三種不同的伺服器端加密模式來保護 Amazon S3 中的靜態資料：SSE-S3、SSE-C 或 SSE-KMS。

SSE-S3 要求 Amazon S3 管理資料和加密金鑰。
SSE-C 要求您管理加密金鑰。
SSE-KMS 要求 AWS 管理資料金鑰，但由您管理 AWS KMS 中的 AWS KMS keys。

使用 Amazon S3 用户端加密，Amazon S3 加密和解密會在叢集上的 EMRFS 客户端進行。
數據元在上傳到 Amazon S3 之前會對數據元進行加密，並在下載後對其進行解密。
您指定的提供程序提供客户端使用的加密密鑰。客户端可以使用AWS KMS(CSE-KMS) 或提供客户端主金鑰 (CSE-C) 的自訂 Java 類。

S3 存儲類型

	S3 Standard	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Glacier Deep Archive
Durability	X X X X X	X X X X X	X X X X X	X X X X X	X X X X X
How many AZ	O O O O O	O O O O	O	O O O O O	O O O O O
Availability	Very High	High	Low	Very High	Very High
Retrive Time	Super Quick	Super Quick	Super Quick	Slow...	Super Slow...
Retrive Frequency	HIGH ----------> LOW				

S3 > bucket > 建立 > 名稱 (deeplearnaws-S3-test) 、版本控制→啟用、標籤、默認加密→禁用 > 創建

click 剛建的 bucket > 上傳 > 添加檔案 (其他選項：標準、服務器加密→否、ACL→擁有者) >

上傳 > click 剛上傳的文件 > 操作 (目前僅能下載、不能設公開 or 訪問 URL)、列出版本

靜態網站：S3 > bucket > 建立 > 名稱

S3 > bucket > 建立 > 名稱 (blog.deeplearnaws.ml) 、取消阻止公開訪問、版本控制→禁用、標籤 (blog.deeplearnaws.ml)、默認加密→禁用 >

創建 > 上傳 > html、訪問控制列表ACL (勾公有訪問權限) > 上傳 >

屬性 > 靜態網站托管 編輯 > 啟用 > 保存 >

Route 53 > 托管區域 > click 域名 (deeplearnaws.ml) > 創建記錄 > 名稱 (blog.deeplearnaws.ml)、別名 (s3網站終端節點) > 創建

區間複製

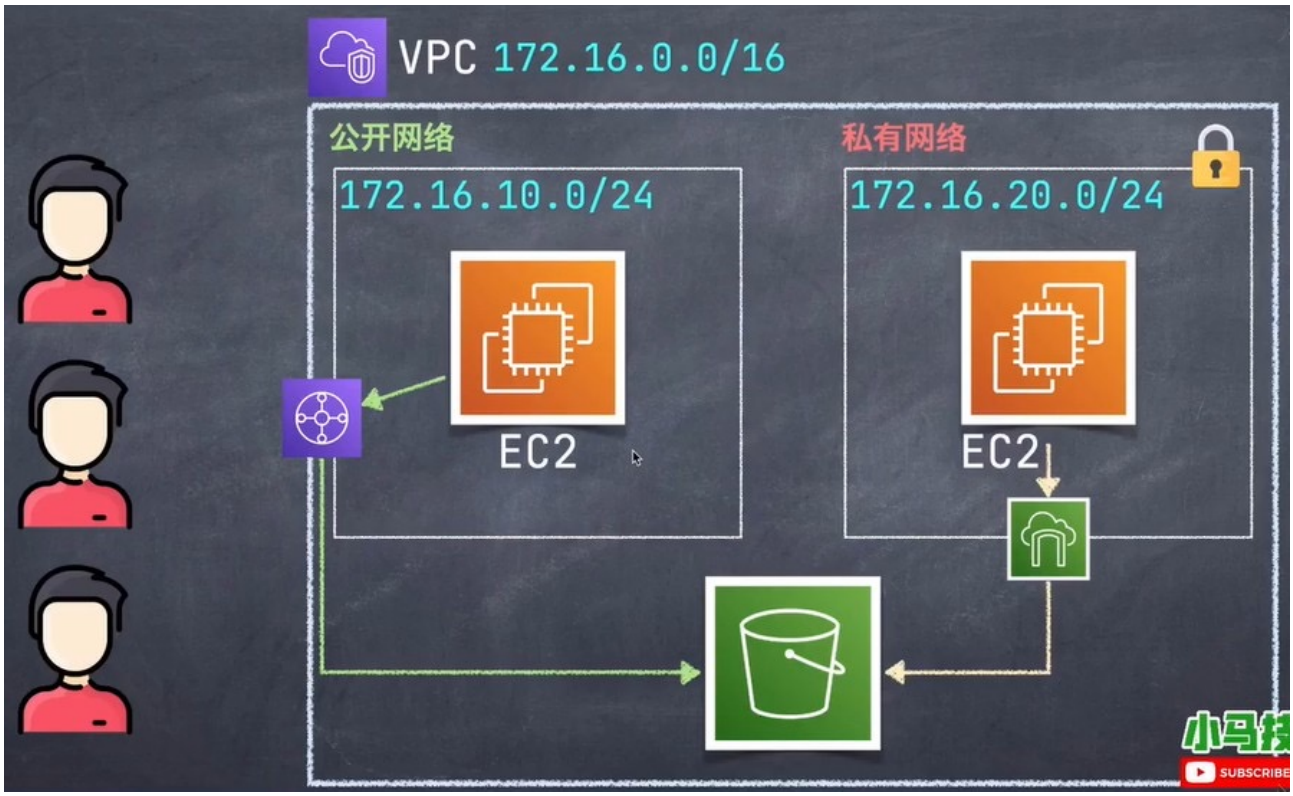
S3 > bucket > 建立 > 名稱 (woyaofuzhi) 、區域、版本控制→啟用、默認加密→禁用 > 創建

S3 > bucket > 建立 > 名稱 (woyaofuzhi backup) 、區域、版本控制→啟用、默認加密→禁用 > 創建

click bucket (woyaofuzhi) > 管理：複製規則→創建 > 名稱、選則規則範圍 (所有)、在帳戶中選 (browse→woyaofuzhibackup) >

IAM→創建、目標存儲類 (標準)、複製時間控制 (RTC) > 保存 (→指標)

S3 gateway終端節點 私有網路訪問S3



命令 aws s3 ls —region ap-northeast-1　列出區域存儲桶一覽表

建 EC2 (名:public-ec2)　以及 建可訪問 S3的角色 KomaRoleS3FullAccess

ssh進 EC2 > 打(上述命令)→沒辦法用 > 操作→安全→修改 IAM 角色 > 選 KomaRoleS3FullAccess > 保存 >

ssh進 EC2 > 打(上述命令)

建 EC2 (名:private-ec2)→子網:私網、自動分配IP:禁用

click　private-ec2　> 操作→安全→修改 IAM 角色 > 選 KomaRoleS3FullAccess > 保存 >

ssh進 EC2 > 打(上述命令)→沒辦法用,因為要設 Gateway >

VPC > 終端節點 > 建立 > AWS 服務(搜尋 S3→選擇 Gateway)、VPC→選目前 私有網路 由表 > 創建 >

ssh進 EC2 > 打(上述命令)