**Mô hình triển khai và dự phòng LDAP tỉnh Bình Thuận**

**1. Mô hình triển khai hiện tại**

**1.1. Mô hình triển khai**

A picture containing waterfall chart

Description automatically generated

**1.2. Mô hình kết nối**

Diagram

Description automatically generated

**1.3. Giải thích mô hình**

***Proxy Zone:***

- Máy chủ haproxy-mc-dvc cài đặt dịch vụ proxy và loabancer HAProxy, có nhiệm vụ làm proxy và cân bằng tải cho hệ thống MC, DVC, LGSP.

- Máy chủ haproxy-mail-01 cài đặt haproxy, MongoDB Primary phục vụ cho hệ thống thư điện tử công vụ.

***Citizen Zone:***

- Máy chủ DVC01 và DVC02 cài đặt phần mềm dịch vụ công trực tuyến.

- Máy chủ CSDLTTHC cài đặt phần mềm Cơ sở dữ liệu thủ tục hành chính.

***DVC-MC App Zone:***

- Máy chủ tthcc01 và tthcc02 cài được phần mềm TTHCC.

- Máy chủ MC01 và MC02 cài đặt phần mềm Một cửa điện tử tập trung

- Máy chủ Sphere cài đặt phần mềm sphere quản lý giao diện cho trang Dịch vụ công trực tuyến.

***LGSP App Zone:***

- Máy chủ Management cài đặt các phần mềm:

+ Lotus: quản lý tập trung cho hệ thống.

+ CAS: cài đặt phần mềm Single Sign On (SSO) giúp đăng nhập tập trung cho toàn hệ thống.

- Máy chủ VDXP cài đặt phần mềm VPXP.

- Máy chủ OpenID cài đặt phần mềm OpenID.

- Máy chủ LGSP01 và LGSP02 cài đặt mềm LGSP. Ngoài ra, máy chủ LGSP01 còn được cài đặt phần mềm CAS nhằm dự phòng và cân bằng tải cho CAS trên máy chủ Management.

***Mail Zone:***

- Máy chủ Mail1 cài đặt các phần mềm Postfix, Dovecot làm máy chủ xử lý thư điện tử.

- Các máy chủ Webmail01, Webmail02 và Webmail03 được cài đặt ứng dụng webmail, giúp gửi/nhận thư điện tử trên giao diện web.

- Máy chủ Webmail4 cài đặt ứng dụng lotus mail để quản trị hệ thống thư điện tử.

***DVC - MC Database Zone:***

- Máy chủ DB-Primary cài đặt phần mềm MongoDB làm cơ sở dữ liệu cho hệ thống.

***LGSP DB Zone:***

- Máy chủ LDAP cài đặt phần mềm OpenLDAP chứa tài khoản người dùng (công vụ).

- Máy chủ esb-server cài đặt các phần mềm ESB, MongoDB và Redis.

- Máy chủ DVCDB02 cài đặt phần mềm OpenLDAP và MySQL làm sơ sở dữ liệu cho OpenID.

***Mail DB Zone:***

- Máy chủ MongoDB cài đặt aribiter giám sát cho cụm replicate của MongoDB.

***Lưu ý:***

- Ngoài máy chủ chạy dịch vụ HAProxy và máy chủ thư điện tử, tất cả các máy chủ còn lại trong hệ thống cần được đặt trong vùng mạng an toàn, không truy cập trực tiếp từ Internet.

- Nếu máy chủ nào còn nằm vùng mạng ngoài (ngoài 2 máy chủ kể trên) thì việc di chuyển chúng vào vùng mạng an toàn là cần thiết. Việc di chuyển này không làm thay đổi kiến trúc tổng thể của hệ thống.

**2. Triển khai mô hình dự phòng LDAP**

LDAP như trình bày ở mục 1 chỉ chạy trên một máy chủ, không đảm an toàn thông tin cho hệ thống. Nhằm đảm bảo dự phòng cho LDAP khi một máy chủ xảy ra sự cố, chúng tôi khuyến nghị cài đặt LDAP trên 2 máy chủ khác nhau theo mô hình Master – Master kết hợp với Keepalived. Cụ thể LDAP mới sẽ được cài đặt trên hai máy chủ LGSP01 và LGSP02.

Mô hình kết nối dự phòng LDAP đạt được sau khi cài đặt:

Diagram

Description automatically generated

Mô hình LDAP Master - Master với Keepalived:

Diagram

Description automatically generated

Giải thích mô hình:

- OpenLDAP được cài đặt trên 2 máy chủ LGSP01 và LGSP02 theo mô hình Master – Master cho phép đọc/ghi dữ liệu trên cả 2 máy. Dữ liệu của ldap được đồng bộ lẫn nhau, đảm bảo tính nhất quán. Trên 2 máy chủ cũng được cài đặt Keepalived, trong đó LGSP01 đóng vai trò Master, LGSP02 làm Backup.

- Các phần mềm (SSO, Mail, MC,… ) kết nối đến LDAP thông qua IP ảo (Virtual IP). Yêu cầu đọc/ghi dữ liệu của các phần mềm này thực sự được xử lý bởi LGSP01 (Master Keepalived), LGSP02 chỉ đóng vai trò dự phòng (Backup Keepalived) cho LGSP01.

- Nếu kết nối đến LGSP01 có vấn đề hay máy chủ bị sự cố thì máy chủ LGSP02 sẽ tự động trở thành Master Keepalived xử lý dữ liệu thay thế cho LGSP01.

- Khi LGSP01 hoạt động trở lại, nó sẽ tiếp tục đóng vai trò Master Keepalived thay thế cho LGSP02.