Zuhause OnPremise und in der Cloud mit Identity Management

DRAFT: UPDATE NACH OOW

Michael Fischer
ORACLE Deutschland B.V. & Co. KG
München

Schlüsselworte
Identity Management, IAM, IDaaS, Provisionieren, SingleSignOn, Federation, SAML, OAuth.

Einleitung

Mit der Nutzung von Cloud Services kommt die Herausforderung die Benutzer bzw. deren Accounts und Berechtigungen auch in den Cloud Diensten zu managen. Neben dem Anlegen, Ändern, Löschen und Berechtigen von Accounts fallen auch die anderen Zusatzaufgaben rund um dieses Thema an. Dies sind z.B. das Reporting (Wer hat welche Rechte), die Verlängerung von Berechtigungen (auch Rezertifizierung genannt), ein Passwortmanagement und ein Antragssystem. Für den Benutzer soll das natürlich auch möglichst transparent sein. Auch möchte man die Cloud Dienste nicht "herrenlos" nutzbar machen sondern evtl. über das zentrale Anmeldesystem der Firma koppeln. So können Anmeldemöglichkeiten und Anmeldestärken zusätzlich gesteuert werden.

Dieser Vortrag zeigt auf wie diese Aspekte mit einem hybriden Identity und Access Management gelöst werden können.

Zuhause OnPremise und in der Cloud mit Identity Management

Mit der Nutzung der Cloud kommt die Frage auf wie aus Unternehmenssicht die Benutzer bzw. deren Accounts und Berechtigungen gemanagt und überwacht werden. Zudem möchten Benutzer typischerweise eine möglichst transparente Nutzung, d.h. ein Single Sign On und Beantragungen für die Nutzung von Services über das vorhandene Antragssystem.

Damit stellen sich folgende Anfroderungen:

- **Integration von SaaS oder cloudbasierten Services**
  - Im Zuge der Nutzung von cloudbasierten Services sollen diese in das zentrale Anmeldeverfahren integriert werden. So ist an einer Stelle steuerbar wer sich anmelden kann. Kontextsensitivität soll dabei je nach Service genutzt werden. Der Benutzer kann sich so über sein Single-Sign-On an diese Services anmelden. Dabei soll man auf einen „Katalog“ mit vorgefertigten Integrationen zurückgreifen oder Integrationen basierend auf einem der unterstützten Standards (OAuth/OpenIDConnect, SAML, FormFill) erstellen können.
- **Anmeldung / Single Sign On - auch für Eigenentwicklungen**
  - Verschiedene Verfahren zur Integration von Anwendungen und Services sollen zur Verfügung stehen. Entweder per Standard wie SAML oder OpenID Connect oder Eigenentwicklungen basierend auf einem der o.a. Standardprotokolle bzw. einer bereitgestellten Rest-API

- » Mit SAML können z.B. das lokale AD über ADFS oder Services, neben Oracle SaaS, Office 365, Salesforce etc. angeschlossen werden.
- » Über die genannten Standards können starke Authentifizierung (OTP, TOTP) und auch Social Logins genutzt werden

» **Hybrides IAM: Koexistenz bzw. Integration mit bestehenden IAM Systemen**

- » Bestehende IAM oder Antragssysteme sollen über verschiedene Mechanismen angebunden werden können, die von Synchronisation über Workflows bis zur direkten Verwendung einer Schnittstellen reichen sollen.
- » Das daraus entstehende hybride IAM System kann die weiterführenden Funktionen des jeweiligen anderen Systems nutzen. Z.B. die Rezertifizeirung von Accounts oder das Antragswesen durch das OnPremise System
- » Der Endbenutzer bekommt ein Single-Sign-On dass von seiner Desktopanmeldung oder von seinem Corporate Login aus gestartet wird.

» **Cloudmodell: Einfach und skalierbar**

- » Für den Zugang soll es keine Rolle spielen, ob ein Benutzer innerhalb des Unternehmensnetzwerks kommt oder über das Internet
- » Eine sofortige Nutzungsmöglichkeit nach Konfiguration
- » Die Nachweisbarkeit durch entsprechende Reports bzw. Reportingdaten
- » Ein Scale-up für die Nutzung von bzw. durch Millionen von Nutzern

Oracle bietet mit dem Oracle Identity Cloud Service eine Umsetzung eines generischen Services zur Verwaltung von Accounts, Berechtigungen, Single-Sign-On und Reporting. Der Service lässt sich mit einen OnPremise Identity System koppeln, was dann ein hybrides Identity Management (siehe Gartner) ermöglicht. Die Koppelung reicht von einfachen Synchronisationen, über Beantragungen und Workflows bis hin zur (Re-) Zertifizierung der Berechtigungen. Ein Single-Sign-On vom lokalen System, z.B. der Windows Anmeldung, ist möglich. Für den Endbenutzer ist dabei transparent wo sich das System befindet. Die Hauptfunktionen lassen sich in vier Gruppen zusammenfassen.




Umsetzung von Standards	Identity Management	Anmeldung, Authorisierung und Single-Sign-On	Hybrides Identity Management
OpenID Connect, OAuth, SAML, SPML	Mittels UI, Rest-Services oder Synchronisation	Führende oder nachgelagerte Anmeldung und Single Sign On, Rollen	Koppelung über Workflows (OIM), oder Rest-Services, Synchronisation mit AD

Abbildung 1: Kernfunktionen IDCS Stand Juni 2017

Der Oracle Identity Services beinhaltet die Erfahrungen von Oracle mit den eigenen Cloud Services und über 17 Millionen verwalteten Benutzern und Mandanten. Die unterliegende Micro-Services Architektur ermöglicht ein sanftes service-seitiges Nachrüsten von Funktionen wie z.B. kontextbasierte Authentifizierung.

Führende Analysten bewerten Funktionsumfang und Nutzbarkeit positiv. Beispielsweise bewertet Gartner 2017 die Access und Governance Funktionen von Oracle beide Male mit der Positionierung im „Leader Quadrant“.

Die folgenden Anwendungsfälle sind Beispiele zur Nutzung des Services. Diese lassen sich selbstverständlich untereinander koppeln.

1. Hybrides Management von Benutzern
In diesem Fall können Benutzer sowohl OnPremise verwaltet werden als auch in dem entsprechenden Cloud Service:

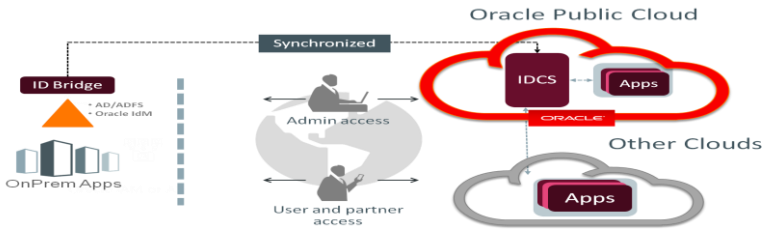

Abbildung 2: Hybrides Identity Management (hier Synchronisation mit OnPremise AD/LDAP)

Die Vorteile dieser Koppelung sind:

» Benutzer die im OnPremise System gepflegt werden sind automatisch im cloudbasierten Identity System vorhanden und können so die „nur“ an das cloudbasierte IAM System angeschlossene Applikationen ebenfalls nutzen. Die Nutzung ermöglicht neben dem SSO, dass im nächsten Abschnitt beschrieben wird, bis hin zur Beantragung von cloudbasierten Systemen (wie bspw. SaaS Services). Aus Sicht der Verantwortlichen ergibt sich eine holistische Sicht auf alle Accounts und Berechtigungen. Das sind Anforderungen aus dem Bereich der Regularien.

» Benutzer die nicht im OnPremise System gepflegt werden, wie bspw. Kunden oder Bewerber etc. werden nur im cloudbasierten System gepflegt. Das vereinfacht das Sizing einer bestehenden OnPremise Lösung. Über delegierte Administration können auch Mandanten abgebildet werden.

2. Nahtloser Zugriff auf (Oracle) Public Cloud Applications
Der Identity Cloud Service bietet die Möglichkeit verschiedene Cloud Services über ein SSO zu integrieren. Eine manuelle Konfiguration über SAML oder OAuth ist grundsätzlich möglich, für einige Oracle Cloud Services und einige Applikationen wie beispielsweise Salesforce ist eine Vorkonfiguration vorhanden.

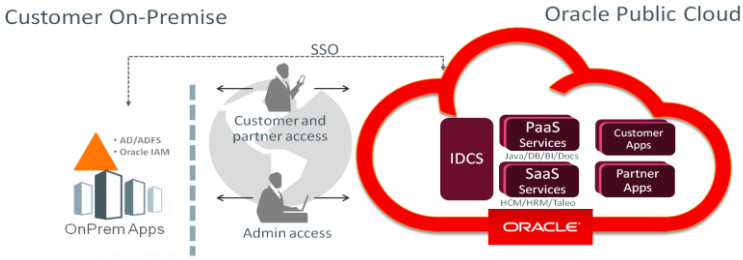

Abbildung 3: Cloud SSO & Integrated Cloud IDM

Vorteil dieser Koppelung ist, dass nur ein SSO zum OnPremise System konfiguriert werden muss, alle weiteren Systeme werden an den IDCS angeschlossen.

3. Identity und Access für Eigenentwicklungen und/oder auslagern des Benutzermanagements

IDCS kann verwendet werden, um den Anteil an der Entwicklung für IAM Services (Anmeldemöglichkeit, SSO, Benutzerpflege) zu reduzieren. Neben den aufgeführten Funktionen sind Self-Services zum Management der Profildaten, Zurücksetzen des Passworts etc. vorhanden. Verantwortliche verfügen zusätzlich über delegierte Administration und Reporting Funktionen.

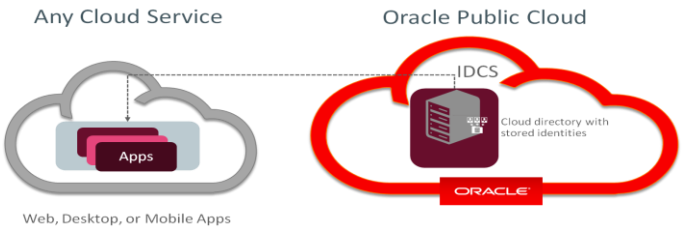

Abbildung 4: Cloud SSO & Integrated Cloud IDM

Um Benutzern die Nutzung von Anwendungen (z.B. Firmenwebportal) oder Apps (z.B. Fitness App) zu ermöglichen, müssen diese erfasst und gemangt werden. Je nach Daten muss auch die Einwilligung der Benutzer dabei berücksichtigt werden (sogenannter User Consent).

Damit wird diese Funktion in beiden Fällen als Service genutzt und ist von der Entwicklung und Weiterentwicklung der Eigenentwicklungen getrennt. Die Skalierung funktioniert transparent anhand der Anzahl der Nutzer, es ist keine Verwaltung von Instanzen notwendig.

Zusammenfassung und Ausblick

Oracle Identity Cloud Service (IDCS) stellt eine cloudbasierte IAM Plattform zur Verfügung. Damit können sowohl Mitarbeiter, Externe, Partner, Kunden und Dinge (z.B. Geräte oder IoT) verwaltet und angebunden werden. Durch vorgefertigte Integrationen, sowohl bzgl. der Anbindung von OnPremise IDM Systemen als auch SSO Systemen ist eine einfache Nutzung möglich. Für den Benutzer ist der Service Dank SSO transparent. Oracle selbst hat diesen Service in seine neuen Oracle Public Cloud Services (OPC) eingebunden und die bestehenden OPC werden auf diese Plattform migriert. Ein mit OPC bestehender IDCS Service kann, je nach Lizenz, dann auch für andere Dinge genutzt werden.

Weitere Cloud Security Services ergänzen oder nutzen den Identity Cloud Service (IDCS):

» Oracle CASB (Cloud Access Broker) nutzt den IDCS um Rückschlüsse auf den eingeloggten Benutzer ziehen zu können und im Rahmen der Remediation, der Incident Behandlung, entsprechende Vorschläge machen zu können (z.B. deaktivieren des Accounts im IDCS oder Rücksetzen der Konfiguration in einem Account)

» Cloud Security Monitoring Services (noch nicht live) zur Überwachung verdächtiger Operationen in Cloud und OnPremise Umgebungen. Hierbei ist meist der vermeintlich genutzte Account und dessen Berechtigungen oder die Berechtigungshistorie von Interesse.

Weitere Informationen

- Tests mit dem Identity Cloud Service sowie weitere Informationen und Dokumentation unter https://cloud.oracle.com/en_US/identity Der Service ist aktuell (Juli 2017) in den Oracle Rechenzentren in den USA und für EMEA in Amsterdam verfügbar

- Weiterführende Informationen zu Security & Oracle finden Sie im Internet unter http://www.oracle.com/security

Kontaktadresse:
Michael Fischer
ORACLE Deutschland B.V. & Co. KG
Riesstr. 25
D- 80992 München

Telefon: +49 (0) 172 8323654
E-Mail michael.fischer@oracle.com
Internet: www.oracle.de