

Open in app ↗

Sign up

Sign In

Medium

Search

哪裡能找到便宜的SSL Apache 為例



Alex Ian · Follow

8 min read · Oct 12, 2018



Share



透過 Google 登入 Medium



廖昶哲

jash.liao@gmail.com

以昶哲的身分繼續使用

為了建立帳戶，Google 會將您的姓名、電子郵件地址和個人資料相片提供給「Medium」。詳情請參閱「Medium」的《[隱私權政策](#)》和《[服務條款](#)》。

有鑒於最近各大資訊公司對於網站安全的要求有所提升，如Chrome對於沒有SSL的網站會標示為不安全，而沒有SSL的網站在Google的搜尋排名也會有所下降，並且最近Facebook也加強了其應用程式的審查，所有要使用Facebook登入功能的網站，都必須使用https的傳輸協定，否則便無法使用Facebook的各項功能（說實在，我都不知道要怎麼在localhost的port進行開發或測試了），所以現在要上線網站，SSL可說是必備的項目了。

但在線上找到的網域或伺服器供應商所推出的SSL捆綁方案，其售價都非常可觀，雖然其成本可能在報價時能由案主負擔，但如果是一些自行開發的Side Project，購買SSL則會成為一大負擔。

保護 1 個網站

最低只要

NT\$1,602/年

特價促銷 - 現省 29%

續約價格每年 NT\$2,288⁴

加入購物車

保護 1 個網站的安全

強大的 SHA2 和 2048 位元加密

可以使用 DV、OV 與 EV SSL 憑證 ?

EV SSL 會讓瀏覽器網址列變綠色 ?

提升網站的 Google 搜尋排名

保護多個網站

UCC/SAN SSL ?

最低只要

NT\$3,623/年

特價促銷 - 現省 29%

續約價格每年 NT\$5,176⁴

加入購物車

最多保護 5 個網站 ?

強大的 SHA2 和 2048 位元加密

可以使用 DV、OV 與 EV SSL 憑證 ?

EV SSL 會讓瀏覽器網址列變綠色 ?

提升網站的 Google 搜尋排名

保護所有子網域

萬用 SSL ?

最低只要

NT\$7,460/年

特價促銷 - 現省 30%

續約價格每年 NT\$10,657⁴

加入購物車

保護 1 個網站及其所有子網域的安全

強大的 SHA2 和 2048 位元加密

可以使用 DV 與 OV SSL 憑證 ?

提升網站的 Google 搜尋排名

G姓公司提供的SSL價格

而我在Google亂逛的時候，就這家非常便宜的SSL憑證供應商 —

<https://www.ssls.com/>。當中最底的價格只要不到200塊台幣/年，前提是你要有能夠海外付款的信用卡。當然，便宜的代價是，它只使用系統的方式進行檢查，因此它的安全性也會相對較低，domain限域也較大，只適合用於一些小的CASE或是安全需求較低的應用。

The screenshot shows the SSLs.com website with the headline "Buying SSL just got easier!". Below the headline, there are filters for "PERSONAL", "BUSINESS", "ECOMMERCE", "ONE DOMAIN", "MULTI-DOMAIN", and "SUBDOMAINS". A link "What is an SSL" and a "CHEAPEST" button are also visible. Three SSL certificate products are displayed:

Product	Price	Assurance
PositiveSSL (Comodo, 1 domain, www.site.com + site.com, Domain validation, Low assurance)	\$5.88 /YR (was \$8.95 /YR)	Low assurance
EssentialSSL (Comodo, 1 domain, www.site.com + site.com, Domain validation, Medium assurance)	\$14.88 /YR (was \$20.99 /YR)	Medium assurance
EV SSL (Comodo, 1 domain, www.site.com + site.com, EV (greenbar), Very high assurance)	\$78.99 /YR (was \$144.99 /YR)	Very high assurance

只要5.88美金，不到200塊新台幣，不過一分錢一分貨，可靠程度也較低

...

如何設置憑證？

假設你已經設置好Linux、安裝好Apache，並使用 httpd.conf 設置好domain，接下來可開始伺服器連線。

1. 設置伺服器端openSSL

預設安裝的Apache並沒有SSL的支援，需要安裝額外的套件。

1.1 確保所有軟體套件皆為最新版本

```
$ sudo yum update -y
```

1.2 安裝 mod_ssl 套件來提供SSL的支援

```
sudo yum install -y mod_ssl
```

1.3 重啟Apache

```
sudo systemctl restart httpd
```

接下來，你可以試試看在瀏覽器手動為你的Domain使用https://連線，會顯示「你的連線不是私人連線」，那是因為你還沒有合法的證書，當你點擊「進階」->「繼續前往」，應該可以看到Apache的預設頁面



你的連線不是私人連線

攻擊者可能會試圖從 [redacted] 竊取你的資訊 (例如密碼、郵件或信用卡資料)。瞭解詳情

NET::ERR_CERT_COMMON_NAME_INVALID

進階

返回安全性瀏覽

其實SSL的連線已經啟動，只是證書並不可信

2. 建立金鑰和簽名檔

建立SSL可信任的憑證，需要生成一組金鑰和簽名來對傳輸的資料進行

2.1 前往金鑰目錄

```
$ cd /etc/pki/tls/private/
```

2.2 產生新的私有金鑰 (custom.key 為金鑰名稱)

```
$ sudo openssl genrsa -out custom.key 2048
```

2.3 為金鑰設置高階權限

```
$ sudo chown root.root custom.key  
$ sudo chmod 600 custom.key  
$ ls -al custom.key
```

2.4 使用金鑰生成簽名檔

```
$ sudo openssl req -new -key custom.key -out csr.pem
```

生成簽名檔時會需要填寫以下資訊 (以下是範例答案) :

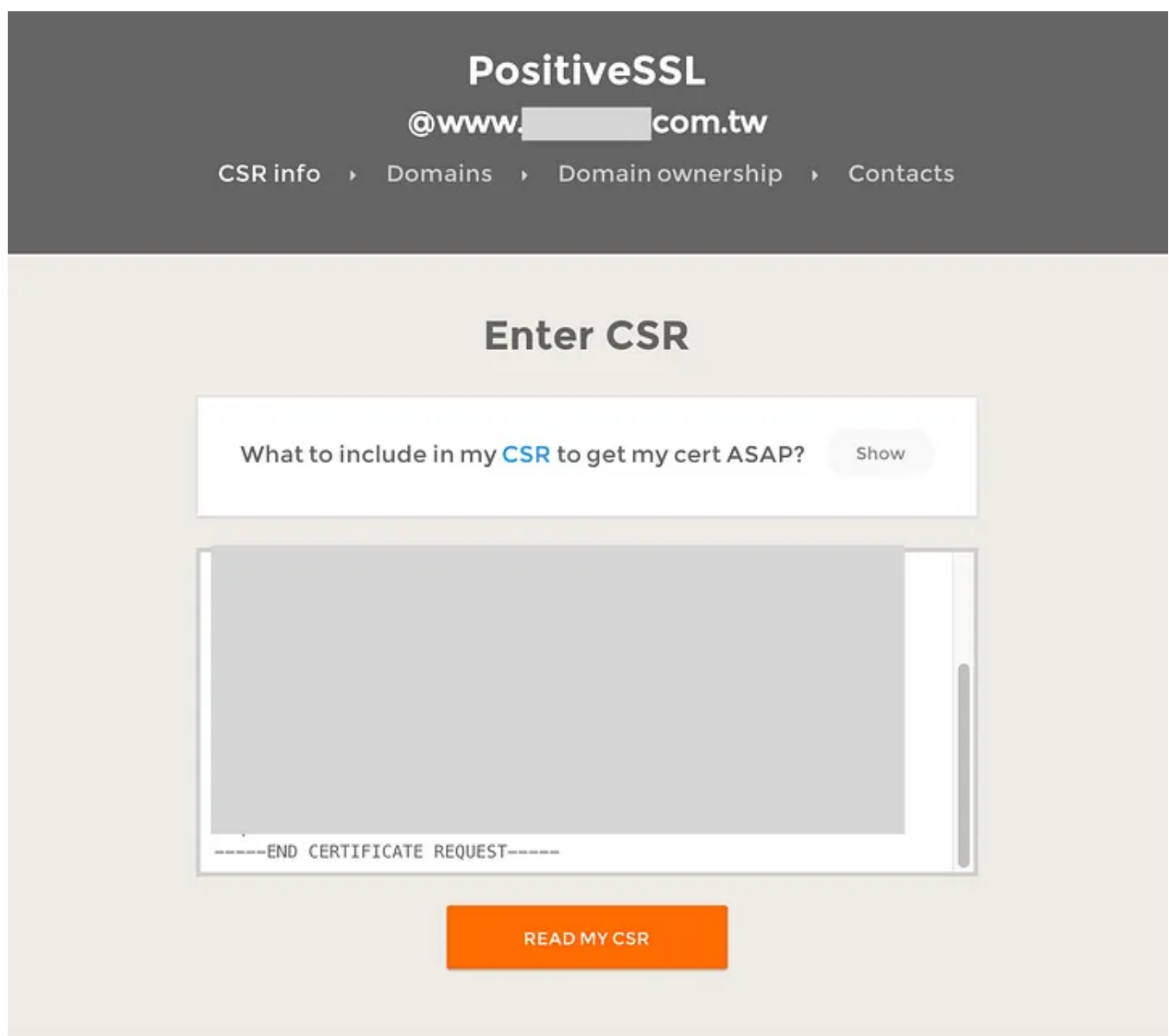
- Country Name (國家/地區名稱) : TW (兩字的地區簡寫)
- State or Province Name (州或省名稱) : Taipei
- Locality Name (地區名稱) : Taipei
- Organization Name (組織名稱) : MyCompany
- Organizational Unit Name (組織單位名稱) : IT division
- Common Name (通用名稱) : www.yourdomain.com
- Email Address (管理員電子郵件地址) : service@yourdomain.com
- A challenge password (一組挑戰密碼) : 12345678
- An optional company name (公司名稱) : MyCompany

填寫完畢後，便會建立 `csr.pem` 簽名檔，使用 `$ sudo nano csr.pem` 打開檔案，樣子大概會像這樣

```
-----BEGIN CERTIFICATE REQUEST-----  
.....  
-----END CERTIFICATE REQUEST-----
```

3. 在 www.ssllabs.com 建立憑證

3.1 前往<https://www.ssllabs.com/>，假設你已經購買了一組 PositiveSSL 證書，會要求你加入SCR，便把 `csr.pem` 檔的內容全選複製到方框中

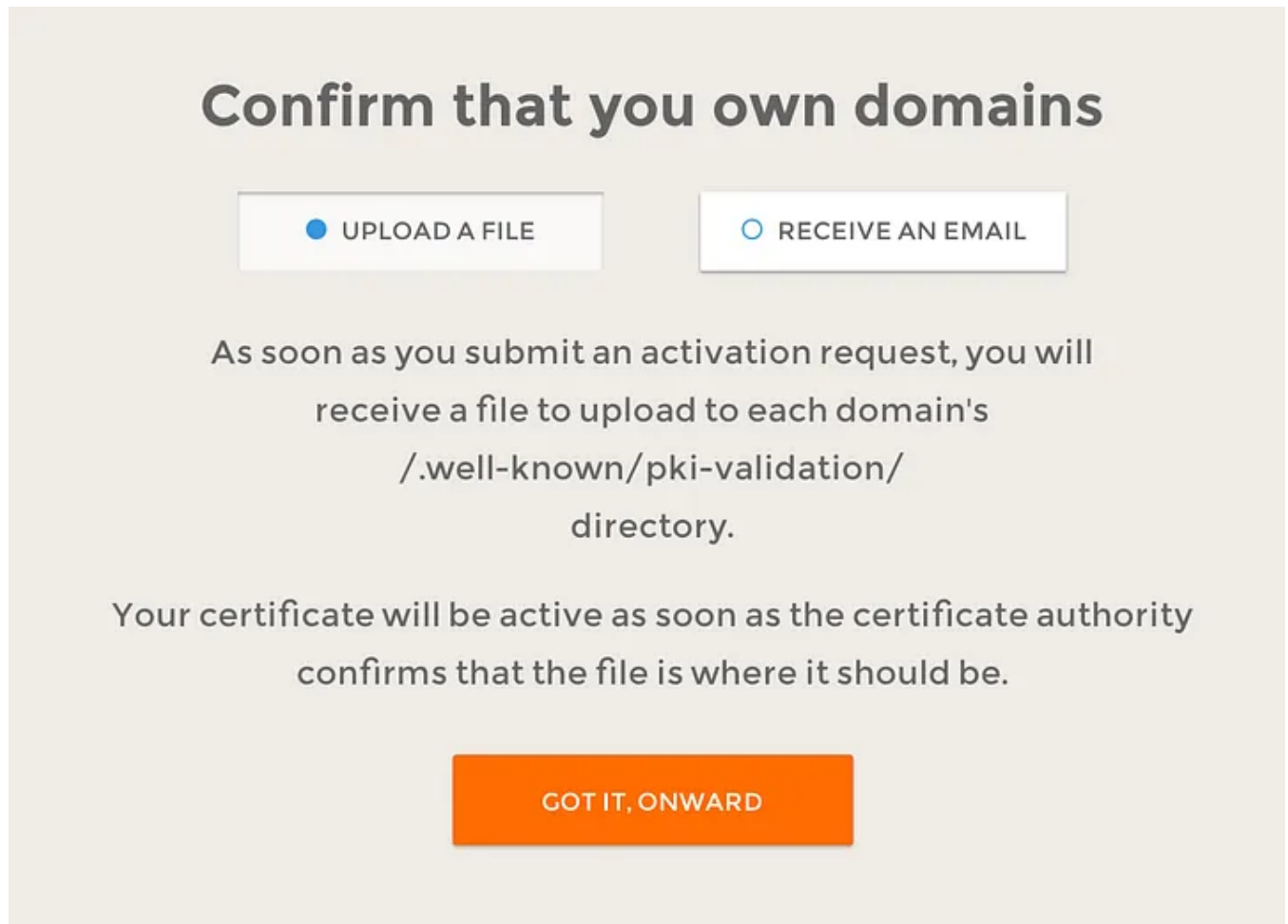


3.2 接下來它們會讀取你簽名檔中的內容，包含企案名稱、地區等，

3.3 確認SSL證書所覆蓋的domain是否正確，最後會詢問關於你的資訊（如地址、聯絡電話等）

3.4 最後會需要你選擇驗證Domain擁有權的方式，我們選擇Upload a file，按下「GOT IT, ONWARD」，會出現「SAVE ACTIVATION FILE」，下載下來的會是一個編號名稱的txt檔。

3.5 使用FTP打開根目錄，把下載的檔案放到網站 `/.well-known/pki-validation` 目錄中，該SSL供應商進行驗證，沒有則可自行建立資料夾。



* 注意事項：確保該檔案目錄（<https://www.mydomain.com/.well-known/pki-validation/XXXXXXXXX.txt>）能夠被讀取，才能驗證成功。

3.5.a 為目錄設置最低權限

```
$ sudo chmod 777 /var/www/html/.well-known/pki-validation
```

3.5.b 確保443port 指向網站根目錄

```
$ cd /etc/httpd/conf.d/ssl.conf
```

檢查 DocumentRoot 是否正確

DocumentRoot “/var/www/html”

3.6 稍候片刻，等待驗證成功後，檢視你擁有的證書頁面，會顯示Active，這時候點擊證書號碼進入內頁，點擊右上方的「Download」下載憑證。

Cert #	Name	Valid	Status	Expires	Domains
# [redacted]	PositiveSSL	1 yr	Active ▾	1 [redacted]	[redacted]

3.7 下載解壓縮後會得到三個檔案，我們只需要用到 *.ca-bundle 與 *.crt 檔，建議把檔案都放到 /etc/pki/tls/certs/ 目錄中（在command line中，可使用 `$ sudo nano` 新增檔案）

3.8 打開在 ssl.conf

```
$ sudo nano /etc/httpd/conf.d/ssl.conf
```

3.9 在 ssl.conf 中設置證書檔案路徑並儲存

```
SSLEngine on
SSLCertificateKeyFile /etc/pki/tls/private/xxxxx.key
SSLCertificateFile /etc/pki/tls/certs/xxxxx.crt
SSLCertificateChainFile /etc/pki/tls/certs/xxxxx.ca-bundle
```

3.10 最後重啟Apache

```
$ sudo service httpd restart
```

再次進入網站，發現憑證已經生效了



. . .

後記

如果你發現自己的Domain驗證許久還沒生效，可以使用 <https://www.sslls.com/> 內左方的CHAT進行一對一客服資詢，服務還蠻好的，馬上就能幫你啟動成功。

參考資料

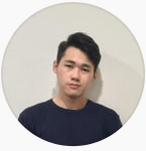
- https://docs.aws.amazon.com/zh_tw/AWSEC2/latest/UserGuide/SSL-on-an-instance.html
- <https://helpdesk.sslls.com/hc/en-us/articles/206957109-How-can-I-complete-the-domain-control-validation-DCV-for-my-SSL-certificate->

Ssl

Https

Aws Ec2

Tls



Follow



Written by Alex Ian

108 Followers

大膽假設，小心求證 Frontend Developer from Macau. Working in Taiwan. <https://alex-ian.me/>

More from Alex Ian



Alex Ian

Debounce & Throttle—那些前端開發應該要知道的小事(一)

降低瀏覽網站所消耗的效能就成為開發者的義務，而Debounce和Throttle概念便是降低互動事件頻繁觸發的解答。

4 min read · Jul 6, 2019



602



4



udes - OTHER

n array includes the given value,
like `indexOf`).

relative	Apply filters	Show all	?						
Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Blackberry Browser	Opera Mobile *	Chrome for Android	Firefox Android
4-46	3.1-8	10-33	3.2-8.4						
47-73	9-12	34-57	9-12.1		2.1-4.4.4	7	12-12.1		
74	12.1	58	12.2	all	67	10	46	74	68
75-77	TP								



Alex Ian

polyfill是什麼？

人在江湖，身不由己，在接案的過程中，總有一些你不想接、但也不得不接的案子，而且客戶的需求總是想要包山包海（卻拿不出摺摺）。而網站的前端開發者最常遇到的難題，絕對是瀏...

5 min read · May 26, 2019



83



debugger & breakpoint



Alex Ian

debugger 與 breakpoint— 那些前端開發應該要知道的小事(四)

距離這個主題的前一篇文章相隔了快一年 XD，除了工作和生活導致個人怠惰以外，同時也對主題發想感到腦塞，難得想到主題，就來充數一下。

5 min read · Sep 28, 2020



19



Console

```
"data-id: block-1"
```

```
"data-id: block-2"
```



Alex Ian

addEventListener的第三個參數—那些前端開發應該要知道的小事(二)

前言

5 min read · Jul 15, 2019



5



1



See all from Alex Ian

Recommended from Medium



 Malcolm Pereira


Mutual TLS with Ingress-Nginx Controller

Simple walk through to get up and running with M-TLS; Mutual TLS—client certificate validation with Ingress-Nginx controller in a local...

13 min read · May 30

 2 



 Vaishnav Manoj in DataX Journal

JSON is incredibly slow: Here's What's Faster!

Unlocking the Need for Speed: Optimizing JSON Performance for Lightning-Fast Apps and Finding Alternatives to it!

16 min read · Sep 28



6.3K



78



Lists



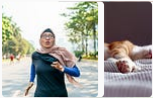
Staff Picks

495 stories · 412 saves



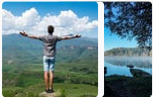
Stories to Help You Level-Up at Work

19 stories · 283 saves



Self-Improvement 101

20 stories · 822 saves



Productivity 101

20 stories · 758 saves



SONARQUBE- SCANNER

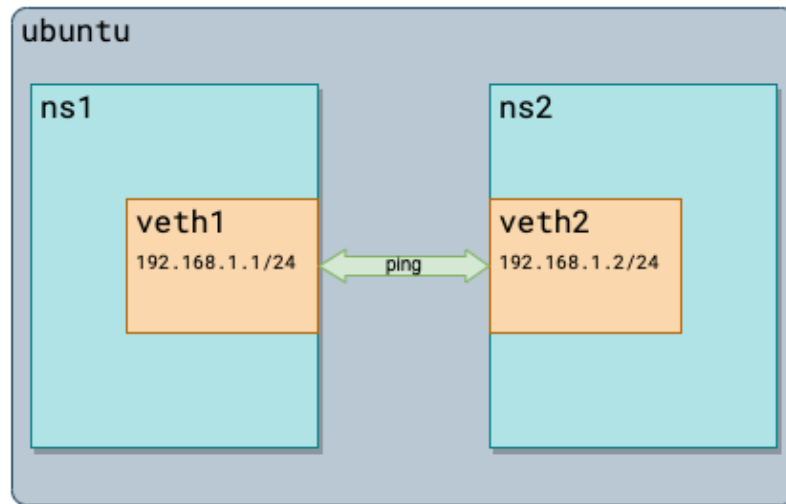


Ayoub Chamchi

SonarQube | SonarScanner :

Installation

2 min read · Jun 7



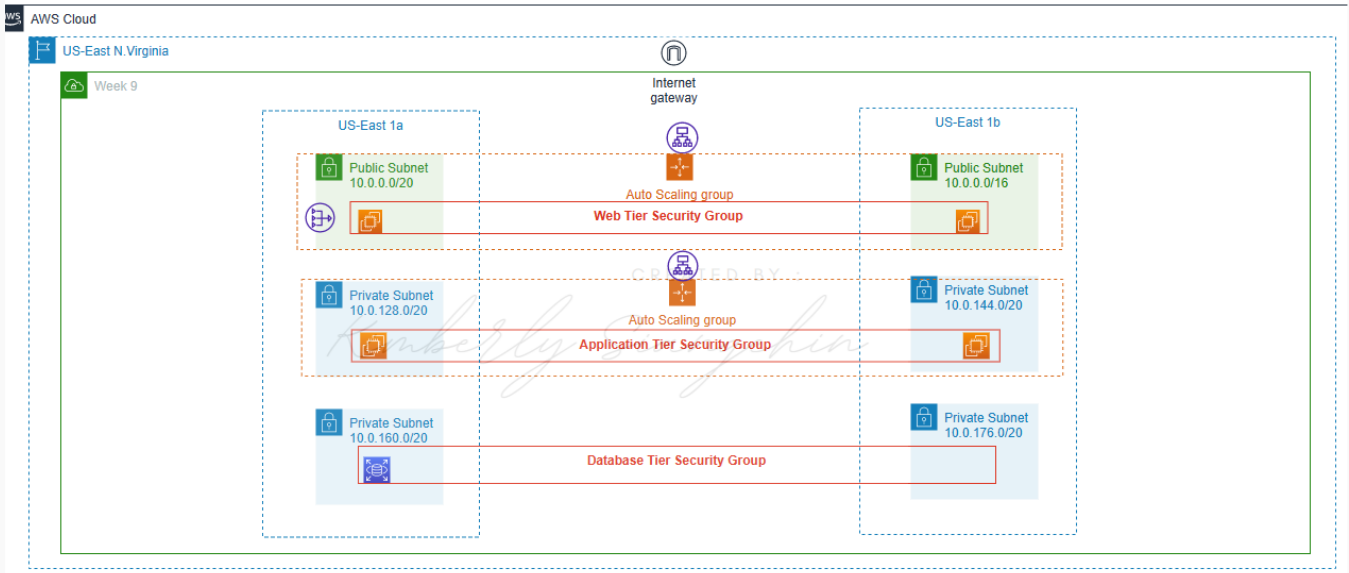
Amazingandyyy

Introduction to Network Namespaces and Virtual Ethernet (Veth) Devices

Network namespaces and virtual Ethernet (Veth) devices are powerful concepts in Linux that allow you to create isolated network...

6 min read · May 29





Ammar Suhail

AWS Three-Tier Architecture Hands-on Exercise

Scenario:

10 min read · Jul 11



sonarqube



DeshDeepakDhobi (DD)

How to install and configure SonarQube on AWS EC2 Ubuntu 22.04 and 20.04 (Full Setup)?

Humans do make mistakes and when it comes to mistakes in the codes it is too much to manage and handle and there comes SonarQube to rescue.

9 min read · May 28



See more recommendations