UDV Technologies One Identity Manager

Access management automation and privileges control

OVERVIEW

Problem: The Customer is looking for the solution to automate access approval and provisioning processes.

Project milestones: Define access approval and access provisioning procedures. Develop and implement data templates for usage analytics. Integrate with existing systems. Customize the Self-Service Portal for corporate end users.

Result: The implemented solution based on One Identity Manager (IDM) allows the Customer to automate access management. Additional benefits include granular control and usage analytics.

Plans: Further plans focus on business and system role management development and implementation, including business role lifecycle management, integration with new IT systems and the SIEM solution used by the Customer.

CUSTOMER PROFILE

The Customer is a Financial institution, operating in more than 150 cities across CIS.

The Companies that are part of the conglomerate share the IT resources and use common mail system.

The Company employs about 5 000 employees, including staff and external contractors

STARTING POINT

HR-management is facilitated by a hybrid HR system comprising two solutions from different vendors.

User account management is automated via in-house developed scripts supported by the HR admins and target system support personnel.
According to internal Customer procedures, obtaining access requires the user to complete the required training courses and pass the corresponding test in the WebTutor solution, adopted by the Customer.

Access provisioning starts with the access request from the end user. Support engineers, security admins and target system admins verify access legitimacy, confirm prerequisites are complete, obtain the list of approvers and finally configure the access. All of the above is performed in a manual mode. No unified access provisioning regulations exist – lists of approvers are solely based on the existing practice.

Provisioning access on a user request basis requires significant manual labor for both request and approval processing.

Furthermore, no tools are implemented that verify the correctness of the access provisioned or help with access revocation.

Management concerns

Although access provisioning that is based on a user request has proven itself to be secure, it has long been outdated in terms of flexibility and associated costs. It requires the Company to maintain the relevance of multiple regulations, as well as various lists of approvers. The growing number of employees leads to further increase in the overhead associated with approval and provisioning processes.

Average end user access provisioning may take up to 5 days.

Security administrator position

IT security in financial institutions is strictly regulated by the state, however each regulation has specific requirements related to access control and management.

The mix of the human factor introduced during prerequisites verification, approver lists generation and processing, as well as during actual access provisioning, with the absence of control over these processes, is prone to errors, such as excessive access privileges or incorrect access configuration.

Verification of the access privileges granted to each user is very labor-intensive. There is a need for a tool, that would allow security team to maintain the full view of the access matrix and highlight excessive or illicit access privileges that may cause security incidents.

PROJECT TASKS

- Perform a deep analysis of the existing access management process, including unification and optimization of the approval process. Formalize the request form for all systems.
- Develop basic access privilege set, sufficient for provisioning and revoking access to target systems.
- Integrate One Identity Manager with the existing HR systems, WebTutor competence management system and target systems, incl. MS Active Directory and MS Exchange. Integration with HR systems utilizes the existing data plane service based on IBM WebSphere MQ and software APIs.
- Develop automation for access provisioning and revocation, access approval and privilege delegation via Self-Service Portal.
- Develop and implement automated access authorization procedures to monitor and verify all granted privileges.
- Deploy reporting functions concerning user roles, access authorization states, target systems' owners, internal IDM processes, access-related risks for multiple departments and Company as a whole.

RESULTS

One Identity Manager has become a versatile tool for consolidating and automating user credentials management as well as access management for corporate IT services.

Automating access approval and provisioning allowed the Customer to decrease the corresponding labor of the first line support engineers and security administrators and led to a significant minimization of the processing time per each request bringing it to **2 hours average**.

Automated basic access provisioning based on HR events, collected from the HR systems, requires **no more than 3 minutes**.

Access privilege control is performed during access authorization. Authorization is initiated either automatically or per security administrator's request. Access authorization is a robust method of controlling active privileges.

Detailed reporting allows the Customer to analyze security risks, related to access provisioning.
IDM Self-Service Portal streamlined and simplified access request, revocation and approval processes for all target systems and provided the tool for secure privilege delegation, which has a positive influence on the access provisioning time.

FUTURE PLANS

Further optimization of the access management via One Identity Manager focuses on expanding automated basic access provisioning, development and implementation of the business and system role management.

Company business plans require developing and deploying new business processes. One Identity Manager supports implementation of arbitrary new processes via a built-in visual editor.

IDM can be integrated with new systems incl. new target IT systems and other special systems, e.g. security incident management system.