Carsten Olt

SAP Cloud Identity Services

Überblick, Best Practices und typische Anwendungsfälle

Xiting E-Book

www.xiting.com

Inhalt

Einleitung 1
SAP Cloud Identity Authentication Service (IAS) 4
SAP Identity Directory Service (IdDS) 6
SAP Cloud Identity Provisioning Service (IPS) 7
Integration mit vorhandenen IDM-Lösungen 9
Unsere Empfehlungen (Key Takeaways) 10
Über den Autor 11
Über Xiting 12

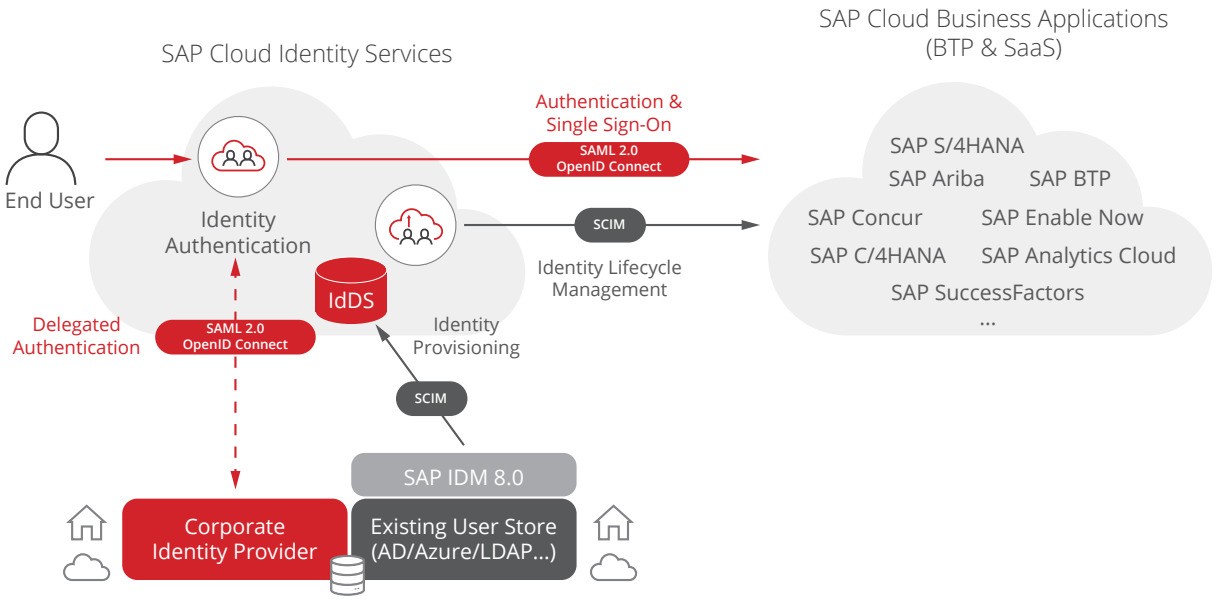
Einleitung

Die SAP Cloud Identity Services sind eine Gruppe von Diensten in der SAP Business Technology Platform (SAP BTP), mit denen Sie das Identitäts- und Zugriffsmanagement (IAM) zwischen Systemen integrieren können. Ziel ist es, systemübergreifend ein nahtloses Single-Sign-On (SSO)-Erlebnis zu bieten und gleichzeitig sicherzustellen, dass System- und Datenzugriffe sicher sind.

Um allen Interessenten und Kunden im Kontext hybrides IAM einen schnellen und auf das wesentliche komprimierten Überblick zu den SAP Cloud Identity Services (SCI) zu liefern, haben wir dieses E-Book erstellt. Zielgruppe sind Architekten, Projektverantwortliche, SAP-Berater und IDM-Administratoren, die sich einen ersten Überblick verschaffen möchten.

Ergänzend zu unserem Xiting QuickStart Implementation Service sowie den Informationen aus dem zugehören Blog, umreißt es die Grundlagen und gängigen Einsatzgebiete der SAP Cloud Identity Services und erklärt, warum und weshalb diese Komponenten für jeden SAP-Kunden relevant sind.

Die SAP Cloud Identity Services sind ein von SAP betriebener Public-Cloud-Service, der in verschiedenen Regionen weltweit verfügbar ist. Die beiden Komponenten **Identity Authentication** (IAS) und **Identity Provisioning** (IPS) sind elementare Bausteine eines IAM für SAP-Cloud-Anwendungen. Sie basieren auf demselben Technologie-Stack und sind Bestandteil vieler SaaS-Lösungen der SAP SE oder können im Bundle erworben werden.



Diese Services haben sich als Standard zur **Authentifizierung** und **Benutzerverwaltung** etabliert und bilden die Kernkomponenten der BTP. Sie ermöglichen den Aufbau zentraler Instanzen, um den Zugriff auf alle Anwendungen im SAP-Cloud-Universum zu sichern und die Benutzerverwaltung zu automatisieren. Besonders in einer sich ständig weiterentwickelnden hybriden SAP-Landschaft ist es unerlässlich, alle Identitäten an einem Ort zu verwalten und zu konsolidieren. Die SAP Cloud Identity Services unterstützen wichtige Industriestandards wie SCIM, SAML 2.0, OAuth2 und OpenID Connect, wodurch flexible Einsatzszenarien und Integrationsmöglichkeiten in vorhandene IAM-Systeme in einer Multi-Vendor-Landschaft ermöglicht werden.

Der **SAP Cloud Identity Authentication Service (IAS)** repräsentiert einen zentralen Identity Provider. Im IAS werden zentral alle SAP-Cloud Anwendungen angebunden. Mit diesem Ansatz möchte man das Onboarding weiterer SAP-Cloud-Anwendungen standardisieren, sodass hier immer dasselbe Schema angewendet wird. Dadurch wird der gesamte Onboarding-Prozess für neue SAP-Anwendungen stark vereinfacht. Für die Authentifikation von Anwendern verwendet der IAS gängige Standards wie Security Assertion Markup Language 2.0 (SAML 2.0) und OpenID Connect.

Der **SAP Cloud Identity Provisioning Service (IPS)** wird dazu verwendet, Benutzeridentitäten basierend auf Vorgaben und Filterregeln aus einem bestimmten Quellsystem in den Identity Directory Service zu provisionieren.

Der **Identity Directory Service (IdDS)** wird von den beiden Services IAS und IPS als Benutzerdatenbank in der SAP-Cloud-Umgebung verwendet. Über ein Gruppenkonzept wird die Bereitstellung der Benutzer- und Gruppen in die SAP-Cloud-Anwendungen automatisiert. Änderungen wie die Neuanlage eines Mitarbeiters, Anpassungen an Benutzerdaten- und Gruppen-Zuweisungen oder das Deaktivieren eines Kontos werden erkannt und per Job in geplanten Intervallen automatisiert umgesetzt. Somit können neue Identitäten in der SAP-Cloud-Umgebung erzeugt oder bestehende angepasst bzw. gelöscht werden.

Identity Authentication **IAS**	Identity Directory **IdDS**	Identity Provisioning **IPS**
▪ Dient als Main Identity Provider für SAP-Cloud- und On-Premise-Anwendungen ▪ Konsolidiert und automatisiert das Trust Management ▪ Standardisiert den Onboarding-Prozess für neue SAP-Cloud-Anwendungen ▪ Unterstützt gängige Standards wie SAML 2.0 und OpenID Connect ▪ Kann einfach mit dem bestehenden Identity Provider verbunden werden und unterstützt Proxy-Mode und Identitätsverbundszenarien	▪ Zentrale Benutzerdatenbank, die von den SAP Cloud Services IAS und IPS genutzt wird ▪ Grundlage für den Identity Lifecycle ▪ SCIM 2.0 REST API zur Unterstützung des programmierbaren Zugriffs ▪ Unterstützt 20 benutzerdefinierte Schemata mit jeweils 20 benutzerdefinierten Attributen ▪ Beständigkeit von Benutzern ist für viele Funktionen und SAP-Cloud-Anwendungen, einschließlich SAP SuccessFactors und SAP Task Center, unerlässlich ▪ Verfügt über Attribute wie die SAP Global User ID und kann mit Attributen aus anderen Quellsystemen angereichert werden	▪ ID Lifecycle für Cloud-basierte SAP-Anwendungen ▪ Integriert sich mit SAP Identity Management für hybride Landschaften und Nicht-SAP-IDM-Lösungen ▪ Unterstützt das Industriestandardprotokoll SCIM ▪ Dedizierte Konnektoren für die wichtigsten Anwendungen – normalisiert Systemschnittstellen auf den SCIM-Standard ▪ Bietet ein leistungsstarkes JSON-Transformations-Framework ▪ Hat keine Funktionsparität und zielt nicht darauf ab, IDM-Lösungen zu ersetzen.

Zu den Vorteilen bei Einsatz der SAP Cloud Identity Services gehören:

1. **Zentralisiertes Identitätsmanagement:** SAP Cloud Identity Services bieten ein zentrales Repository für die Verwaltung von Benutzeridentitäten, wodurch die Verwaltung von Zugriffsrechten und Privilegien über mehrere Systeme hinweg vereinfacht wird.

2. **Verbesserte Effizienz:** Durch Einsatz des Identity Directory (IdDS) als zentrales Repository für alle SAP-Benutzeridentitäten können Unternehmen den Verwaltungsaufwand stark reduzieren und Prozesse automatisieren. Alle Benutzer werden an einem zentralen Ort gespeichert ohne die Benutzeridentitäten in jedem einzelnen Service verwalten und aktualisieren zu müssen.

3. **Single Sign-On:** Durch Speichern der Benutzeridentitäten- und Attribute im Identity Directory kann Single Sign-On für Benutzer über verschiedene SAP-Anwendungen- und Dienste hinweg bereitgestellt werden. Dies bietet eine nahtlose und sichere Benutzererfahrung, da Benutzer sich nur einmal anmelden müssen, um auf alle benötigten SAP-Dienste zuzugreifen.

4. **Integration mit anderen Systemen:** Durch die Persistenz von Benutzeridentitäten im Identity Directory können Sie SAP-Dienste einfacher in andere Systeme integrieren, z. B. Identity Provider, Security Information and Event Management (SIEM)-Tools und IDM-Lösungen. Dies verringert das Risiko von Fehlern oder Inkonsistenzen.

5. **Verbesserte Benutzererfahrung:** Die SAP Global User ID (UUID) erleichtert Benutzern den Zugriff auf mehrere Systeme mit einer einzigen Anmeldung und bietet eine nahtlosere und effizientere Erfahrung.

6. **Verbesserte Governance:** SAP Cloud Identity Services bieten in Kombination mit weiteren Services wie SAP Cloud Identity Access Governance (IAG) Tools und Funktionen für die Prüfung und Berichterstattung über den Benutzerzugriff und helfen Organisationen dabei, gesetzliche und Compliance-Anforderungen zu erfüllen.