amazon web services

Boas práticas de segregação de VPC

Boas práticas de segregação de VPC

Casos práticos

Junho 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Sumário

Introdução

Este documento tem como objetivo mostrar possíveis cenários de segregação de VPC's, forma de isolamento de redes na AWS.
Sabemos que existem muitas dúvidas em relação a qual a melhor arquitetura de VPC para determinada aplicação e não existe necessariamente uma solução, tudo dependerá da necessidade de cada projeto e a escolha deverá ser feita baseada em estratégias que muitas vezes podem ser definidas pela área de negocio em conjunto com a área de gestão em nuvem da sua empresa.
Com a leitura desse documento você entenderá um pouco mais sobre cada uma

das opções e estará apto a decidir qual o melhor cenário para determinada aplicação.

Iremos abordar 4 cenários que são nomeados como:

- VPC por ambiente;
- VPC dividida em contas AWS;
- VPC de gerência com VPC's por ambientes;
- VPC única com divisão de subnets por ambiente.

Conceitos

O intuito desse tópico é expor alguns conceitos, os quais serão utilizados no decorrer desse documento.

VPC

Forma de segregação/isolamento de rede na AWS. Permite você criar redes privadas e públicas, assim como segregação de subnets.

NACL

Camada de segurança opcional para a sua VPC que age como firewall para controle de trafego de entrada de saída. Esse tipo de controle é no nível de subnet, equivalente a firewall stateless.

Security Group

Atua como firewall virtual, o qual controla tráfego de entrada e saída no nível de instâncias, equivalente a um firewall stateful.

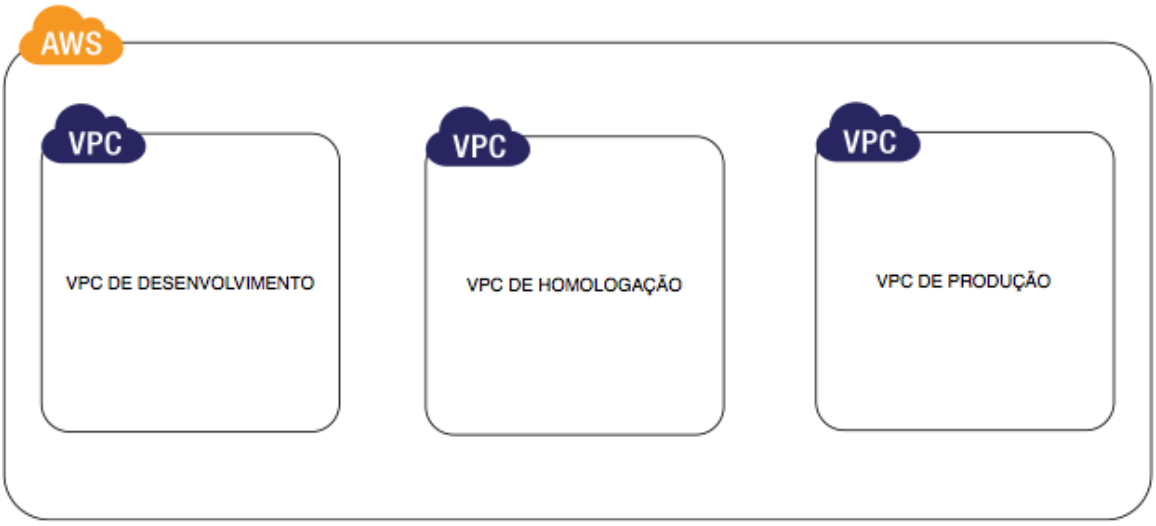
VPC Peering Connection

Serviço o qual, permite comunicação/conexão de rede entre VPCs.

Segregação de VPC

VPC por ambiente

O intuito dessa estratégia de segregação de rede, é termos para cada ambiente (ex: Produção, Desenvolvimento, Homologação, Testes) uma VPC.
Com isso, teremos isolamento entre as redes e o que trafegado dentro de cada uma delas, não é visível pelas outras VPCs.
Vale salientar também que quando necessário, realizar a segregação entre a redes públicas e privadas, dentro da VPC específica.
Nesse modelo, é possível também criar Zona de DNS Interna, no escopo de VPC e fazer os devidos apontamentos semelhantes em todos os ambientes. Por exemplo se existir apontamento para banco como, *"banco.acme.local"*, pode ter o mesmo apontamento em todas as VPCs e destinos diferentes de acordo com cada ambiente. Dessa forma, é mais fácil realizar os deploys, sem alteração nos endpoints.
Conforme pode ser verificado um exemplo da aplicabilidade desse tipo de rede abaixo:



Pontos de Segurança
- Os ambiente estão dentro de uma mesma conta (no caso de algum possível acesso não autorizado a conta da AWS, toda ela estará comprometida);

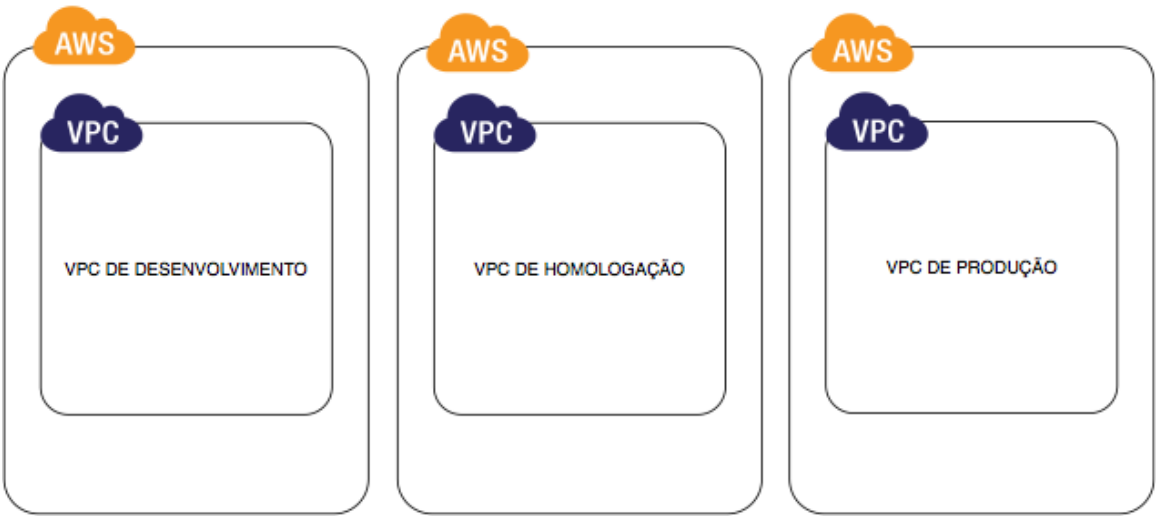
Pontos sobre Operabilidade
- Desacoplamento de ambientes;

- Fácil segregação;
- Manutenção de várias VPCs;

Aspectos Financeiros
- Controle financeiro/ambiente deverá ser feito utilizando TAGs e "Detailed Billing";

VPC divididas por contas AWS

Nesse tipo de abordagem, a ideia é termos para cada workload uma conta AWS em separado.
Dessa forma, os workloads ficarão completamente isolados e em contas separadas, sendo assim necessário a criação de todas as devidas VPCs e subnets para cada workload específico.



Pontos de Segurança
- Utilizando contas completamente separadas por ambiente, no caso de vulnerabilidade de acesso à conta, afetará somente uma específica;

Pontos sobre Operabilidade
- Gerenciamento de diversas contas/regras de segurança;
- Caso seja necessário comunicação entre as VPC, será necessário utilização de VPC Peering;.

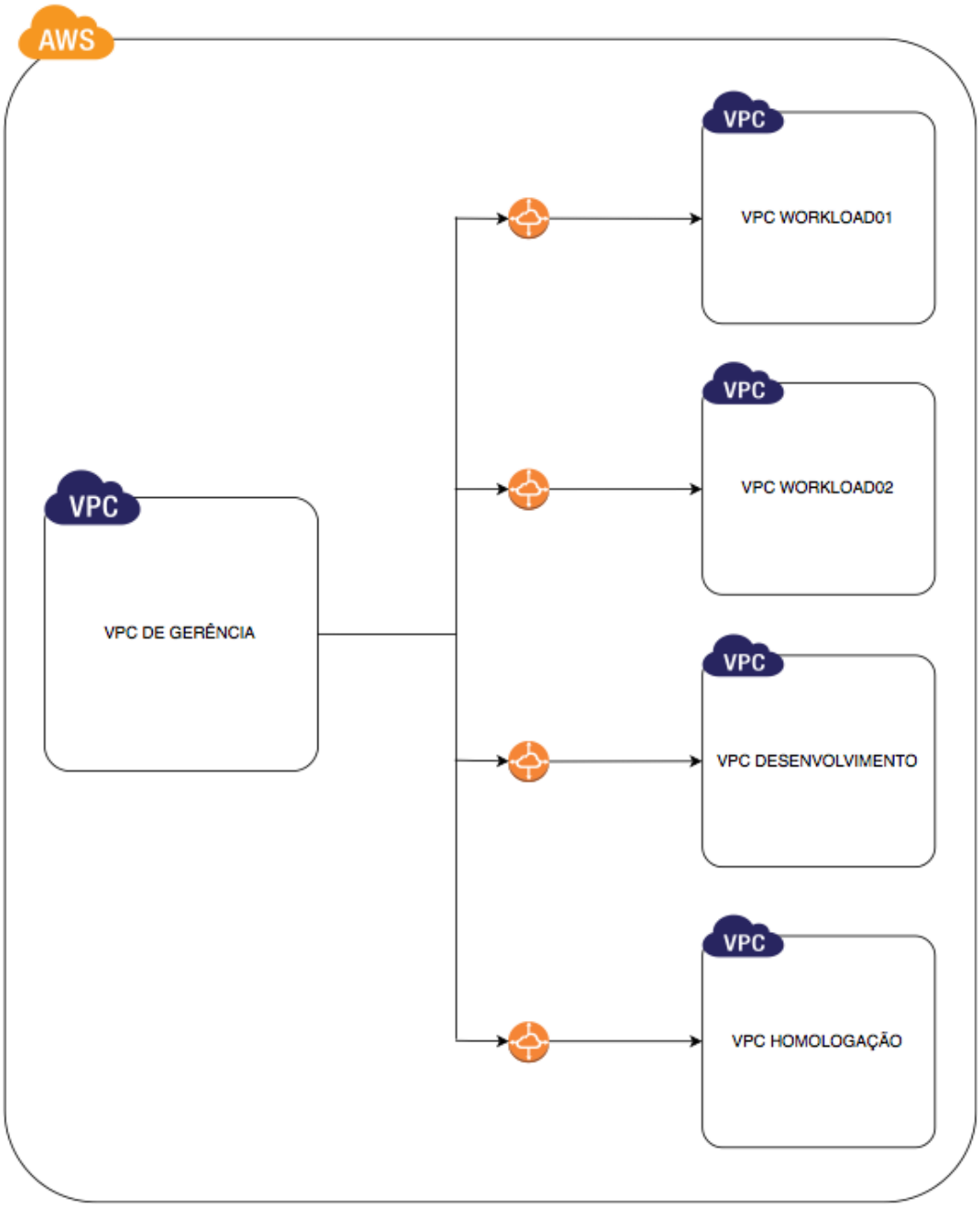
Aspectos Financeiros
- Correlação direta entre custo e ambiente separado;

VPC de gerência com VPC's por ambientes

Falando um pouco sobre essa arquitetura é ter uma VPC de gerenciamento, a qual centralizará serviços do tipo: repositórios de usuários, centralizador de logs, monitoramento. Dessa forma, não é necessário, ter esse tipo de serviço em cada uma das VPCs e sim utilizar uma central, a qual todas as VPCs terão visibilidade.

As VPCs de ambientes podem ou não ficar distribuídas em contas diferentes, a conexão entre elas é possível através de uma funcionalidade chamada, *VPC Peering Connection*. Vale lembrar que o serviço em questão, só irá conectar VPCs presentes na mesma região da AWS, para conexões em outras regiões a comunicação é possível por meio de internet e com garantia de segurança através de uma VPN.

Abaixo pode ser observado a aplicabilidade desse tipo de arquitetura de VPC's:



Pontos de Segurança

- Os ambiente estão dentro de uma mesma conta (no caso de algum possível acesso não autorizado a conta da AWS, toda ela estará comprometida);

Pontos sobre Operabilidade

- Complexidade de gerenciamento, com diversas regras de bloqueio e liberação,

assim como diversas tabelas de rotas;
- Manipulação de diversas contas (no caso de utilização de VPC/contas);
- Caso seja necessário comunicação entre as VPC, será necessário utilização de VPC Peering;

Aspectos Financeiros
- Controle financeiro/ambiente deverá ser feito utilizando TAGs e "Detailed Billing";
- Possíveis custos adicionais com VPC peering;

VPC única com divisão de subnets por ambiente

E para finalizar, sobre essa arquitetura de VPC, o objetivo é centralizar as aplicações em uma única VPC e distribuir as aplicações e seus ambientes de desenvolvimento, homologação e produção em subnets.

Na tabela de rotas da VPC, por padrão permite que todas as subnets criadas se comunicam entre si, com isso seu ambiente de desenvolvimento poderá se comunicar com seu ambiente produtivo, o bloqueio desses controles será feito através de ajustes no Security Group.

Abaixo pode ser verificado a aplicabilidade desse tipo de arquitetura de VPC's:

Pontos de Segurança

- Os ambiente estão dentro de uma mesma conta(no caso de alguma vulnerabilidade, toda a conta pode ser comprometida);

Pontos sobre Operabilidade

- Facilidade de gestão, pois todos os elementos estão dentro de uma mesma conta;
- Caso seja necessário comunicação entre as VPC, será necessário utilização de VPC Peering;

Aspectos Financeiros

- Overhead para fazer controle de custos por ambiente;

Contribuidores

Os contribuidores para a construção desse documento são:

- Cláudio Freire Júnior, Arquiteto de Soluções, Amazon Web Services
- Thiago Paulino, Arquiteto de Soluções, Amazon Web Services

Conclusão

A Amazon Web Services provê uma plataforma bastante flexível, a qual você pode disponibilizar suas aplicações, de acordo com as necessidades específicas de cada negócio.
No que tange a segregação de VPC especificamente, não existe uma forma correta ou errada e sim a que mais atende as necessidades.