MIGRATING YOUR IDM SYSTEM TO THE CLOUD

WHITE PAPER

Brought to you by:

sath

OVERVIEW

There is now more pressure to move all areas of an organization's IAM system into the Cloud. While, in the past, applications would run on a physical server in an organization's own data centers. Cloud is fast becoming the new normal within cybersecurity. The power of Cloud computing now brings all its advantages into the IAM domain. With increased adoption of new technologies like Cloud, mobile and big data technologies, critical data crossing in and out of an organization has security teams constantly asking, "who has access to what" and "what are they doing with this access?" Cloud computing has increased security measures to more easily answer these questions.

While Identity Access Management has been around for decades one of the issues is the amount of resources dedicated to hosting an on-premise IAM system. The total cost is high because of the amount of personnel required to maintain, update and monitor the system. A Cloud based solution has drastically changed the way resources are allocated to an IAM system.

One of the initial defenses of an on-premise solution is that a company has better control to secure its own environment. As cloud providers have developed consistent, proven and reliable security processes for the many clients they serve, it is difficult not to admit that the cloud providers are doing a better job to secure the environment at a lower cost than most of the individual companies.

Another issue to consider is that most of the innovation and business difference making solutions are now cloud base solutions. To keep your business competitive, innovating and with time saving efficiencies, you need to adopt the use of cloud based solutions in your environment. Once you accept and move into a hybrid cloud environment, you'll have the realization that over time everything will end up in the Cloud. With that understanding, you now need to determine the best way to transition your current environment into a Cloud based solution.

Sath delivers a full comprehensive implementation service to transition your organization from an on-premise IAM solution to the Cloud. Utilizing the Sath solution allows organizations to not only move quickly and efficiently into the Cloud but also to leverage the experience and expertise of an organization who specializes in these moves. Moving to the Cloud will enable organizations to manage business processes more effectively, provide consistent highly secured systems, incorporate innovative solutions, promote business agility and at a reduced cost compared to an on-premise IAM solution

TRANSITION TO THE CLOUD AT A GLANCE

Transitioning to the Cloud is a complex process. At Sath we break this down into 10 well-defined steps:

1. Construct Business Case
2. Conduct Analysis
3. Perform Assessment and Planning
4. Implement IDM Solution/Sath Hub
5. Connect Authoritative Source
6. Migrate Directories and Data Stores
7. Pilot Rollout Considerations/Possibilities
8. Disconnected Application Onboarding
9. Migrate Connected Systems to SCIM Interface
10. Follow-up Post Production Support

SCOPE AND DEFINITIONS

For the purpose of this white paper going forward we will make the assumptions that the IDM system is used to manage about ~20,000 internal users and approximately 50,000 external users. The number of systems where the provisioning and reconciliation process is automated is approximately 120. The number of systems managed by the IDM systems which facilities manual provisioning is approximately 200. The IDM system is used to manage the following processes:

REQUEST PROCESS

Request process is the process of requesting accounts, entitlements and roles within the IDM. After process approval, users' access gets provisioned on the target systems or devices.

PROVISIONING ROLE, ENTITLEMENT AND ACCOUNT

The provisioning process is the act of using a person's account information and entitlements from the IDM system to create that person's profile in the target systems with the appropriate permissions.

PASSWORD SELF SERVICE

End-users can log into the IDM system with the organization's network ID and password or by using other authentication mechanisms. The passwords for logging into the IDM system is not managed separately.

CERTIFICATIONS/ACCESS REVIEW
Certification is the process of reviewing user roles in the IDM system and asserting its validity.

REPORTING
Reporting is the process of extracting the data from the internal database of the IDM system. A report can be generated and used for monitoring and auditing purposes.

RECONCILIATION
The reconciliation process means fetching account profiles and permissions from target systems and publishing it into the IDM system. If accounts present in the target system are not present in the IDM system, various remediation actions like revoking access, creating a request, creating a certification can be performed based on the business requirements.

The following are the key components in the Sath Identity Hub Data Model. The data model requirements, even though commonly used across the industry, are different for each organization.

ACCOUNT
An account is a digital identity with a set of credentials and attributes that is given to a person to authenticate themselves to devices and applications. A person can have multiple identities for respective applications or for performing different tasks.

APPLICATION
An application is software that processes data. Software is generally divided into data processing software and control, system and operating software. Typically, an application is supported using multiple systems such as database, web server, active directory, etc. This systems software is referenced here as target systems. Access to application can be provided by using an account in a target system and adding entitlements to an account provisioned in a target system.
Example: “Application A” requires an entitlement named “App A person” in AD target system.

TARGET SYSTEM
A target system is system software where an Account for a person is physically created, either manually or through automated integrations. It is technically known as application in IDM. A target system may be connected, partially connected or disconnected.

CONNECTED SYSTEM
A connected system will have fully automated provisioning.

PARTIALLY CONNECTED SYSTEM
A partially connected system will have manual provisioning and auto reconciliation.

DISCONNECTED SYSTEM
A disconnected system will have manual provisioning and manual or no reconciliation.

FORM
When a person is provisioned into a target system their digital profile is created. A digital profile consists of name and demographic data. This profile contains a matching attribute and a person identifier. The setup of profile data for each target system is done through forms.
Using forms, target system owners can customize the fields to be included for provisioning. A field marked account name and matching attribute must be unique across all persons. A field marked matching attribute is used to match the person profile in the IDM and the account in the target system.

ENTITLEMENT
Entitlements represent permissions in a target system. An entitlement can only be granted to a person who has an account in the target system. An entitlement can represent access levels, activity permissions or membership to a group, in the respective target system only. Entitlements are granted in IDM and get translated into target systems' configuration when provisioning of that entitlement is complete.

ROLE
A Role is the logical representation of a Persons' functional and/or job responsibilities. Roles can be broad, e.g. "Employee"; or specific, e.g. "AP clerk level 1". Roles are collections of Entitlements. When a role is assigned to a Person they are granted all entitlements associated with that role.
A role is most useful when an application requires granting of multiple entitlements across many target systems.

WORKFLOW
A workflow is the sequence of business processes through which a piece of work passes from initiation to completion (e.g. request a catalog item). It is used to route requests to approvers for approval and to route manual provisioning tasks to second level approvers for fulfillment.

BUSINESS CARE

Before the start of your migration to the Cloud you must first establish the expectations for the migration, define the process and set benchmarks. Sath does all of this with each customer by developing a business case. Within the business case an assessment of prioritization of objectives is outlined. This specifically defines which objectives are of most value to the

customer. Once the objectives are prioritized, the outline of the scope of the project is established. Defined within the scope is what is to be included and what will not be included in the project.

Once all this is established we can determine the operating cost of the identity management system within the Cloud.

From all of this a project plan is developed and put in place.

CONDUCT ANALYSIS

After the initial business requirements are gathered from the application owners and stakeholders, the analysis phase is started. The main objective of the analysis phase is to transform the high-level requirements into unambiguous and stakeholder approved requirements. The outcome of the analysis phase should be a detailed functional requirements document which outlines the business processes and expected behavior of the Cloud IDM system. It will be used to eliminate the ambiguity of expectations regarding the system.

The first step in the process of migration is to analyze the existing on-premise IDM system and understand the various IAM components, data models and business processes associated with each of the target systems. The requirements for the target system should contain detailed information about the applications, target systems, system owners, roles and permissions in the target system. Any business logic that has been implemented in the existing on-premise IDM system for the target system will also be captured.

PREFORM AN ASSESSMENT AND PLANNING

After the initial analysis of the existing IDM system, the planning phase will begin. This phase will determine various project tasks and sub-tasks including scopes, deliverables, resources and budget for each of the tasks. A well-defined communication, risk management, change management and release management plans will be devised in the planning phase. The milestones for the project, timeline for each of the project tasks and the resources required are established. The key performance indicators, service level agreements and critical success factors are defined as well.

Key performance indicator examples are:

- Number of applications onboarded
- Number of provisioning failures encountered in a week
- Number of accounts and entitlements incorrectly catalogued in the system

- Number of incidents created by the end-users in a week/month/quarter
- Number of entitlements assigned to the users without authorization
- Number of entitlements and accounts assigned to the users in IDM and not provisioned in the target system

Service level agreement examples are:
- Response time
- Number of hours estimated
- Post production support
- Responsibilities of the project and the support team

The critical success factors are customized to meet the organization's specific strategic objectives. Critical success factor examples are:
- User experience
- High availability system
- Less system downtime

The design and architecture documents will be developed by the architects in the planning phase. The technical design will contain the technical specifications of the system and connectors to the target system, assumptions, user interface design and description, security requirements, implementation specifics like software and languages used, testing and corrections procedures. The testing plan should contain the testing objectives, test cases, testing schedule, bug reporting and defect tracking procedures.

IMPLEMENT SATH IDENTITY HUB

After the planning and design phase, the next activity will be to install the Sath Identity Hub. The Sath Identity Hub is used to create a seamless migration from an on-premise IDM system to a Cloud IDM system. The Sath Identity Hub Installation will include the installation and configuration of a NoSQL database, microservices to perform various functionalities, load balancer and security infrastructure. An initial upstream sync will be performed for all the target systems, roles and entitlements in the existing IDM system. Then the basic installation of the new cloud IDM system is completed. The applications and users in the existing IDM systems will be migrated over to the new systems in well-defined specific phases.

The Sath Identity Hub provides a single pane of glass as the user interface during migration activities. The users will not experience any kind of interruption in service. Users will login to Sath Identity Hub to request access and view their existing roles. The Sath Identity Hub will be responsible for routing requests to the correct IDM system, either the on-premise or the Cloud IDM system

CONNECT AUTHORITATIVE SOURCES

The authoritative sources for an IDM system is defined as a system with a reliable source of information. The IDM system accepts this data to perform various operations like creating and updating a user profile or assigning roles and entitlements. The authoritative sources can include; HR systems, vendor management systems and customer databases, which can be used to create a user profile in an IDM system. The learning management system (LMS) is a type of authoritative source where the data from the system is used to update user's qualifications in an IDM system. After installing the Cloud based IDM system, the first step to perform is to connect the authoritative sources. At this point, the authoritative sources are connected to both IDM systems. The connection between the authoritative sources to the old IDM system cannot be discarded until the migration is completed.

Before connecting the authoritative sources to the Cloud IDM system, the schemas for the authoritative sources will be determined. The mapping between the IDM attributes and the system attributes are clearly defined. The authoritative source will be identified as the downstream system where the IDM reads the data from or an upstream system where the IDM provisions data. If there is a discrepancy between the IDM system and the authoritative sources, the overwrite rule should be clearly defined to indicate whether the data in the IDM system should be modified or the data in the authoritative source needs to be modified. The periodic synchronization will be implemented depending upon the business requirements.

MIGRATE DIRECTORIES AND DATA STORES

The authoritative sources for an IDM system is defined as a system with a reliable source of information. The IDM system accepts this data to perform various operations like creating and updating a user profile or assigning roles and entitlements. The authoritative sources can include; HR systems, vendor management systems and customer databases, which can be used to create a user profile in an IDM system. The learning management system (LMS) is a type of authoritative source where the data from the system is used to update user's qualifications in an IDM system. After installing the Cloud based IDM system, the first step to perform is to connect the authoritative sources. At this point, the authoritative sources are connected to both IDM systems. The connection between the authoritative sources to the old IDM system cannot be discarded until the migration is completed.

Before connecting the authoritative sources to the Cloud IDM system, the schemas for the authoritative sources will be determined. The

mapping between the IDM attributes and the system attributes are clearly defined. The authoritative source will be identified as the downstream system where the IDM reads the data from or an upstream system where the IDM provisions data. If there is a discrepancy between the IDM system and the authoritative sources, the overwrite rule should be clearly defined to indicate whether the data in the IDM system should be modified or the data in the authoritative source needs to be modified. The periodic synchronization will be implemented depending upon the business requirements.

PILOT ROLLOUT CONSIDERATIONS/POSSIBILITIES

The migration process occurs in a multi-phase approach, during which time a group of applications are migrated in each phase. There will be an initial reconciliation of all the access in the target system into the Cloud IDM system. All the access that is assigned to the users, as part of the initial reconciliation, are considered authorized. After the migration of a target system is completed, all the provisioning and de-provisioning requests for that target system will be routed to the Cloud IDM system from the Sath Identity Hub. End-Users will login to the Sath Identity Hub to request access. This process will minimize confusion during the migration process and help to resolve issues quicker. If there is a bug identified in the provisioning or deprovisioning process, the requests are routed back to the old on-premise IDM system. After the bug fix is implemented, the requests will be re-routed to the Cloud IDM system. The group of applications to be migrated in each phase of the migration is determined by various factors. The applications can be grouped according to business units, geographical location, risk levels, business importance or end-user population (employee, vendor, student, faculty etc.).

DISCONNECTED APPLICATION ONBOARDING

The Sath Identity Hub will be used for the automated provisioning of disconnected applications. It provides a self-service capability to the business user to onboard their application(s) as disconnected target systems. It encapsulates the technical complexity from the end user and automates the process of creating a disconnected target system. The technical details required for creating a target system, roles and entitlements is collected and stored in a spreadsheet. The business analysts then input the details to onboard the application using the “New Application Wizard”. The New Application Wizard is either a three or five step process.

NEW APPLICATION WIZARD

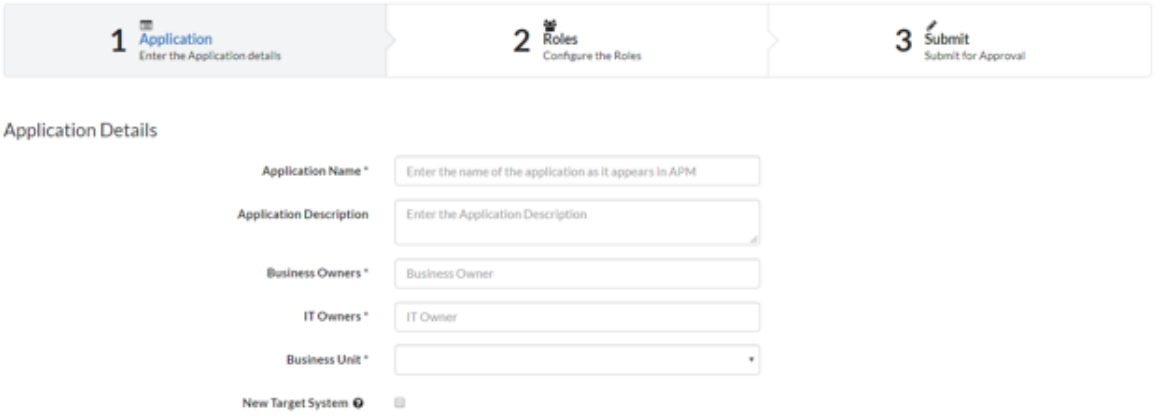


*Fig: Three-step wizard process used when a new target system is not required to onboard an application into IDM system

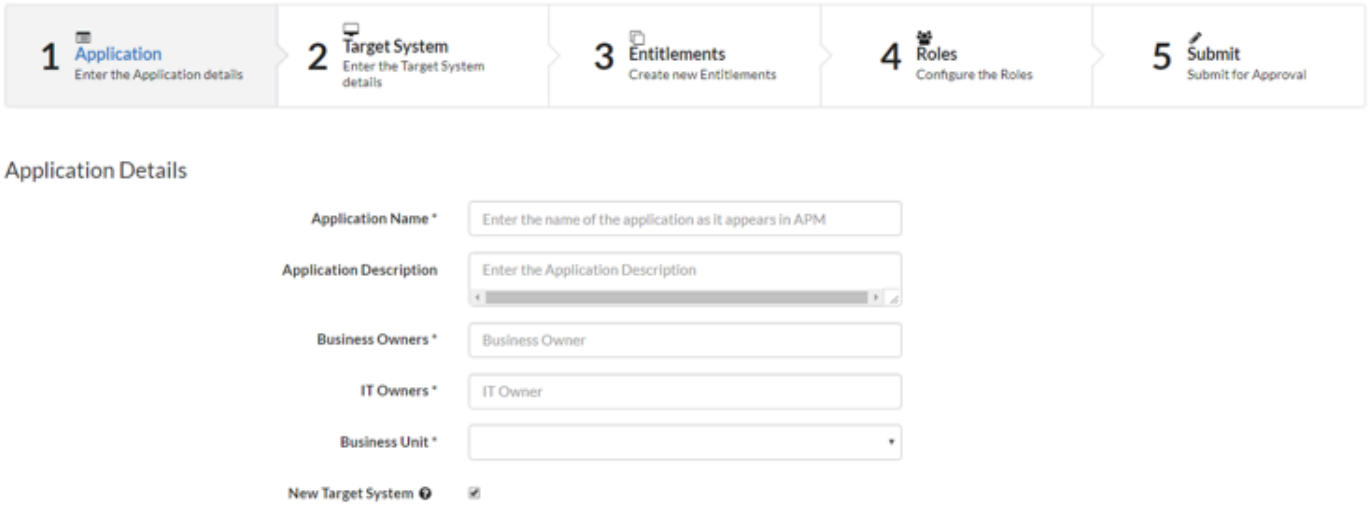


*Fig: Five-step wizard process to create a new disconnected target system and entitlements

After the request for creating a new disconnected target system is approved by the application owner and the Identity and Access Management Support team, the disconnected application is automatically provisioned in the Cloud IDM system.

MIGRATE CONNECTED SYSTEMS TO SCIM INTERFACE

The System for Cross-domain Identity Management (SCIM) standard is designed for the CRUD operations of user identities in IT systems. Using SCIM connectors for the IDM system increases the interoperability.

Connections to the SCIM based target system can be authenticated by HTTP Basic Authentication or OAuth 2.0 authentication or other custom authentication mechanisms. SCIM interface provides a REST API which supports everything from patching a specific attribute on a resource to doing massive bulk updates. IDM system will make a REST API call to the SCIM interface and the SCIM interface will translate the request of the IDM to the target system. Implementing SCIM interfaces will make migrations to other IDM systems simpler.

FOLLOW-UP POST PRODUCTION SUPPORT

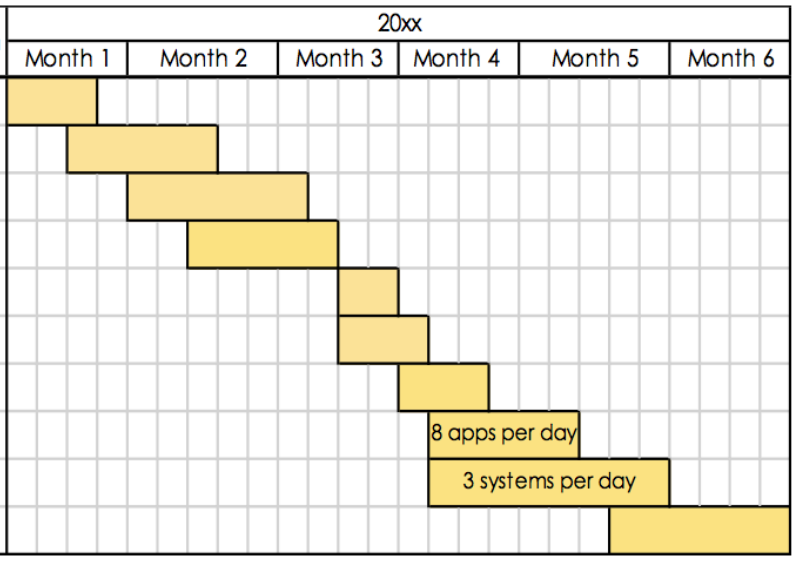
A knowledge base will be created with all the documentation from the planning, design and implementation phases. This documentation will include;

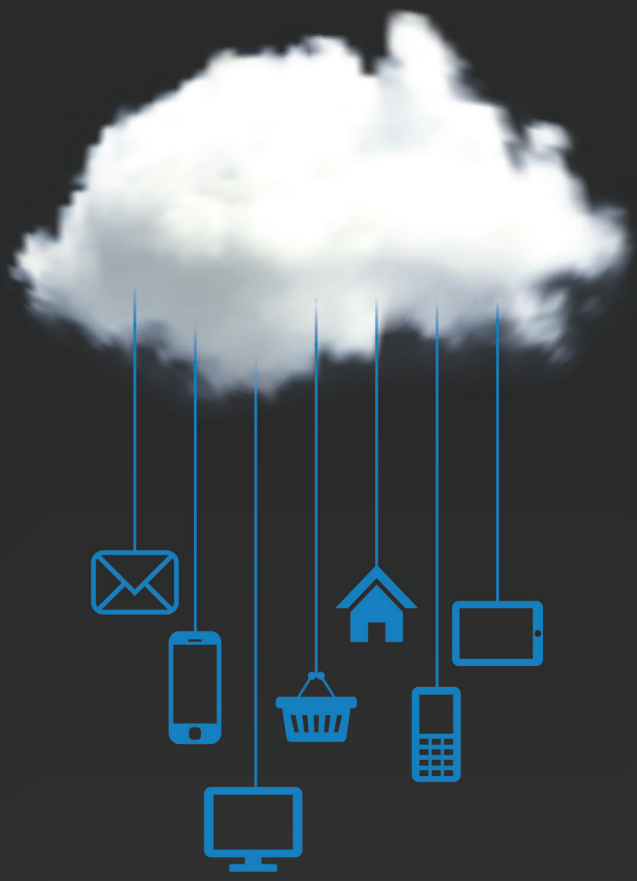
- Functional requirements
- Business requirements
- Technical design
- Testing documentation

A detailed run-book with the procedures to perform operations that needs to be performed on a regular basis will be provided to the support team. The source code for the connectors will also be a part of the project deliverables. The project team will provide knowledge transfer to the support team and will be available for the post production support for two weeks after go-live

TYPICAL CLOUD TRANSITION TIMELINE

Task Name	Duration
Business Case	3 weeks
Analysis	5 weeks
Assessment and Planning	5 weeks
Implement IDM Solution /Sath Hub	5 weeks
Connect Authoritative Sources	2 weeks
Migrate Directories and Data Stores	3 weeks
Pilot Rollout	3 weeks
Disconnected Application Onboarding	5 weeks
Connected Systems to SCIM Interface	8 weeks
Post Production Support	6 weeks





sath

855 SATH COM | 125 W. Central Rd. | Schaumburg, IL | 60195 | teamSATH@sath.com | sath.com