Solving Identity Fragmentation

Peter Abrahamsson and Artur Alves
Oracle
DOAG

Keywords:

Oracle Unified Directory, Consolidation, Virtualization, Cloud, IDCS, Federation, Access Management

Introduction

Here we discuss the challenges identity fragmentation posses to on-premise enterprise identity architectures, in the cloud or both in a hybrid configuration. We present different solutions to this challenge by leveraging Oracle Unified Directory (OUD) virtualization capability in a federation use case involving Oracle Identity Cloud Service, IDCS.

Identity stores seen as silos

A typical enterprise landscape today is having multiple identity silo's across HR departments, IT, Security and Marketing. In conjunction with this you would have thousands of applications that need access to those identity silos. You can easily have thousands of those applications, and in some enterprises getting full control of these apps is hard or even impossible.

Enterprise life-cycles add even more complexity with mergers and acquisitions. During those cycles it is common to have to maintain existing acquired company identity silos in parallel with the acquiring company identity silos. This is mostly because, while data can be moved, transferred and transformed fast, applications from an acquired company might have to stay around for a long time while the business processes get consolidated in the merged company.

At the same time the definition of what we consider identity data is constantly being broadened; user profiles, access data, and authorization data is no longer the norm, the definition now includes geo location, mobile data and so on. The fragmentation of this identity is the apparent when it is scattered across heterogeneous data sources at multiple locations.

For example, employee information is stored in HR databases or in Microsoft Active Directories, customer and partner data in CRM databases, and additional LDAP directories. Companies require aggregated user data from various data sources in real time. As a consequence, application-specific directories proliferate, copying and synchronizing identity data, which leads to high administration and maintenance costs, inconsistent identity data, and compliance issues.

Why consolidate identity fragmentation?

Painful symptoms for managing these fragmented identities in all those different silos results of high administrative costs that are also subject to errors with serious security concerns. Administering security on a fragmented identity structure would not just lead allot of unnecessary cost overhead to maintain these separate identity silos but would also yield a very ineffective implementation with expensive and complex certification processes with little assurance of having a compliant identity architecture – leading to high risks. Costly integration (or cloud) projects due to having to consider multiple identities.

There are two possible way to address these problems for identity silos

- Directory Consolidation: The concept of having multiple directory sources merged or synchronized to a single directory infrastructure.
- Directory Virtualization: A more organic approach of consolidation which reduces disruption the existing applications due to not the fact that there is no alternation of the original source.

Virtualization provides a virtualization layer to meet the requirements of applications needs without changing source directories. This achieved by adding or merging identity fragments on the fly and exposing it as single source of truth.

Adding to this many businesses require a certain data structures that is not provided out of the box by an LDAP directory. It may differ on the schema (different types of attribute in the entries) or the values (same attribute name with different semantic of values).

Where are we heading?

"According to the new ***Worldwide Semiannual Public Cloud Services Spending Guide*** from International Data Corporation (IDC), worldwide spending on public cloud services will grow at a 19.4% compound annual growth rate (CAGR) -- almost six times the rate of overall IT spending growth – from nearly $70 billion in 2015 to more than $141 billion in 2019. The new spending guide expands on IDC's previous public cloud services forecasts by offering greater detail on industry and geographic spending levels. "- IDC

While businesses are moving to the cloud in an impressive rate, they will likely continue to have their large and cumbersome identity silos remain on-premises for years to come. This means that a natural precursor step for enterprises with pure cloud in mind is to consider having a hybrid cloud approach on their agenda first, especially for their on-premise identity silos.

From the scope of this article it is safe to say that there will be plenty of business introducing additional services in the cloud. The identity silos of these additional services will likely need integration with the on-premise identity platforms. The immediate challenge surrounding this is that LDAP (the protocol that is typically used to access directories) is not firewall friendly, and therefore not easily exposed to the cloud services.

But it doesn't make sense to build new cloud-based services that cannot interoperate with our own enterprise services, or cannot work with target online communities (like social networks). Therefore, alternative APIs and protocols must be adopted, like:

- HTTPS as transport
- REST APIs, like SCIM for identity access and lifecycle
- OpenID Connect for authentication (as complement to LDAP bind)
- OAuth 2 or SAML 2.0 for federation agreements between parties

An example of an Identity-as-a-Service (IDaaS) platform capable of bridging the cloud and on-premise worlds based on those industry standard APIs and protocols is Oracle Identity Cloud Service (IDCS).

The on-premise Identity Silos

Corporate directories

The corporate LDAP directory is typically where all the identities in an enterprise are typically stored and controlled. Furthermore, nowadays an identity is not just your e-mail address or your phone number; it could be anything which helps an organization maintains a unique relationship with you for a period of time, such as an IP address, a unique Cookie, an IMEI number of your mobile device.

This makes a directory as the backbone of modern enterprises. What started as an alternate storage mechanism for simple attributes is now a core part of identity framework in an organization. Most Identity platforms have a directory server with large and complex deployments with many applications and use cases.

Active Directory

Microsoft Active Directory (AD) is widely adopted by the vast majority of medium/big organizations, some with several deployments for specific services (aka, silos). It's therefore a common use case for an identity consolidation/virtualization project.

HR Databases

Today a large portion of identities exist in HR databases. Adding to that they are typically located in multiple sources spread out through the enterprise, either located on the cloud or on-premise. Similarly to Active Directory and other corporate directories it is typically the backend of complex deployments with many application dependencies.

IDCS and hybrid Cloud

Oracle Identity Cloud Service (IDCS) is a cloud-native service designed to be an integral part of the modern enterprise security fabric, protecting users and applications whether they are on-premise or in the cloud. IDCS is part of a strategic hybrid solution—giving organizations the ability to integrate centralized workflows for access and governance across on-premises and cloud applications. IDCS is global and scalable, which by virtue of being hosted on the Oracle Cloud, inherits strong security at the logical, physical and data security levels. And it was built to be completely open with a standards-first and API-first philosophy to ensure interoperability and compatibility. While there is allot more to say about IDCS we will the next section show it playing a federation role in the solving of identity fragmentation solution presentation part of this article.

Oracle Unified Directory

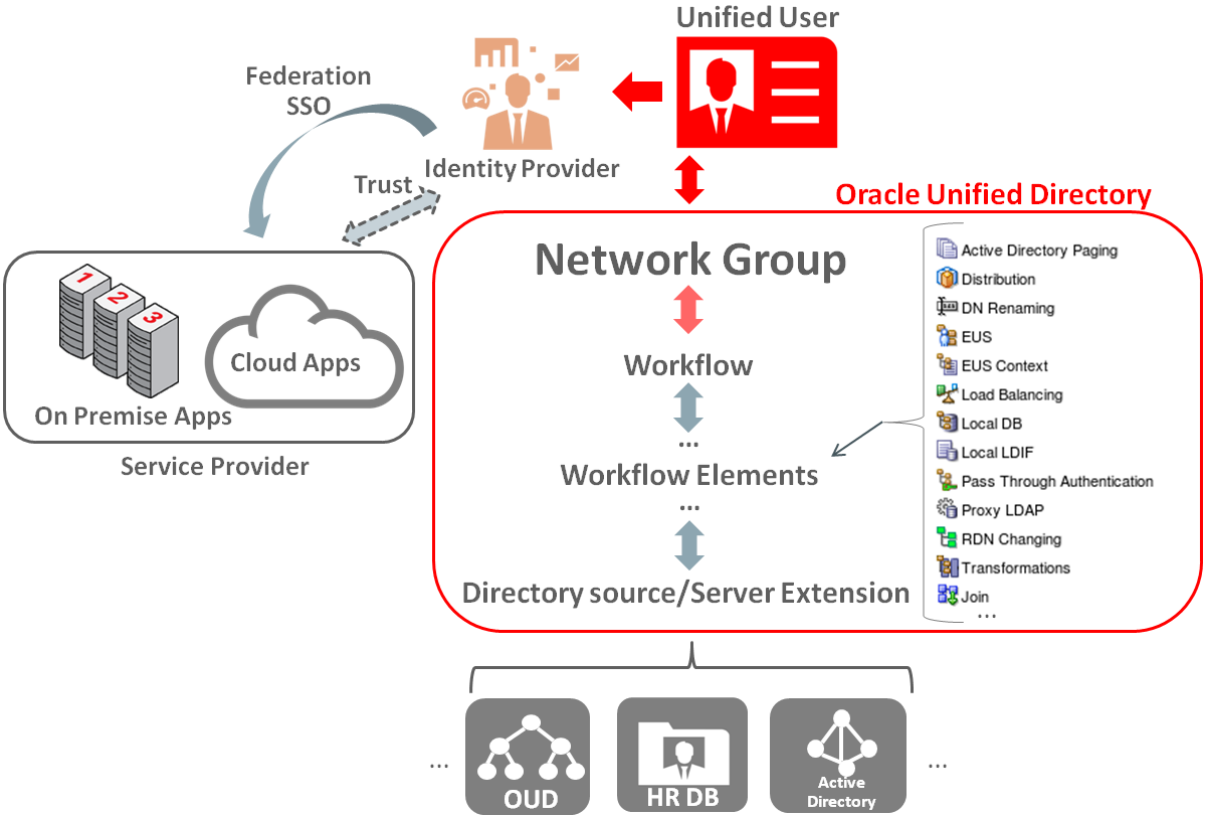
Oracle Unified Directory (OUD) is a comprehensive next generation directory service entirely developed in Java. It is fully LDAP v3 compliant, easy to deploy and manage, and has monitoring capabilities that addresses large deployments with high performance.

OUD at its core excels as a reliable and performing identity store, designed to meet modern directory challenges like with new mobile, social and cloud apps, and ready for services generating frequent updates and writes. An example is to store and compute the geo-location of the friends of a user with a mobile app as he travels to the city center for an anniversary dinner. OUD changes the scenario by eliminating the need to overbuild a monolithic system by providing key features such as distributed global indexing, robust and flexible replication services with partial and fractional replication, directory synchronization for identity and password unification with DIP, Web-based UI - Oracle Directory Services Manager (ODSM), and REST services support very soon.

OUD's unique design allows it to be flexibly configured for core LDAP storage, LDAP Proxy, synchronization and replication with an existing OUD or ODSEE instance and to address the primary use case of this paper: Solving Identity fragmentation through virtualization. OUD is able to solve this by providing a broad set of identity virtualization and transformation workflow elements, or to simply act as a directory proxy.

Solving Identity Fragmentation

In the solution we will show how you can combine different OUD virtualization building blocks (out of the box) in different combinations to fulfill a wide range of virtualization use cases to address fragmentation.



Contact address:

Name: Peter Abrahamsson
Company: Oracle
Address: Oracle Spain | Severo Ochoa 55 | Edificio Norte | Parque Tecnológico de Andalucía
Phone: +34952108393
Email: peter.abrahamsson@oracle.com
Internet: Security