UbuntuNet CONNECT 2018

Contribution ID: **64** Type: **Presentation**

A Microservice Approach to Identity Management

Identity management is a security discipline that involves identification, authentication and authorization of individuals to system or network resources. It is a process that provides confidence of resource access or denial, based on supplied identity information. The digital ecosystem space is dynamically changing with more online content but access management is still a challenging component. An efficacious centralized identity management system can lead to improved data security, reduced access costs to resources and easier policy implementation.

Research and education institutions in many African countries, mainly because they operate in resource constrained environments, are faced with a challenging dimension in the identity management space. In addition, unpredictable power outages at the data centers can cause irreparable system damage, and most systems and network engineers/administrators lack the necessary technical expertise to fully and effectively operate an identity management system. The number of users has not helped the cause with most institutions habiting thousands of users. This has led to creation of silos of identities as and when required for resource access (such as email, network, Enterprise Resource Planning (ERP) and monitoring systems) and management of this information is not only time consuming but rather hectic and error-prone.

Most institutions operate monolithic identity applications without high availability, no redundancy considerations or backup strategies and a failure can lead to unprecedented outcomes. A loss of identities for thousands of users can be damaging to the institution's reputation and the recovery costs are substantial. In other instances, institutions do not operate any identity system due to infrastructure costs and setup complexities, and this poses a serious security threat to data resources as no accountability can be generated on access.

The microservice architecture structures applications as a set of loosely coupled services delivering specific functionality or capability and enables continuous delivery and deployment of the applications. Kubernetes automates deployment, scaling and operation of cloud-native distributed applications across a cluster of hosts in a containerized setup. It provides self healing of applications, infrastructure abstraction (allows application portability) and efficiency as many applications can reside independently on the same hardware with no negative impact on another. OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol (LDAP) providing mainly centralized user management in form of a hierarchical directory service.

This paper will focus on a low-cost approach to implementing a multi-domain (institutional domains), resilient and distributed identity management system using openLDAP on Kubernetes for National Research and Education Networks (NRENs), a case of the Research and Education Network for Uganda (RENU). Microservices will be used to represent the different instances of the identity systems for each institution and run on a cluster with replication across the nodes. This allows for self-healing of applications, seamless update/upgrade and application high availability achieved through service replication over a set of cluster nodes. Systems and network engineers/administrators can then focus on the user end and performance with no infrastructure worries.

Summary

Sub-Theme

SMART Research: Services and tools

Primary author: Mr MWOTIL, Alex (Research & Education Network for Uganda, Makerere University)

Co-authors: Prof. BAINOMUGISHA, Engineer (Makerere University); Mr MBONIMPA, Nicholas (Research & Education Network for Uganda (RENU))

Presenter: Mr MWOTIL, Alex (Research & Education Network for Uganda, Makerere University)

Session Classification: UbuntuNet-Connect