1. Multiple AWS accounts interconnect in a hub-and -spoke style using the AWS Transit Gateway. How to reduce both the administrative overhead and the costs while providing shared access to services required by workloads in each of the VPCs?
   1. Sol: Build a shared services Amazon Virtual Private Cloud (Amazon VPC)
   2. Transit VPC: 需額外管理EC2 instance

Transit VPC uses customer-managed Amazon EC2 VPN instances in a dedicated transit VPC with an Internet gateway.

* 1. Fully meshed VPC Peering connection:所有VPC點對點，難管理
  2. VPCs connected with AWS Direct Connect: 太花時間

1. 儲存資料庫密碼，每90天自動rotation.

You would like to store a database password in a secure place, and enable automatic rotation of that password every 90 days.

* 1. Sol: AWS Secrets Manager :
     + 自行設定rotation period
     + 與Amazon RDS (MySQL, PostgreSQL, Aurora)整合
  2. [易混淆]AWS Key Management Service (AWS KMS)：KMS is an encryption service, it's not a secrets store.
  3. Systems Manager Parameter Store：可用來儲存passwords, database strings, Amazon EC2 instance IDs, AMI ID等，無法自動rotate.

1. Configure Security Group and network access control list (network ACL) of the Amazon EC2 instance.
   1. Security Groups are stateful: 只須設定單向
   2. Network access control list (network ACL) are stateless：雙向(inbound and outbound)都須設定。
2. Sharing sensitive data stored in the RDS database to external AWS accounts with a copy of database (usually for audit).
   1. Sol: Create and share encrypted snapshot and allow access to AWS KMS key.
3. Steps to be taken to encrypt an existing Amazon RDS database:
   1. Sol: Take a snapshot > Encrypt the snapshot > Restore DB with the snapshot.

[RDS 只有在建立時可以啟用加密(enable encryption)]

* 1. 建立並加密Read Replica(RR)，將RR轉成standalone DB，停用原本的DB；master未加密，RR不能加密。
  2. Enable Multi-AZ for the database: Multi-AZ 用在HA。

1. 在EC2上執行的應用程式要存取S3和DynamoDB，如何設置權限
   1. Sol: Attach the appropriate IAM role to the Amazon EC2 instance profile
   2. 說明：可以將存取資訊(AWS credentials)放在EC2或其他地方供應用程式使用，但這樣會增加管理的負擔及洩漏的風險；

使用IAM role會產生暫時的credentials供應用程式使用，開發者不須管理。

1. A solution can offer user-level and account-level access permissions for the data stored in Amazon S3 buckets that are accessed cross-account.
   1. Sol: S3 Bucket Policies: 支援user-level and account-level存取限制，也能設定cross account存取。
   2. IAM role:只能控制單一 AWS account底下的存取。
   3. Access Control Lists (ACLs): 提供其他的AWS account存取
   4. Security Groups: a virtual firewall for Amazon EC2 instances

存取控制方法比較