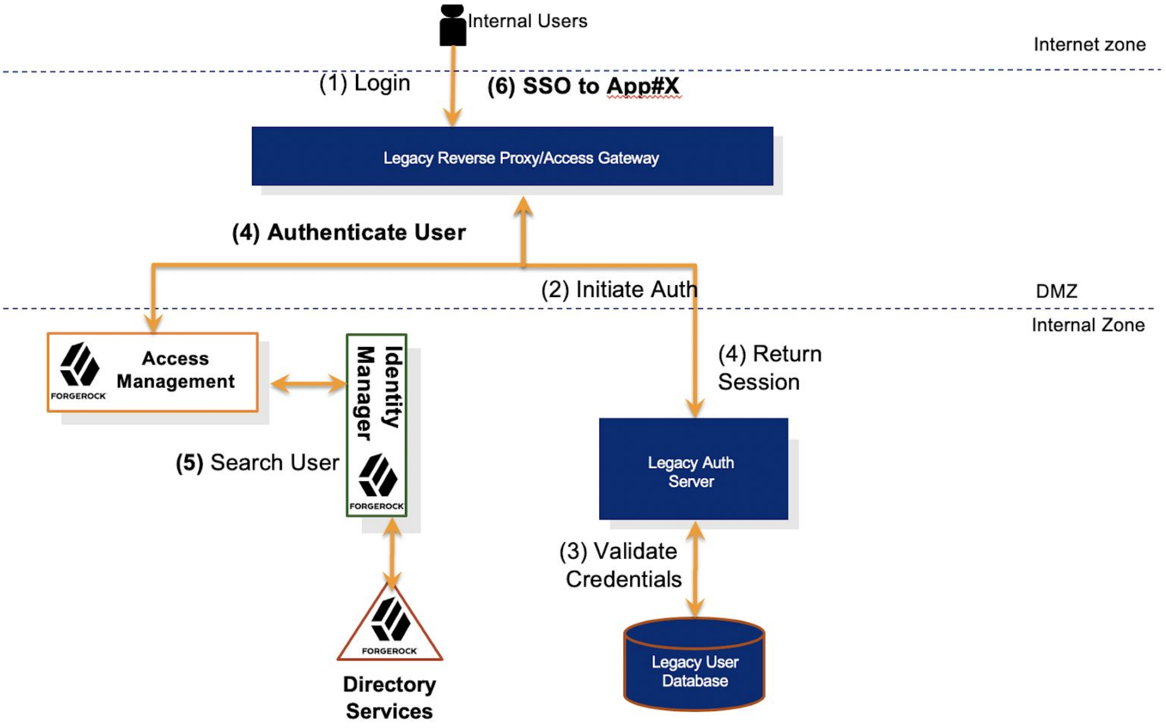

Figure 2 - AM based SSO Framework for OAM11G

2.2.1 Scope Definition

The toolkit provides a collection of custom nodes and a migration tree that can handle very complex migration scenarios, including bidirectional SSO between OAM11G and ForgeRock AM.

The framework can be easily extended to support migration from any OAM11G platform that exposes client SDKs/APIs for operations such as:

- Validating existing OAM11G tokens
- Calling the authentication API, with a username and password as input

2.2.2 Extensible Framework for Bidirectional SSO

Powered by ForgeRock Intelligent Authentication and the powerful capabilities of authentication trees, the framework has built-in capabilities to detect:

- An existing OAM11G session;
- Whether users are provisioned (or partially provisioned) in ForgeRock Directory Server;
- Whether users have already been migrated, but are missing passwords.

Validation of a user-entered password in OAM11G is used as a decision point that determines whether the password is ready to be provisioned in ForgeRock IAM.

The Migration authentication tree provides these capabilities. Successful authentication using this tree results in a valid ForgeRock Access Manager SSO token that enables subsequent execution of outbound SSO flows using OIDC or SAMLv2.

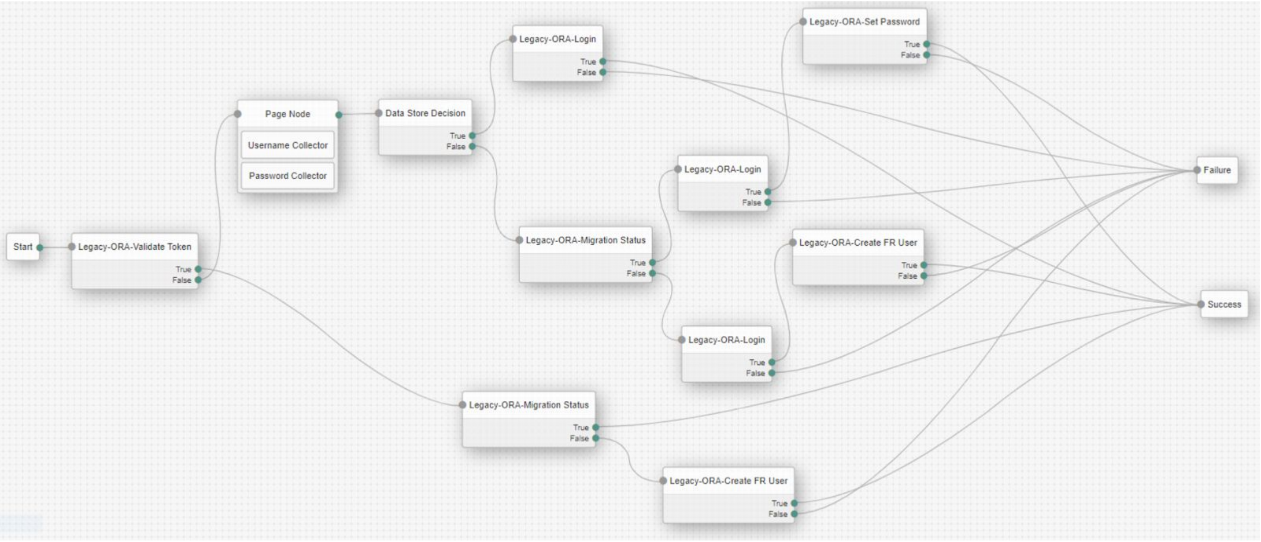

Figure 3 - Migration Authentication Tree

2.2.3 Migration Accelerators Package

The following high-level configuration of modules and extensions are included in this package:

System	Type	Name	Description
AM	Node	Legacy-ORA-Validate Token	Retrieves a token from an existing cookie, validates the token against OAM11G and provides the username and outcome as output in the shared state.
AM	Node	Legacy-ORA-Migration Status	Searches ForgeRock IDM to obtain the user identity based on the username from the shared state.
AM	Node	Legacy-ORA-Create FR User	Calls the ForgeRock IDM API to provision the managed user.
AM	Node	Legacy-ORA-Login	Based on the username and password from the shared state, executes the OAM11G login method call.
AM	Node	Legacy-ORA-Set Password	Updates the ForgeRock IDM managed user object with the password captured and stored in the shared state.
AM	Tree Hook	LegacyORASessionTreeHook	Manages cookies if a successful login is performed into OAM11G by the tree.
AM	Authentication Tree	oracleMigrationSsoTree	Implements migration login and bidirectional SSO.
AM	Custom Nodes	openam-modernize-oracle-auth-nodes-1.0-SNAPSHOT.jar	Custom AM nodes that are used in the migration authentication tree.

2.2.3.1 External Libraries Needed for Rebuilding the Code

- The source files have the following 5.2.1.RELEASE Spring dependencies:
  - spring-beans-5.2.1.RELEASE
  - spring-core-5.2.1.RELEASE
  - spring-jcl-5.2.1.RELEASE
  - spring-web-5.2.1.RELEASE
- The source files also use the Oracle Access Manager Access SDK. The following JAR files must be downloaded from the Oracle downloads page and added to the WEB-INF/lib directory:

- identitystore.jar
- jps-api.jar
- jps-common.jar
- jps-internal.jar
- jps-unsupported-api.jar
- oamasdk-api.jar
- oraclepki.jar
- osdt_cert.jar
- osdt_core.jar
- osdt_xmlsec.jar

2.3 Solution Design

2.3.1 Migration Authentication Tree

The execution of the Migration tree depends on the current state of the user profile:

- Existing user profile and password – no provisioning is required
- Existing user profile but no password – authentication to OAM11G and provisioning of the user password is required
- Existing legacy SSO session – only provisioning of the user profile can be executed
- No existing user profile – upon successful authentication to OAM11G, both the user profile and user password are provisioned and SSO is triggered

MiAMI Accelerator Login OAM11G - Extensible Framework for Bi-Directional SSO

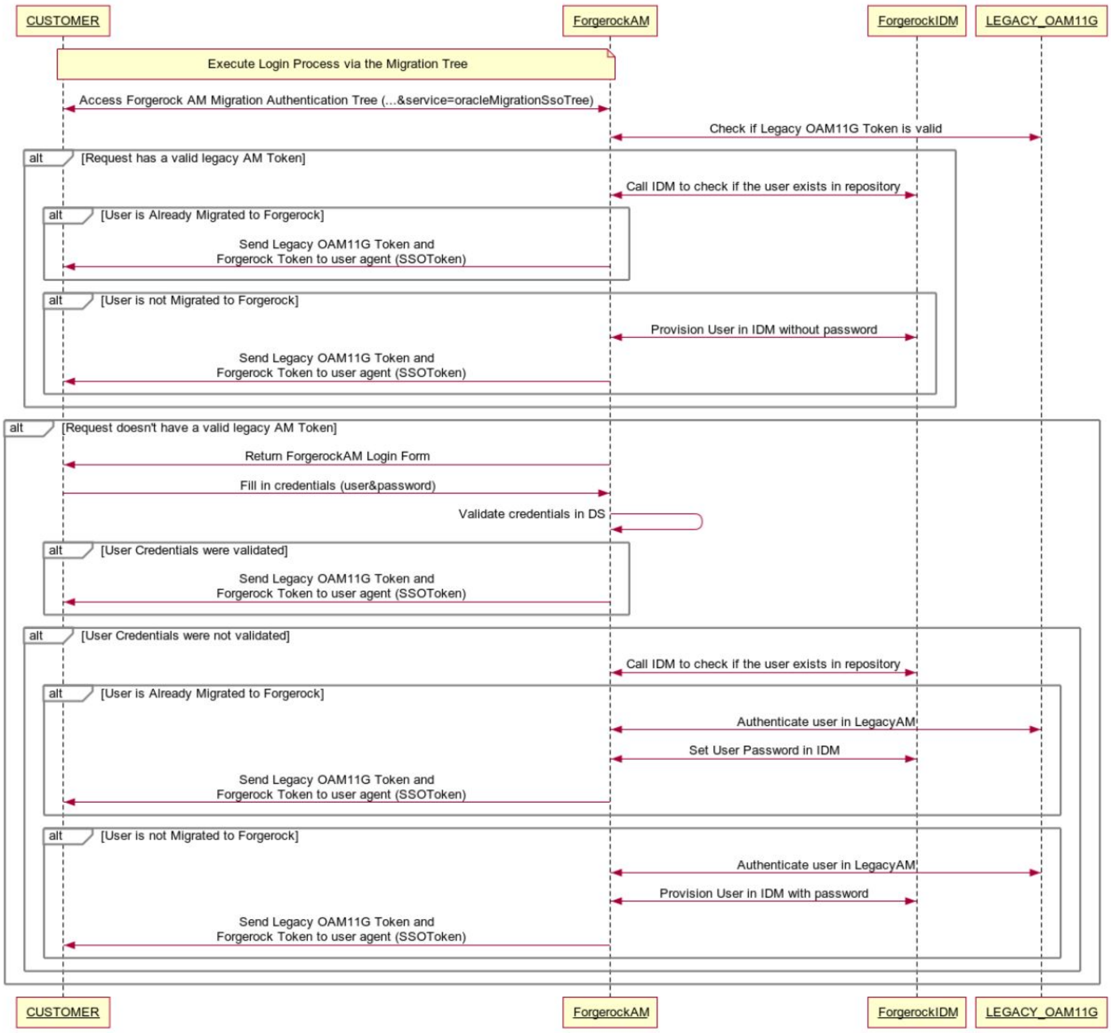
CUSTOMER
ForgerockAM
ForgerockIDM
LEGACY_OAM11G
Execute Login Process via the Migration Tree
Access Forgerock AM Migration Authentication Tree (...&service=oracleMigrationSsoTree)
Check if Legacy OAM11G Token is valid
alt [Request has a valid legacy AM Token]
Call IDM to check if the user exists in repository
alt [User is Already Migrated to Forgerock]
Send Legacy OAM11G Token and Forgerock Token to user agent (SSOToken)
alt [User is not Migrated to Forgerock]
Provision User in IDM without password
Send Legacy OAM11G Token and Forgerock Token to user agent (SSOToken)
alt [Request doesn't have a valid legacy AM Token]
Return ForgerockAM Login Form
Fill in credentials (user&password)
Validate credentials in DS
alt [User Credentials were validated]
Send Legacy OAM11G Token and Forgerock Token to user agent (SSOToken)
alt [User Credentials were not validated]
Call IDM to check if the user exists in repository
alt [User is Already Migrated to Forgerock]
Authenticate user in LegacyAM
Set User Password in IDM
Send Legacy OAM11G Token and Forgerock Token to user agent (SSOToken)
alt [User is not Migrated to Forgerock]
Authenticate user in LegacyAM
Provision User in IDM with password
Send Legacy OAM11G Token and Forgerock Token to user agent (SSOToken)
CUSTOMER
ForgerockAM
ForgerockIDM
LEGACY_OAM11G

Figure 4 - Extensible Framework for BI-Directional SSO

2.3.2 Scenarios

2.3.2.1 ***Scenario 1*** - The user has a valid legacy OAM11G SSO token in the browser, and accesses the authentication tree

- The user (not previously migrated) authenticates first to the legacy OAM11G instance.
- The user accesses the authentication tree.
- Upon accessing the tree, the user is automatically logged in because a valid legacy OAM11G SSO token is present in the browser. As a result, a user profile is created in ForgeRock IDM and AM, with no password set.

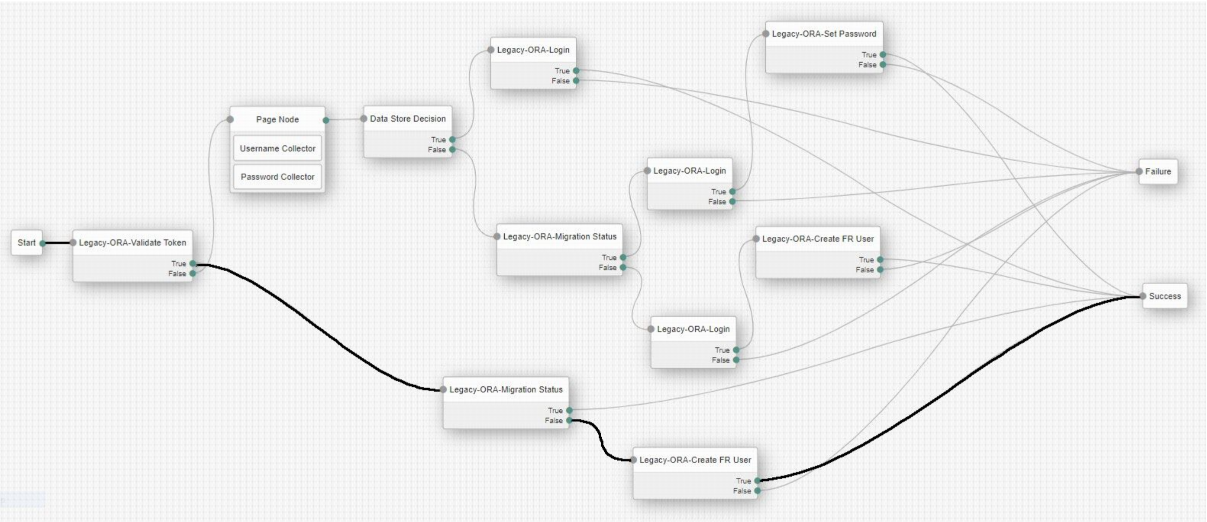

Figure 5 - Scenario 1

2.3.2.2 ***Scenario 2*** - The user accesses the authentication tree, with no legacy OAM11G SSO token in the browser, after previously he accessed Scenario 1 - was created with no password

- The user accesses the authentication tree. The tree is prompting the user for the username and password.
- After providing credentials, the user is successfully authenticated. This happens because the user was successfully logged in to the legacy OAM11G. Since the Data Store Decision node returned false but the user was already migrated, and the legacy login was successful, the password is also updated in DS.

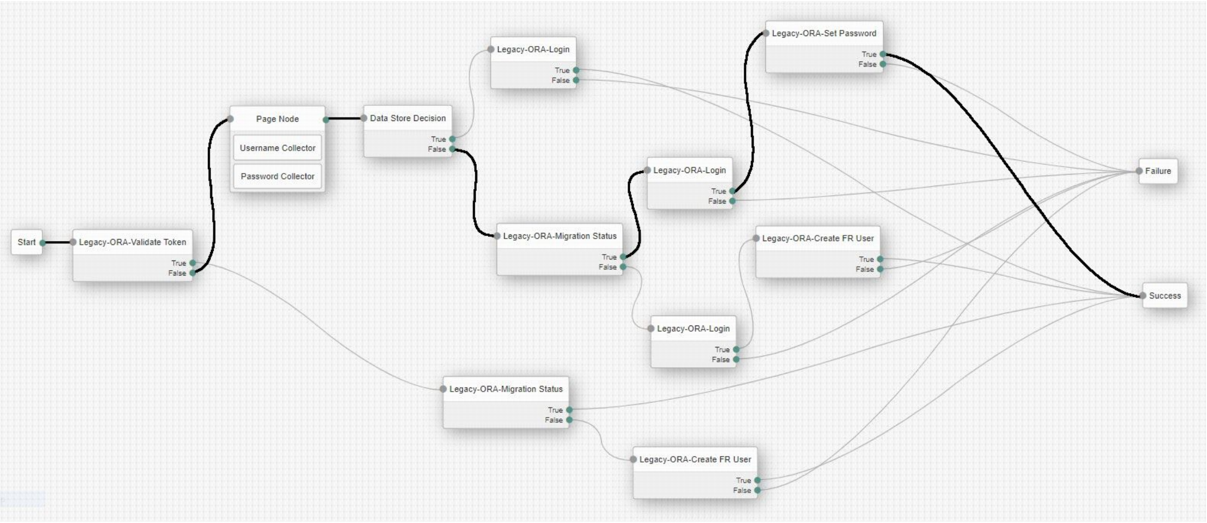

Figure 6 - Scenario 2

2.3.2.3 ***Scenario 3*** - The user is not migrated, does not have a valid legacy OAM11G SSO token, and accesses the authentication tree

- The user accesses the authentication tree. The tree prompts the user for the username and password.
- After providing credentials, the user is successfully authenticated. This happens because the user was successfully logged in to the legacy OAM11G instance, and the user's profile was successfully provisioned in ForgeRock DS, including the password.

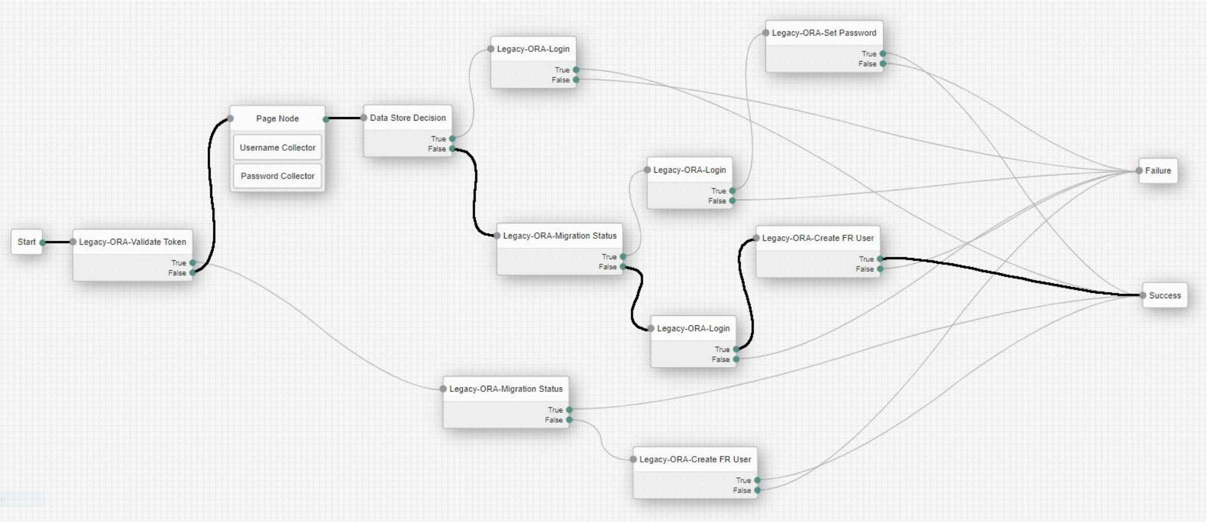

Figure 7 - Scenario 3

2.3.2.4 ***Scenario 4*** - This scenario is triggered when the user has a valid legacy OAM11G SSO token in the browser and is already migrated

- The user (previously migrated) authenticates first to the legacy OAM11G instance.
- The user accesses the authentication tree.
- The outcome of this scenario is that the user is authenticated automatically to both the legacy OAM11G instance and to ForgeRock AM after execution of the tree has completed.

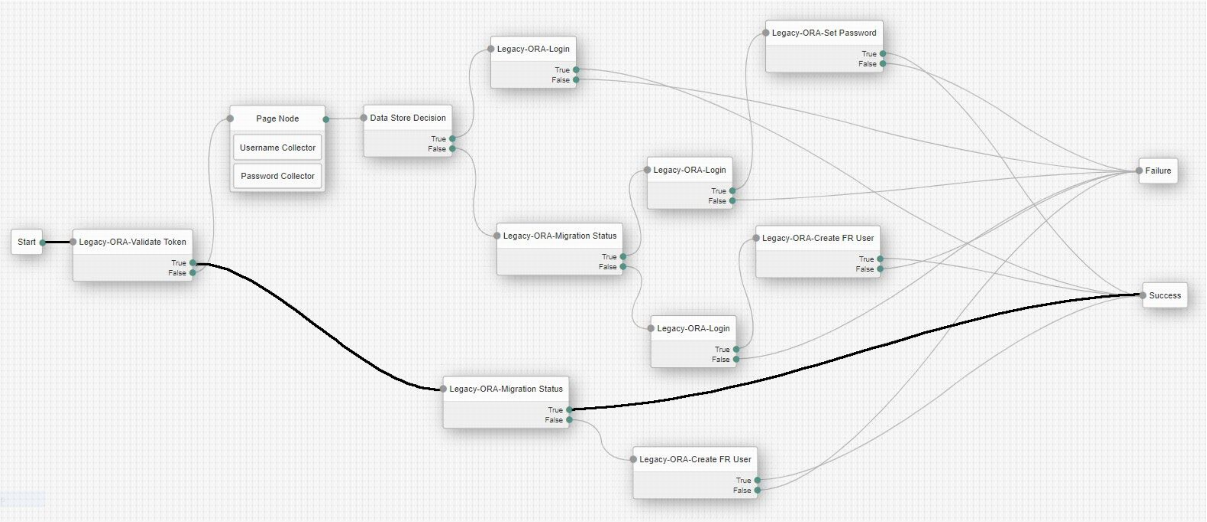

Figure 8 - Scenario 4

2.3.2.5 ***Scenario 5*** - This is the standard scenario triggered when the user is already migrated, and a Data Store Decision node authenticates the user successfully

- The user accesses the authentication tree. The tree prompts the user for the username and password.
- The outcome of this scenario is that the user is authenticated automatically to both the legacy OAM11G instance and to ForgeRock AM after execution of the tree has completed.

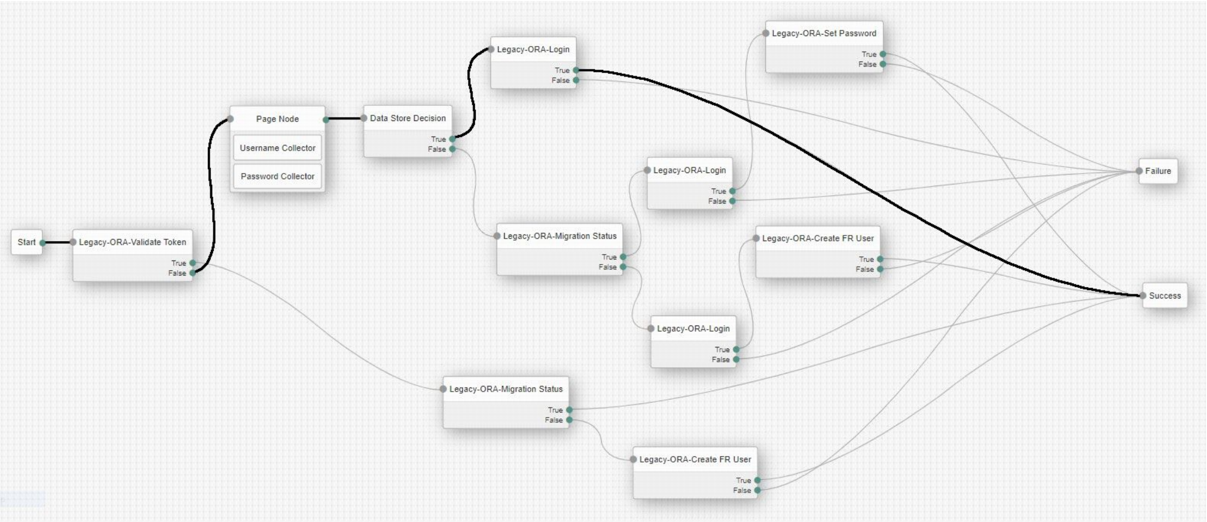

Figure 9 - Scenario 5

2.3.3 Secret Stores

The passwords used in the toolkit authentication tree nodes must be saved in secret stores for security reasons.
The toolkit uses AM secret stores as described in the ForgeRock documentation.

3 ForgeRock Bulk User Migration Toolkit for OUD

3.1 Target Customer Deployment

The ForgeRock Bulk User Migration Toolkit accelerates migration activities in customer scenarios with one or more of the following requirements:

Topic	Answer
Complexity of mapping rules requirements between OAM11G identity source (OUD) and ForgeRock Directory Server as target IAM	Medium or High
OAM11G identity source type is LDAP-based; LDIF based export/import is available	NO
Must preview or monitor the bulk migration process	YES
Must schedule the migration process or provide a chunked migration	YES
Requires a cut-off from OAM11G to ForgeRock IAM.	YES

3.2 High Level Reference Architecture

The Bulk User Migration Toolkit reference architecture solution is based on the following ForgeRock Identity Platform core components:

- ForgeRock Directory Server
- ForgeRock Identity Manager

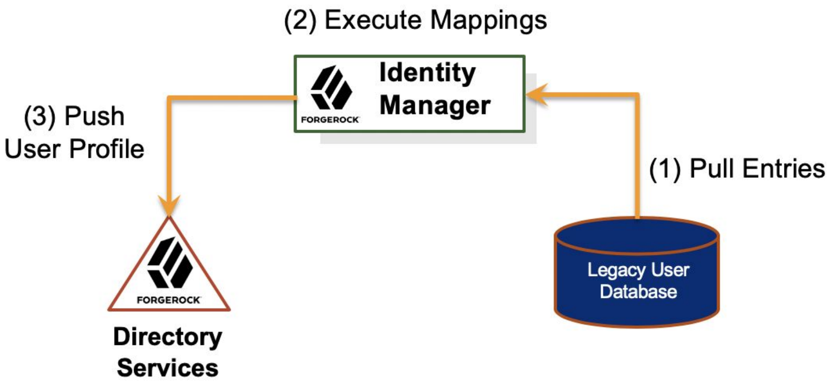

Figure 10 - Bulk User Migration from OUD

3.2.1 Scope Definition

This toolkit implements one-way synchronization from an external OUD user store to the ForgeRock IDM repository. After synchronization, identities and groups are synchronized to ForgeRock Directory Server as the next-generation user store.

The toolkit can be extended to work with any compliant source connector. User objects in the source system file are synchronized with the managed users and groups in the ForgeRock IDM repository, then pushed to ForgeRock DS based on mappings that you provide.

Inbound and outbound mappings can be extended for the specific customer scenarios.

The sample source connector type is LDAPv3, but you can also use Adapter if needed.

3.2.2 Identity Management Bulk Reconciliation Process

One-time and incremental import of user profiles and groups from a legacy OUD LDAPv3 store or another similar user store, followed by export to ForgeRock DS, is usually a requirement in the migration process.

When OAM11G systems use custom schema, synchronizing information can be complex.

Mapping the extended schema, such as attributes, object classes and group membership used for core IAM transactions, can be cumbersome and time-consuming.

The Migration Accelerators include the following assets for mapping custom schema:

- A template that provides user and group reconciliation from OUD to ForgeRock DS.
- Mapping for common group information, such as cn, description, uniqueMember.
- Mapping for common identity information, such as UID, common name, group membership, status, mail, last login, account locked features, number of wrong attempts.

3.2.3 Bulk Migration Toolkit Package

The accelerator assets described below come in a single ready-for-deployment package, making it easy for customers or partners to deploy them in a new or existing ForgeRock Identity Platform implementation.

The following high-level configuration of modules and extensions are included in the ForgeRock Bulk Migration Toolkit Package:

System	Type	Name	Description
IDM	Managed Object	managed.json	Enhanced user object definition that brings several other typical attributes in the IDM definition
IDM	Managed Object	managed.json	New group managed object definition
IDM	Mapping	sync.json	Source mapping set for OUD11G to IDM managed object (user, group)
IDM	Mapping	sync.json	Source mapping set for OUD11G to IDM managed object (user, group)
IDM	Connector	provisioner.openicf-legacyOUD.json	Source connector that pulls user identities and groups from OUD11G (LDAPv3 connector)
IDM	Connector	provisioner.openicf-ldap.json	Target connector that pushes identity information and groups inside ForgeRock Directory Server (LDAPv3 connector)

3.3 Solution Design

3.3.1 IDM Managed User Object Definition

The following custom fields have been added to the IDM managed object definition:

Attribute Name	Type	Description
uniqueId	String	External unique identifier
passwordSha512	String	Password SSHA512 encoded from external system

groups	String	The static groups in which the user belongs
lastFailedLogin	String	Last failed login timestamp
lastSuccessfulLogin	String	Last successful login timestamp
lockoutTime	String	Timestamp when the account was locked
loginTryCount	String	Number of invalid username/password login attempts
employeeNumber	String	For internal based IAM, the unique identifier of the employee
employeeType	String	For internal based IAM, the type of the employee
organization	String	For internal based IAM, the organization of the employee
departmentNumber	String	For internal based IAM, the unique identifier of the user department

3.3.2 IDM Group Managed Object Definition

The following new managed object and fields have been added to the IDM managed object definition:

Attribute Name	Type	Description
cn	String	Common name of the group
description	String	Description of the group
displayName	String	Display name of the group

uniqueMember	String	The static users that are members of this group

3.3.3 User mappings: OUD -> ForgeRock IDM mappings -> ForgeRock DS

The following mappings are implemented:

Source Attribute (OUD11G ldap)	Target Attribute (IDM)	Target Attribute (FR DS)	Description
uid	userName	uid	Unique user identifier
userPassword	passwordSha512	userPassword	External user password
cn	cn	cn	Full name
givenName	givenName	givenName	First name
inetUserStatus	accountStatus	inetUserStatus	User status
sn	sn	sn	Last name
mail	mail	mail	Email address
telephoneNumber	telephoneNumber	telephoneNumber	Telephone number
description	description	description	Description
employeeType	employeeType	employeeType	Employee type
employeeNumber	employeeNumber	employeeNumber	Employee number
o	organization	-	Organization
title	title	-	User title
displayName	displayName	-	User display name
obLastFailedLogin	lastFailedLogin	sunAMAuthInvalidAttemptsData	Invalid authentication information
obLastSuccessfulLogin	lastSuccessfulLogin		
obLockoutTime	lockoutTime		
obLoginTryCount	loginTryCount		
isMemberOf	groups	isMemberOf	User groups
orclGUID	uniqueId	-	External unique identifier
orclIsEnabled	isEnabled	-	User status (ENABLED| DISABLED).

3.3.4 Group mappings: OUD11G -> ForgeRock IDM mappings -> ForgeRock DS

The following mappings are implemented:

Source Attribute (legacyIAM ldap)	Target Attribute (IDM)	Target Attribute (FR DS)	Description
cn	cn	cn	Common name of the group
description	description	description	Description of the group
displayName	displayName	-	Display name of the group
uniqueMember	uniqueMember	uniqueMember	The static users that are members of this group