Aula 3 – Lab Route53 Resolver

Habilite a resolução de nomes DNS do ambiente AWS para o datacenter usando o Rota 53 Resolvers.

Rota 53 Resolver facilita a nuvem híbrida para clientes corporativos, permitindo uma resolução perfeita de consulta dNS em toda a sua nuvem híbrida. Você pode criar pontos finais de DNS e regras de encaminhamento condicional para permitir a resolução de espaços de nome DNS entre seu data center no local e VPCs AWS.

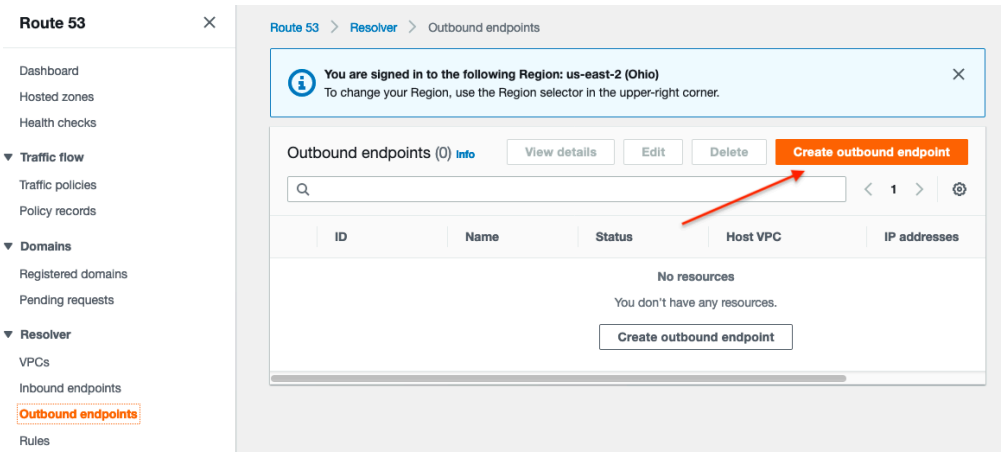
Lembre-se que nosso datacenter simulado no local tem um servidor DNS, fornecendo serviço de nome autoritário para o domínio exemplo.corp onde todos os hosts de aplicativos internos são registrados. Para fornecer uma solução completa de conectividade híbrida, queremos habilitar hosts em nossos VPCs AWS para resolver nomes de hosts no ambiente de datacenter. Isso pode ser alcançado usando resolvers da Rota 53 e regras de encaminhamento condicional para o domínio exemplo.corp, ao mesmo tempo em que permite que as instâncias AWS continuem a aproveitar o serviço de DNS amazon altamente disponível para todas as outras resoluções de nomes dentro do VPC e da internet.

Para este exercício, vamos nos concentrar em estabelecer a resolução de DNS do ambiente AWS para o datacenter simulado, mas é importante notar que o inverso também é possível. Rota 53 Resolvers suporta consultas DNS de entrada que são condicionalmente encaminhadas a partir de um servidor DNS no local. Você pode aprender mais sobre a resolução DNS de entrada na documentação AWS.

3.1 Configure um endpoint de saída do Route53 Resolver

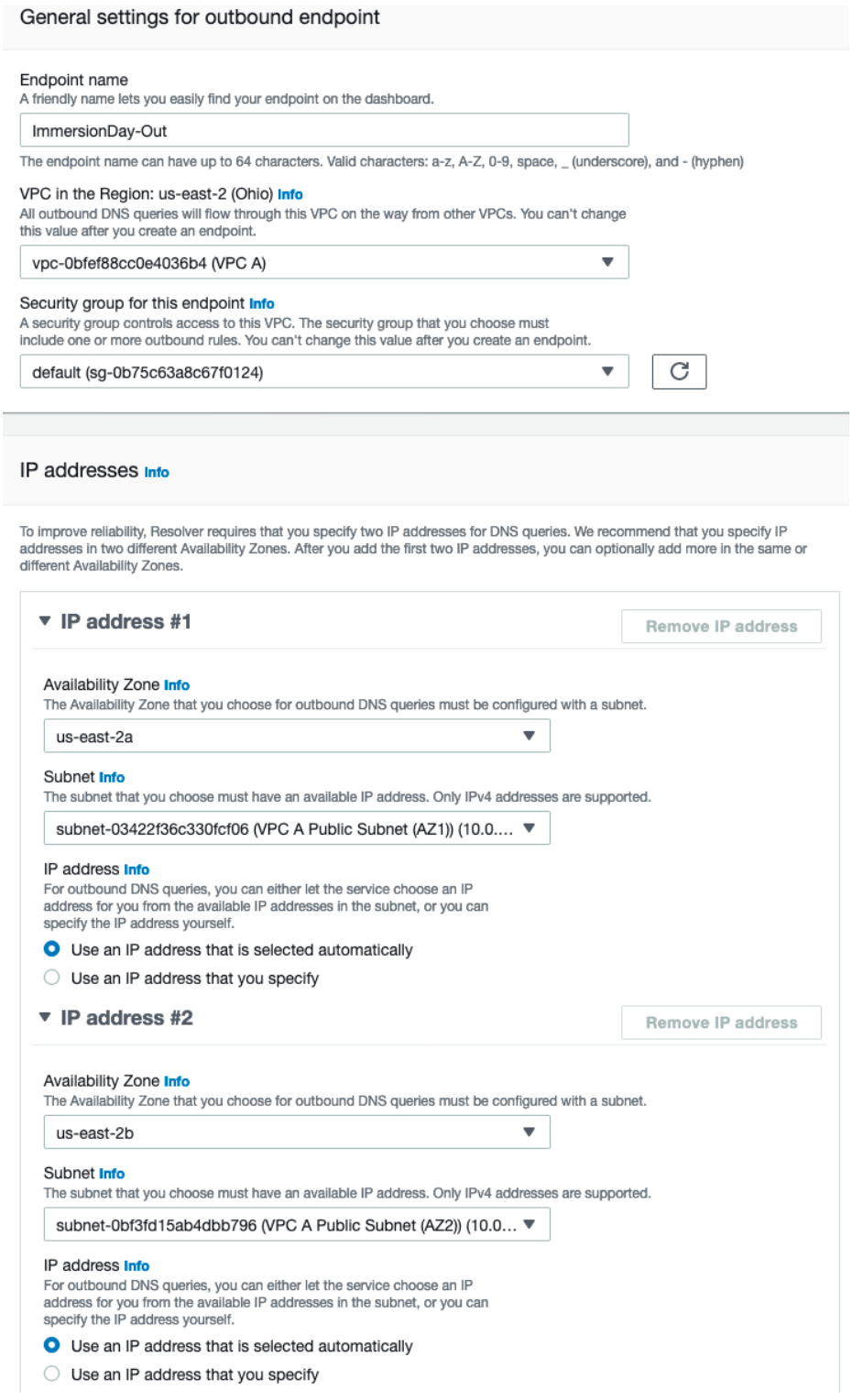
Rota 53 Resolver usa pontos finais para se comunicar com servidores DNS externos. Um ponto final é uma Interface de Rede Elástica (ENI) colocada dentro de um VPC que tem conectividade com o servidor DNS existente. Este pode ser um servidor DNS em execução em uma instância EC2 ou um servidor DNS em execução no local acessível via Direct Connect ou VPN. Como todos os três VPCs em nosso ambiente AWS têm conectividade com o datacenter simulado através do Transit Gateway, podemos usar qualquer um deles para o nosso ponto final. O ponto final criará interfaces em um mínimo de duas zonas de disponibilidade em seu VPC escolhido para alta disponibilidade.

- Navegar para serviços - Rota 53, em "Resolver" selecione "Pontos finais de saída"
- Clique em "Criar ponto final de saída".



- Configure as configurações para o ponto final de saída da seguinte forma:
    - Nome do ponto final: Escolha um nome exclusivo para este ponto final de saída (ou seja, ImmersionDay-Out)
    - VPC: Selecione VPC A do seu ambiente AWS
    - Grupo de segurança para este ponto final: Selecione o Grupo de Segurança padrão para o VPC A, que já contém uma regra que permite conectividade de saída.
    - #1 de endereço IP:
        - Zona de disponibilidade: Escolha o primeiro AZ na região em que você está trabalhando (ou seja, us-leste-2a)
        - Sub-rede: Selecione a sub-rede nesse AZ. (Apenas uma opção aparecerá no drop-down).
        - Endereço IP: Use um endereço IP selecionado automaticamente
    - #2 de endereço IP:
        - Zona de disponibilidade: Escolha o segundo AZ na região em que você está trabalhando (ou seja, us-leste-2b)
        - Sub-rede: Selecione a sub-rede nesse AZ. (Apenas uma opção aparecerá no drop-down).
        - Endereço IP: Use um endereço IP selecionado automaticamente

O diálogo resultante será assim. Clique em "Enviar" para criar o ponto final.

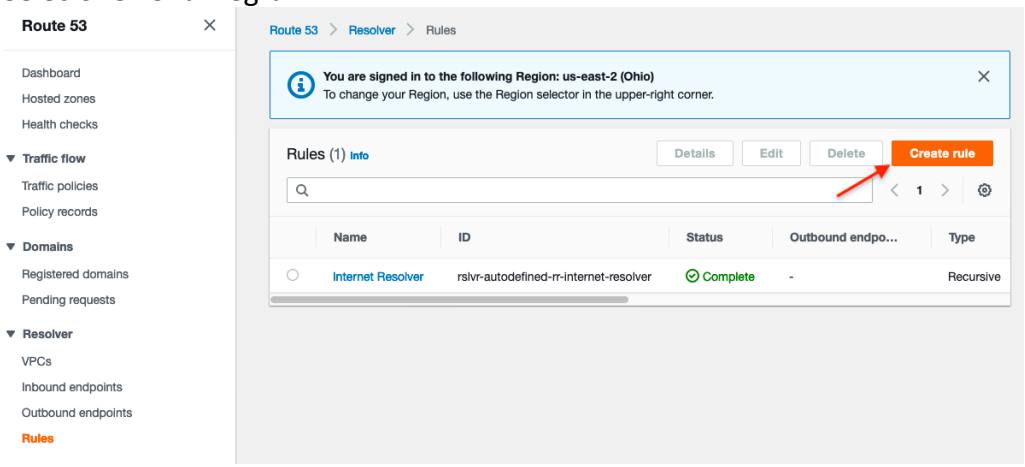


- Aguarde que o status do ponto final mude para "Operacional". Em seguida, prossiga para o próximo passo.

3.2 Crie uma regra de resolver rota 53, por exemplo.corp.

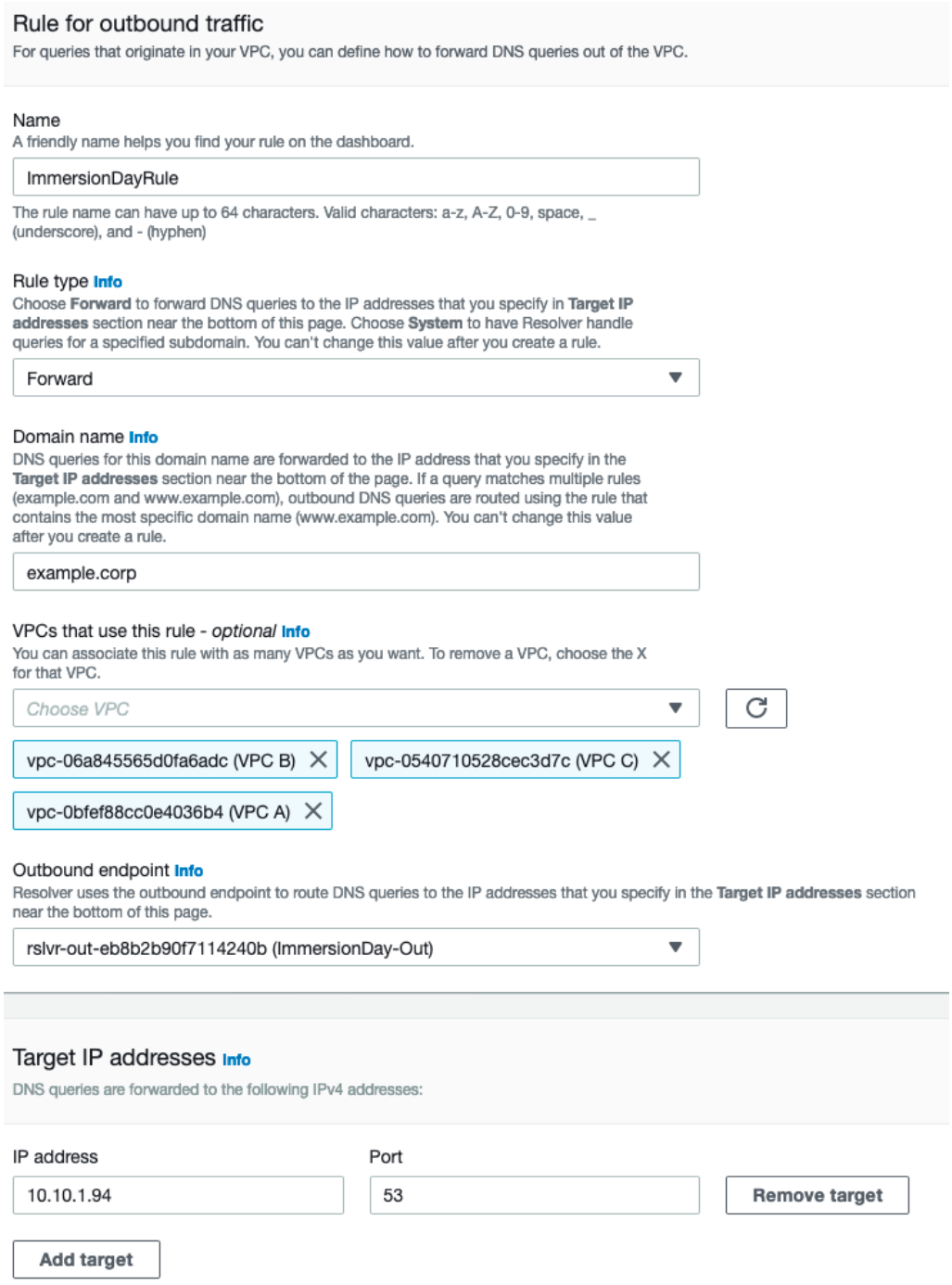
Agora que criamos um ponto final de saída, o Route 53 Resolver é capaz de alcançar nosso servidor DNS de datacenter via VPC A e a conexão VPN do Transit Gateway. Em seguida, precisamos configurar uma regra de resolver rota 53 para direcionar consultas, por **exemplo.corp** para esse servidor DNS. Associaremos a regra com os VPC's A, B e C. Isso fará com que o Rota 53 Resolver use essa regra sempre que o VPC DNS resolver processa consultas de instâncias em qualquer uma dessas três VPCs.

- Ainda no console Route 53, navegue até a guia "Regras" em "Resolver"
- Selecione "Criar regra"



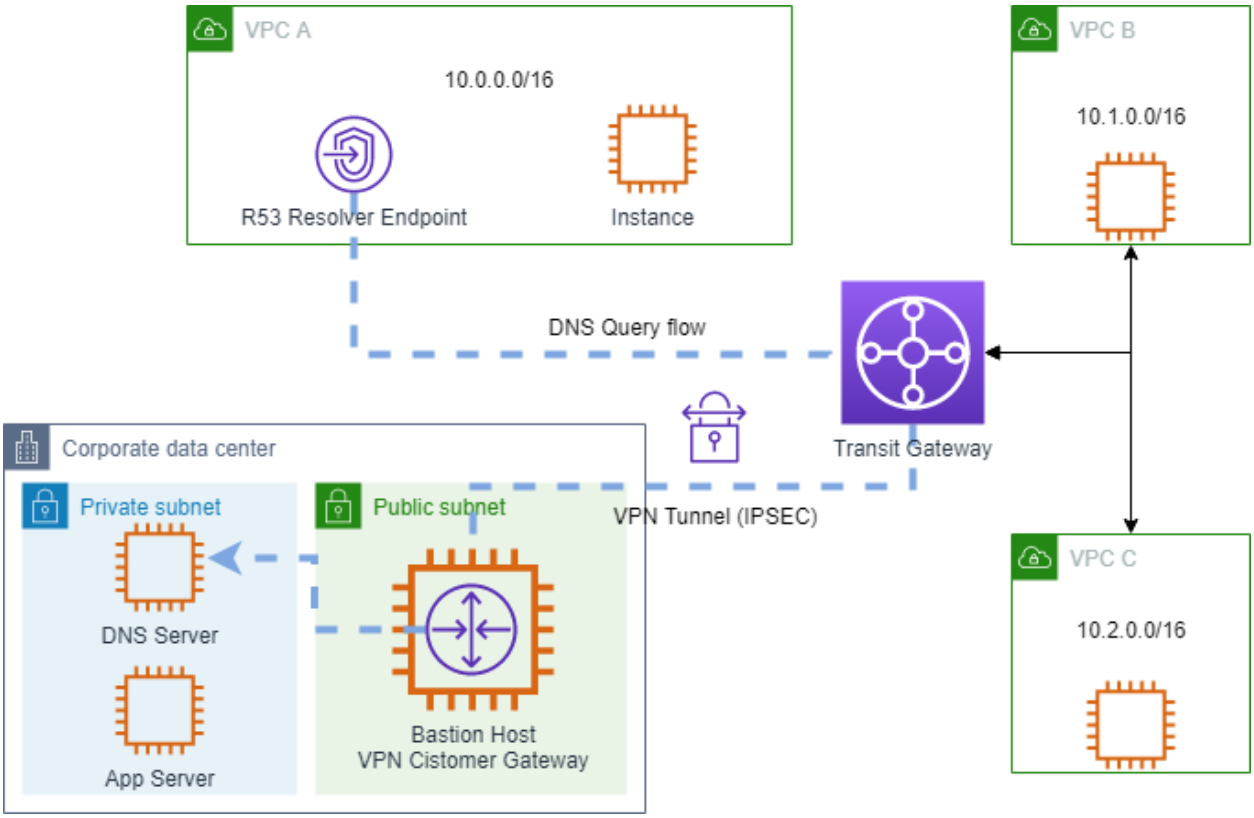
- Fornecer configuração para a regra:
  - Dê à regra um nome único, como "NetworkImmersionDay-rule"
  - Especifique o nome de domínio "exemplo.corp".
  - Associe a regra com todos os seus três VPCs A: VPC A, VPC B e VPC C.
  - Escolha o ponto final de saída que você criou na etapa anterior

- Digite o endereço IP do servidor DNS do datacenter simulado para os endereços IP target.



- Clique em "Enviar" para criar a regra.

3.3 Testando a regra do Resolver da Rota 53



Neste ponto, configuramos o resolve rota 53 para encaminhar consultas ao servidor DNS do datacenter para o domínio exemplo.corp de qualquer um dos AWS VPC's A, B ou C. Podemos testar a resolução de nomes tentando nos conectar ao servidor de aplicativos no local a partir de uma das instâncias EC2 em nossos VPCs AWS.

- SSH em sua instância EC2 em VPC A, B ou C.
- ssh -I chave.pem ec2-user@<PPP>
- Verifique a configuração do servidor DNS na instância examinando resolv.conf:
- cat /etc/resolv.conf
- Observe que a instância está usando o servidor DNS fornecido pelo AWS (por exemplo, 10.0.0.2) e não o servidor DNS no local para resolução de nomes:
- tempo limite de opções:2 tentativas:5
- ; gerado por /usr/sbin/dhclient-script
- pesquisar-nos-west-2.compute.internal
- nameserver 10.0.0.2

- Use o CURL para consultar o servidor de aplicativos no local pelo seu nome de host, myapp.example.corp:\
- curl http://myapp.example.corp

  Se a resolução do nome e o servidor do aplicativo estiverem funcionando, você receberá de volta uma resposta "Olá, mundo".