Homework #3

Due Time: 2023/04/23 (Sun.) 22:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please zip all the files, including one PDF, one XML, and a Dockerfile. Name the zip file "`{your_student_id}.zip`", and submit it through NTU COOL. The zip file should not contain any other files, and the directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- {your_student_id}.xml
+-- {your_student_id}.Dockerfile
```

Grading

- NA accounts for 50 points while SA accounts for 50 points. The final score is the sum between them.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = NA score + SA score + tidiness score.

Network Administration

Short Answers (12%)

1. (4%) 在 OPNSense 防火牆 rule 的設定中，對封包的處置有 Block 跟 Reject 可以選擇。請說明兩者的差別，還有各自在什麼情況下較適合使用。
2. (4%) 在 OPNSense 防火牆 rule 的設定中，Source 跟 Destination 選擇“interface net”和“interface address”的差別是什麼?
3. (4%) 請說明什麼是“stateful firewall”以及“stateless firewall”。OPNSense 是屬於哪一種？

OPNSense (38%)

安裝 OPNSense 並設定他有三個 VLAN interface: VLAN5, VLAN8, VLAN99。對於每一小題，請寫下你詳細的設定步驟。如果需要的話，你可以自己開其他虛擬機 (Alpine, Ubuntu, ...) 來做測試。

1. (6%) 設定 10.5.0.0/24, 10.8.0.0/24, 10.99.0.0/24 給 VLAN5, VLAN8, VLAN99。
   - OPNSense 作為這三個 interface 的 DHCP server。
   - DHCP lease 需包含 8.8.8.8 和 8.8.4.4 這兩個 DNS server。
2. (6%) 設定以下 alias:

Alias Name	Value
GOOGLE_DNS	8.8.8.8, 8.8.4.4
ADMIN_PORTS	22, 80, 443
CSIE_WORKSTATIONS	linux1.csie.org linux2.csie.org linux3.csie.org linux4.csie.org linux5.csie.org

3. (6%) 打開 OPNSense 的 SSH 功能。設定只有 VLAN99 的機器可以透過 ADMIN_PORTS 連到 OPNSense。VLAN5 與 VLAN8 皆不允許。
4. (5%) VLAN99 的機器只能存取以下位址或機器：
   - Google_DNS
   - CSIE_WORKSTATIONS（請提供 traceroute 到 CSIE_WORKSTATIONS 的截圖，若你是 windows 本機可以加參數 -I)
   - 這台 OPNSense（請提供 ssh 到 OPNSense management interface 的截圖）
5. (6%) VLAN5 的機器可以 ping 到 VLAN8 的機器，反之則不行。
6. (5%) 在 2023/05/10 整天，VLAN5 這個 interface 不能通過任何的封包。
7. (4%) 到 System > Configurations > Backups 中，下載 config.xml，將檔名依照你的學號改成如 b07902009.xml 的檔名，連同作業 PDF 一起繳交。

System Administration

Virsh & Docker

請在任意一個工作站 (linux*.csie.org) 上完成此部分題目。

KVM & Virsh (20%)

請下載 Ubuntu Server 22.04 手動安裝 iso 檔，或使用 /tmp2/nasa-hw3/ubuntu.iso

1. **(5%)** 使用 virt-install 新增一個 vm，並用 Ubuntu iso 安裝作業系統，vm 須滿足以下要求：
   - name: 學號（大小寫通用）eg. b11902999
   - vcpus: 2
   - memory: 8 Gigabytes
   - disk: 請放置在 /tmp2/{你的學號}/ubuntu.qcow2, 20G
   - network: 只有 1 個 NAT interface, 並設定 MAC address 的末六碼與學號一樣。e.g. 學號為 b11902987，MAC address 為 52:54:F8:90:29:87。

   安裝 Ubuntu 時需滿足以下要求：
   - username: 學號 eg. b11902999
   - hostname: nasa-hw3

   完成此步驟後請截圖在工作站上 `virsh list` 的輸出畫面、VM 內開機完成的畫面、VM 內登入後的畫面，以及 VM 內執行 `ip a` 指令的輸出畫面。 Hint: 你可能會需要在自己的電腦上裝 vnc viewer。
2. **(5%)** 開啟 Ubuntu 的 serial console，讓你可以在工作站上直接 `virsh console {你的學號}`，便可以不用透過 vnc 來操作 Ubuntu VM。完成後請截圖 `virsh console {你的學號}` 後 VM 輸出的畫面。
3. **(5%)** 請在工作站上用 virsh 對 VM 做一次快照。快照必須符合以下要求：
   - 名稱為: {你的學號}_snapshot
   - 擷取快照時，VM 必須為開機狀態

   完成此步驟後，請在工作站上用 virsh 指令列出所有該 VM 的快照，並截圖下來。
4. **(5%)** 請在 VM 關機後，將 ubuntu.qcow2 與 VM 的設定傳送至另一台工作站。請將搬移後的 VM 開機，並截圖 `ip a` 的執行結果。

Docker (10%)

此部分題目請在上一題新增的 vm 內實作。

1. **(2%)** 使用 apt 安裝 docker 與 docker compose，完成後請截圖 `docker version` 與 `docker compose version` 的結果。
2. **(5%)** Containerize `sl`
   - 請撰寫 Dockerfile，用 alpine 作為 base image 來編譯 sl。

- 修改你的 Dockerfile，使得你可以用 `docker run --rm -it sl` 叫出小火車。
- 為了節省空間，在最後生成的 image 中，不可以留下任何 sl 的原始碼，不可以額外安裝多餘的 package，也不能安裝名稱結尾為 `dev` 的 package。
- 完成後，請截圖小火車，並在作業中附上 Dockerfile 內容。Dockerfile 請取名為 {你的學號}.Dockerfile。
- Hint: 或許可以在產生 Docker image 之前，先用一個 intermediate image 來 compile sl？

3. **(3%)** 使用 docker-compose 部署一個簡單的網頁伺服器
   (a) Git clone https://github.com/aoaaceai/nasa-hw3
   (b) 使用 docker compose 把 service 在背景跑起來，完成後請截圖 `docker compose ps` 的結果。
   (c) 現在你應該可以透過瀏覽器看見剛剛部屬的服務。請在訪問該網站幾次後，在一個 terminal 視窗中同時顯示兩個 container 的 logs，並截圖。

Kubernetes (20%)

Kubernetes Architecture (5%)

(5%) Kubernetes(或稱 K8s) 是一個用於自動部署、管理及擴展容器化應用程式和服務的叢集 (cluster)。請畫一張 Kubernetes 基礎架構圖、說明叢集中每一種 node 所扮演的角色及其基本元件的作用、以及使用 Kubernetes 的好處（e.g., service availability）。

Build Application(5%)

請依照下列步驟建立及運行你的服務。你可以像 Lab 一樣在本機上或配置一臺 ubuntu 22.04 的 VM 並安裝你的 K8s 環境，作業使用的資源不少，建議使用 Ubuntu Server。你也可以從/tmp2/nasa-hw3/ubuntu.iso 或至官網下載並手動安裝 iso 檔。

1. **(0%)** Prerequisites:
   - VM 要求:
     - vcpus: 2 or 4
     - memory: 4GB or 8GB
     - disk: 20G
     - network: NAT or Bridged(recommended) 都可以
   - 安裝 minikube & kubectl [driver: docker/kvm]
2. **(5%)** 現在你要撰寫 YAML configuration file 部署 postgres:14-alpine 的 deployment 及 service. 最後利用 kubectl describe 指令列出 deployment 以及 service 成功運行該服務的截圖。
   - name 設爲 psql-{你的學號 (大小寫通用)}-{depl|svc|pod(對應建立的種類)}
     e.g., psql-b11902999-depl, psql-b11902999-svc
   - deployment replicas 設爲 1
   - port 均設爲 5432
   - Service 要接上你所部署的 deployment

Tips: 建立 postgresql 服務, 你可能需要一些特定參數。通常爲了使得我們的環境更爲簡潔，你有沒有什麼方法將它們寫在同一個 YAML file？

ConfigMap & Secret (2%)

1. **(1%)** 在 K8s, ConfigMap 及 Secret 是什麼?
2. **(1%)** 現在你需要撰寫 Secret YAML file 對你 postgresql 的環境變數作加密 (你可以有其他 optional 的環境變數，但 mandatory 變數不可以列在你的 deployment YAML file 當中), 最後提供 kubectl describe deployment ${YOUR_DEPL_NAME} 的截圖。

CLI bad, I want GUI (5%)

1. **(1%)** 請列出登上 container 的指令及截圖 (不需要登上 postgresql)
2. **(3%)** 你現在已經會建立及部署你的服務了, 並且你發現透過登上 container 去操作 postgresql 非常的不方便，爲此我們需要操作 postgresql 的平臺，請像之前建立 postgresql 一樣建立 YAML configuration file 部署以下服務, 最後利用 kubectl describe 指令列出 deployment 以及 service 成功運行該服務的截圖：
   - container image : dpage/pgadmin4
   - name 設爲 pgadmin-{你的學號 (大小寫通用)}-{depl|svc|pod(對應建立的種類)}
     e.g., psql-b11902999-depl, psql-b11902999-svc
   - deployment replicas 設爲 2
   - port 均爲 80
   - Service 要接上你所部署的 deployment
   - 環境變數使用 key-value pair 即可
     - email: {你的學號 (大小寫通用)}@nasa.com, e.g., b11902999@nasa.com
3. **(0%)** 使用在 Lab 使用的 port forwarding 將其 forward 到你的 host 上，如果你使用的是 Ubuntu Server 及 NAT network, 你需要 double port forwarding。請使用以下指令從本機登陸你的 VM 並依照 Lab 所使用 port forwarding：
   - `ssh -L <host_port>:localhost:<vm_port> YOUR_VM`
4. **(1%)** 接下來你就能從你的 Web Browser 看到 pgAdmin 的 Web UI 了，利用你部署的 email 及密碼登陸，打開 Dashboard 並提供截圖（必須包含右上角 email - e.g., b11902999@nasa.com）。

Persistent Volumes (3%)

(3%) 我們知道當某個 pod 不小心下線，比如當你對你的 deployment 修改某項參數，重新上線之後，你操作過的資料都會消失，所以你現在需要爲 postgresql 建立 PersistentVolume, 請依照以下規則撰寫你的 PV 及修改你的 Deployment YAML file, 最後請提供 kubectl describe 你的 pv 及 deployment 的截圖。

- 將 postgresql 的資料夾/var/lib/postgresql/data 掛載到 node 中/mydata 底下
- PV 大小爲 5G
- 權限爲同一個 Node 可以 Read/Write

Tips: 如果你有興趣可以利用之前所建立的 Web UI 開啓新的 server 以及建立新的 database, 當然如果你會用 CLI 操作 database 也可以。你會發現有了 PV 之後，儘管你 restart deployment, 你的資料也不會消失了。