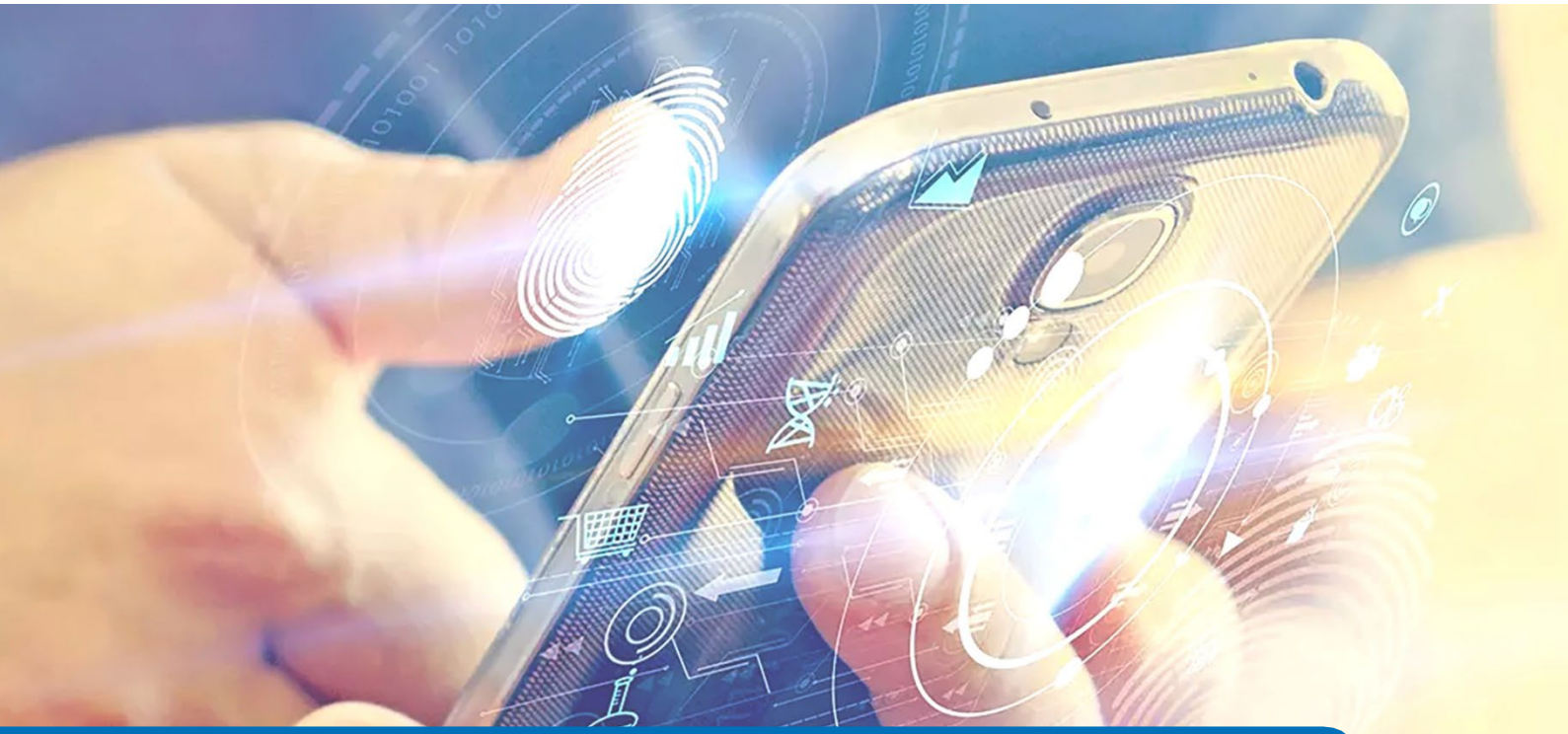


Fallbeispiel

FSP unterstützt einen international tätigen Versicherungskonzern bei der Umsetzung der Multi-Cloud-Strategie

Keycloak-Implementierung einer 2-Faktor-Authentifizierung für die AWS-Management-Konsole

IT-Security stärken durch optimierte Benutzerverwaltung beim Zugang zur AWS-Cloud

IT-Security stärken: Optimierung des Zugangs zur AWS-Cloud

Seit mehreren Jahren nutzt der Kunde die Cloud-Computing-Plattform Amazon Web Services (AWS). Immer mehr Projekte und damit auch Entwickler aus verschiedenen Ländern arbeiten in der AWS-Cloud. Um die Management-Konsole zu verwenden, müssen sie sich für die Plattform anmelden und benötigen die entsprechenden Rechte. Die Benutzerverwaltung beansprucht viele Ressourcen im Cloud-Team, die bei der Weiterentwicklung an anderer Stelle benötigt werden.

Der Zugriff von externen Nutzern über das Internet, und nicht aus dem internen Netzwerk des Kunden, ist unter Sicherheitsaspekten eine zentrale Herausforderung: Zur Gewährleistung der IT-Security war die Einführung eines 2. Faktors unerlässlich. Dies wurde bislang nicht unterstützt.

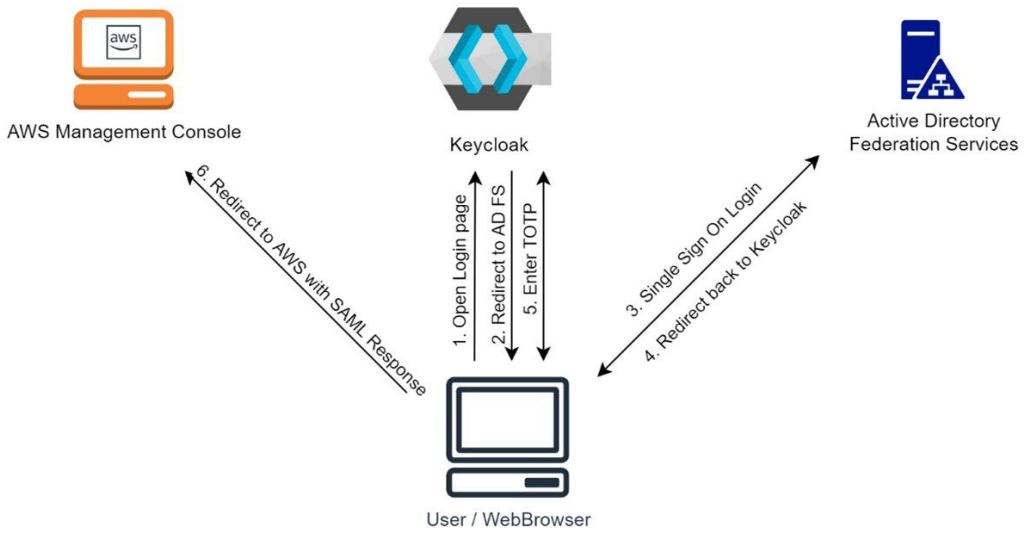
Mit 2. Faktor anmelden

Ziel war es daher, die Anmeldung der Entwickler an der AWS-Management-Konsole sicher und einfach zu gestalten, um die AWS-Cloud auch aus dem Internet heraus zugänglich zu machen – nicht nur für Deutschland, sondern international.

Dabei sollte das vorhandene Windows-Login mittels Single-Sign-On-Zugriff auf Systeme und Anwendungen genutzt werden. Der Kundenwunsch lautete, die erforderlichen Benutzerrechte über vorhandene ActiveDirectory-Gruppen zu vergeben und eine Anmeldung auch für AWS CLI (Command Line Interface) zu ermöglichen. Ziel war zudem, das Mapping von Rechten in AWS-Projekten für Benutzergruppen im ActiveDirectory durch Projektleiter administrierbar zu gestalten.

Keycloak:
Sichere Anmeldung mit System

Die nachfolgende Grafik veranschaulicht, wie diese Herausforderung optimal gelöst wurde: Zur Anwendung kommt die IAM-Lösung Keycloak, die ein sicheres und einfaches Identity & Access Management ermöglicht.



- Einsatz von Keycloak als Identitätsanbieter “in der Mitte” zwischen Active Directory Federation Services und der Anwendung (z. B. AWS Management Console)
- Keycloak ist Service Provider gegenüber ADFS (SAML)
- Keycloak ist Identity Provider gegenüber AWS Management Console
- Ein 2. Faktor Time based One Time Password ergänzt die Anmeldung über das ADFS, verwaltet in Keycloak. Bei der ersten Anmeldung über Keycloak wird dieser 2. Faktor mithilfe eines Wizards für den Benutzer eingerichtet
- Zuordnung von Rollen in AWS zu Gruppen im Active Directory erfolgt über “Composite Roles” in Keycloak
- Beim Anlegen eines Projektes in AWS werden entsprechende Rollen in AWS und Keycloak automatisch definiert (Owner, Maintainer, Developer, Reporter) und dem Projektleiter die Rolle “Owner” zugewiesen
- Projektleiter kann durch Tags an den AWS-Rollen diese Active-Directory-Gruppen zuweisen

Betrieb der Lösung in der Praxis

In der AWS-Cloud wurden drei Umgebungen für Keycloak aufgebaut (Entwicklung, Fachtest und Produktion). Die Produktivumgebung läuft in einem Cluster, sodass der Ausfall einer Instanz nicht dazu führt, dass keine Anmeldung mehr möglich ist.

Aufgrund des geringen Ressourcenbedarfs von Keycloak (CPU, RAM) kann die Lösung kostengünstig betrieben werden. Die Anbindung von Keycloak an das ADFS sowie von AWS an Keycloak erfolgt über SAML 2.0 (Security Assertion Markup Language).

Mittlerweile ist NetIQ Access Manager, der bei einer Konzerntochter im Einsatz ist, als zweiter Identitätsanbieter neben dem ADFS angebunden. Das PowerShell-Tool für die Anmeldung in AWS CLI wurde erstellt.

2. Faktor eingeführt – und weitere Web-Features geplant

Die erfolgreiche Einführung der Lösung hat das Cloud-Team bei der Benutzeradministration deutlich entlastet. Der verpflichtende 2. Faktor gewährleistet die sicherere Authentifizierung.

Keycloak unterstützt SAML 2.0 und OpenID-Connect – damit sind alle modernen Webanwendungen integrierbar.

Wie geht es weiter?

Aktuell wird die Anbindung von OpenSearch (ElasticSearch) für die Kostenanalyse in der Cloud entwickelt. So haben Projektleiter die Kosten ihres Projektes im Überblick, ohne Zugriff auf die Gesamtkosten zu haben. Künftig werden zudem zahlreiche weitere Web-Anwendungen in der Cloud angeschlossen.

Als weiteres Feature ist geplant, auf den 2. Faktor zu verzichten, wenn die Anmeldung von einem gemanagten Notebook aus dem internen Netzwerk des Unternehmens erfolgt.

FSP – Ihr starker Partner für die sichere Digitalisierung

Alle reden über die Digitalisierung – wir packen sie an: Die FSP GmbH bietet seit 2001 Consulting & IT-Services für sichere digitale Kunden- und Geschäftsprozesse. Als anerkannter Partner namhafter mittelständischer und großer Unternehmen aus unterschiedlichen Bereichen beraten wir mit fachlicher, IT- und methodischer Kompetenz und schaffen so die richtigen Lösungen für IAM und sichere Digitalisierung. Von unserem Standort Köln aus sind wir mit einem hoch qualifizierten 50-köpfigen Team deutschlandweit für Sie aktiv.

Wir gestalten Ihre digitale Zukunft

FSP unterstützt Sie ganzheitlich in allen Projektphasen – von der Analyse und Beratung über das Projektmanagement und die Auswahl und Integration der richtigen Produkte bis zum Support. Dabei greifen wir auf die Standardsoftware unserer Partnerunternehmen zurück oder entwickeln bei Bedarf völlig neue, individuelle Lösungen für Sie. Unsere Schwerpunkte:

- **Konzeption und Umsetzung innovativer Digitalisierungsprojekte, z. B. auf den Gebieten digitale Geschäftsprozesse, RPA, digitale Kommunikation und sichere Digitalisierung**
- **Ganzheitliches Identitäts- und Berechtigungsmanagement (Identity & Access Management – IAM)**
- **Operative und steuernde Unterstützung bei der Durchführung von Projekten oder IT-Umsetzungsmaßnahmen**
- **Branchenfachliche Beratung**
- **Optimierung von Prozessen zur Effizienzsteigerung**
- **Projekt-, Test- und Anforderungsmanagement**

Ihr Ansprechpartner

Tobias Peper
Projektleiter Keycloak-Integration

Kontaktdaten

FSP GmbH Consulting & IT-Services
Albin-Köbis-Straße 8 | 51147 Köln
Telefon: +49 (0) 2203 37 10 00 0
E-Mail: info@fsp-gmbh.com | www.fsp-gmbh.com