Modernize IAM Accelerators

There's more pressure than ever to compete in today's digital market. New demands require new technology that is interoperable across digital ecosystems and is capable of knowing, securing, and serving your audience at any touchpoint. The foundation to enabling digital success is identity and access management (IAM), yet many organizations struggle with IAM software that is siloed, inflexible, and unable to scale beyond employees.

The demands of digital transformation require IAM technology that can seamlessly interoperate across your ecosystem, identifying and providing secure access to your consumers, workforce, and things at any touchpoint. The prospect of migrating to a new solution is daunting. But, you don't have to suffer the pain, risk, and expense of ripping out your legacy identity solutions to get the benefits you need to compete in the digital landscape. ForgeRock has a better way.

ForgeRock provides a simple, flexible approach that enables you to coexist and migrate legacy identity management systems to ForgeRock. With our standards- based identity and access management platform, you can quickly and easily build on your existing investments and streamline operations. Most importantly, you can make migration to ForgeRock seamless and invisible to your users.

Overview

The Modernize IAM Accelerators, available as open source from ForgeRock, improve time-to-value for migrations, specifically in the areas of user migration and single sign-on (SSO) between legacy access management systems and the ForgeRock platform when a coexistence strategy is employed. Complex legacy deployments of IAM with many applications often require migration waves over time to minimize operational impact. This drives a need for a coexistence strategy between the legacy vendor and ForgeRock, which is enabled by SSO.

For user migration, just-in-time (JIT) helps customers save time and effort without sacrificing user experience, especially when it's impossible to export passwords from a legacy system in a bulk manner. In addition, bulk user migrations can be complex because of mappings between the legacy and new IAM platform.

ForgeRock has three tool kits to accelerate migration: **Bidirectional Coexist – Core, Bidirectional Coexist – Edge, and Bulk User Migration.** Customers can choose the optimal tool kit (or combination of tool kits) based on their selected migration strategy.

For all three tool kits, ForgeRock has developed a pluggable framework that can be extended to specific legacy systems. For example, an out-of-the-box authentication tree is included for bidirectional SSO (see Figure 1 below) that handles invalid authentication attempts, password synchronization and more. The authentication nodes can be easily extended to most legacy systems with plugins.

The pluggable system, plug-ins, reference architectures, code, and configuration provided as part of the Modernize IAM Accelerators have been designed to achieve a greater than 30% acceleration in the migration from legacy vendors to ForgeRock.

| Start | Collect User Info | Check ForgeRock Directory | Check Legacy Directory | Provision ForgeRock from Legacy Directory | Create Session |

Functional Steps Included in SSO Authentication Tree

Modernize IAM Accelerators Features and Benefits

- Migrate any complex legacy AM system with a coexistence strategy.

- Show immediate value by adding new capabilities (examples: Intelligent Access, MFA, OTP, Full Trust Partner Network Tech, and test migration segments).

- Open source is available at no cost and can be easily extended by customers and partners.

- They provide support for credential migration with passwords.

- ForgeRock has tested and standardized the approach to user migrations (JIT and bulk) and SSO from legacy systems to ForgeRock.

- The modular, pluggable, and flexible system that adapts to the selected migration approach.

- Templates are included for bulk migration.

- The accelerators support implementation and Modernize IAM Accelerators with Deployment Support Services (DSS).

Solution Description

The following tool kits are included as part of the ForgeRock Modernize IAM Accelerators.

Bidirectional Coexist Core

When managing tens or hundreds of legacy applications, customers may choose migration waves to minimize the operational impact on production systems. With this type of use case, coexistence and SSO between legacy IAM and ForgeRock IAM is often needed. Powered by ForgeRock Intelligent Access and the powerful capabilities of authentication trees, this tool kit has built-in capabilities to detect and address many scenarios, including:

- Already provisioned or partially provisioned users in the ForgeRock Directory.

- Already migrated users without a password.

- Detect, extract, and migrate user identities from existing legacy IAM sessions.

- Validate the user-entered password inside the legacy IAM system as a decision point on whether the password is ready to be provisioned in ForgeRock IAM.

Successful authentication will result in a valid ForgeRock Access Manager SSO Token that can allow subsequent executions of outbound SSO flows using OIDC or SAML 2.0.

The tool kit provides a collection of custom ForgeRock Intelligent Access Nodes and a migration tree that can handle complex migration scenarios, including bidirectional SSO between legacy IAM and ForgeRock Access Management. The framework can be easily extended to support migrations from any legacy IAM platform that is capable of exposing client SDKs/APIs for operations such as validate existing legacy IAM tokens and authenticate via API (with a username and password input). The migration tree and nodes are easily extensible to new functions like A/B testing or MFA.

Bidirectional Coexist Edge

This toolkit extends ForgeRock's SSO, JIT, and Intelligent Access capabilities to edge and nonstandard applications with the ForgeRock Identity Gateway. Upon successful authentication events, the tool kit will programmatically authenticate the user in ForgeRock Access Management and send the appropriate ForgeRock SSO Token to the user-agent.

The framework can be easily extended to support migrations from any legacy IAM platform that is capable of exposing client SDKs/APIs.

Whenever one-time or incremental import of user profiles is not possible via ForgeRock Identity Management (IDM), the toolkit triggers a JIT process that orchestrates existing legacy IAM authentication with IDM-based user provisioning activities. This helps customers save time and effort without sacrificing user experience. Some examples of when this process may trigger include when user passwords are stored in a custom hashing schema that cannot be replicated, or when user stores are not LDAPv3 compliant.

Forgerock Identity Gateway has unique capabilities for both reverse proxy (including transparent proxy) and access management-enabled functions. It is the ideal module in the architecture to perform complex tasks such as JIT provisioning of SSO initiation between legacy IAM and ForgeRock IAM.

This tool kit implements JIT user provisioning to ForgeRock IAM during an existing legacy IAM authentication transaction. The JIT requires that the user is successfully authenticated against the legacy IAM system and that a legacy token is issued. The JIT orchestration is performed in ForgeRock Identity Gateway, and the provisioning operation itself is executed via ForgeRock IDM standard managed user provisioning APIs.

Bulk User Migration

One-time and incremental import of user profiles from legacy LDAPv3 store or similar user stores to ForgeRock Directory Services (DS) is often a requirement in the migration process. The custom schema used by legacy IAM systems makes synchronizing information complex to design and implement. It also makes the particular mapping of the extended schema (attributes, object classes, and group membership used for core IAM transactions) cumbersome and lengthy. The following assets have been included in the migration accelerators for this purpose:

- Template for LDAPv3 to LDAPv3 user reconciliation from legacy IAM to ForgeRock DS.

- Mapping for common identity information: uid, common name, group-membership, status, mail, last login, and account locked features.

This tool kit implements one-way synchronization from an external legacy IAM userstore to the ForgeRock IDM repository and then synchronization to ForgeRock Directory Server as the next generation userstore.

- The tool kit can be extended to work with any compliant source connector. User objects in the source system file are synchronized with the managed users in the ForgeRock IDM repository and then pushed in ForgeRock DS based on the provided mappings.

- Both inbound mappings and outbound mappings can be extended for specific customer scenarios.

- The sample source connector is LDAPv3 but may be adapted in the customer context.

Plugins

A set of plug-ins for Oracle Access Manager 11G, Oracle Directory Services Enterprise Edition (DSEE), and CA Single Sign-On (SiteMinder) is included with the accelerators. In addition to these, a generic plug-in is available that can be used for nearly any other legacy platform.

Documentation

Detailed documentation on the solution is available including:

- Reference Architecture and Detailed Solution Guide.

- Guide(s) for specific legacy plug-ins.

- Operational Documentation with instructions on installing, configuring, deploying, and troubleshooting the Modernize IAM Accelerators.

- Training videos.

Deployment and Support

ForgeRock Deployment Support Services are available to support the implementation and use of the ForgeRock Modernize IAM Accelerators.

More Information

Please contact us for a demonstration and more information on getting started with the ForgeRock Modernize IAM Accelerators.