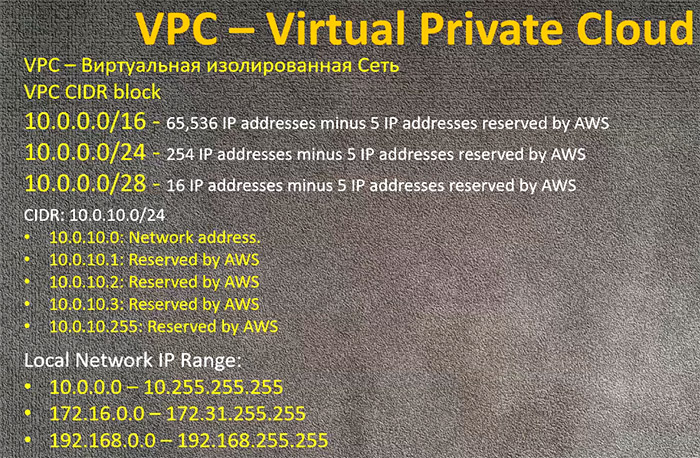
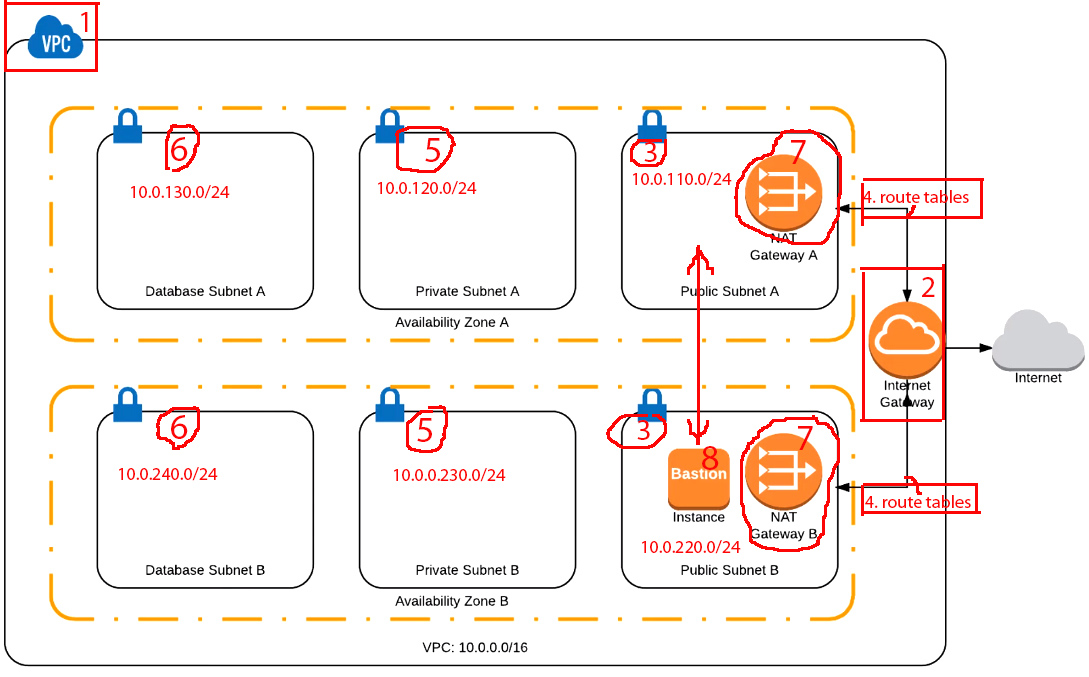
**VPC – Virtual Private Cloud - Виртуальная изолированная сеть**

|  |  |
| --- | --- |
| VPC CIDR blocks | Подсеть с разными cidr блоками |
| Public Subnet | Все серверы имеют PublicIP и прямой доступ в инет |
| Private Subnet | Все серверы НЕ имеют PublicIP и имеют доступ в инет через NAT |
| Database Subnet | Все серверы НЕ имеют PublicIP и НЕ имют доступ в инет |
| Route Table | Таблицы маршрутизации |
| Internet Gateway | Интернет шлюз |
| NAT Gateway | Network Address Translation, эластичный в отличи от NAT instance |
| NAT instance | Сервер позволяющий выход в инет |
| Security Group | Правила файервола (открытые/закрытые порты) можно разрешить IP адреса |
| Network Access Control List | Открывает еще IN OUT порты (входящие/исходящие соединения) можно разрешить и запретить IP адреса |
| Bastion Host | Хост в Public подсети с которого можно подключится к Private и Database адресам |
| VPC Flow Logs | Логи трафика, можно вкл на всю сеть или сетевую карту |
| VPN Gateway | VPN шлюз, для объединения сетей |
| VPC Peering | Объединение VPC сетей |



Создание такой сети:



|  |  |
| --- | --- |
| 1. **Создание VPC – Create VPC** | 1. **Создание Internet Gateway**   VPC-Internet Gateway – Create Internet Gateway |

|  |  |
| --- | --- |
| 1. **Создание Public Subnet A и B** | **3.Авто назначение Public адресов, сеть становится Public**    Все инстанс в этой подсети получать Public адрес |

|  |  |
| --- | --- |
| 1. **Создание Route Tables** | 1. **Создание Private Subnet**   **А: Так же как и Public**  **B: Создаем Route Table пустое (после создания NAT Gateway добавит правило)** |

|  |  |
| --- | --- |
| **Добавить Private подсети в новый Route Table** | 1. **Создаем DataBase Subnet**   **А: Так же как и Public**  **B: Создаем Route Table пустое (по умолчанию все пакеты в сети локальные, ничего не менять)**  **С: Добавить ассоциации к DataBase subnet** |

|  |  |
| --- | --- |
| 1. **Создать NAT Gateway для каждой Subnet**     **Добавить еще одну RouteTable чтобы разнести**  **Private A и B на разные NAT Gateway**  **В RouteTable 2 таблицы – для PublicSubnet A и B** | **Отредактировать для каждой RouteTable добавить маршрут в NAT Gateway**  **RouteA идёт в Gateway A**  **RouteB идёт в Gateway B** |

1. **Создание BastionHost**

Создать Security Group для нашей VPC в ней разрешить SSH отовсюду

Создаем LaunchConfiguration и AutoScaling Group с минимум и максимум одним сервером

|  |  |
| --- | --- |
| Выбрать VPC и Public Subnets    Остальное по умолчанию | Для проверки создаем инстанс с сетевыми настройками:  Наша сеть и Private Subnet    Security group с доступом по SSH  И второй в DataBase subnet и доступ по SSH |

**VPC Flow Logs**

Лог файлы сетевых пакетов на уровнях:

1 VPC

2 Subnet

3 Network Interface

Прежде создать IAM Role и указать записывать события в CloudWatch logs

|  |  |
| --- | --- |
| **В IAM – Create Policy**  в закладке JSON вставить код из ссылки  <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html> | **В IAM – Create Role** |

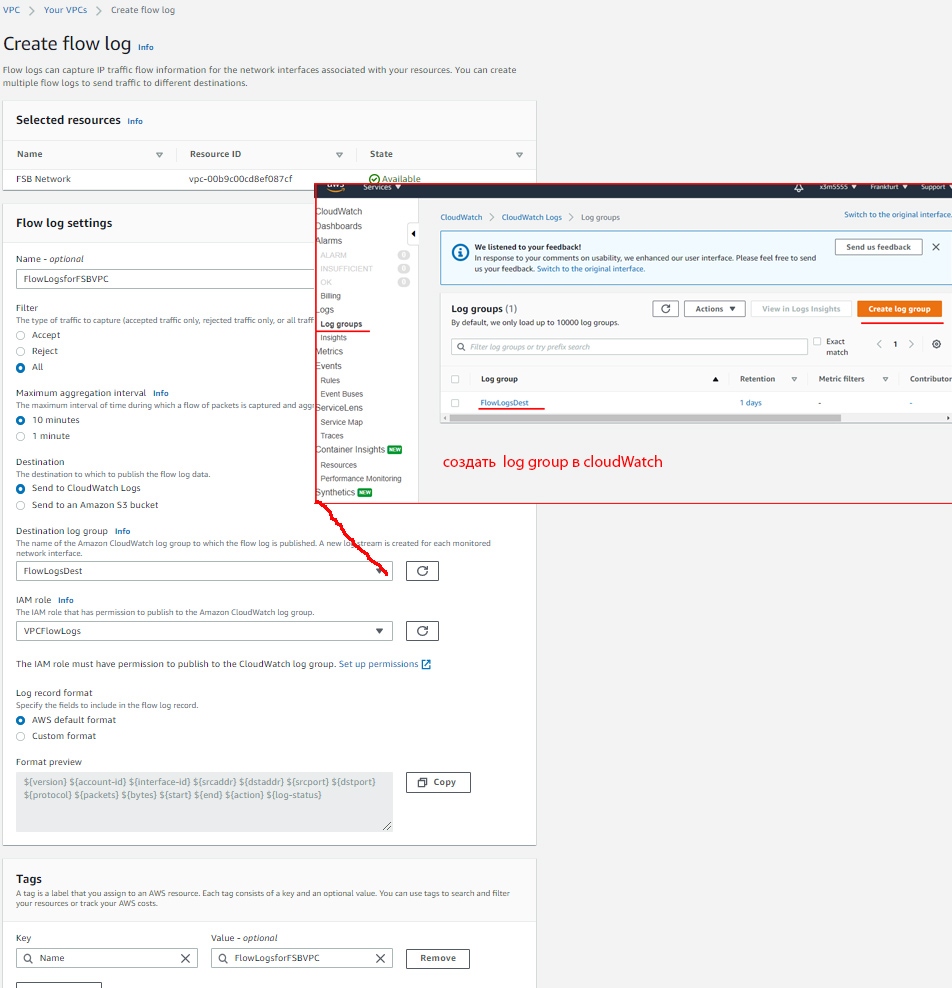
Затем выбрать созданную роль, закладка Trust relationships – Edit trust relationships:

Вставить код из ссылке выше



В настройках VPC закладка Flow logs – Create Flow logs

Destination log groups создается в CloudWatch

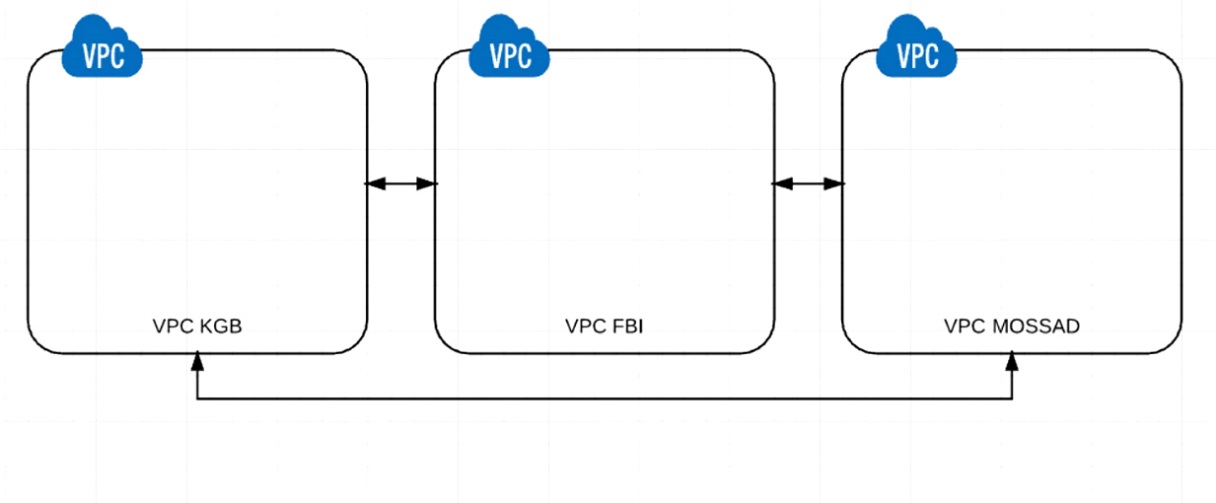


**VPC Peering**

https://www.youtube.com/watch?v=dlIvxxydShU&list=PLg5SS\_4L6LYsxrZ\_4xE\_U95AtGsIB96k9&index=30



Между каждыми сетями надо делать пиринг, чтобы видели друг друга



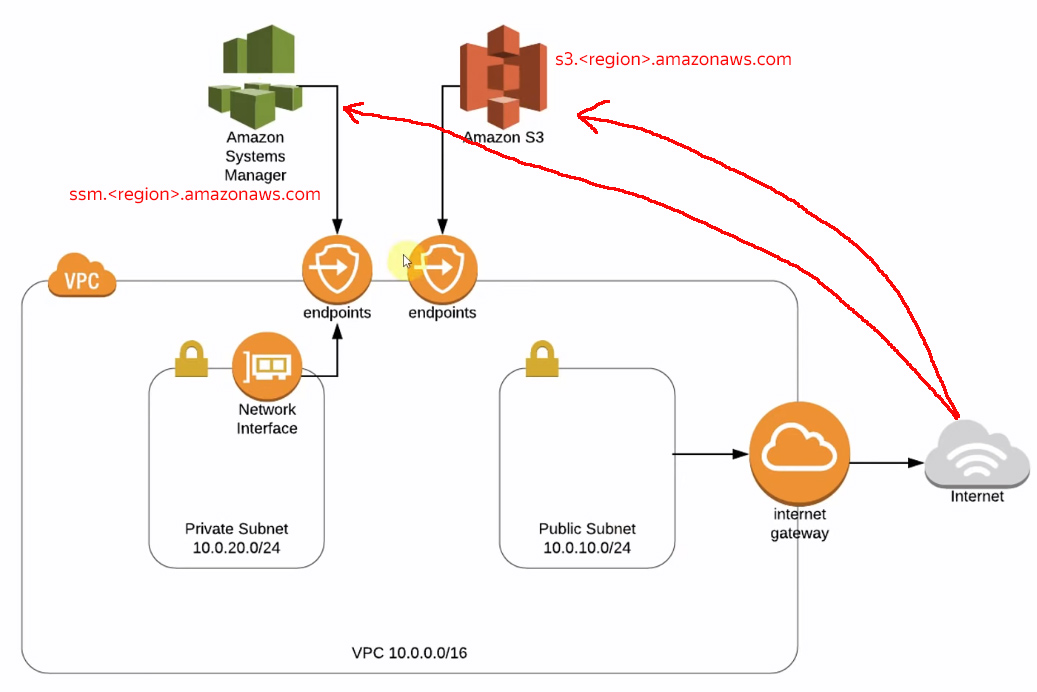
Создать пиринг в Peering Connections > Create Peering Connection указать две VPC, потом сделать раутинг:

Указать направление в адресное пространство сети на vpc perring

Для двух сетей объедининных пирингом должны быть разные CIDR блоки адресов

**VPC Endpoint - Внутренний доступ к сервисам AWS**

Доступ к ресурсам амазона идет через интернет по внешним адресам, если подсеть в VPC не имеет доступ к интернету, то не имеет доступа и к сервисам амазона, для доступа к службам создается VPC-endpoint, который создает канал связи со службами



После этого в подсетях появятся новые маршруты указывающие направление к службам через endpoint