# it-sa EXPO Congress 2021 in Nürnberg

## Treffen Sie unsere Sicherheits-Experten live

von ASCONSIT | Veröffentlicht am 23. September 2021


Die wichtigsten und aktuellsten IT-Security Themen vor Ort jetzt wieder real erleben.

Für die neusten Trends im Identitäts- und Accessmanagement bietet ASCONSIT smarte und effiziente Lösungen mit Software, Consulting, Entwicklung und Support. Die Schwerpunktthemen in Nürnberg sind:

Optimale Identity und Access Governance (IAG) Softwarelösungen

**1. Active Roles und ActiveDirectory (AD) als "IdM light"**

Die Sicherung des AD in einer hybriden Umgebung ist voller Ungewissheiten und Risiken. Admin-Zugänge im AD, fehlende Durchsetzung von Policies, unübersichtliche Zuweisungen von Rechten, Anforderungen durch Audits, uneinheitliche Praktiken für AD und AAD sind die aktuellen Herausforderungen. Diese gehen wir gerne mit Ihnen gemeinsam an.

One Identity bietet mit *Active Roles* ein kompaktes System diese Herausforderungen in kurzer Zeit zu lösen.

Active Roles stellt folgende mögliche Unterstützung für Sie bereit:

- Account Lifecycle Management
- Prinzip der minimalen Rechte (Least-Privilege-Prinzip)
- Richtlinienprüfung und deren Durchsetzung
- Access Control
- Automatisierung durch Workflow mit Hilfe einer Scripting Engine
- Self-Services im Web-Portal
- Synchronisation mit anderen Systemen und
- zentrales Reporting und vollständige Änderungshistorie

**2. Neueste Features des OI IM Release 8.2 im Überblick**

- Moderne Web Applikations-Architektur in noch benutzerfreundlicherer und anpassungsfähigerer Darstellung auf Basis der Angular-Plattform
- Datenbank Verbesserungen in Form von Azure SQL Managed Instanzen
- Verbesserte und erweiterte MS Azure AD Integration
- Split der zentralen Datenbank in zwei Datenbanken (1. Datenbank für Datenhaltung und 2. Datenbank für Prozesse und deren Objekte → Verbesserte Performanz)
- LDAP Konnektor Erweiterung für ältere LDAP Systeme
- Erste MS Teams Integration
- weiter verbesserte SAP-Integration durch Web Service Integration
- deutlich verbesserte EPIC Integration im Gesundheitsbereich
- neue verbesserte Application Governance
    - Neben den bisherigen Access Anfragen und Bestätigungen und Rezertifizierungen sollen Fachbereiche in der Lage sein, ihre eigenen Apps mit Berechtigungen zu pflegen
    - Dazu gehört der komplette Überblick, Eigentümerschaft, SoDs, KPIs aus Business Sicht
    - Das IT Team hat den Fokus auf die eigentliche Pflege der Plattform

- Neue Business Service Sicht für die Verwaltung von Applikationen, Active Directories und Datenbanken
    - Der Business Service enthält alle relevanten Objekte, die zu diesem Service gehören
    - Damit entsteht eine neue Schicht zur besseren Verwaltung und Clusterbildung
- Benutzerkonten, Gruppen, Gruppenobjekte, die nicht in der Datenbank existent sind, werden als "ausstehend" gekennzeichnet → Verbesserte Verarbeitung von Daten und bessere Übersichtlichkeit

Privilegiertes Access Management

**Privileged Access Management (PAM)**

Privilegierte Konten sind in Unternehmens-IT-Umgebungen heutzutage eine Notwendigkeit, denn Administratoren benötigen erweiterte Berechtigungen für die Verwaltung der Umgebung.

Privilegierte Konten führen jedoch gerade dadurch zu massiven Compliance- und Sicherheitsrisiken und sind deshalb das bevorzugte Angriffsziel von Hackern.

Aus diesem Grund ist es für Unternehmen von essenzieller Bedeutung, privilegierte Zugriffe effektiv und sicher zu verwalten.

**Wir empfehlen folgende Punkte für eine sichere Verwaltung von privilegierten Konten:**

- Führen Sie eine Bestandserfassung Ihrer privilegierten Konten durch, einschließlich der Benutzer und Systeme, die diese verwenden.
- Stellen Sie sicher, dass Ihre privilegierten Kennwörter zuverlässig gespeichert sind.
- Setzen Sie strenge Verwaltungsprozesse zur Änderung von Kennwörtern für privilegierte Konten durch.
- Sorgen Sie nach Möglichkeit für klare Verantwortlichkeiten und gewähren Sie nur das erforderliche Mindestmaß an Berechtigungen.
- Prüfen Sie die Nutzung von privilegiertem Zugriff regelmäßig.

**Safeguard von One Identity**

Privilegierte Zugriffe sicher speichern, verwalten und analysieren mit Safeguard von One Identity.

Der Safeguard ermöglicht, Schäden durch Datenverlust oder -missbrauch zu minimieren und bietet Unternehmen eine sichere Methode zum Schutz privilegierter Konten und nachhaltiger Verbesserung der IT-Sicherheit.

Hierfür wird der Safeguard auf einer gehärteten Instanz betrieben, auf die nicht jeder Zugriff hat. Die Anwendung bietet bestmöglichen Schutz für sämtliche privilegierte Konten, in dem er eine Sitzungsverwaltung und -überwachung mit umfassenden Analysemöglichkeiten kombiniert. So können auffällige Aktivitäten und Bedrohungen frühzeitig erkannt und entsprechende Schutzmaßnahmen initiiert werden.

Für einen eindeutigen Account-Zugriff und ein vereinheitlichtes Lifecyle Management zusammen mit dem

Identity Manager bieten die beiden Produkte in Kombination die Möglichkeit von Privileged Account Governance (PAG).

**Produktmerkmale & Features:**

- Richtlinienbasierte Freigabekontrolle
- Ermittlung von risikobehafteten Benutzern
- Analyse des Benutzerverhaltens
- Warnen und Blockieren in Echtzeit
- Individuelle Sicherheitskonzepte für privilegierte Passwörter und Sitzungen
- Systematische Befehls- und Anwendungskontrolle via weißer/schwarzer Liste
- Unterstützung zahlreicher Protokolle (SSH, Telnet, RDP, HTTP(s), ICA und VNC)
- REST-basierte API für eine vereinfachte Integration von Anwendungen und Systemen

**Ihr Nutzen auf einen Blick:**

- Erfüllung von Compliance-Anforderungen
- Effiziente Erstellung von Überwachungsberichten
- Vereinfachung der Verwaltung privilegierter Konten und Sessions
- Abmilderung des potenziellen Schadens von Sicherheitsverstößen
- Verbesserter Schutz für sensible Daten und Unternehmensinformationen
- Identifizierung von privilegierten Benutzern mit hohem Risiko, riskantem Verhalten und ungewöhnlichen Ereignissen

Cloudintegrierte IAM-Lösungen

**SAP-Lösungen**

Die fortschreitende Entwicklung der Verlagerung von Anwendungen in die Cloud, die Kombination von On-Premise und Cloud-basierten Landschaften erfordern geeignete IAM-Lösungen. SAP bietet mit der SAP Cloud Plattform (SCP) umfassende Cloud Identity Services.

**SAP Cloud Identity Authentication Service (IAS)**
beinhaltet Authentifizierung, Single Sign-On und Benutzerverwaltung. Es kann selbst als Identitätsanbieter fungieren oder als Proxy zur Integration in eine vorhandene Single-Sign-On-Infrastruktur verwendet werden.

**SAP Cloud Identity Access Governance (IAG)**
beinhaltet die Zugriffssteuerung, Compliance Management, Kontroll- und Risikomangement, Self-Service, Berechtigungs-Risikoanalysen und Rollendesign. Jeder der im Lieferumfang von SAP Cloud IAG enthaltenen Services kann unabhängig oder in Kombination integriert werden.

**SAP Cloud Identity Provisioning Service (IPS)**
stellt automatisiert Identitäts-Lifecycle-Prozesse zur Verfügung. Hierzu stehen Berechtigungen und

Identitäten für die lokalen Geschäftsanwendungen und Cloud- Anwendungen bereit. Es lässt sich als Gegenstück des SAP Identity Managements erklären in einer hybriden Umgebung. Der Dienst bietet gemeinsam mit dem SAP Cloud Platform Identity Authentication Service (IAS) und mit dem Cloud-basierten Governance Service (SAP Cloud Identity Access Governance (IAG)) eine Lösung für das Access- und Identity-Management. Unternehmen, die eine hybride IT-Landschaft haben, können durch den SAP IPS eine Lösung für die Zugriffs- und Identitätsverwaltung innerhalb der Cloud- Anwendungen erhalten.

**Azure Management**
Auch moderne IAM-Lösungen stehen heute vor der Herausforderung einen sicherheitsrelevanten Umgang mit Public Cloud Lösungen zu gewährleisten. Mit AD Management von One Identity ist eine hybrid-fähige Lösung verfügbar. Sie stellt die Verwaltung von Azure/Office 365 Objekten wie Benutzer und Gruppen in den Phasen Erstellung, Lesen, Anpassen, Löschen sicher. Lizenzmanagement mit dynamischer Population von Lizenzinformationen sind möglich.

**Vereinbaren Sie Ihren persönlichen Termin mit den Sicherheits-Experten von ASCONSIT vorab unter:**


## 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