it-sa EXPO Congress 2021 in Nuremberg

Meet our IAM-experts live

by ASCONSIT | Published on 23. September 2021



Experience the latest and most important IT security issues on site.

ASCONSIT offers smart and efficient software, consulting, development and support solutions for emerging identity and access management trends. Key topics presented in Nuremberg include:

Optimised identity and access governance (IAG) software solutions

1. Active Roles und ActiveDirectory (AD) as an “IdM light” solution

Storage of the AD in a hybrid environment gives rise to a wide range of risks and uncertainties. Current challenges include admin access to the AD, a lack of compliance with policies, unclear assignment of privileges, auditing requirements, inconsistent AD and AAD procedures. We would like to tackle these with you.

With Active Roles is One Identity’s compact system for solving these problems quickly.

Active Roles offers the following support:

- Account lifecycle management
- Least privilege principle
- Review and implementation of guidelines
- Access control
- Automation using a workflow featuring a scripting engine
- Self-services via the web portal
- Synchronisation with other systems as well as
- Central reporting and full change history

2. New features of OI IM release 8.2 at a glance

- Modern web application architecture with even more user-friendly and adaptable presentation based on the Angular platform
- Database improvements in the form of Azure SQL Managed Instances
- Improved and extended MS Azure AD integration
- Splitting of the central database into two databases (database 1 for data retention, and database 2 for processes and their objects → improved performance)
- LDAP connector enhancement for older LDAP systems
- First MS Teams integration
- Further improved SAP integration through web service integration
- Significantly improved EPIC integration for the healthcare sector
- New improved application governance
    - In addition to access requests, confirmations and re-certifications, divisions should be able to update their own apps with privileges
    - This includes a full overview, ownership, SoD, KPIs from a business point of view
    - The IT team can focus on actual platform maintenance

- New Business Service screen for managing applications, active directories and databases
    - The Business Service screen contains all relevant objects related to this service
    - This gives rise to a new layer for more effective administration and cluster formation
- User accounts, groups and group objects that do not exist in the database are indicated as ‘pending’ → improved data processing and greater clarity

Privilegiertes Access Management

Privileged Access Management (PAM)

Privileged accounts have become a necessity in corporate IT environments, as administrators need extended privileges to be able to manage the environment.

However, privileged accounts lead to massive compliance and security risks as a result, making them popular targets of hacking attacks.

This is why it is essential that companies manage privileged access effectively and safely.

We recommend the following measures to ensure privileged accounts are managed safely:

- Prepare a list of your privileged accounts, including the users and systems that use the accounts.
- Make sure that your privileged passwords are stored reliably.
- Establish strict administrative processes for changing passwords of privileged accounts.
- Ensure clear responsibilities wherever possible, and do not grant more than the minimum of privileges required.
- Perform regular checks of privileged access use.

Safeguard von One Identity

Safeguard by One Identity allows for privileged access to be safely stored, managed and analysed.

Safeguard helps to minimise damage due to loss or misuse of data, as well as offering companies a safe method for protecting privileged accounts and for improving IT security in a sustainable manner.

For this purpose, Safeguard is operated on a hardened instance with limited access. The application provides optimum protection for all privileged accounts

by combining session management and monitoring with comprehensive analysis options. Suspicious activities and threats can therefore be detected early on, and corresponding protection measures can be initiated.

Used together, the two products allow for Privileged Account Governance (PAG) featuring unique account access, uniform lifecycle management and the Identity Manger.

Product characteristics & features:

- Guideline-based authorisation control
- Identification of risky users
- User behaviour analysis
- Real-time alerts and blocking
- Individual security concepts for privileged passwords and sessions
- Systematic command and application control via whitelisting/blacklisting
- Support of numerous protocols (SSH, Telnet, RDP, HTTP(s), ICA and VNC)
- REST-based API for easier integration of applications and systems

Your benefits at a glance:

- Observance of compliance demands
- Efficient creation of monitoring reports
- Easier management of privileged accounts and sessions
- Attenuation of potential damage caused by security breaches
- Improved protection of sensitive data and company information
- Identification of privileged high-risk users, risky behaviour and unusual events

Could-based IAM solutions

SAP solutions

The ongoing development to shift applications to the cloud, and the resulting combined on-premise and cloud-based landscapes, require suitable IAM solutions. With its SAP Cloud Platform (SCP), SAP offers comprehensive cloud identity services.

SAP Cloud Identity Authentication Service (IAS)

features authentication, single sign-on and user management. It can be used as an identity service provider or as a proxy for integration into an existing single sign-on infrastructure.

SAP Cloud Identity Access Governance (IAG)

features access control, compliance management, control and risk management, self-service, privilege risk analyses and role design. Each of the services included in SAP Cloud IAG can be integrated independently or combined with others.

SAP Cloud Identity Provisioning Service (IPS)

offers automated identify lifecycle processes. Privileges and identities for local business applications and cloud applications are provided for this purpose. It can be described as the counterpart of SAP Identity Management for a hybrid environment. Together with the SAP Cloud Platform Identity Authentication Service (IAS) and the cloud-based governance services (SAP Cloud Identity Access Governance (IAG)), this service constitutes a solution for access and identity management. SAP IPS is a solution for access and identity management in cloud-based applications for companies operating a hybrid IT landscape.

Azure Management

Even contemporary IAM solutions need to face the challenge of ensuring that public cloud solutions are handled appropriately with regard to security issues. AD Management by One Identity is a solution that is compatible with a hybrid system. It ensures management of Azure/Office 365 objects such as users and groups during creation, reading, updating and deleting. The solution allows for licence management with a dynamic population of license information.

Arrange your personal meeting with ASCONSIT's security experts in advance at:

ASCONSIT GmbH

Zeppelinstraße 21
21337 Lüneburg

Tel.: +49 4131 / 60 41 68 - 0
Fax : +49 4131 / 60 41 68 – 75
E-Mail: info@asconsit.com