OpenIDM 2.0 - FAQ

Deployment Platform

Supported WebServers/AppServers?

OpenIDM provides a stand-alone installation and aside from a database installation and optional reporting tools comes as a self contained, light weight package. This provides for less variability in deployment environments, more rapid development and simplified maintenance.

Supported Database as repository storage?

Currently DB2 and MySQL are supported RDBMS systems for production subscriptions, and OrientDB for Proof-of-Concept subscriptions. For more details on particular versions supported, refer to the product documentation as well as the release notes.

How does it behave in a multi-server cluster deployment with failover?

OpenIDM relies on the HA of the database as well as an MVCC (multi version concurrency control) layer for the ability to concurrently and safely operate on the same data set. With the RESTful architecture we also take advantage of the proven scalability and reliability of HTTP load balancers and associated infrastructure, which many enterprises have already invested in. Further enhancements to cluster awareness are on the roadmap, but it is already possible to set up OpenIDM in an active-active or active-passive set-up.

Architecture

Is OpenIDM based on Sun Identity Manager or Oracle Waveset in any way?

ForgeRock OpenIDM is entirely built from scratch by ForgeRock and Community - although ForgeRock announced a while ago to adopt the Sun Microsystems Open Source project "Identity Connector Framework" under the new name OpenICF. OpenICF is an integral part of the OpenIDM connector layer to integrate with resource.

Is file-based management the only way to add/update/remove target system configurations?

Configuration is stored in the repository (Database), and OpenIDM supports multiple ways to view or manipulate the configuration.

- *REST based interface to create, read, update, delete configuration*
- *File based “view” to create, read, update, delete configuration*

The REST based interface provides a platform for adding additional tooling layers in the form of UIs and command line going forward.

The file based view supports automatic detection and applying of changed configuration without requiring system restarts for quick development purposes.

Is file-based management the only way to change the scripts/provisioning rules? Does it require a restart of the OSGI module?

Provisioning rules are regular configuration and hence follow the mechanism described above and support automatic detection and application of changed configuration.

Scripts that are embedded in configuration follow the same mechanism.

Stand-alone script files currently do not support automatic change detection, but is an enhancement planned in addition to being able to store and manipulate them in the same fashion as the remaining configuration.

Outbound Services

Supported/sample Reporting/BI solutions?

As the recon report data as well as audit logs can be directed to database tables as well as comma delimited files, any reporting and BI tool that can operate on these can be used.
TODO: fill in details from Gael’s report work

Repository

Does it support multiple system accounts on same system per virtual identity?

Yes, OpenIDM supports correlating and/or explicitly mapping multiple accounts on the same system to a virtual identity.

Is the user password stored within the repository? What encryption mode does it offer?

OpenIDM optionally can be set up to store the password in the repository. The encryption is configurable and extensible, by default uses a customer provided cryptography key from the keystore and configurable cipher is used. If not explicitly specified, the default cipher is "AES/CBC/PKCS5Padding".

Is any user identity information stored within the repository? Is the set of data stored extensible?

OpenIDM supports:
- Direct mapping between external systems (and only keeping track of links)
- Mapping between external system and representation store in OpenIDM (called managed object)
- Mapping between two representations in OpenIDM (e.g. layered or different views)

For choices 2. and 3. any property (including user identity information) can be stored in OpenIDM, the choice of what is stored where is fully under the control of the user as well as the level of protection (e.g. encryption) applied.
The data model in OpenIDM is fully user configurable (and hence also extensible), a default canonical model acts as a starting point.

Archival/Restoration

Any functionality to perform export/import of audit data?

The audit event mechanism is pluggable and out of the box is configured to log both to comma delimited (csv) files as well as the database (repository)

Are audit data tamper-proof?
TODO:

Authentication

Does it offer authentication via a target system resource, or must it always use the password stored in the internal repository storage?

TODO:

Does it offer integration with OpenAM's SSO functionality?

yes, optionally authentication and authorization can be delegated to OpenAM

Basic Self-Service UI

Is the challenge question/answer customizable per user?

TODO:

Can self-service profile updates/password change be selectively provisioned to target systems, instead of always all systems?

Yes, OpenIDM provides for explicit scriptable extension points to decide whether a property change should apply to a specific target system or not.

Delegated Admin

What administrative roles does OpenIDM offer, in terms of Restful API support (or even Basic UI if there is)?

OpenIDM provides a highly flexible way to define and customize access policies.
When using built-in authentication the script based access policies can decide based on any available context data (including user, organizational, role information) whether access for a given URL, action or data should be granted.
When using OpenAM its extensive authorization capabilities (including fine grained authorization) can be used to control access.

Can administrators be given authority to edit users only within a particular organization/container?

Yes

Can administrators be given authority to view or edit only?

Yes

Integration

What system resources can OpenIDM integrate with and provision to?

Resource Name	Type
Active Directory	.NET
Database Table	DB
Scripted SQL	DB
DB2	DB
MySQL	DB
Oracle	DB
MS SQL Server	DB
LDAPv3	LDAP
Exchange	.NET
SPMLv2	WebServices
RACF	Mainframe
Web TimeSheet	Cloud
Google Apps	Cloud
CA Unidesk	GroupWare
XML File	File
CSV File	File
Tivoli Access Manager	SSO
Solaris	OS

VMS	OS
Oracle ERP	ERP
SalesForce.COM	Cloud

Where can i find more information about connectors and how to build a custom connector?

More information about connectors and how to build a custom connector can be found at the OpenICF Community website .