CLOUD COMPUTING IDENTITY AS A SERVICE *IDAAS*

http://www.tutorialspoint.com/cloud_computing/cloud_computing_identity_as_a_service.htm

Employees in a company require to login to system to perform various tasks. These systems may be based on local server or cloud based. Following are the problems that an employee might face:

- Remembering different username and password combinations for accessing multiple servers.
- If an employee leaves the company, it is required to ensure that each account of that user is disabled. This increases workload on IT staff.

To solve above problems, a new technique emerged which is known as **Identity-as-a-Service *IDaaS*.**

IDaaS offers management of identity information as a digital entity. This identity can be used during electronic transactions.

Identity

Identity refers to set of attributes associated with something to make it recognizable. All objects may have same attributes, but their identities cannot be the same. A unique identity is assigned through unique identification attribute.

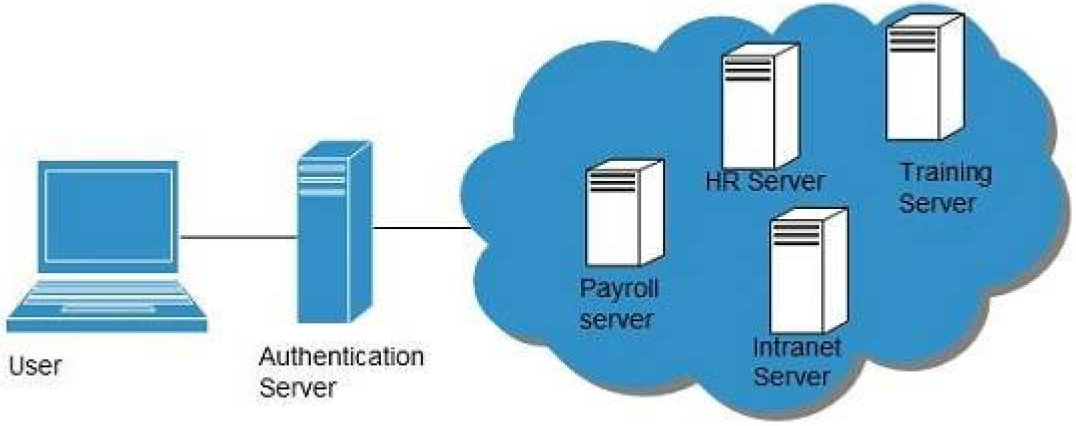
There are several **identity services** that are deployed to validate services such as validating web sites, transactions, transaction participants, client, etc. Identity-as-a-Service may include the following:

- Directory services
- Federated services
- Registration
- Authentication services
- Risk and event monitoring
- Single sign-on services
- Identity and profile management

Single Sign-On *SSO*

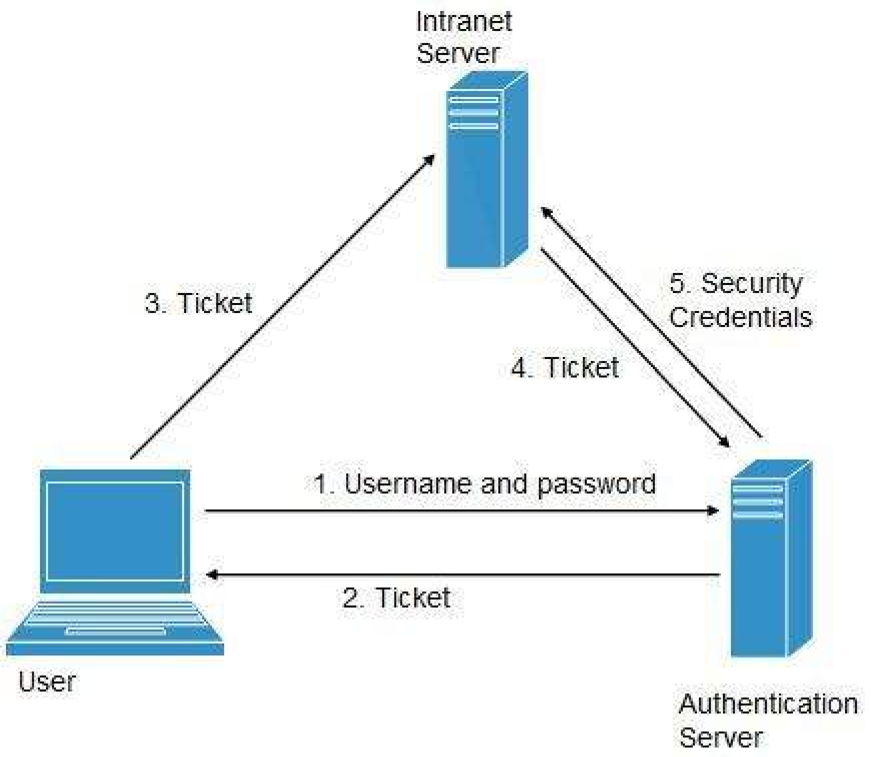
To solve the problem of using different username and password combinations for different servers, companies now employ Single Sign-On software, which allows the user to login only one time and manage the access to other systems.

SSO has single authentication server, managing multiple accesses to other systems, as shown in the following diagram:



SSO Working

There are several implementations of SSO. Here, we discuss the common ones:



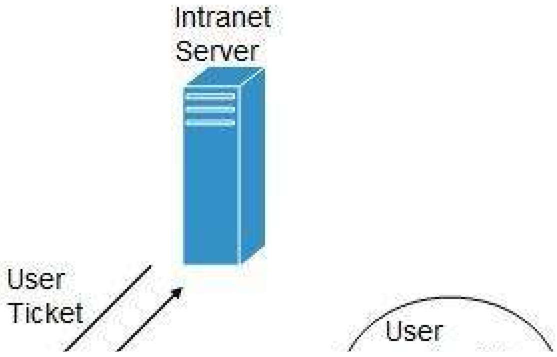
Following steps explain the working of Single Sign-On software:

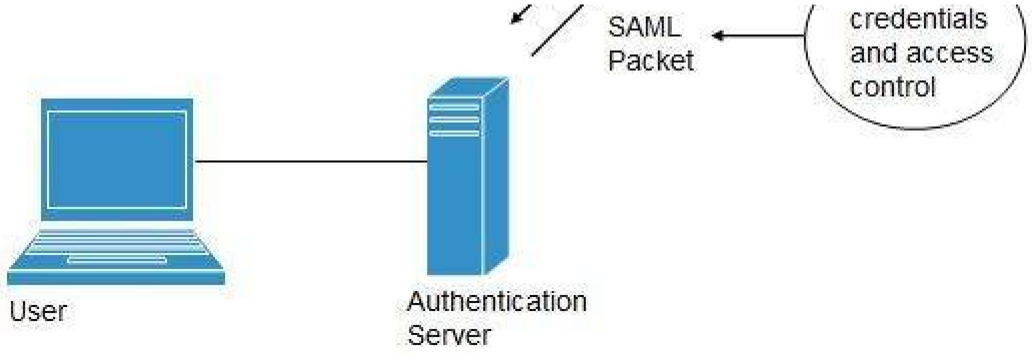
- User logs into the authentication server using a username and password.
- The authentication server returns the user's ticket.
- User sends the ticket to intranet server.
- Intranet server sends the ticket to the authentication server.
- Authentication server sends the user's security credentials for that server back to the intranet server.

If an employee leaves the company, then disabling the user account at the authentication server prohibits the user's access to all the systems.

Federated Identity Management *FIDM*

FIDM describes the technologies and protocols that enable a user to package security credentials across security domains. It uses **Security Markup Language** *SAML* to package a user's security credentials as shown in the following diagram:





OpenID

It offers users to login into multiple websites with single account. Google, Yahoo!, Flickr, MySpace, WordPress.com are some of the companies that support OpenID.

Benefits

- Increased site conversation rates
- Access to greater user profile content
- Fewer problems with lost passwords
- Ease of content integration into social networking sites