

TECHNOLOGY BLOG
AMIS
CONCLUSION

Home » Platform Technology



Just launched: the Oracle Identity Cloud Service – for authentication and authorization across the cloud and on premises

Lucas Jellema November 2, 2016 Platform Technology No Comments

News flash: According to a post on LinkedIn by Oracle's Chief Identity Architect Vadim Lander, the IDCS is live, as of November 1st.



An important missing link until now in Oracle's cloud story: a robust identity management and centralized authentication solution – used for Oracle's own management of users and their access to Oracle SaaS, PaaS and IaaS services and offered to customers for their identity and access management to the applications they run on the Oracle PaaS platform.



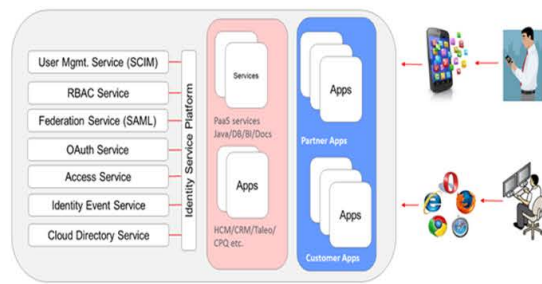
Oracle states that the previous generation of what will be IDCS has been operational for Oracle PaaS and SaaS apps in 19 data centers globally, and for the past 4 years, currently authenticating over 35 Million identities daily, and catering to over 35,000 customers across Oracle SaaS, PaaS and IaaS.

In the Fall of 2016, the Identity Cloud Service is expected to be finally launched externally (at the time of writing, it was apparently just brought to life). Its objective is simplify access, improve security, and reduce the management cost of new cloud resources as well as Oracle's own cloud products through successful single sign-on with Oracle Identity Cloud Service.



IDCS is part of a broader Identity Management Hub that comprises traditional on-premise products like the Oracle Identity Governance, Access Management and Directory Services, combined with the shiny new cloud security products that include API Platform Cloud Service and IDCS itself. The last two are cloud-based products designed to protect an enterprise's application APIs and identities in the cloud respectively.

The functionality of IDCS is visualized in the next figure:



The main capabilities initially proposed for IDCS are:

- User Management and Cloud Directory Services ("the cloud identity hub")

LUCAS JELLEMA

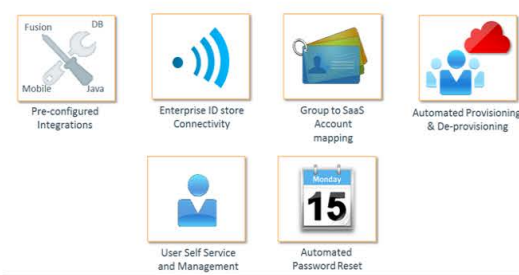


Lucas Jellema, active in IT (and with Oracle) since 1994. Oracle ACE Director and Oracle Developer Champion. Solution architect and developer on diverse areas including SQL, JavaScript, Kubernetes & Docker, Machine Learning, Java, SOA and microservices, events in various shapes and forms and many other things. Author of the Oracle Press book Oracle SOA Suite 12c Handbook. Frequent presenter on user groups and community events and conferences such as JavaOne, Oracle Code, CodeOne, NLJUG JFall and Oracle OpenWorld.

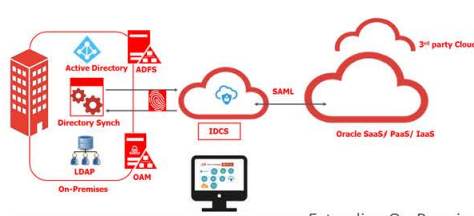
[View all posts](#)

Follow us on **LinkedIn**

MICROSOFT CORP.
EXHIBIT 1050



IDCS integrates with on premises and 3rd party cloud solutions using the SCIM standard. System for Cross-domain Identity Management (SCIM) is an open API standard for managing identities across independent solutions. Through SCIM, IDCS enables plugability of applications into user provisioning process.

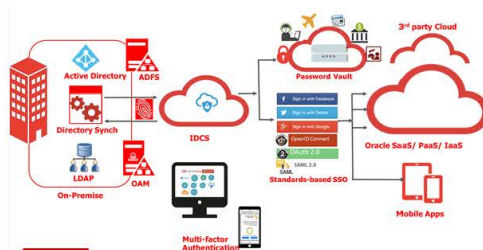


Some of the cloud applications for which IDCS will provide OOTB SCIM connectors are Workday, Office 365, AWS, Google Apps, SalesForce, ServiceNow, Concur, WexEx, Box. Customers can add their own custom SCIM connectors

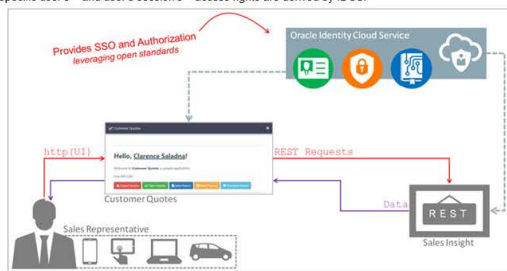
- Authentication and Single Sign On across applications running in the Oracle Public Cloud, 3rd party clouds and on premises using among others OpenID Connect, a standard authentication protocol that provides Federated SSO leveraging the OAuth 2.0 authorization framework, and SAML (Security Assertion Markup Language) an open-standard data format for exchanging authentication and authorization data between parties.



Federated authentication using SAML is set up with IDCS as Service provider and the on premises LDAP – for example MS Active Directory – as the identity provider to provide seamless Web SSO for the Cloud applications.



- Authorization to applications, services and specific operations is handled through OAuth 2.0 – a standard framework for authorization, commonly used for third-party authorization requests with consent. IDCS records users, groups or business roles and application roles, privileges and entitlements. At run time, a specific user's – and user's session's – access rights are derived by IDCS.



- Identity Event Service for integrating applications with Identity Life Cycle for business processes

Some form of analytics and governance seems a logical next area for IDCS to evolve into.

Oracle announced the intended acquisition of Cloud Access Security Broker Palerra, whose LORIC product will be added to IDCS.

Announcing: Oracle's Intention To Acquire Palerra
Palerra's LORIC Product Protects Applications, Workloads and Sensitive Data Stored Across Cloud Services

- Leading Cloud Access Security Broker (CASB)
 - Usage Visibility
 - Data Security
 - User Behavior
 - Security Configuration
 - Automated Incident Responses
- Real-time Response to Cloud Security Incidents across all leading cloud services



LORIC protects and assures compliance of applications, workloads and sensitive data stored across cloud services. Palerra offers a combination of visibility into cloud usage, data security, user behavior analytics, and security configuration, with automated incident responses. Customers can respond to cloud security incidents in real-time, protecting sensitive company data and workloads across many 3rd party cloud services. As such there seems a potential relation if not overlap with the Security Analytics option in [Oracle Management Cloud](#).

Oracle + Palerra Accelerates Cloud Adoption with Comprehensive Identity and Security Services



- Cloud Usage Visibility
- Automatically Configure Security
- Strongly Authenticate Users
- Help protect Applications and APIs from Unauthorized Access
- Detect Anomalous User Behavior
- Protect Sensitive Data
- Facilitate compliance with Regulations and Security Policies
- Automatic Incident Response

Many existing or upcoming cloud services in the Oracle PaaS portfolio depend on IDCS and are eagerly awaiting its release. Some can only be launched when IDCS is live – such as API Platform CS – and others will undergo substantial refactoring when they switch to IDCS for user management and authentication – presumably this includes MCS.

Download the [AMIS OOW16 Highlights](#) for an overview of announcements at OOW16.

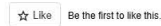
RESOURCES

Slides from OOW 16 presentation [Secure Oracle SaaS and PaaS with Oracle Identity Cloud Service](#).

SHARE THIS:



LIKE THIS:



Related Posts

Fastest creation of a Lean VirtualBox VM Image with Oracle Database 11gR2 XE, the Node.JS 7.x and the Oracle DB Driver for Node

Connect Oracle Enterprise Manager 13 to Amazon's Cloudwatch

Dbvisit Standby upgrade

Tags: [authentication](#), [authorization](#), [identity management](#), [OAuth2.0](#), [openid connect](#), [paas](#), [sami](#)

About The Author



Lucas Jellema

Lucas Jellema, active in IT (and with Oracle) since 1994. Oracle ACE Director and Oracle Developer Champion. Solution architect and developer on diverse areas including SQL, JavaScript, Kubernetes & Docker, Machine Learning, Java, SOA and microservices, events in various shapes and forms and many other things. Author of the Oracle Press book Oracle SOA Suite 12c Handbook. Frequent presenter on user groups and community events and conferences such as JavaOne, Oracle Code, CodeOne, NLJUG JFall and Oracle OpenWorld.

- Java
- Architecture
- Big Data
- Cloud
- Continuous Delivery
- Internet Of Things
- Microsoft Azure
- Platform Technology
- Python

BEKIJK ONZE VACATURES



CONTACT US

