

Công ty TNHH TMDV Giải Pháp Việt
Khóa thực tập : NS014
Mentor : Võ Đại Vương
Thực tập sinh : Hồ Hải Dương

BÁO CÁO KẾT QUẢ BÀI TẬP TUẦN 6

MỤC LỤC

Phần 1	1
1.1. Yêu cầu	1
1.2. Hình ảnh demo.....	1
Phần 2	3
2.1. Yêu cầu	3
2.2. Các bước thực hiện	3
2.3. Kết quả.....	3
2.4. Hình ảnh demo.....	4
Phần 3	5
3.1. Yêu cầu	5
3.2. Các bước thực hiện	5
3.3. Kết quả.....	5
3.4. Hình ảnh demo.....	5
Phần 4	6
4.1. Yêu cầu	6
4.2. Các bước thực hiện	6
4.3. Kết quả.....	6
4.4. Hình ảnh demo.....	7
Phần 5	7
5.1. Yêu cầu	7

5.2. Các bước thực hiện	7
5.3. Kết quả.....	7
5.4. Hình ảnh demo.....	8
Phần 6.....	9
6.1. Spam Detector.....	10
6.2. Virus Detector	10
6.3. Mail Filter – Rules Engine.....	10
6.4. Quarantine Management.....	10
6.5. Giám sát & Log	10
6.6. Cluster Management.....	10
6.7. Hỗ trợ TLS/SSL	11

BÀI LÀM

Phần 1

1.1. Yêu cầu

- Tạo 2 máy ảo chạy Proxmox Mail Gateway (PMG) trên nền ảo hóa Proxmox VE.
- Đặt hostname lần lượt là:
 - mx1.gr2p11.site
 - mx2.gr2p11.site
- Ghi chú rõ IP và hostname vào phần Note của VM để hỗ trợ quá trình kiểm tra.
- Cấu hình phần cứng cho mỗi VM gồm: 2 vCPU, 4GB RAM, 30GB Disk.

1.2. Hình ảnh demo

Key ↑	Value
cores	2
cpu	x86-64-v2-AES
ide2	backup-cmc:iso/proxmox-mail-gateway_8.2-1.iso,media=cdrom
memory	4096
name	ns14-w06-duonghh
nodename	intern
numa	0
ostype	l26
pool	duonghh
scsi0	local-lvm:30,iothread=on
scsihw	virtio-scsi-single
sockets	1
vmid	4201

Key ↑	Value
cores	2
cpu	x86-64-v2-AES
ide2	backup-cmc:iso/proxmox-mail-gateway_8.2-1.iso,media=cdrom
memory	4096
name	ns14-w06-duonghh
nodename	intern
numa	0
ostype	l26
pool	duonghh
scsi0	local-lvm:30,iothread=on
scsihw	virtio-scsi-single
sockets	1
vmid	4202

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Vietnam
Timezone:	Asia/Ho_Chi_Minh
Keymap:	en-us
Email:	admin@gr2p11.site
Management Interface:	ens18
Hostname:	mx1
IP CIDR:	103.27.63.219/25
Gateway:	103.27.63.129
DNS:	8.8.8.8

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Vietnam
Timezone:	Asia/Ho_Chi_Minh
Keymap:	en-us
Email:	admin@gr2p11.site
Management Interface:	ens18
Hostname:	mx2
IP CIDR:	103.27.63.218/25
Gateway:	103.27.63.129
DNS:	8.8.8.8

Phần 2

2.1. Yêu cầu

Thực hiện tạo cluster gồm 2 node PMG: mx1.gr2p11.site (master) và mx2.gr2p11.site (node). Đồng bộ cấu hình giữa 2 node trong hệ thống. Sau khi tạo cluster, truy cập được giao diện quản lý tập trung qua node master.

2.2. Các bước thực hiện

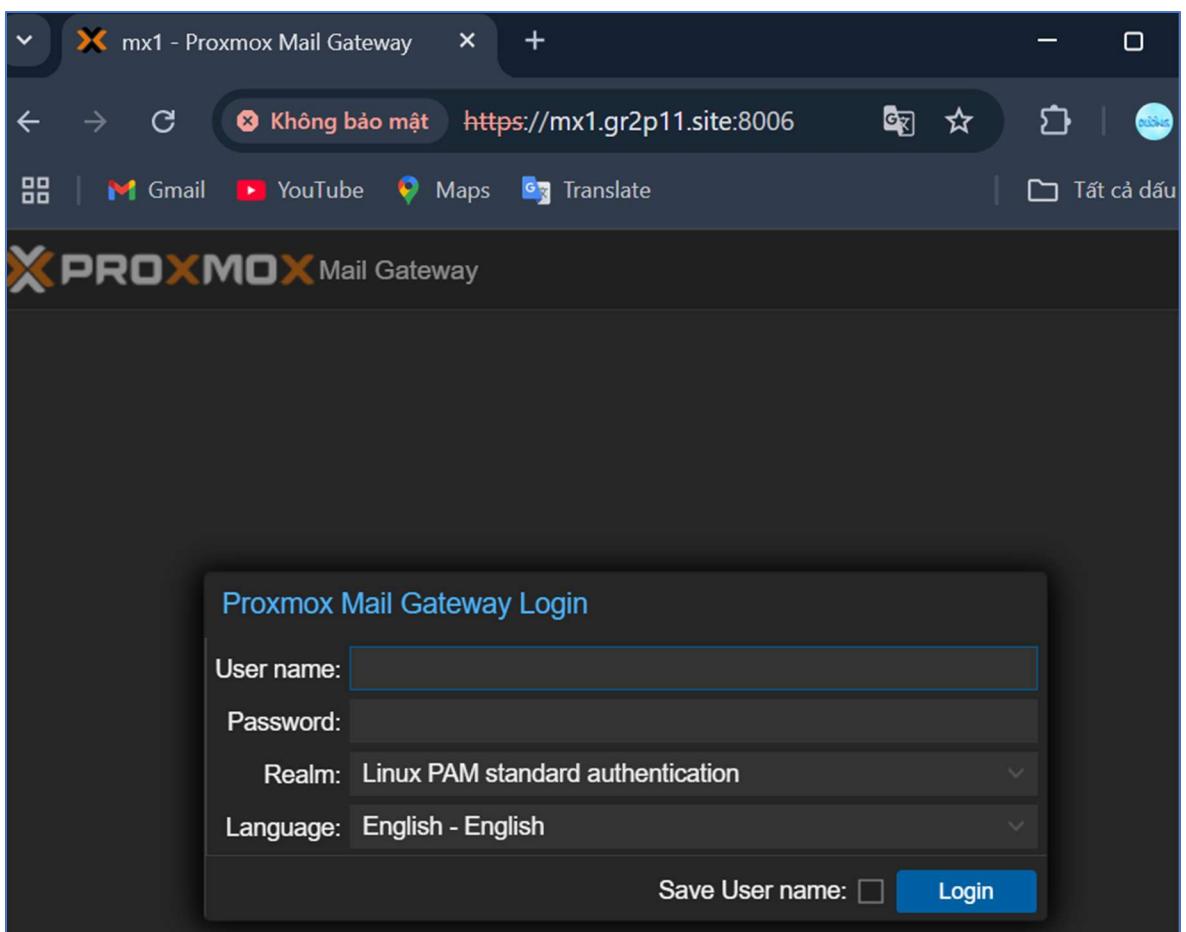
- Truy cập vào PMG node mx1 và bảo đảm đã cấu hình xong cơ bản như hostname, IP tĩnh, timezone, etc.
- Trên mx1, khởi tạo cluster bằng lệnh: pmgcm create
- Trên mx2, chạy lệnh để join vào cluster từ mx1: pmgcm join 103.27.63.219 --fingerprint
'30:39:1B:56:4C:39:33:BD:E4:7A:32:73:ED:81:9E:A6:9A:75:DC:D9:EF:7C:01 :90:EF:CA:59:EF:F4:92:16:6F'
- Sau khi xác nhận, hệ thống sẽ tự động: Dừng các dịch vụ liên quan. Xoá CSDL cũ và đồng bộ lại từ mx1. Tạo khóa xác thực mới (pmg-authkey.key, pmg-csrf.key, ...). Sync dữ liệu quarantine và cấu hình.
- Kiểm tra trạng thái cluster: pmgcm status

2.3. Kết quả

- Cluster PMG đã được thiết lập thành công với mx1 là master, mx2 là node.
- Các thông tin cấu hình và dữ liệu được đồng bộ hóa tự động giữa hai node.
- Giao diện quản trị PMG có thể truy cập tập trung tại địa chỉ <https://mx1.gr2p11.site:8006>.

2.4. Hình ảnh demo

```
root@mx2:~# pmgcm join 103.27.63.219 --fingerprint '30:39:1B:56:4C:39:33:BD:E4:7A:32:73:ED:81:9E:A6:9A:75:DC:D9:EF:7C:01:90:EF:CA:59:EF:F4:92:16:6F'
stop all services accessing the database
save new cluster configuration
cluster node successfully joined
updated /etc/pmg/pmg-authkey.key
updated /etc/pmg/pmg-authkey.pub
updated /etc/pmg/pmg-csrf.key
copying master database from '103.27.63.219'
copying master database finished (got 36645 bytes)
delete local database
create new local database
GRANT
GRANT
GRANT
GRANT
insert received data into local database
creating indexes
run analyze to speed up database queries
ANALYZE
syncing quarantine data
syncing quarantine data finished
root@mx2:~# pmgcm status
NAME(CID)-----IPADDRESS----ROLE-STATE-----UPTIME---LOAD---MEM---DISK
mx2(2)          103.27.63.218    node   S        00:26   0.18   60%   10%
mx1(1)          103.27.63.219    master  S        00:26   0.00   58%   10%
```



Phần 3

3.1. Yêu cầu

Cấu hình hệ thống cân bằng tải (Load Balancing) giữa hai máy chủ PMG (mx1.gr2p11.site và mx2.gr2p11.site) sao cho toàn bộ email gửi và nhận sẽ được xử lý luân phiên hoặc dự phòng qua hai gateway. Mục tiêu là tăng tính sẵn sàng và độ tin cậy của hệ thống email nội bộ.

3.2. Các bước thực hiện

- Truy cập vào giao diện web của mx1 và mx2 tại cổng 8006.
- Vào Mail Proxy → Transports.
- Tạo bản ghi chuyển tiếp (relay) như sau:
 - Relay Domain: gr2p11.site
 - Host: mail.gr2p11.site
 - Protocol: smtp
 - Port: 25
 - Use MX: No
 - Comment: mx1 replay to zimbra
- Kiểm tra lại cấu hình: Cả hai PMG đều có cấu hình giống nhau, bảo đảm gửi email từ bên ngoài vào domain gr2p11.site sẽ được chuyển tiếp tới Zimbra server tại mail.gr2p11.site.

3.3. Kết quả

- Cả hai PMG (mx1 và mx2) đã được cấu hình transport chuyển tiếp về Zimbra.
- Các email gửi đến domain gr2p11.site thông qua một trong hai PMG sẽ được forward về mail.gr2p11.site để xử lý tiếp.
- Việc truy cập giao diện web của mx1 và mx2 trên cổng 8006 đã thành công, xác nhận các máy chủ đang hoạt động và sẵn sàng xử lý email.

3.4. Hình ảnh demo

The screenshot shows the Proxmox Mail Gateway 8.2.0 configuration interface. The left sidebar has 'Mail Proxy' selected. The main area shows the 'Configuration: Mail Proxy' screen with the 'Transports' tab active. A table lists a single relay entry:

Relay Domain ↑	Host	Protocol	Port	Use MX	Comment
gr2p11 site	mail.gr2p11.site	smtp	25	No	mx1 replay to zimbra

Relay Domain ↑	Host	Protocol	Port	Use MX	Comment
gr2p11.site	mail.gr2p11.site	smtp	25	No	mx1 replay to zimbra

Phần 4

4.1. Yêu cầu

Cấu hình hệ thống sao cho toàn bộ email gửi đi và nhận vào từ máy chủ Zimbra (đã triển khai trong Week 5) sẽ đi qua hai máy chủ PMG để thực hiện lọc, kiểm tra virus/spam trước khi đến Zimbra hoặc đi ra ngoài.

4.2. Các bước thực hiện

- Zimbra được thiết lập để gửi email thông qua máy chủ mx1.gr2p11.site bằng cách chỉnh cấu hình relay:


```
postconf -e "relayhost = [mx1.gr2p11.site]:25"
postfix reload
```
- Trên giao diện quản lý domain, bản ghi MX trả về mx1.gr2p11.site và mx2.gr2p11.site.
- PMG đã được cấu hình transport map để relay email đến mail.gr2p11.site.
- Gửi thử email từ Gmail đến địa chỉ nội bộ Zimbra.

4.3. Kết quả

- Email gửi từ Gmail về admin@gr2p11.site được tiếp nhận đầy đủ thông qua hệ thống PMG.
- Đây là minh chứng cho việc cấu hình nhận email thông qua PMG hoạt động hiệu quả.
- Việc gửi từ Zimbra ra bên ngoài qua PMG không được demo thành công trong tuần này, do gặp một số lỗi kỹ thuật và thời gian hạn chế.

4.4. Hình ảnh demo



Phần 5

5.1. Yêu cầu

Cấu hình các bản ghi DNS để bảo đảm email gửi ra từ hệ thống có thể xác thực danh tính hợp lệ, tránh bị đánh dấu spam. Bao gồm: PTR, SPF, DKIM, DMARC.

5.2. Các bước thực hiện

- Sử dụng lệnh nslookup để tra IP các máy chủ mail:


```
nslookup 103.27.63.219
nslookup 103.27.63.218
nslookup 45.122.223.79
```
- Kết quả trả về tương ứng các hostname:


```
103.27.63.219 → mx1.gr2p11.site
103.27.63.218 → mx2.gr2p11.site
45.122.223.79 → mail.gr2p11.site
```
- Truy cập DNS quản lý tên miền gr2p11.site và thêm bản ghi TXT. Kiểm tra khóa DKIM đã tạo: /opt/zimbra/libexec/zmdkimkeyutil -q -d gr2p11.site
- Truy cập DNS, thêm bản ghi TXT với selector tương ứng.
- Thêm bản ghi TXT vào DNS. Kiểm tra bằng công cụ DMARC Lookup: <https://mxtoolbox.com/DMARC.aspx>

5.3. Kết quả

- Các bản ghi PTR cho IP đều ánh xạ đúng về hostname tương ứng.
- SPF kiểm tra thành công với IP của cả ba máy gửi.
- DKIM xác minh chữ ký thành công.
- DMARC thiết lập thành công và xác nhận qua giao diện tra cứu.

5.4. Hình ảnh demo

```
C:\Users\HP>nslookup 103.27.63.219
Server: Unknown
Address: 192.168.169.140

Name:    mx1.gr2p11.site
Address: 103.27.63.219

C:\Users\HP>nslookup 103.27.63.218
Server: Unknown
Address: 192.168.169.140

Name:    mx2.gr2p11.site
Address: 103.27.63.218

C:\Users\HP>nslookup 45.122.223.79
Server: Unknown
Address: 192.168.169.140

Name:    mail.gr2p11.site
Address: 45.122.223.79
```

```
C:\Users\HP>nslookup -q=TXT gr2p11.site
Server: Unknown
Address: 192.168.28.173

Non-authoritative answer:
gr2p11.site      text =
                  "v=spf1 ip4:45.122.223.79 ip4:103.27.63.219 ip4:103.27.6
3.218 ~all"
gr2p11.site      text =
                  "v=spf1 ip4:45.122.223.79 ~all"
```

The screenshot shows two main sections of a web-based email delivery tool.

Top Section:

- Input field: gr2p11.site
- Buttons: DMARC Lookup, Find Problems, Solve Email Delivery Problems
- Link: dmarc

Middle Section:

Text input field containing the DMARC record: v=DMARC1; p=none; rua=mailto:admin@gr2p11.site; sp=none; aspf=r

Tag	TagValue	Name	Description
Tagv	Tag ValueDMARC1	NameVersion	DescriptionIdentifies the record retrieved as a DMARC record. It must be the first tag in the list.
Tagp	Tag Valuenone	NamePolicy	DescriptionPolicy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
Tagrua	Tag Valuemailto:admin@gr2p11.site	NameReceivers	DescriptionAddresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URLs.
Tagsp	Tag Valuenone	NameSub-domain Policy	DescriptionRequested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
Tagaspf	Tag Valuer	NameAlignment Mode SPF	DescriptionIndicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).

Bottom Section:

Type	TXT
Name	b045e4b8-3324-11f0-841c-3e866c23fc8._domainkey
Priority	0
Content	"v=DKIM1; k=rsa; p=MIIBljANBgkqhkiG9wOBAQEAAQ8AMIIIBgKCAQEAvv1gBSIBBF62NyU+aD1Alyu/xvL7ZQ/WEOt6+fIONc2rsVARWKcalNCocUnXxu41KgUKcQoMxEOMPZ923giqgLgh3kHgjOkiyFOxz3UhxhS9drWpONRzb63CHsIYHYbOhbs/4NLtG+U2uhJHbn8OpHUsC2xJTab341vb65SzoijNSEWwoiUNvaq1FHQE0ZB4HKxx6HBM0B56+MazGfbKg9205UKX4J6TIS5/uJWiYJ6wn0ngfls4/eUDLTj2AWiPfgjCiYujuIFMPttP+iWBQu+LssCC5KlyHXhn5FlxTTWNPFsPDFzobKEW/bT8UA140VNfESiMsNQUnQzgbUzQIDAQAB"
TTL	300
Delete Edit	

Phần 6

Proxmox Mail Gateway (PMG) là một hệ thống gateway lọc email mạnh mẽ, thường được triển khai giữa Internet và máy chủ mail nội bộ (ví dụ như Zimbra, Exchange...). Ngoài chức năng chuyển tiếp (relay), PMG còn cung cấp nhiều tính năng bảo mật và giám sát nhằm ngăn chặn spam, virus, và các nguy cơ tấn công qua email.

6.1. Spam Detector

PMG sử dụng SpamAssassin để phân tích và đánh giá các thư có dấu hiệu spam.

Có thể tùy chỉnh mức độ spam theo điểm số (spam score), thêm whitelist hoặc blacklist theo domain, IP hoặc nội dung.

Thư bị đánh dấu spam sẽ bị chuyển vào quarantine để người quản trị kiểm duyệt trước khi chuyển đến người nhận.

6.2. Virus Detector

PMG tích hợp sẵn ClamAV – phần mềm diệt virus mã nguồn mở.

Tự động quét tất cả các email đính kèm, cảnh báo nếu có tệp nguy hiểm.

Ngoài ra, có thể cấu hình thêm các engine antivirus khác nếu cần thiết.

6.3. Mail Filter – Rules Engine

PMG hỗ trợ tạo ra các rule lọc mail chi tiết, bao gồm:

- Định nghĩa các điều kiện: IP, tiêu đề, nội dung, người gửi/người nhận...
- Thực hiện hành động: chặn, đánh dấu, forward, thêm tiêu đề,...

Điều này rất hữu ích cho doanh nghiệp muốn kiểm soát nội dung thư theo chính sách riêng.

6.4. Quarantine Management

PMG cho phép người dùng cuối truy cập giao diện web để kiểm tra và xử lý các thư bị cách ly.

Người dùng có thể whitelist, delete, hoặc release thư để nhận về hộp thư chính.

6.5. Giám sát & Log

Giao diện quản trị hiển thị chi tiết lượng email gửi/nhận, tỉ lệ bị chặn, lý do bị chặn.

Hỗ trợ theo dõi theo thời gian thực, xem log chi tiết từng email (header, trạng thái xử lý...).

Hữu ích cho việc kiểm tra lỗi, truy vết khi có sự cố hoặc yêu cầu từ người dùng.

6.6. Cluster Management

Hệ thống hỗ trợ tính năng cluster để bảo đảm tính sẵn sàng cao (high availability).

Giao diện web cho phép dễ dàng quản lý các node trong cluster: thêm, xóa, thay đổi vai trò node.

Cấu hình đồng bộ giữa các node tự động qua giao diện.

6.7. Hỗ trợ TLS/SSL

Có thể bật TLS để mã hóa email khi truyền giữa các server, giúp tăng độ bảo mật. PMG cũng hỗ trợ cấu hình TLS inbound và outbound riêng biệt.

HẾT./.