An Oracle White Paper

December 2013

Oracle Directory Server Enterprise Edition used by PSA Peugeot Citroën for authentication, access control and corporate directory services, for over 15 years

Introduction

With its two brands, Peugeot and Citroën, the Group PSA Peugeot Citroën is an international carmaker, with sales offices in 160 countries and 200,000 employees worldwide. PSA Peugeot Citroën is also involved in financing activities, logistics and automotive equipment.

In the late 1990s, the first intranet websites began to appear in the company. In the meantime, the LDAP V3 protocol was published, and specified in many RFC documents. Gradually, providing an LDAP interface became a selling point. While the popularity of LDAP increased on the market, the use of the LDAP infrastructure at PSA has also increased.

PSA's Infrastructure – Business Strategy Evolving Over Time

First step: solution to authenticate users and rights to access web sites

The first Directory Server infrastructure was deployed in October of 1997, to provide an authentication and access control solution for web servers and the new messaging system. The content was initialized by merging data extracted from the HR database, and the security repositories of the mainframe and NT network. In addition, a new administration tool was built, a web app.
Rapidly, it became an impossible nightmare for security administrators to manage people and their rights, with additional tools for each new technology.

Going further: building an IAM solution based on an LDAP repository

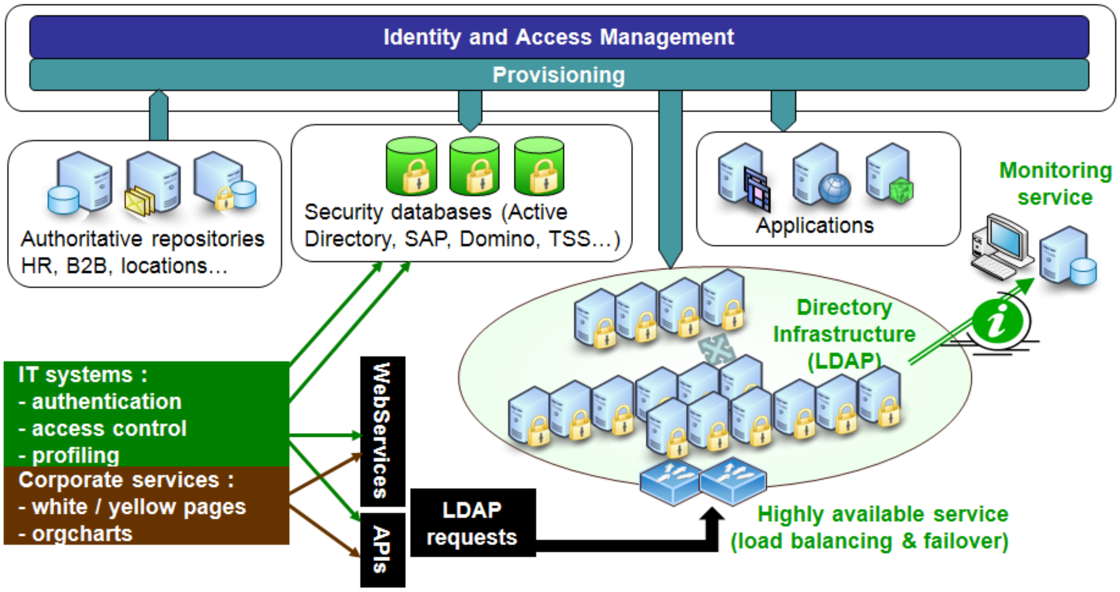
In 1999, an ambitious project called "REUNIS" was launched. The challenge initiated by the Global Risk Management team was to build a security repository, with a unique web-based GUI, which could be used to manage access rights to various applications, with disparate technical environment.
Identity and Access management tools were at that time in their very early stages - in fact they didn't really exist. Carried away by the success of the first experience with an LDAP infrastructure, the idea that came to light was to use it as a centralized security repository.

The project focused on gathering reliable identity descriptions from repositories, and aggregating them in an LDAP directory. Then, on developing homemade web apps offering all the features needed to describe additional identities (not found in an authoritative repository), and manage passwords, certificates, roles, profiles, and access rights. The external changelog mechanism was identified as a way of tracking, in chronological order, each action performed, and propagating it elsewhere, for example to update other databases (Top Secret, Active Directory, SAP, ...).

Giving the LDAP infrastructure its true role

Now, the new “REUNIS” project is on the way, based on IAM products. It’s time to put the LDAP infrastructure back in place, because an IAM system and an LDAP infrastructure do not necessarily adhere to the same requirements: data accuracy and integrity versus availability and performance.

Today, as far as PSA Peugeot Citroën is concerned, the directory infrastructure is a set of technical components, providing access to consistent, reliable and understandable people-centric data, for authentication, access control, profiling or other purposes.

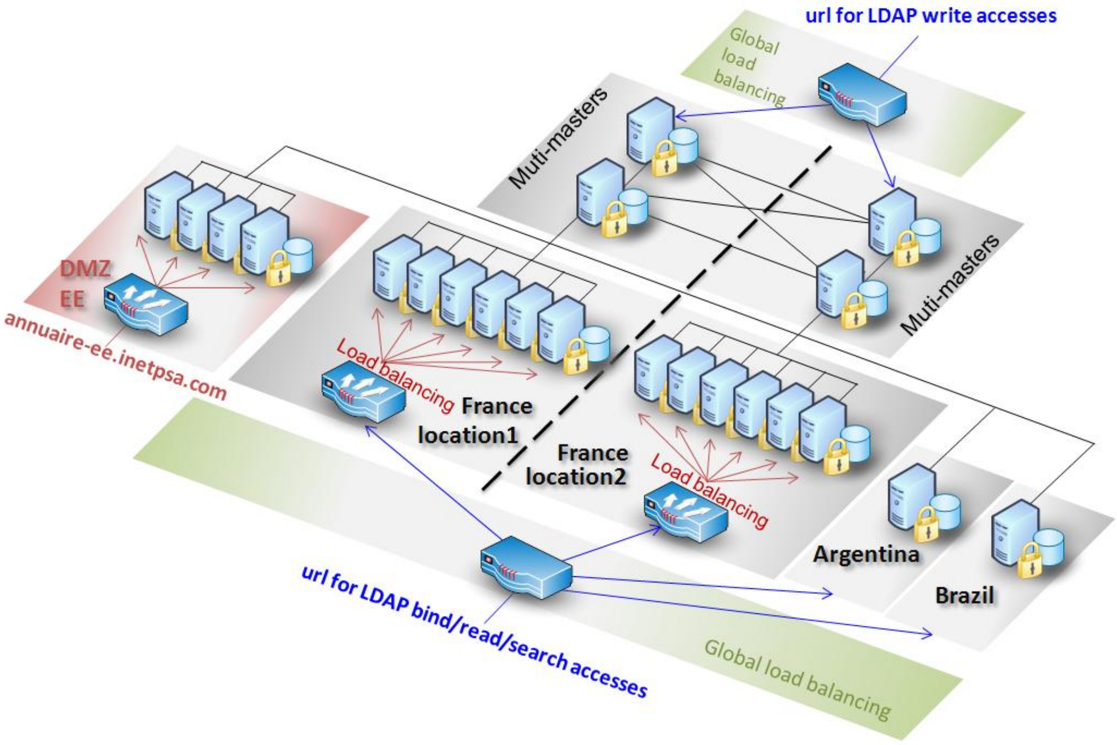

Identity and Access Management
Provisioning
Authoritative repositories HR, B2B, locations…
Security databases (Active Directory, SAP, Domino, TSS…)
Applications
Monitoring service
Directory Infrastructure (LDAP)
IT systems :
- authentication
- access control
- profiling
Corporate services :
- white / yellow pages
- orgcharts
WebServices
APIs
LDAP requests
Highly available service (load balancing & failover)

Data owned by authoritative repositories (HR databases, telecom systems, localization repositories, etcetera) are gathered and aggregated in the identity and access management system. As it hosts the security repository, the IAM system adds security data (password, access rights, roles), and, via its provisioning capabilities, feeds the directory infrastructure with whole pertinent data.

Directory Service deployment

A highly available deployment

As described above, the directory service is one corner stone, involved in the operational process for the majority of PSA's information systems. The whole topology consists of 28 LDAP servers, spread over fourteen physical servers (two quad-core processors, 48 GB, DMX SAN arrays). LDAP servers are running on Solaris 10 virtual zones (two per physical machine). They are located in France (two data centers), in Brazil, and Argentina.



The version currently installed is ODSEE 11gR1. A total of 1,600,000 entries (including 550,000 identities) are stored, and fully replicated on each server. Nearly 80 attributes are indexed. The topology is based on four masters, configured with multi-master replication agreements.

The service level required for read operations is very critical. The approach chosen to provide scalability and high availability is to use redundant server components. Replication is used across data centers, and over a transcontinental WAN for Mercosur. Inside each data center, the connections are load-balanced. The directory service is reachable via the same unique URL, regardless of where the connection is initiated. A global load balancing service is used to send each connection to

Argentina, Brazil, or France, according to the location of the client and the availability of each site.

LDAP content and usage

Because LDAP technology was designed for this, our approach from the beginning has been to publish data describing users and promote its usage broadly. The selection of what to publish in the LDAP infrastructure is driven by two criteria: the information should be relevant for a large public and should be managed in a repository, or at least have an identified owner and defined business rules.

The directory infrastructure is intended for use by servers and network components, but not by the end user equipment (PC, laptop, etc.). The total number of requests increases constantly. The projection estimated for 2014 is about 100 billion requests per year, which is equivalent to 273,000 requests daily. The average etime is 1.2ms and the rate of requests processed in less than 10ms is around 99.4%.

Monitoring the Directory Infrastructure

The need to monitor the LDAP topology soon became clear: locate expensive queries, questionable practices, follow the increase in simultaneous connections and requests. And also decipher what was really happening when a user said “it does not work”.

Explore, a homemade solution, was built in 2003 (well before Oracle Enterprise Manager Grid Control). Explore provides information on the overall number of requests; average, minimum and maximum response time. All figures are available globally, for each IP or account used to authenticate the connections. The content of the “cn=monitor” suffix is regularly read and stored as well. A simple request is executed from various locations, to check service availability and performance. Logs are also aggregated and stored in a database to be analyzed retrospectively.

To ensure a good quality of service (response time and availability), two aspects are always kept in mind: firstly infrastructure scalability and redundancy, and secondly the quality and quantity of generated requests.
Infrastructure scalability is easy to achieve. The trick is only to monitor the activity and adjust the number of servers (horizontal scalability). To achieve the second point, anonymous access has been forbidden. Each LDAP connection is authenticated by a functional account, identifying each component. As home-grown applications are not allowed to send LDAP requests directly, Web services and specific APIs (for Java, PHP, PERL and C) have been developed. For off the shelf software, a validation process of the generated LDAP requests has been built up. Other solutions such as provisioning and extractions have been implemented for mass processing.

Benefits of using Oracle Directory Server Enterprise Edition

Up to 2007, PSA developed the directory-based project "REUNIS", still used to manage IT access to most PSA applications, whatever the technology concerned. The design of a new REUNIS, based on IAM products, is in progress. But the reliability and robustness of the directory server, and its changelog mechanism, have allowed PSA to build a reliable solution, years before the maturity of the market.
HR and the security management systems have been connected. The accounts of hired employees are created automatically and those of departing employees are automatically closed. The IAM features are designed to be used by functional people (not IT). Behind each granted or revoked functional profile, a technical description is hidden for the purpose of provisioning automation. Accounts, groups and memberships are provisioned on TSS, SAP, Domino, LDAP, Active Directory systems, and about 80 other applications.

Regarding the use of the directory server for authentication and access control, the infrastructure is operational 24/24, 7/7, without major problems. And yet, the number of requests has grown from 54 million to 190 million per day, on average. The product has proven its reliability, scalability, and performance level. It’s a standardized and simple way to have access, from a single point, to data describing people, otherwise scattered across several repositories. The published data are broadly used, and their massive usage ensures their accuracy

Conclusion and Perspectives

Oracle Directory Server is used to provide authentication, and user information for access control. Corporate directory services are also based on this product (organization charts, and white pages). With 1,600,000 entries stored, and an average of 200 million requests per day, it’s a critical component involved in the daily usage of 12,500 components worldwide (applications based on J2EE technologies, software products, UNIX operating systems, and HTTP proxy servers in DMZ environments).
The promotion of the directory service is a success beyond expectation. However, due to the decision to open access to the LDAP infrastructure widely, there are now difficulties in implementing stricter controls. Spikes, LDAP browsing or expensive queries are still flagged.

Several case studies are still in progress or planned. Different challenges are to be dealt with (including avoiding spikes caused by applications making large numbers of requests, deploying global account lockouts without a full multi-master topology, going further in the centralized management of UNIX access rights by addressing the issue of granting access rights specific to each UNIX server, and using the LDAP directory for authentication and access control when connecting to a database .)

ORACLE®

PSA use case for ODSEE
December 2013
Author: Etienne Remillon

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together