In dieser Artikelserie möchten wir einen Überblick über mögliche Optionen für Unternehmen geben und eine kurze Einschätzung über Stärken und Schwächen der jeweiligen Lösungen vornehmen. Bitte beachten Sie, dass diese Einschätzungen **keineswegs als abschließend betrachtet werden können** und **keine individuelle Beratung** ersetzen.

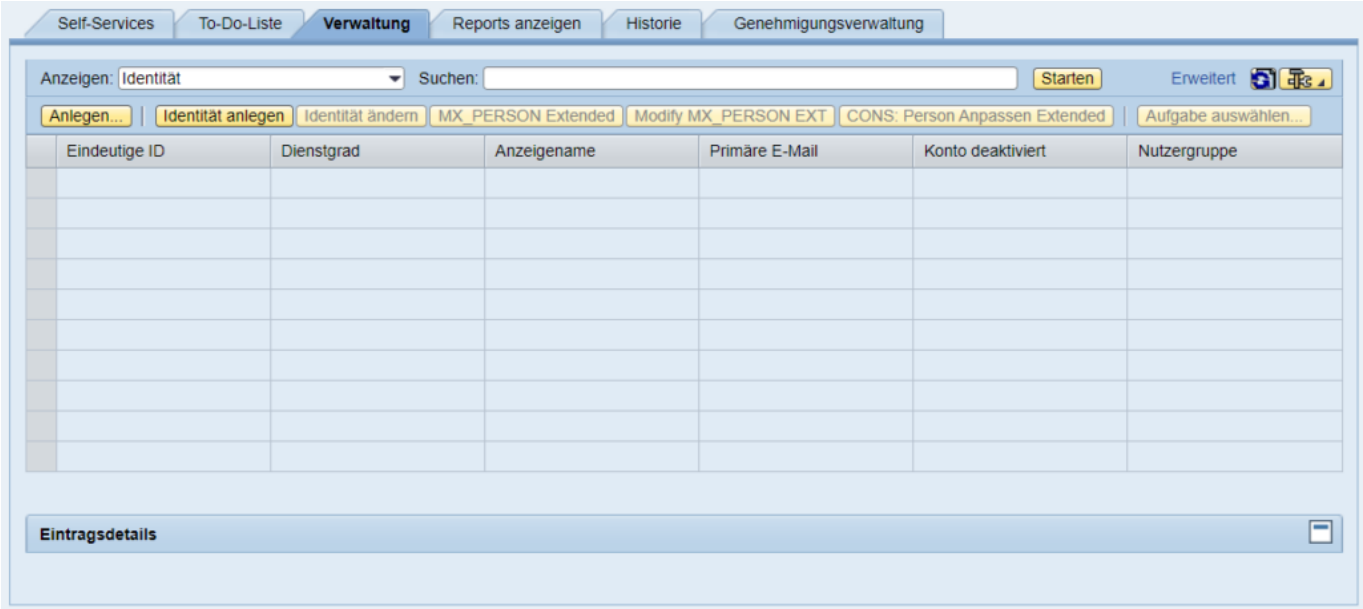
- Teil 1: Das Ende einer Ära – Die Zukunft nach SAP IDM
- **Teil 2: SAP – Cloud Identity Services, GRC edition for SAP HANA**
- Teil 3: Cloud Services – Microsoft Entra, Okta, Omada Identity
- Teil 4: On-Premise Lösungen – z.B. One Identity, SIVIS

Dieser Teil wirft einen vertieften Blick auf die diversen SAP-Lösungen, die für Unternehmen aller Größen und Branchen von zentraler Bedeutung sind. Als Einführung behandeln wir das fortlaufende Betreiben von SAP Identity Management, was sicherlich zumindest eine vorübergehende Lösung vieler SAP Kunden sein wird. Zu den Schlüsselkomponenten der Zukunft gehören die SAP Cloud Identity Services in Kombination mit SAP Identity and Access Governance (IAG). Darüber hinaus beleuchten wir die Bedeutung von SAP CAP (Cloud Application Programming) Applikationen, die ggf. zum Schließen der funktionalen Lücken der Cloud Infrastruktur beitragen können. Abschließend wird auf SAP GRC (Governance, Risk, and Compliance) eingegangen, welches eine entscheidende Rolle bei der Gewährleistung von Unternehmenskonformität und Risikomanagement spielt, jedoch nicht selten auch für die Implementierung eines Identity Managements verwendet wird.

- Option A: Weiteres Betreiben von SAP IDM 8.0
- Option B: Mit SAP IDM 8.0 in die Cloud?
- Option C: SAP Cloud Identity Services – IAS/IPS + IAG
- Option D: SAP Cloud Identity Services und CAP-Erweiterungen
- Option E: SAP GRC 12.0 / edition for SAP HANA

Option A: Weiteres Betreiben von SAP IDM 8.0

Das letzte Service Pack von SAP IDM 8.0 wurde vor mittlerweile mehr als 3 Jahren veröffentlicht. Etwas spitz formuliert: Welchen Support will SAP hier eigentlich einstellen? Für die meisten Probleme haben sich Kunden im Laufe der Zeit praktikable Lösungen oder Workarounds gebaut und können auch ohne Patches auskommen.



Wir werden sie nicht vermissen – Die SAP IDM Standard UI

Doch ganz so einfach können sich die jeweiligen IT-Architekten der Unternehmen die Entscheidung nicht machen. Die Problematik liegt hier vor allem die IT-Sicherheit der darunterliegenden AS Java-Komponenten, für welche stetige Sicherheits-Updates angeboten werden. Wer die Komponenten nicht stetig „up to date“ hält, riskiert langfristig die Integrität seiner Systemlandschaft.

Die Strategie IDM 8.0 weiter zu betreiben, sollte man demnach eher als ein „Abwarten“ bezeichnen, bevor dann der unweigerliche Wechsel erfolgt. Darüber hinaus ist nicht ganz auszuschließen, dass ein verlängerter Support für einige (Groß-)Kunden oder sogar generell angeboten wird und die Karenzzeit für IDM 8.0 erhöht. Ob lediglich der Support eingestellt oder es eine Art Nutzungsverbot für den AS Java geben wird, ist unklar.

Vorteile

- Keine zusätzlichen initialen Aufwände.
- Abwarten einer Konsolidierung des Marktes bzw. abwarten bzgl. neuer Entwicklungen von SAP, um später eine bessere Entscheidung treffen zu können.

Nachteile

- Laufende Investition in eine tote Software

- Geringere Verfügbarkeit von Spezialisten absehbar
- Ab 2030+ Einschränkungen in der IT-Sicherheit absehbar
- Ggf. Nutzungsverbot ab 2030+

Einschätzung

Aus unserer Sicht ist das Abwarten und Weiterbetreiben von SAP IDM 8.0 eine valide Strategie. Dies gilt insbesondere für beide Extreme von Implementierungen: Besonders kleine und agile Lösungen können problemlos weiter betrieben und rechtzeitig abgelöst werden. Komplexe Implementierungen müssen ohnehin über Jahre hinweg abgelöst und migriert werden.

Besonders Unternehmen, die innerhalb der nächsten Jahre eine Cloud-Transformation ihrer IT-Architektur vornehmen, sollten sich genau überlegen, ob man die dafür notwendigen IAM-Aufwände nicht direkt in den Aufbau einer neuen Software steckt. Was jedoch ausdrücklich weder von uns noch von SAP empfohlen werden kann, ist eine langfristige Planung mit SAP IDM 8.0.

Option B: Mit SAP IDM 8.0 in die Cloud?

Mit einem Post in den DSAG-Foren hat die Firma ROIABLE auf sich Aufmerksam gemacht und einen BTP-Port für SAP IDM 8.0 angekündigt. Die Idee ist so einfach wie genial: Da grundsätzlich „nur“ der Support für den AS Java eingestellt werden soll, könnte man doch (stark vereinfacht ausgedrückt) die IDM-Komponenten auf die SAP BTP übertragen und dort als Service anbieten. Dies klang zunächst vielversprechend, nicht weniger, weil bei der Firma ROIABLE die hochkarätigsten Entwickler im SAP IDM Umfeld ansässig sind. Doch nach einer Rücksprache dürfte dieser Ansatz seitens SAP auf wenig Akzeptanz stoßen, was für eine praktikable Umsetzung notwendig wäre.

Vorteile

- Minimaler Portierungsaufwand
- Wegfall der ungeliebten Komponente AS Java
- Ggf. Performance-Vorteile
- Bessere Integration in Cloud-Netzwerke

Nachteile

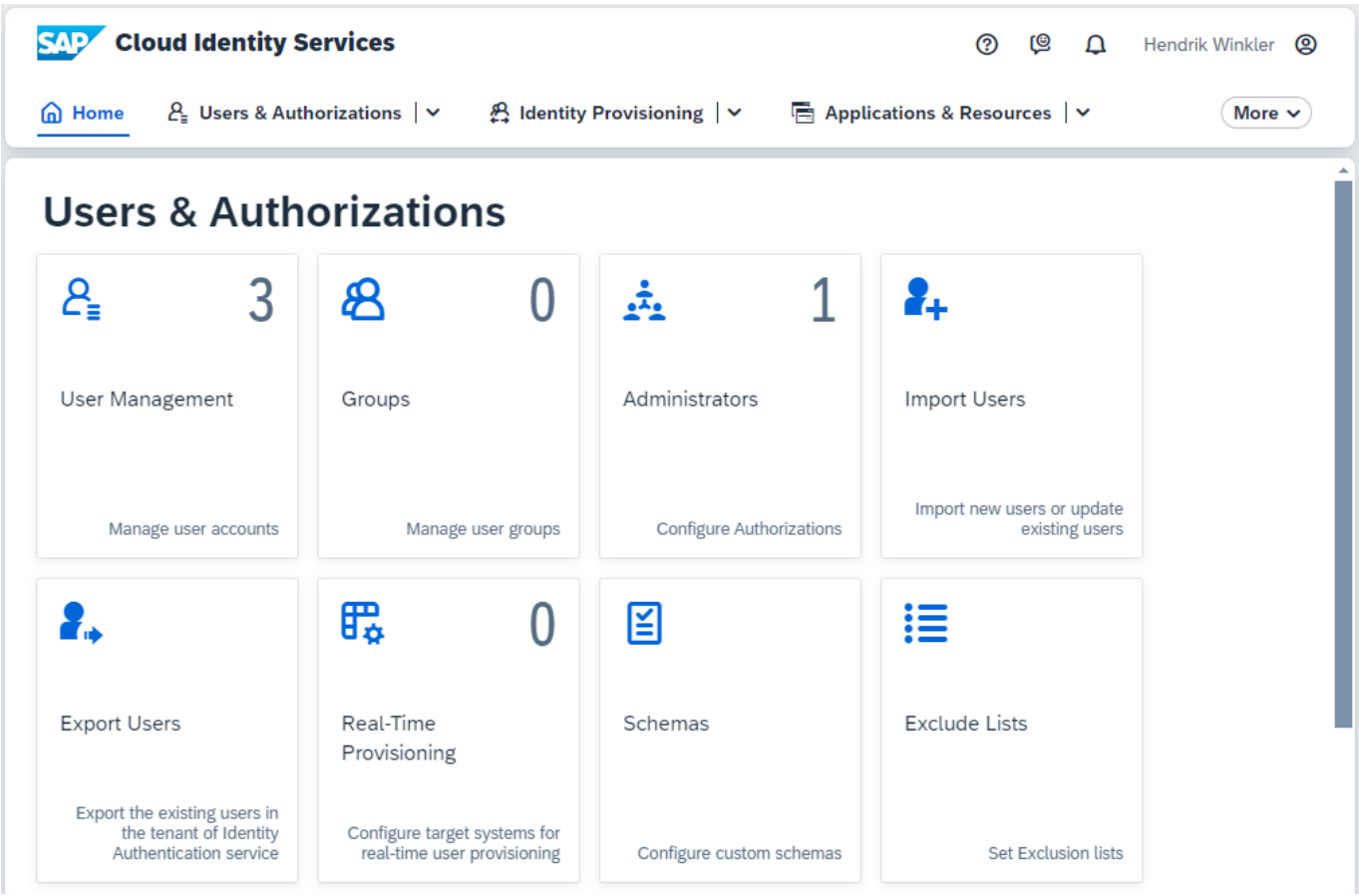
- Nicht von SAP unterstützt
- Keine Planungssicherheit

Einschätzung

Die Idee klingt so verlockend, dass wir sie hier mit aufführen möchten. Sie sollte jedoch, aufgrund der äußeren Umstände, nicht ernsthaft als Strategie deklariert werden.

Option C: SAP Cloud Identity Services – IAS/IPS + IAG

Willkommen im Dschungel der SAP-Cloud-Services. Die beiden BTP-Services für Identity Authentication (IAS) und Identity Provisioning (IPS) wurden unter dem Namen SAP Cloud Identity Services zusammengefasst.



Modern, aufgeräumt, und essentiell für die BTP – SAP Cloud Identity Services (IAS/IPS)

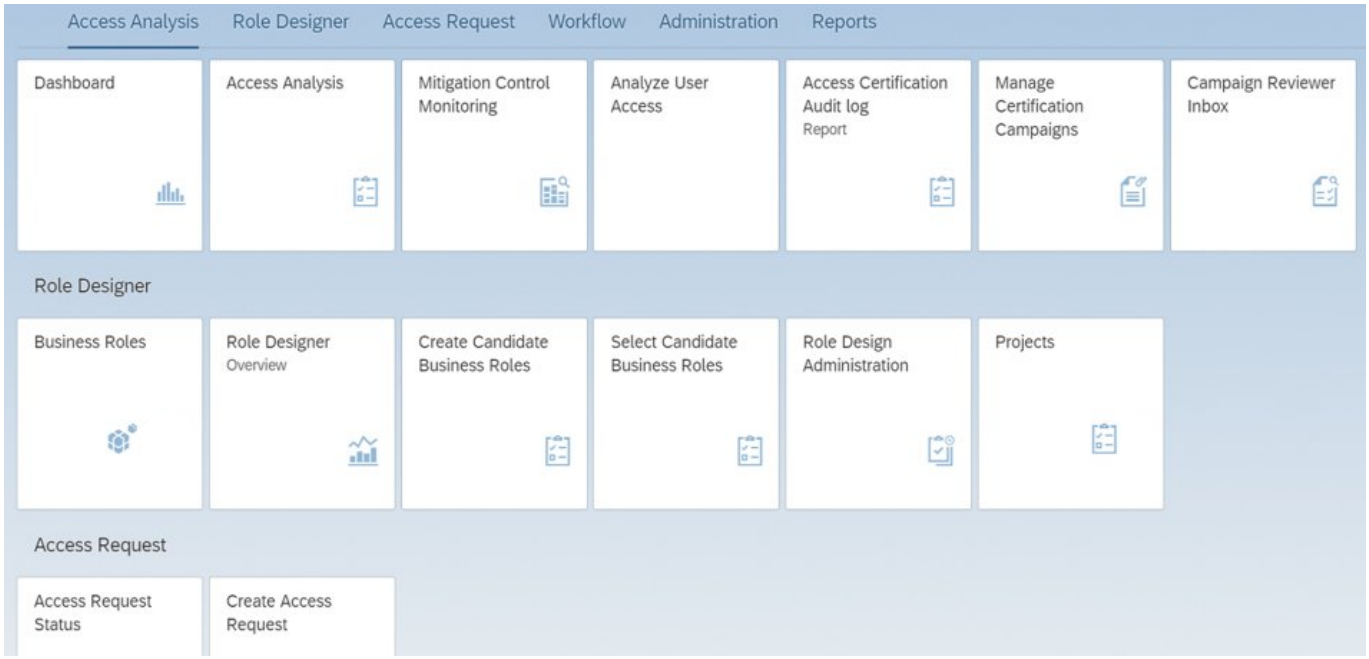
IAS und IPS sind als Teil der SAP Cloud Identity Services verfügbar und spielen eine wichtige Rolle im SAP Business Technology Platform (SAP BTP) Ökosystem, insbesondere wenn es um die Integration und das Management von Identitäten und Zugriffsberechtigungen geht.

Für SAP BTP-Kunden sind IAS und IPS grundlegende Dienste, die besonders relevant sind, wenn Sie andere SAP-Cloud-Lösungen wie SAP SuccessFactors oder SAP S/4HANA Cloud verwenden. SAP BTP ist so konzipiert, dass es seine Cloud-Lösungen mit integrierter Identitätsauthentifizierung ausliefert, was bedeutet, dass für einen nahtlosen und sicheren Zugriff auf diese Anwendungen IAS/IPS erforderlich ist.

Was die Kosten betrifft, so sind IAS und IPS standardmäßig im Rahmen der SAP BTP verfügbar und benötigen keine zusätzliche Lizenzierung, wenn sie im Zusammenhang mit einer SAP-Cloud-Lösung, einer SAP-On-Premise-Anwendung oder einem SAP-System auf SAP HANA Enterprise Cloud verwendet werden. Kunden erhalten standardmäßig einen produktiven und einen Test-Tenant ohne zusätzliche Lizenzkosten. Wenn jedoch zusätzliche Tenants benötigt werden, müssen diese separat erworben werden.

Für Kunden, die den Cloud Platform Enterprise Agreement (CPEA) Vertrag nutzen, ist das Preismodell verbrauchsbasiert, was bedeutet, dass Sie nur für die tatsächlich genutzten Dienste zahlen, mit der Option, zusätzliche Cloud-Credits zu erwerben, um ihr anfängliches Engagement zu erhöhen und so Überverbrauch zu vermeiden. Kunden können ihre Service-Nutzung über das SAP BTP Cockpit verwalten und erhalten monatliche Abrechnungen, um Transparenz über die anfallenden Gebühren zu erhalten.

SAP Cloud IAG (SAP Cloud Identity Access Governance) ist der „Cloud-Nachfolger von GRC“ und steckt, unserer Einschätzung nach, entwicklungstechnisch noch in den Kinderschuhen. Warum die Anführungszeichen? Erwartungsgemäß würde SAP entsprechend der Strategie auch GRC vollständig durch Cloud IAG ablösen wollen. Dies widerspricht sich jedoch mit der Ankündigung für SAP GRC edition for HANA in 2026 (mehr dazu im Absatz zu SAP GRC).



Inhouse Konkurrent!? – SAP Cloud IAG

SAP IAG bietet Funktionen, die Sie stark an GRC erinnern werden: Zugriffsanalyse, Business-Rollenmanagement, Zugriffsüberprüfung und Workflows, die es Unternehmen ermöglichen, ihre Zugriffsrichtlinien effektiv umzusetzen und gleichzeitig Compliance-Anforderungen zu erfüllen.

Vorteile

- Schnelle Bereitstellung und niedrigere Gesamtbetriebskosten (im Einzelfall zu kalkulieren)
- IAS/IPS sind gesetzt für hybride SAP-Landschaften
- Zentraler Identity Provider für Cloud- und On-Premise-Anwendungen
- Unterstützt standardisierte Authentifizierungsmethoden, auch durch bestehende Identity Provider (z.B. Login durch Apple-ID)
- IAS ermöglicht Single-Sign-On-Funktionalität
- Dynamische Anpassung der Konto- und Benutzerberechtigungen

Nachteile

- Möglicherweise weniger geeignet für sehr spezifische, nicht standardisierte IAM-Prozesse
- Eingeschränkte Entwicklungsmöglichkeiten für individuelle Anpassungen
- Erfordert möglicherweise Prozessstandardisierung

- Begrenzte Überwachungsmöglichkeiten im Vergleich zu SAP IDM
- Schwierigkeiten bei der Fehleranalyse in Cloud-Interaktion
- Die BTP und Cloud Identity Services werden vergleichsweise schnell weiterentwickelt. Dies muss nicht immer ein Vorteil sein, wenn eine minimale und stabile Lösung gewünscht wird.

Einschätzung

Die SAP Cloud Identity Services sind gesetzt, wenn Sie in der SAP BTP agieren. Diese Lösungen können jedoch nach unserer Einschätzung nicht als vollständige IAM-Produkte betrachtet und eingesetzt werden. Eine Einschätzung, die SAP zu teilen scheint und mit Microsoft Entra die Cloud Identity Services größtenteils zu Middleware-Lösungen degradiert. Der Einsatz von Cloud Identity Services, als Ersatz von SAP IDM, lässt sich daher nur in bestimmten Fällen empfehlen:

- Unternehmen mit Cloud-Fokus bzw. hybriden Landschaften: Da IAS und IPS speziell für Cloud-Umgebungen entwickelt wurden, eignen sie sich gut für Unternehmen, die eine starke Cloud-Präsenz haben oder planen, ihre IT-Infrastruktur in die Cloud zu verlagern.
- Unternehmen mit einfachen, standardisierten IAM-Prozessen: Hier ist im Einzelfall zu prüfen, ob die IAM-Prozesse so stark vereinfacht werden können, dass der Einsatz von IAS/IPS und IAG ausreicht.
- Unternehmen, die schnelle und skalierbare Lösungen benötigen: Da beide Dienste Cloud-basiert sind, bieten sie eine schnelle Bereitstellung und Skalierbarkeit, was besonders für wachsende Unternehmen von Vorteil sein kann.

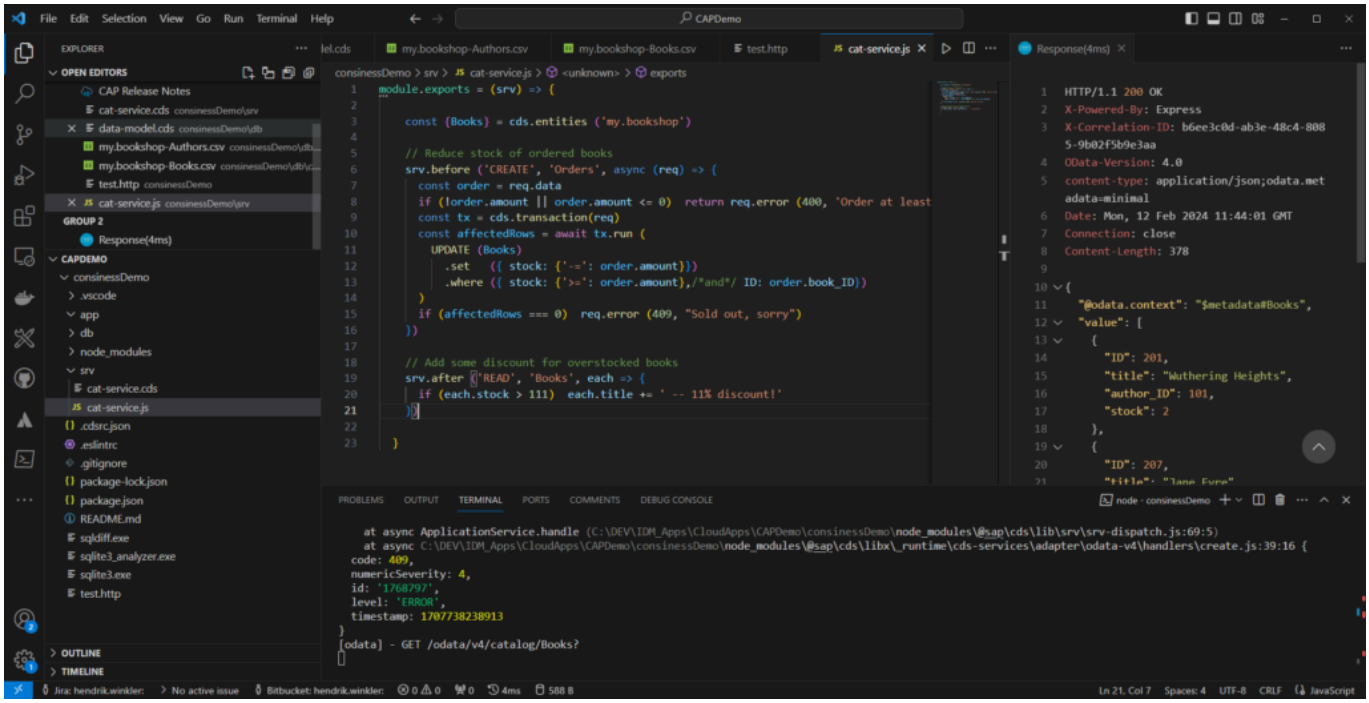
Für folgende Unternehmensarten könnten IAS/IPS weniger geeignet sein:

- Unternehmen, die (noch) keine Cloud nutzen wollen/können.
- Unternehmen mit sehr spezifischen, nicht standardisierten IAM-Anforderungen: Wenn ein Unternehmen hochspezifische Anforderungen an die Authentifizierung und Identitätsverwaltung hat, die über die Standardfunktionen von IAS und IPS hinausgehen, könnte eine maßgeschneiderte Lösung erforderlich sein.

Letztlich hängt die Entscheidung für oder gegen IAS/IPS von den spezifischen Anforderungen und Zielen des jeweiligen Unternehmens ab.

Option D: SAP Cloud Identity Services und CAP-Erweiterungen

Die Schwächen von SAP IAS und IPS, wie ihre eingeschränkte Flexibilität bei individuellen Anpassungen und begrenzte Überwachungsmöglichkeiten, können durch die Entwicklung eigener CAP-Anwendungen (Cloud Application Programming Model) gemindert werden. CAP bietet eine umfassende Programmierumgebung, die es ermöglicht, maßgeschneiderte Erweiterungen und Anpassungen zu entwickeln, die speziell auf die Bedürfnisse des Unternehmens zugeschnitten sind.



Der Einstieg in SAP-Entwicklung war noch nie so einfach mit CAP Tutorials aus dem SAP Developer Center

Beispielsweise können eigene CAP-basierte Applikationen entwickelt werden, um erweiterte Funktionalitäten in ihre BTP zu integrieren, die über die Standardfunktionalität von IAS/IPS und auch IAG hinausgehen, wie beispielsweise komplexe Genehmigungsworkflows oder individuell angepasste Benutzerverwaltungsprozesse.

Darüber hinaus bietet CAP eine flexible Plattform, um die Integration von IAS/IPS mit anderen Systemen und Diensten zu optimieren. Dies kann besonders nützlich sein, um eine nahtlose Verbindung zwischen Cloud- und On-Premise-Systemen in hybriden IT-Landschaften zu ermöglichen. Durch die Nutzung von CAP können

Unternehmen somit die Einschränkungen von IAS/IPS ausgleichen und ein umfassenderes, auf ihre spezifischen Anforderungen abgestimmtes Identitäts- und Zugriffsmanagement-System schaffen.

Vorteile

- Möglichkeit für Drittanbieter, Services zu implementieren, die individuell zu den Kundenbedürfnissen passen
- Für Quereinsteiger ist der Zugang zur SAP-Entwicklung mit CAP deutlich vereinfacht
- Verwendung von SAP Cloud Platform Workflow möglich
- Entwicklung von Migrationspfaden SAP IDM -> SAP Cloud für einen nahtlosen Übergang und Wiederverwendung von Bestandsprozessen

Nachteile

- Abweichend von der SAP-Standard-Lösung
- Entwicklungen müssen zunächst abgewartet werden

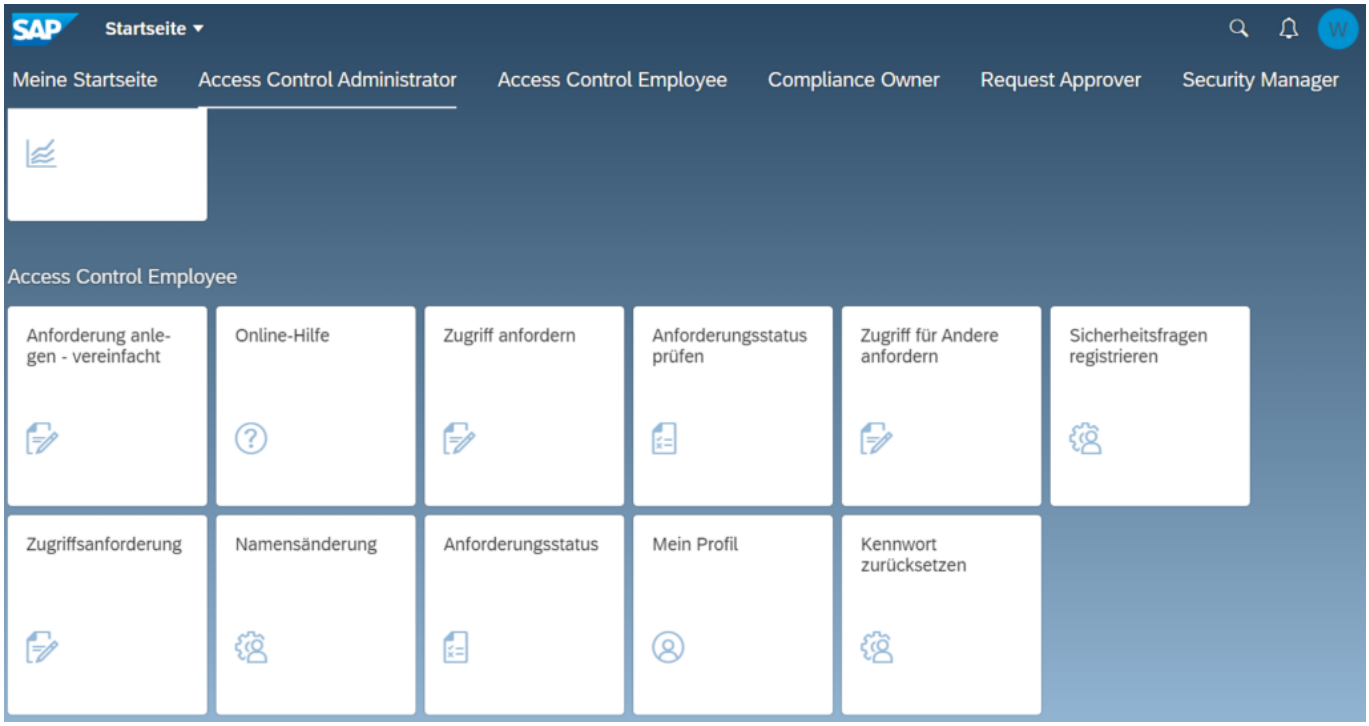
Einschätzung

Die Erweiterbarkeit vom Standard war schon immer eines der Hauptargumente für den Einsatz von SAP. Durch die Standardisierung der Cloud Identity Services könnten viele Kunden vor unlösbare Hürden gestellt werden, die zu einer Abwanderung in Lösungen von Drittanbietern führen würde. Mit dem CAP hat SAP jedoch eine Plattform geschaffen, die prinzipiell eine freie Entwicklung zusätzlicher Module durch Drittanbieter ermöglicht und nativ in das SAP BTP Ökosystem integrieren lässt.

Es sind bereits die ersten Entwickler damit beschäftigt, IAM-Module, die IAS/IPS erweitern oder in Teilen sogar ersetzen zu implementieren. Für Unternehmen, die eine IT-Architektur mit der SAP-Cloud als zentrales Element planen, wäre dieser Ansatz vermutlich der eleganteste. Jedoch bleibt zunächst abzuwarten, welche Möglichkeiten und Limitationen sich aus der Entwicklung von CAP-Applikationen für das IAM ergeben. Sobald es Neuigkeiten bzgl. dieser Option gibt, werden wir zeitnah darüber berichten.

Option E: SAP GRC 12.0 / edition for SAP HANA

Der immense Erfolg von GRC AC 12.0 und seinen Vorgängern konnte von SAP nicht ignoriert werden und mit einer offiziellen Ankündigung von SAP GRC edition for SAP HANA sind bei Weichen gestellt. SAP GRC lebt!



GRC 12.0 kommt mit einem umfangreichen Satz von Fiori-like Apps

GRC ist ein Compliance-Tool, umfasst aber weit mehr als die in IAM-Kreisen bekannten Module, was positive Synergieeffekte für die weitere Entwicklung der GRC-Plattform mit sich bringt. Die für das IAM relevanten Module sind unter dem Produkt GRC Access Control zusammengefasst:

- ARA – Access Risk Analysis
- EAM – Emergency Access Management
- BRM – Business Role Management
- ARM – Access Request Management
- UAR – User Access Review

Das größten Argumente gegen GRC waren (bzw. sind), dass die Lösung zum einen nicht im Stil eines Identity Management zur Verwaltung von Identity Lifecycles gedacht und gebaut wurde und zum anderen eine mangelnde Integration von nicht-

SAP-Produkten. Um diese Lücken zu schließen, war die vorgegebene Architektur von SAP sowohl SAP IDM als auch GRC einzusetzen. Diese wurden durch die Umsetzung einer der vielfältigen (jedoch in der Praxis umständlichen) Integrationsszenarien zwischen IDM und GRC miteinander verbunden.

Die Summe der vorhandenen Komponenten hat, kombiniert mit dem bewährten ABAP-Stack, nicht wenige Unternehmen dennoch dazu bewegt, GRC Access Control als IDM-light zu verwenden. Etwaige Funktionslücken wurden durch die hervorragende Erweiterbarkeit über Jahre durch Eigenentwicklungen geschlossen. Diese Unternehmen könnten sich jetzt als glückliche Gewinner herausstellen und über einen aktuellen und zukunftssicheren Technologie-Stack, erweiterte Fiori-Oberflächen und bessere Reporting-Funktionalitäten freuen.

Vorteile

- Bewährter Technologie-Stack basierend auf ABAP/HANA DB
- Etablierte und ausgefeilte Lösung für den Lifecycle von Berechtigungen und Business-Rollen (Access Governance)
- Flexible Gestaltung von Workflows mit MSMP (Multi Step Multi Process)
- Gute Verfügbarkeit von GRC-Experten, sowie ABAP und Fiori-Entwicklern
- Zukunftssicher
- Einfache Integration von ABAP-Landschaften

Nachteile

- Strategisch eigentlich als Compliance- und nicht als IAM-Lösung konzipiert worden
- Für die Anbindung von non-SAP Systemen müssen ggf. eigene Konnektoren entwickelt werden
- Anpassbarkeit ist im Vergleich zu SAP IDM aufwendiger
- Sehr komplexe Lösung (Problematisch für Neukunden bzw. Kunden, die an schlanken Lösungen interessiert sind)
- Inhouse-Konkurrenz durch SAP Cloud IAG

Einschätzung

Auch wenn SAP diese Ansicht offiziell wohl ungern bestätigen würde: GRC ist definitiv eine ernsthaft zu erwägende Option für Unternehmen, die aktuell das Tandem aus SAP und IDM verwenden. Nicht ohne Grund hat sich über die letzten

Jahre eine „GRC-Fangemeinde“ in der SAP-Welt etabliert, die weit größer ist als IDM jemals werden konnte. Es sollten im konkreten Fall Überlegungen angestellt werden, wie man die fehlenden Funktionen aus IDM in GRC überträgt. Das sollte vor allem dann möglich sein, wenn es sich um stark SAP-zentrische Infrastrukturen handelt, die Wert auf komplexe Sonderfälle und Risikoanalysen legen.

Sollte SAP-Software gesetzt sein und Cloud-Integration (noch) keine Rolle spielen, ist die Entscheidung für GRC eigentlich schon automatisch gefallen. Jedoch: SAP GRC ist sehr komplex, gilt als kostspielig und dieser Aufwand darf nicht unterschätzt werden.

Zusammenfassung

Wir hoffen, dass dieser Überblick Ihnen dabei hilft, ihre zukünftige IAM-Architektur zu planen. Selbst im direkten SAP-Umfeld, bieten sich je nach zu verwaltender Infrastruktur, zahlreiche Möglichkeiten, um Identitäten und Berechtigungen zu verwalten. Wie schon im einleitenden Artikel erwähnt, ist die grundsätzliche Frage bzgl. der Cloud-Ausrichtung unabdingbar, um eine Entscheidung zu treffen. Diesbezüglich empfehlen wir Ihnen auch den Teil 3 dieser Artikelserie, in dem unter anderem die von SAP offiziell angekündigte Nachfolgerlösung Microsoft Entra besprochen wird.

Weiter zum Teil 3: Cloud Services – Microsoft Entra, Okta, Omada Identity

Über den Autor



Hendrik Winkler ist Partner der consiness und Lead Architekt für Identity und Access Management Lösungen. Er kann auf umfangreiche Expertise in SAP ABAP, GRC, Cloud-Technologien und SAP Identity Management zurückgreifen. Mit über zehn Jahren in der IT-Branche hat er sich auf die Entwicklung und Implementierung von komplexen IAM-Systemen spezialisiert, wobei er stets ein Auge auf Sicherheit, Benutzerfreundlichkeit und Compliance hat.

Der Artikel ist auch bei Linkedin erschienen:

https://www.linkedin.com/posts/hendrik-winkler-81464b204_sap-idm-l%C3%A4uft-aus-der-wartung-aber-was-activity-7160273038616240128-mW5U?utm_source=share&utm_medium=member_desktop