Identity Management in University System

Emanuil REDNIC, Manole VELICANU
Academy of Economic Studies, Bucharest

The Identity Management became to be a real and important problem for distributed environments. First off all the access to distribuited resoruces, the distributed comunication, virtual workspaces, virtual repositories influence in developing this field of security. How this all started? How this can be implemented? How this can be maintanced in a distributed environment?

Keywords: *Lightweight Directory Access Protocol, Identity Management.*

1 Introduction

From the trivial email address to the organization provided by the LDAP - Directory Services, Identity Management had known a real fast and feasible development in the latest years. Main important LDAP providers are grouped in two categories:

- Freeware / Open Source LDAP
- Closed Source LDAP

In the first category can be mentioned:

- Apache Directory Project

The Apache Directory project is a set of applications written in Java and consisting of an LDAPv3 server (with triggers, stored procedures, views and other capabilities more normally associated with the transactional DB world) and native support of Kerberos5, Password Change protocol and a modest DNS and DHCP capability. It comes with a fixed (currently) back-end (JDBM). The project also includes Apache Directory Studio, which is a Java client (using the eclipse framework) optimized for use with Apache Directory Server. Runs on multiple platforms. Apache V 2.0 License.

- Fedora Directory Server

The Fedora Directory Server project is part of the Fedora development sponsored by Red Hat. It is written in C and uses a 10-year-old code (genus is Michigan University -> Netscape Directory Server -> Fedora Direcory Server) base even though it has only recently been Open Sourced.

- OpenDS

The OpenDS project is written in Java and is a relatively new Directory Server project being developed under jav.net and seems largely led by Sun Microsystems.

- OpenLDAP

The high-quality LDAP reference design originally based on the University of Michigan's work. Actively developed and widely implemented. GPL.

In the second category can be mentioned:

- Oracle Internet Directory: (OID) is Oracle Corporation's directory service, which is compatible with LDAP version 3.
- CA Directory: CA Directory contains pre-caching engine which can index all attributes that are used in LDAP search filters, and caching all attributes returned in search results.
- Active Directory (AD) is an implementation of LDAP directory services by Microsoft for use primarily in Windows environments. Its main purpose is to provide central authentication and authorization services for Windows based computers. Active Directory also allows administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory stores information and settings in a central database

2. Identity Management Metrics

From the above listed LDAP servers, most used LDAP servers are OID and AD due to their performance: highly managed numbers of users, quick and fast ldap operations: ldapsearch, ldapadd, ldapmodify, bulkload, ldifde. From the latest version of OID: 10.1.4.2., OID provide the synchronism mechanism with all types of others LDAP servers; at the beginning the main LDAP on which Oracle was focused to integrate with OID was AD, due to highly usage of this LDAP server through the PC users in the En-

terprise organizations.
Another big advantage of the OID, is that it comes integrated in a Enterprise Management Metrics System, how this works:

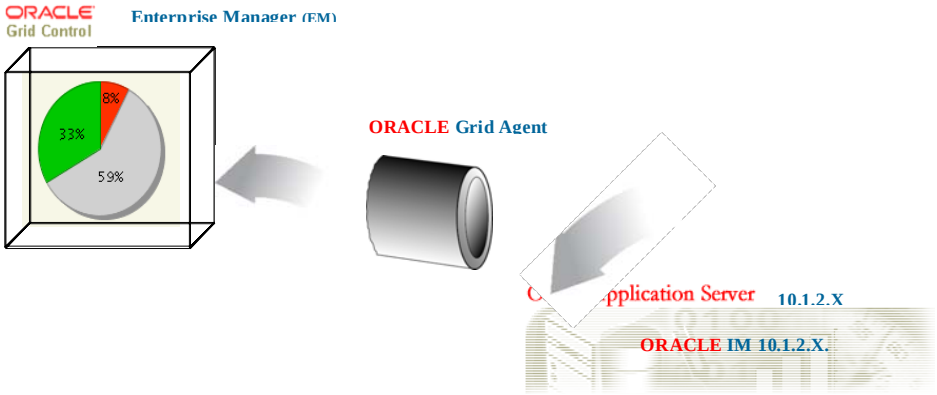

Fig.1. Oracle EM – Oracle Application Server – Identity Management Architecture

The EM web sites all integrates metrics measurement for all components integrated in Application Server, such as HTTP Server, the OC4J container, deployed Single Sign On (SSO) application. In the EM organization all the above components are known as targets. The performance metrics graphics can be achieved for the entire environment and as well for subcomponents.
As part of Application Server, HTTP Server manage to handle all the http tasks from either deployed application, or the ones included in the OC4J container, ones that are used for Identity Management: SSO and OIDDAS Delegated Administration Services.

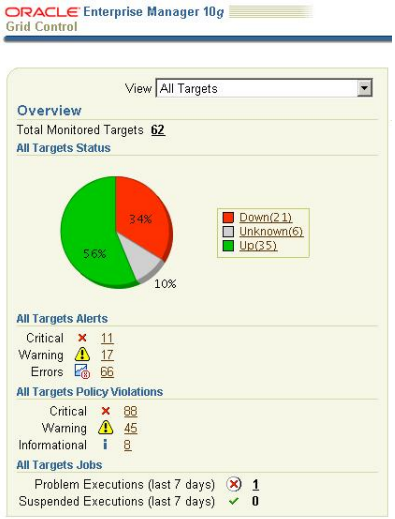

Fig.2. Overview of all targets in Oracle EM

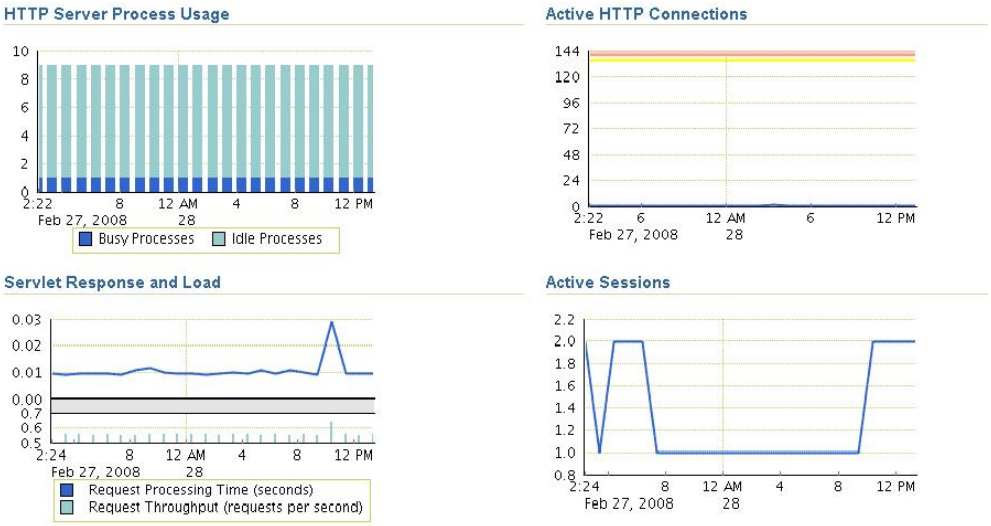

Fig.3. HTTP Graphics Metrics

Measuring the performance of SSO requests is mandatory to involve as well the HTTP Server performance metrics. In the following figure, it shows how EM split performance

metrics graphics for each type of issues, which influence it: active connections, active sessions, the usage of HTTP Server, the behavior of the partner application servlet deployed in OC4J container.

3. Identity Management as part of High Availability (HA) environment

In order to reflect the role of Identity Management in a HA environment, first it should be referenced how a HA environment looks like:

Scenario:

- Oracle RAC DB 10.1.2.x
- Oracle AS Cluster IM
- Linux

In order to create a matrics system for a HA Identity Management, it is mandatory not to omit the following factors:

- Geographic repartition
- Status of HA nodes
- Costs
- Amount of data managed
- Hardware requirements

The most used tool even for HA environments remain EM, due to its functionality:

- Oracle Enterprise Manager based monitoring available for all infrastructure databases
- Oracle Enterprise Manager based monitoring available for all OID LDAP instances and OID Server Manageability metrics available here

Daily LDAP operations load metrics generated by custom scripts that use the OID Server Manageability metrics.

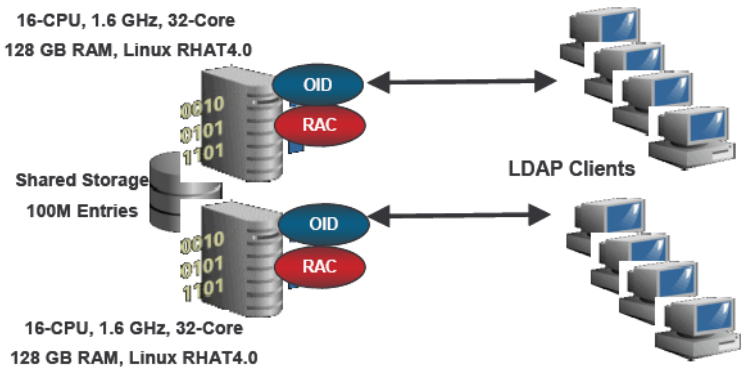

Fig.4. HA Environment Configuration

4. Directory Information Tree (DIT) creation for University System

Starting from organization structure of University Campus, DIT will be created in order to keep the same level of organization as the ones met in the real organization.

First level: the realm should be, for example: dc=university, dc=ro, dc=com.

Second level: the container should be related to departments that are part components of University Campus, and going a level down, to the distinguish name (dn) is added: common name (cn) cn=accounting, cn=universities, or cn=guard assurance.

Third level, if going on the universities branch, to the dn it should be add cn=finance, cn=cibernetics or cn=fabiz.

Fourth level, if going on teaching branch, should be related to the boards that are part components of a university.:
cn=databases,cn=cibernetics,cn=universities, cn=users,<realm>

If going on students branch, to the dn it should be added the specialization common name: cn=business software, cn=cibernetics, cn=universities, cn=users, <realm>.

The last level, on the student branch, should be the student name entrance itself, or on teachers branch, the teacher's name:

- cn=emannuil rednic, cn=business software, cn=cibernetics, cn=universities, cn=users, <realm>

The utility of groups is very high in such IM DIT. It makes more flexible the tree organization, in such a way that is reducing the level of branches, which makes the reference to a leaf to be made in a shorter time. The groups have different branches in the realm:

cn=groups, dc=university, dc=ro, dc=com. With the usage of the groups is very easy to handle the members of a master program, for example, the students are already present in the infrastructure database, all is needed to add them to the members to that specific master group:
cn=database master, cn=groups, dc=university, dc=ro, dc=com.
Group organization can be applied for all types of level of education in the university, for the Pre Bachlors, Master, or PhD school.

- dc=university, dc=ro, dc=com
  - cn=groups
- cn=database masters
  - cn=users
- cn=universities
  - cn=cibernetics
    - cn= business software
      - cn=emanuil rednic

Fig.5. DIT simulation for University Campus

5. LDAP metrics simulation

The metrics system for LDAP operation is based on the following operations:

- Total operations TO
- Total connections TCN
- Total authentication failures TF
- Total binds TB
- Total unbinds TU
- Total searches TS
- Total compares TCC
- Total modifications TM
- Total modrdns TMD
- Total additions TA
- Total deletions TD

where

(5.1.) TO = TCN + TCN + TF + TB + TU + TS + TCC + TM + TMD + TA + TD

(5.2.) TBV = TB + TU

(5.3.) TR = TCN + TF

(5.4.) TMO = TS + TCC + TM + TMD + TA + TD

(5.5.) TO = TBV + TR + TMO

On short time TO has a positive bent, and for long time TO will have a seasonal behavior done by the TD and TA, which reduce them selves or the difference between them is very low, sample: the admitted number of students after a admission session (TA) in comparison with the bachelor degrees which stop their studies and not continue with a master or phd. This fact can be achieved due to limited numbers of students in University Campus.
Making a comparison with the Cobb Douglass Function: $AL^{\alpha}K^{\beta}$, also TF can be written as:

(5.6.) TF= $AL^{\alpha}K^{\beta}$,

Where A is the level of knowledge to use informatic products
L - level of learning the new system
K – level of hardware equipment

6. Conclusion

1.Identity Management is a solution for more and more world wide in the enterprise organization, makes it possible to manage the members of a virtual community, the access, authorization and maintenance of a high volume of resources.
2.The tuning of metrics system for IM/LDAP performance depends of what organization system should be implemented in Directory Services
3.All the functions implemented in the (5.5) formula should be analyzed more deeply, this of course will be the subject of a future article.

References:

Emanuil REDNIC, “Temporary resources allocation modeling and software printed in “Economic computation and economic cybernetics studies and research”, December 2003