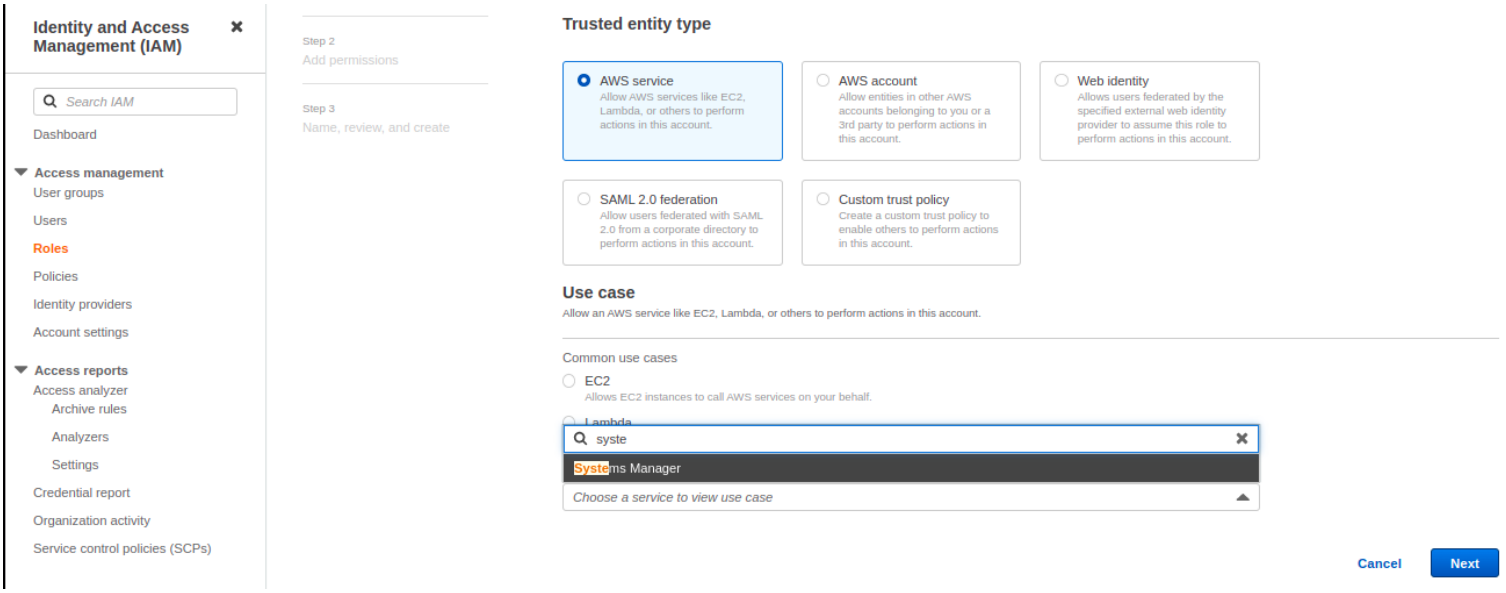
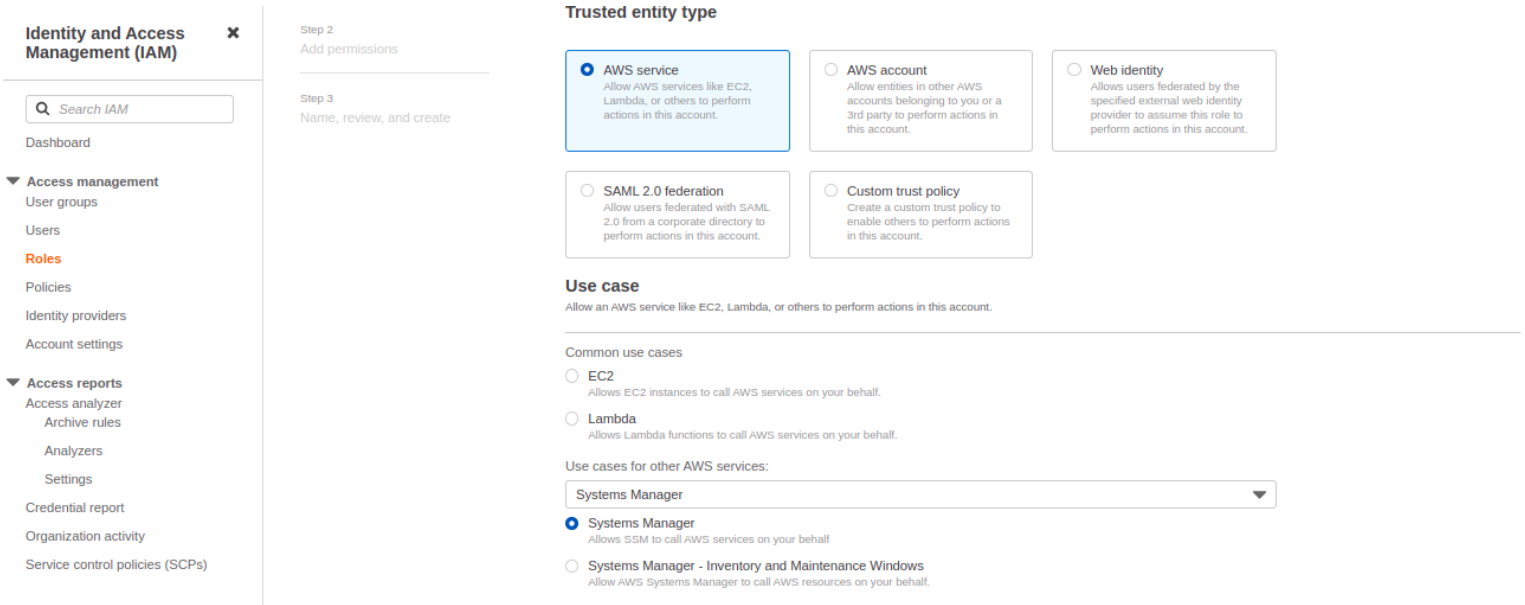
Instalação de agente de segurança com SystemManager AWS

Criar IAM role SSMtoSNS com a Policy : AWSSNSFullAccess

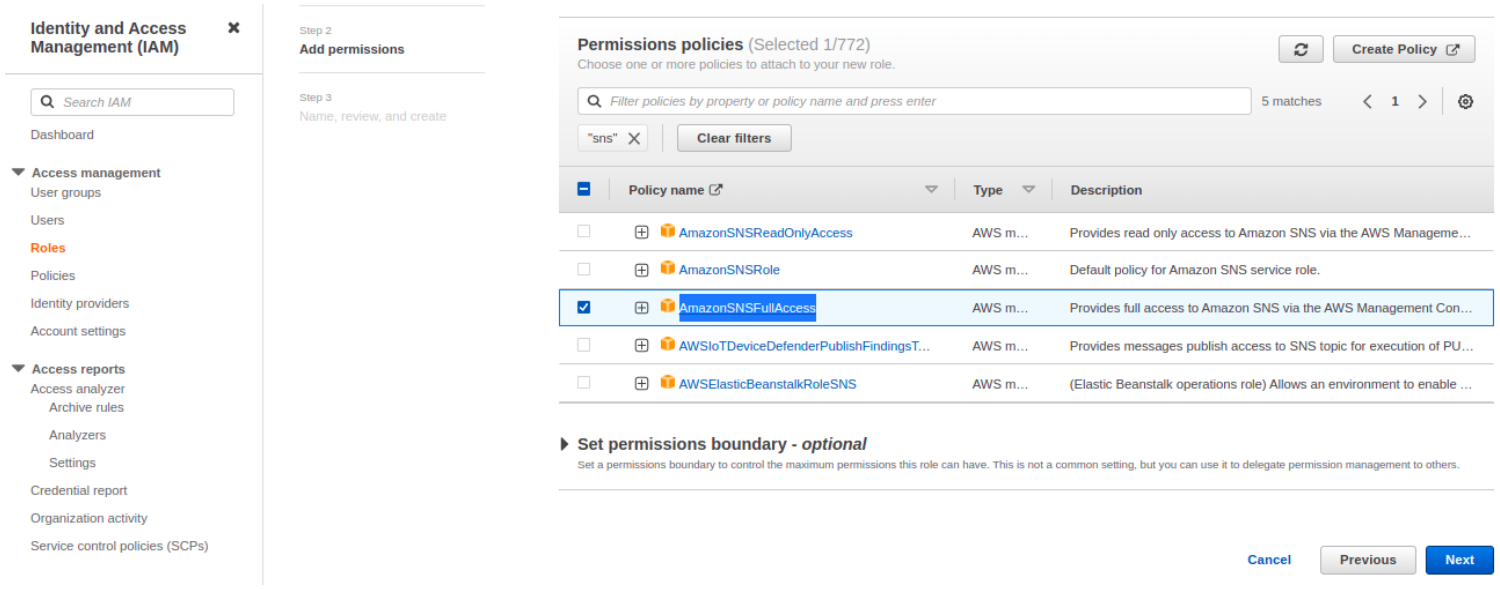
Selecione SystemManager



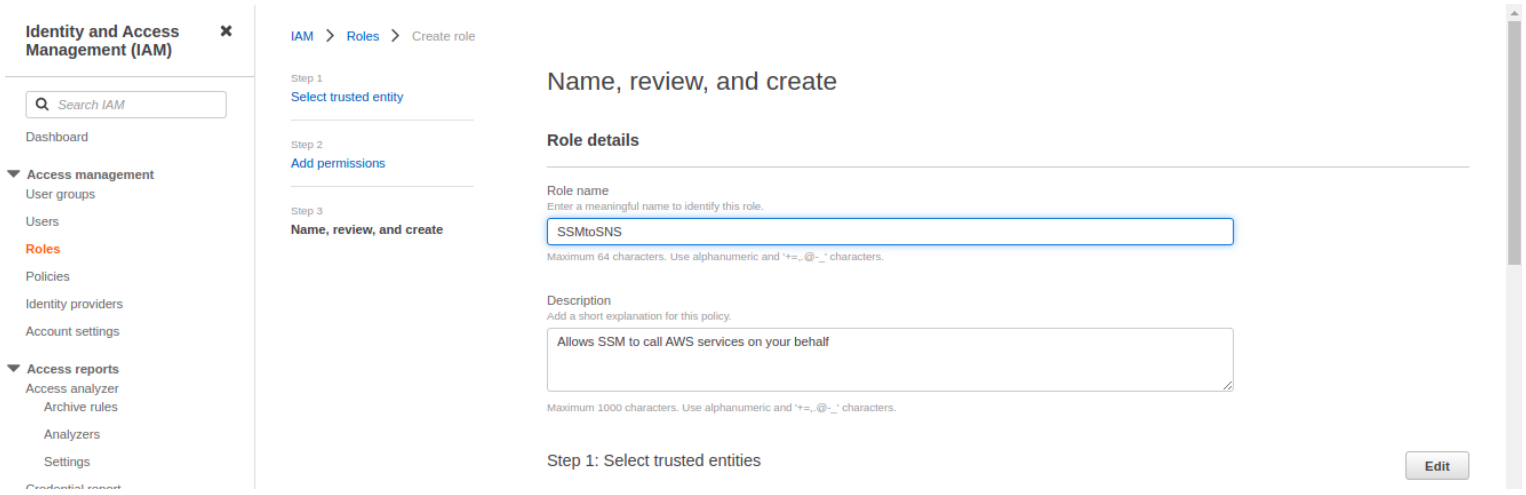
Procure por SystemManager e Next



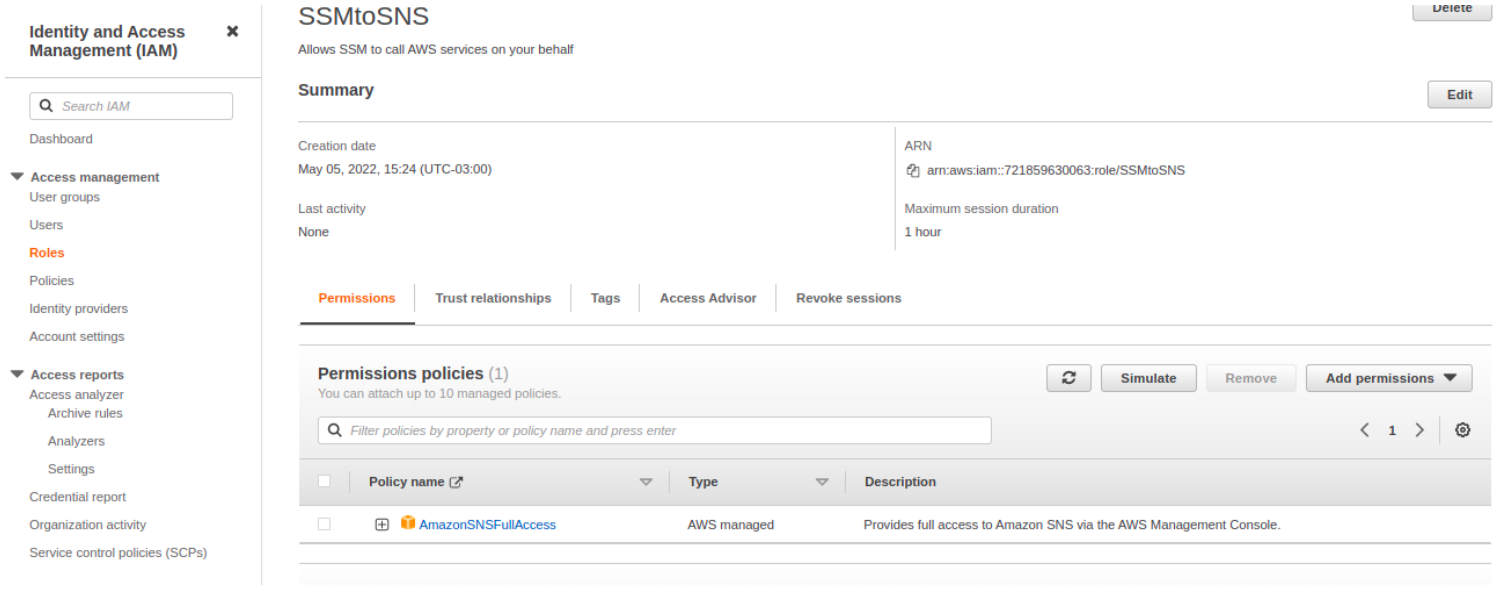
Procure a role AmazonSNSFullAccess e selecione



De nome a sua role “sujestão” SSNtoSNS e clique em Create role

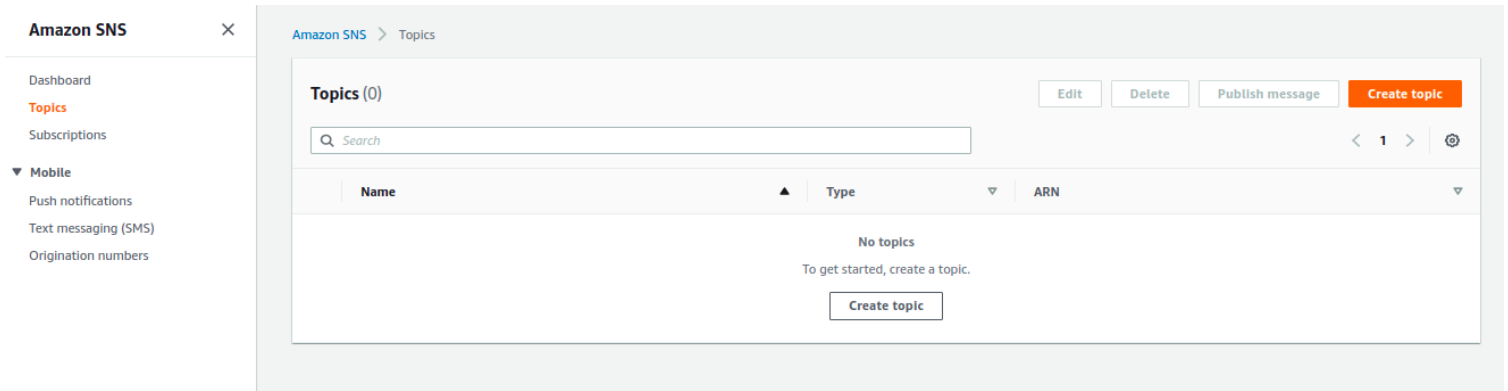


Confira e seguimos para criar um tópico de notificação

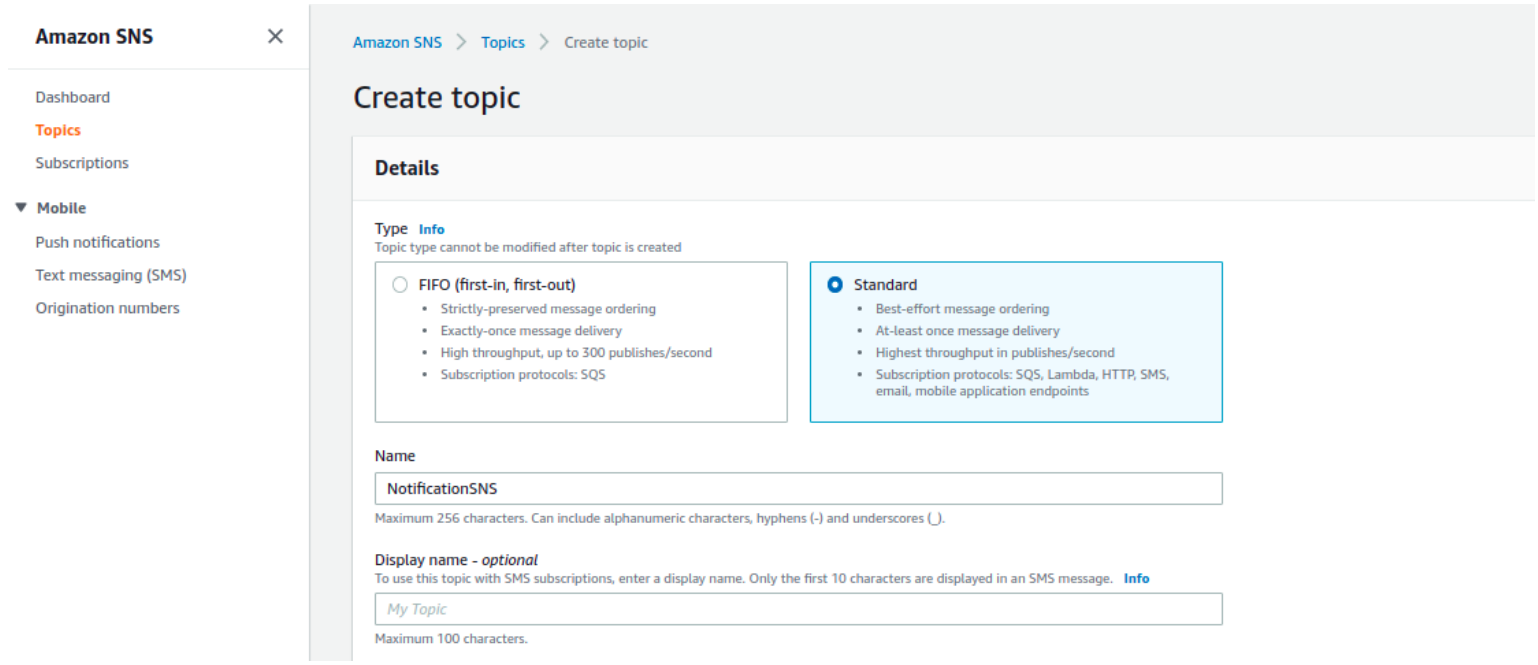


Acesse pagina do AWS Simple Notification Service

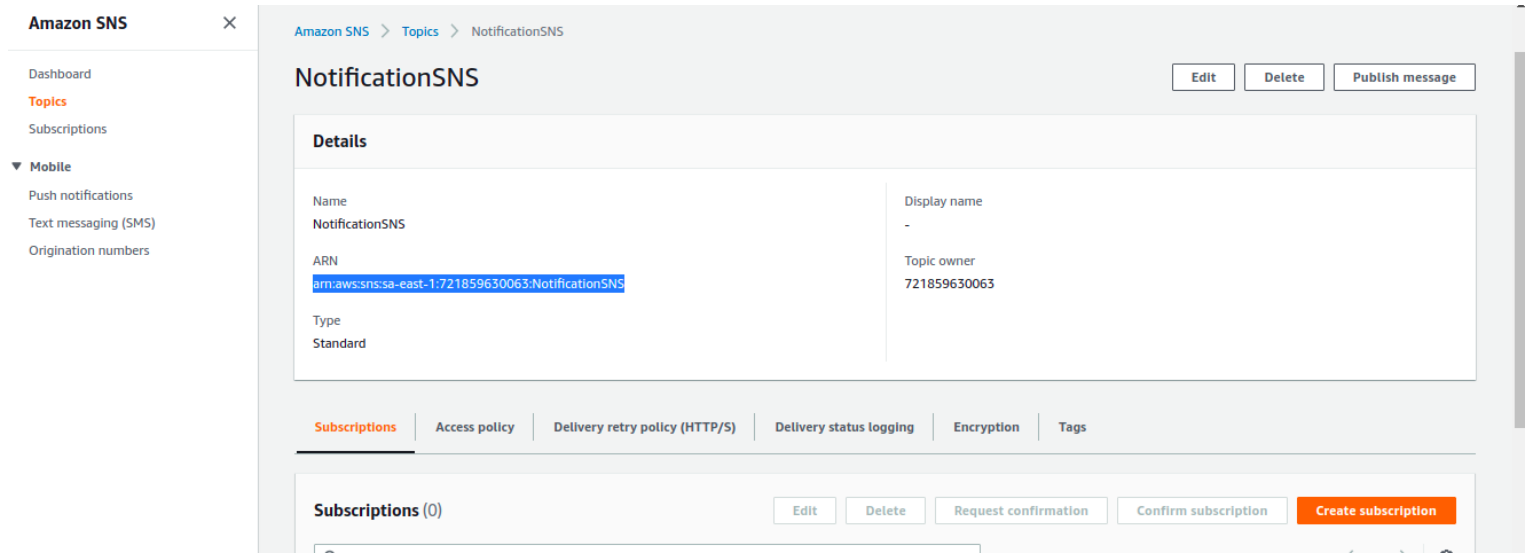
Crie um novo tópico após crie uma nova subscription escolha a opção de e-mail para receber as notificações e insira seu email após criada a sub confirme a inscrição no seu e-mail e salve a arn do tópico



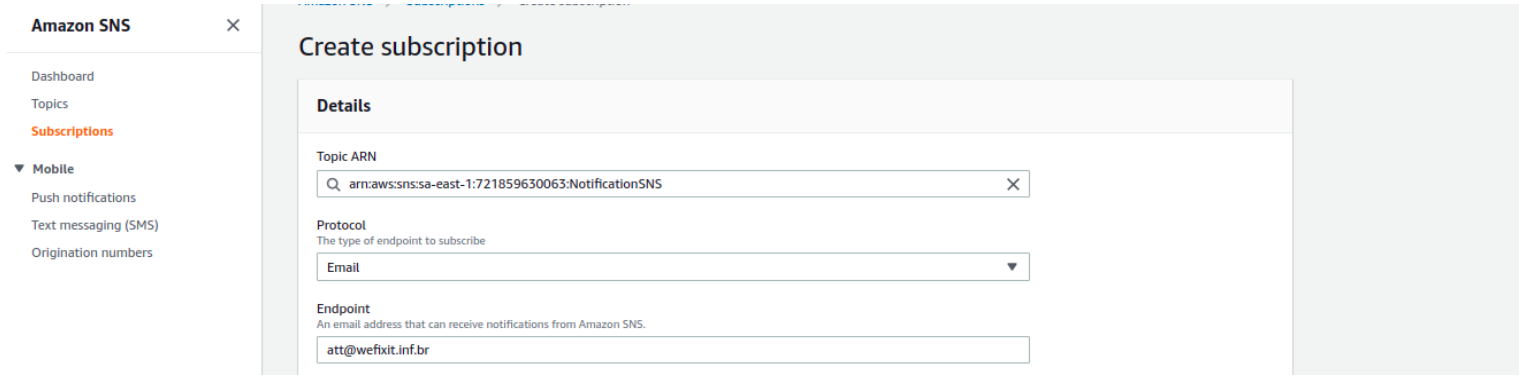
De nome ao tópico e clique em Create topic e salve a arn: do tópico



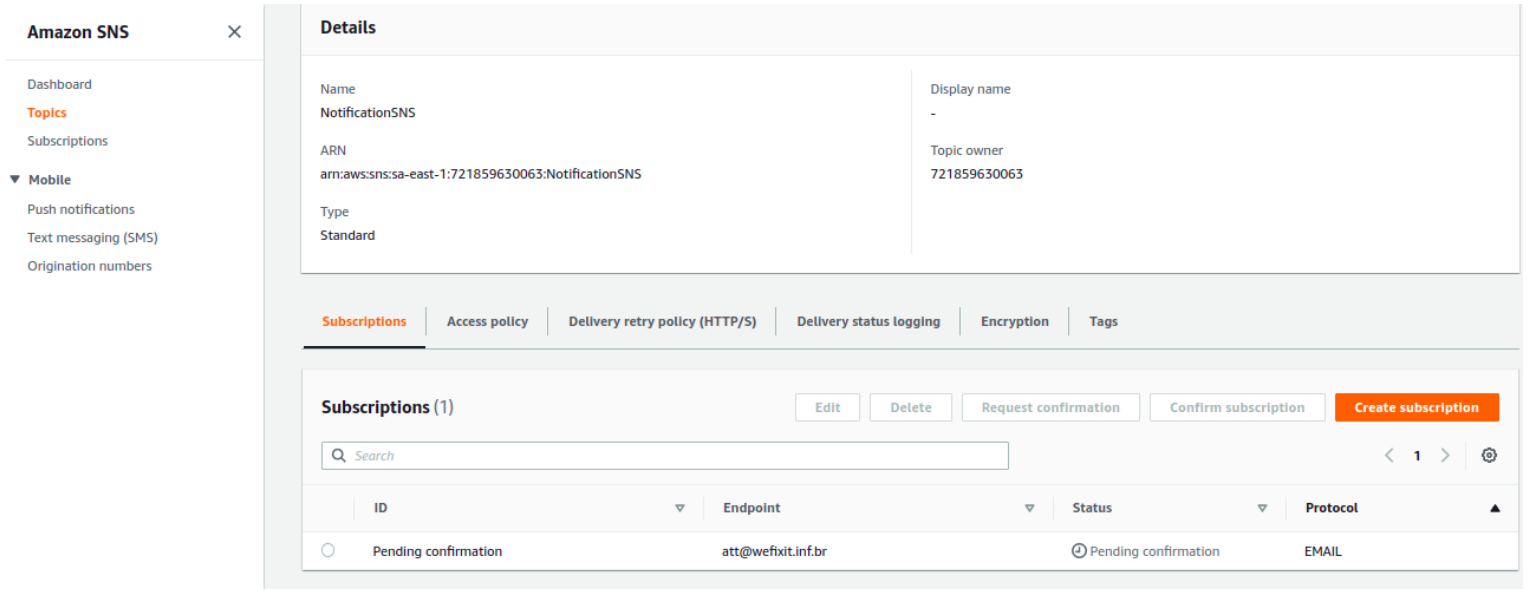
Agora vamos criar subscription



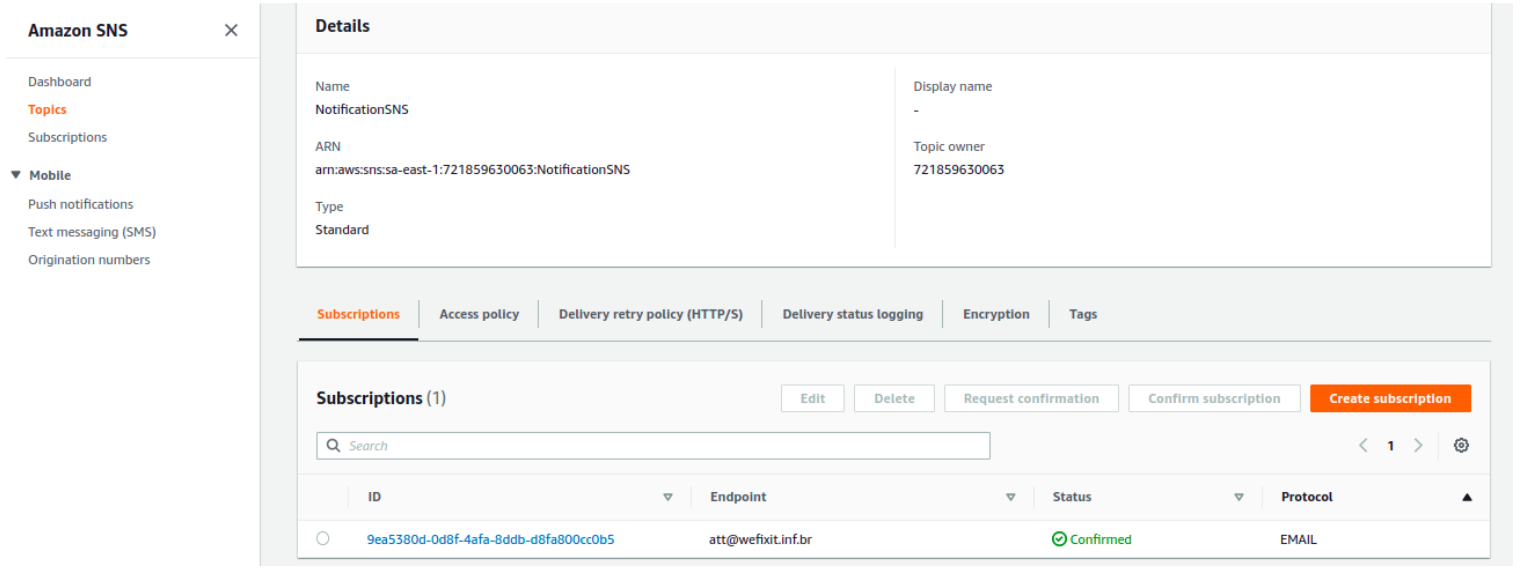
Selecione email e insira seu email



Acesse seu email e confirme a inscrição

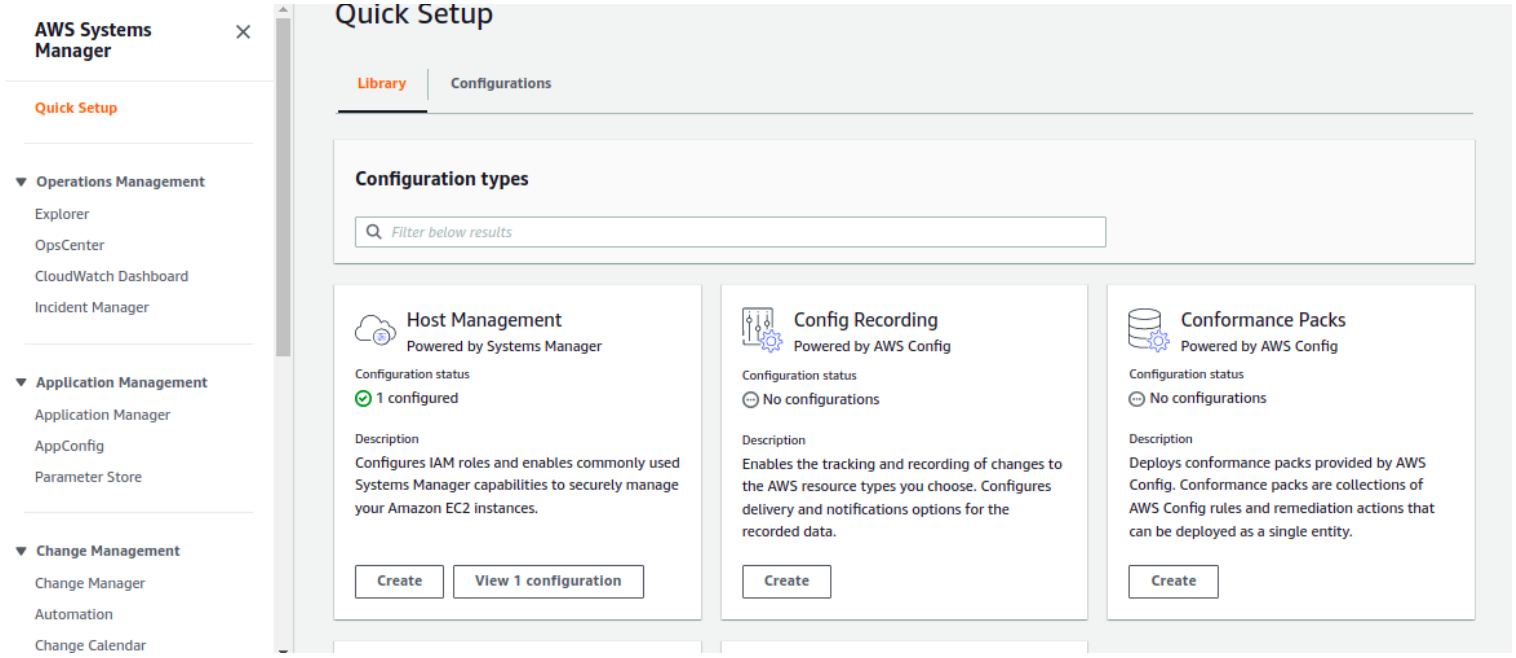


Após confirmar seu email e verificar o status deve estar confirmado

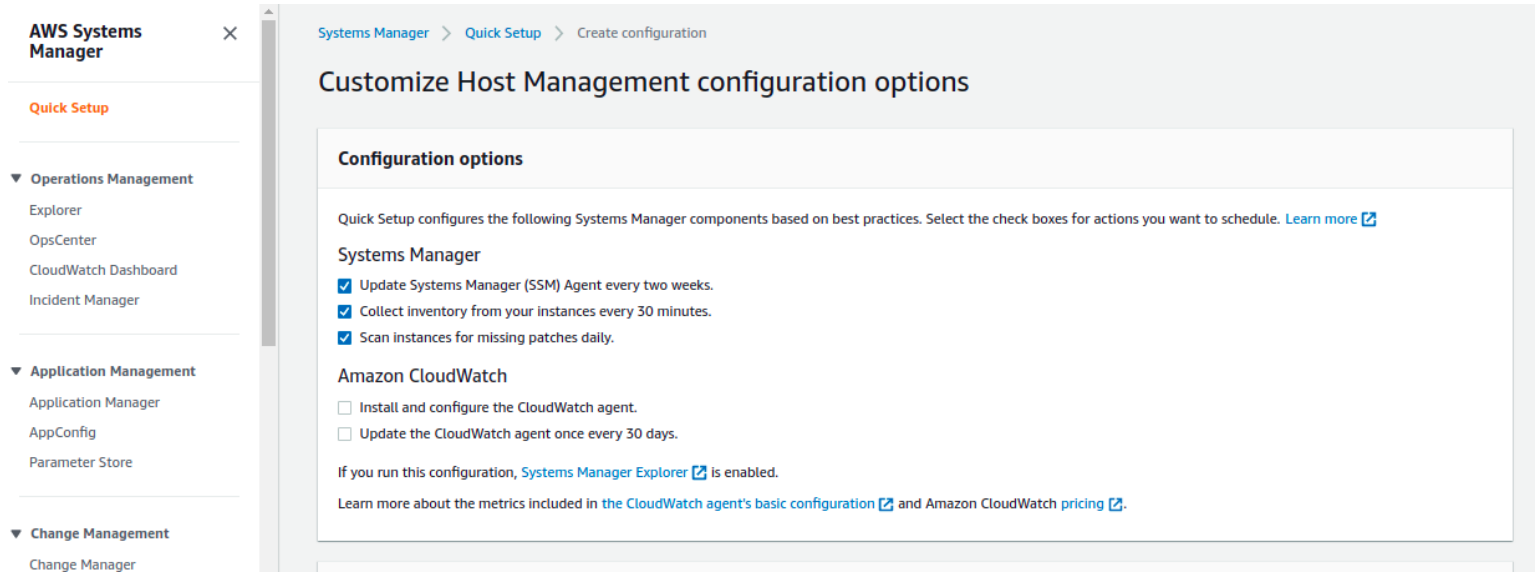


Acesse pagina do AWS SystemManager quick setup e clique em Get Started

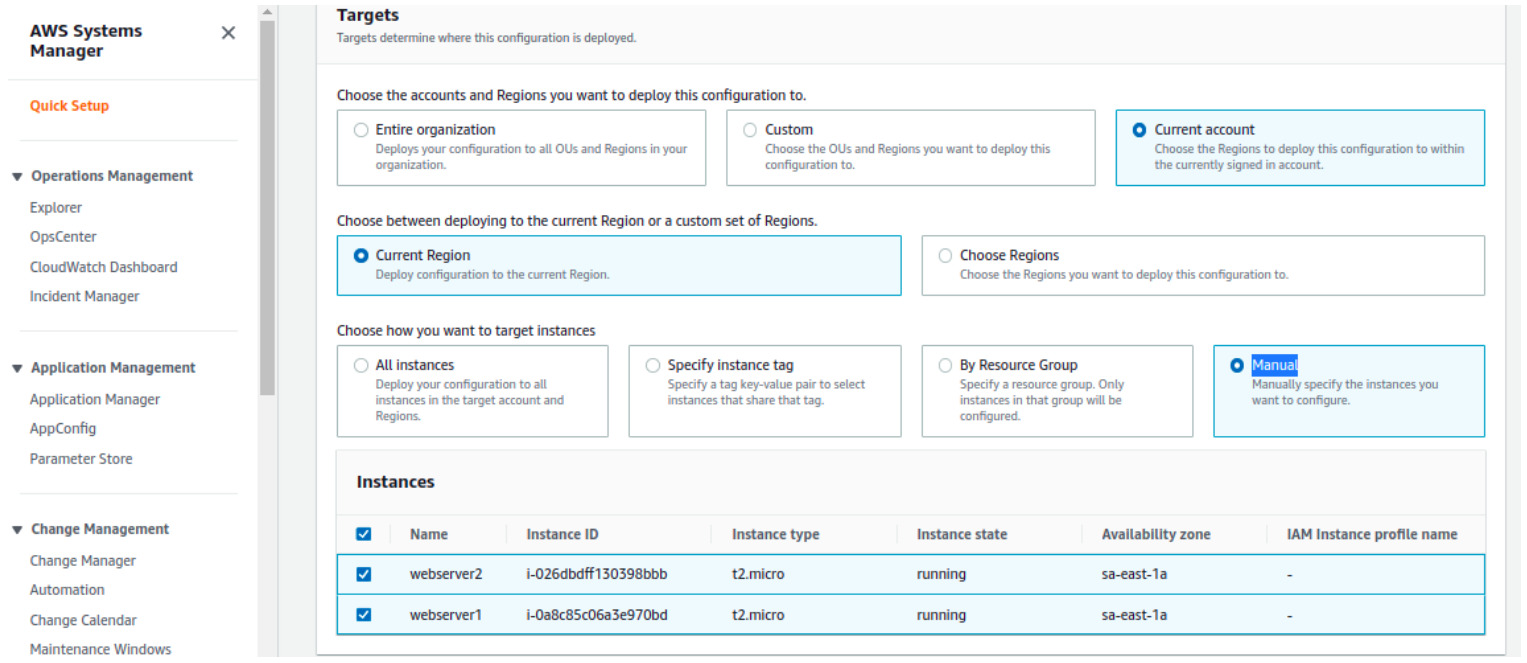
Selecione Host Management e clique em Create

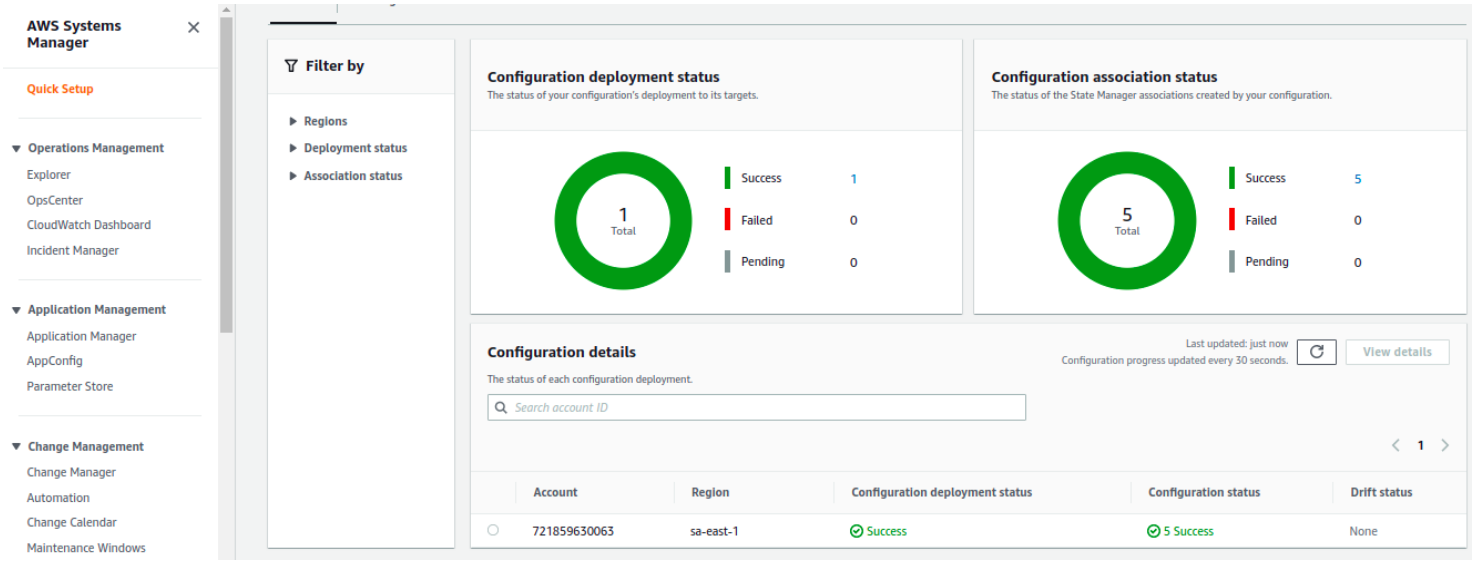


Mantenha as opções selecionadas

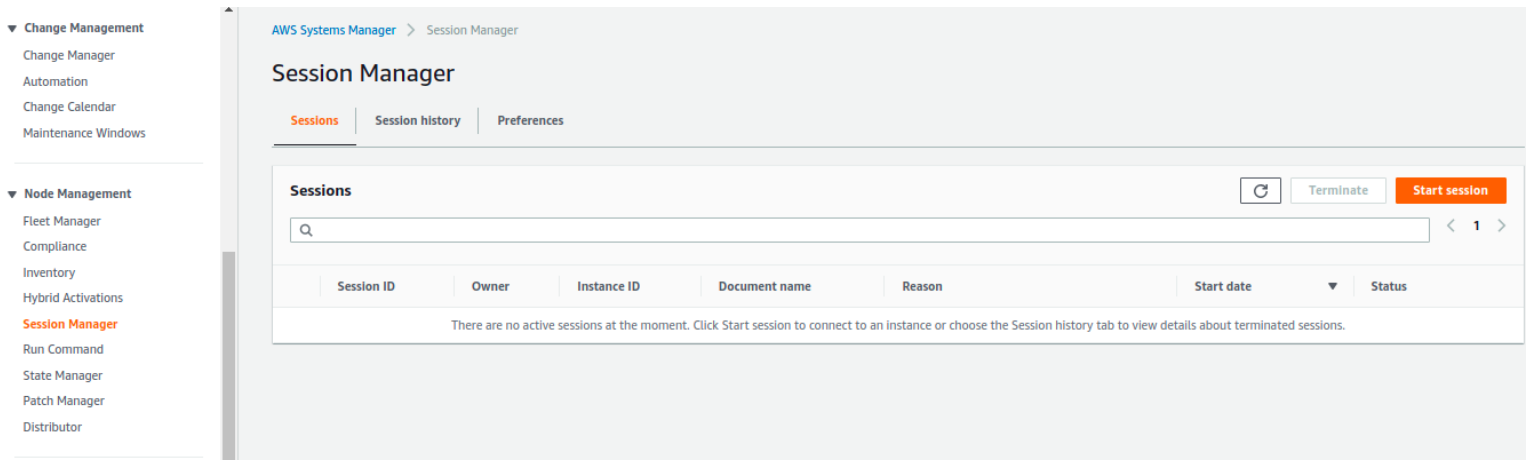


Abaixo em Targets marque Current account > Current Region > Manual e selecione as Instâncias criadas com Terraform e clique em Create pode levar de 5 a 10 para finalizar

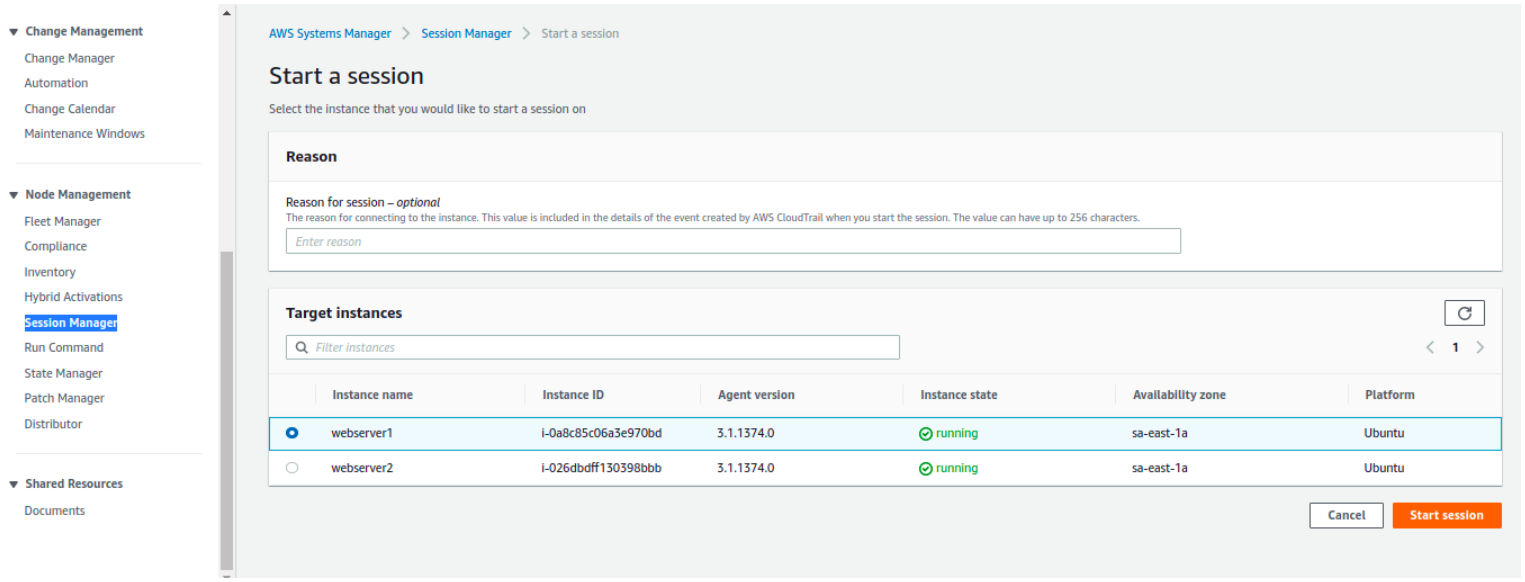




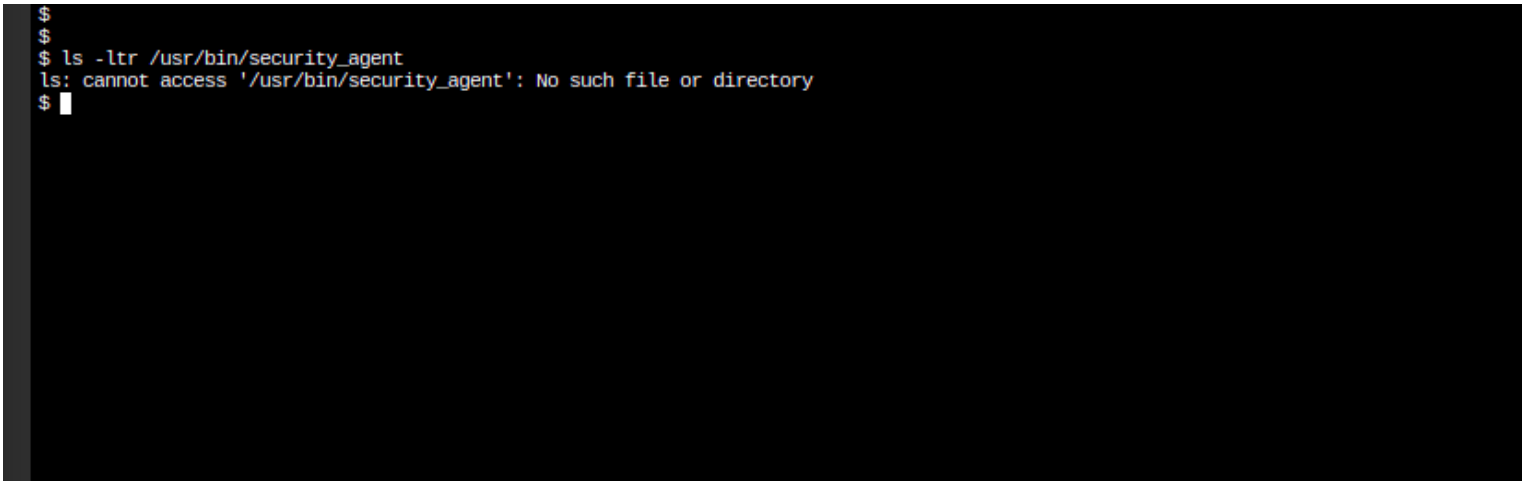
Vamos testar a conexão com Instâncias na seção Session Manager clique Start Session



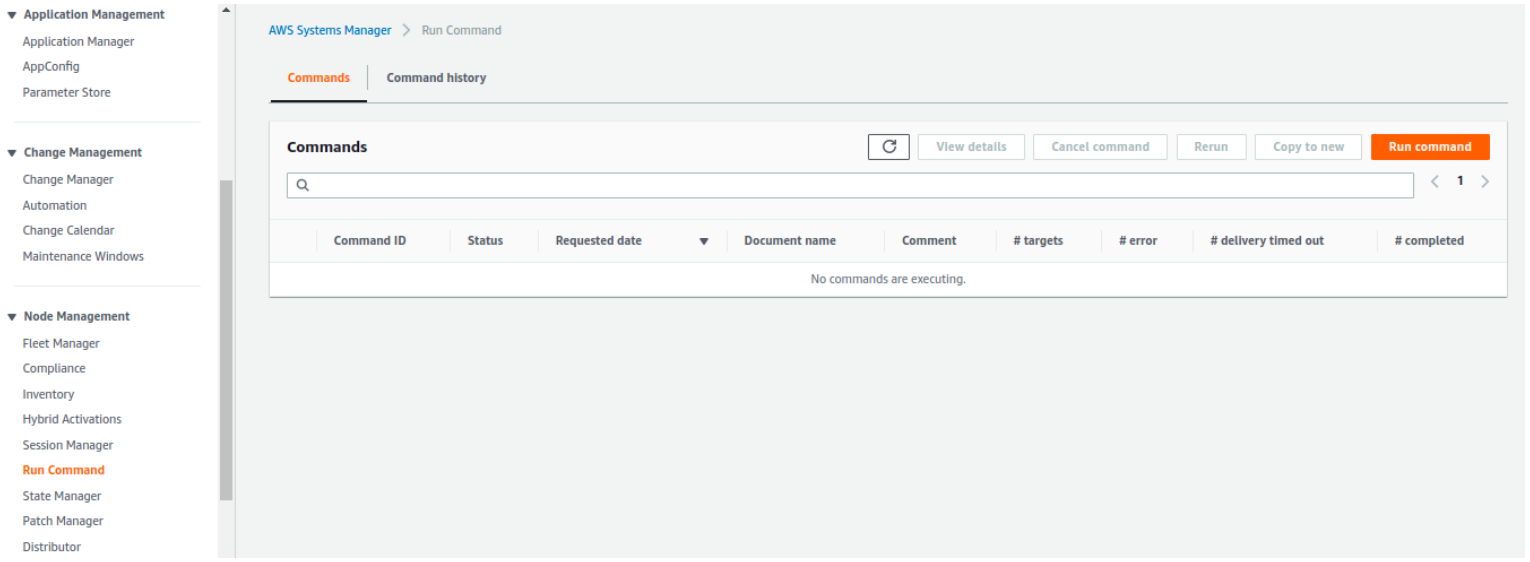
Selecione a Instância e clique em start



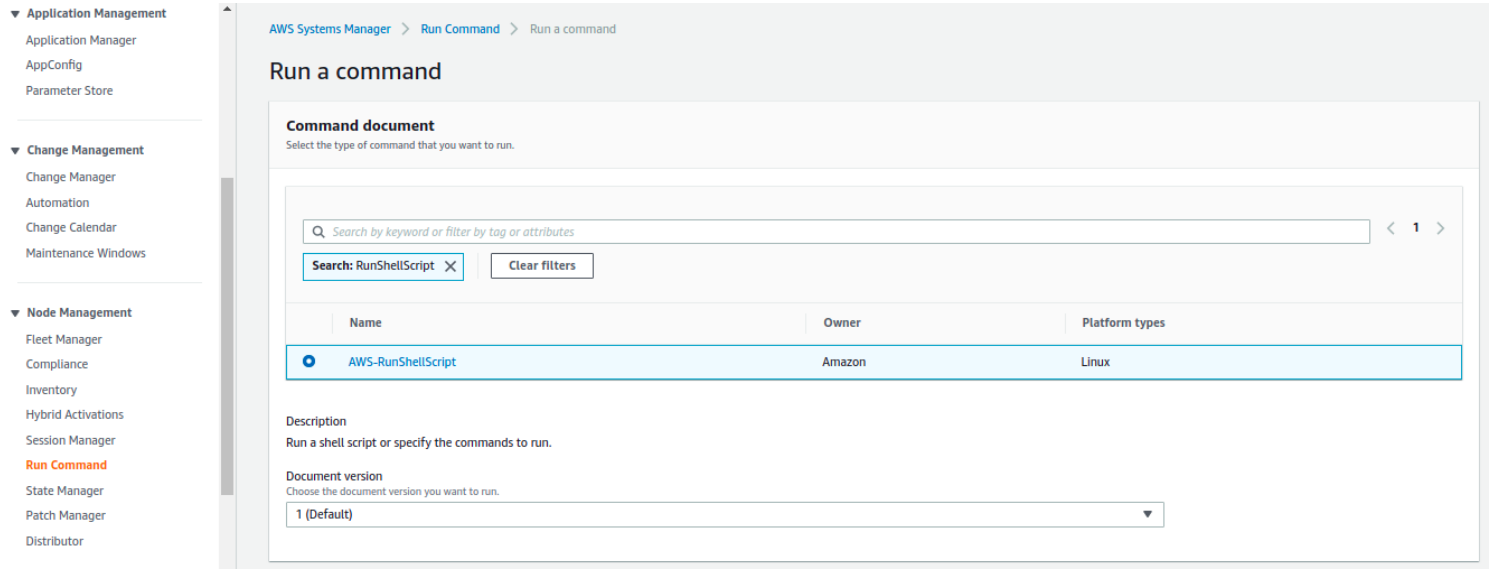
Execute o comando ls -ltr /usr/bin/security_agent a pasta estará vazia



No menu a esquerda do SystemManager acesse Run Command para provisionamento do "agente" clique em Run Command



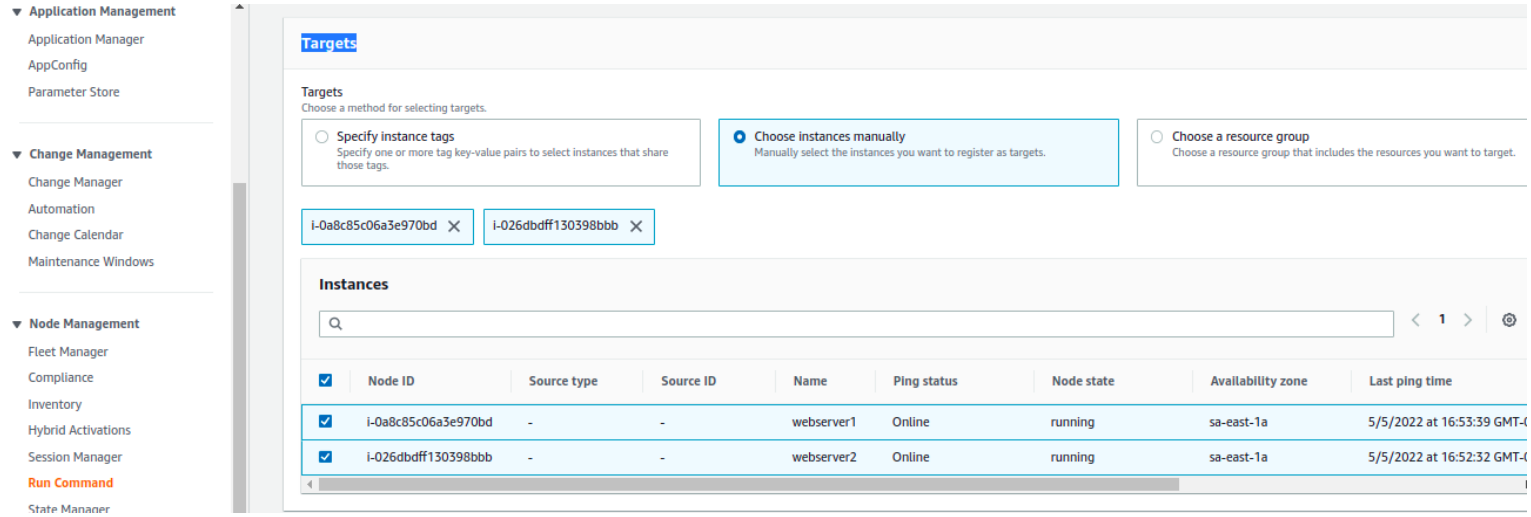
Clique em Run e selecione AWS-RunShellScript



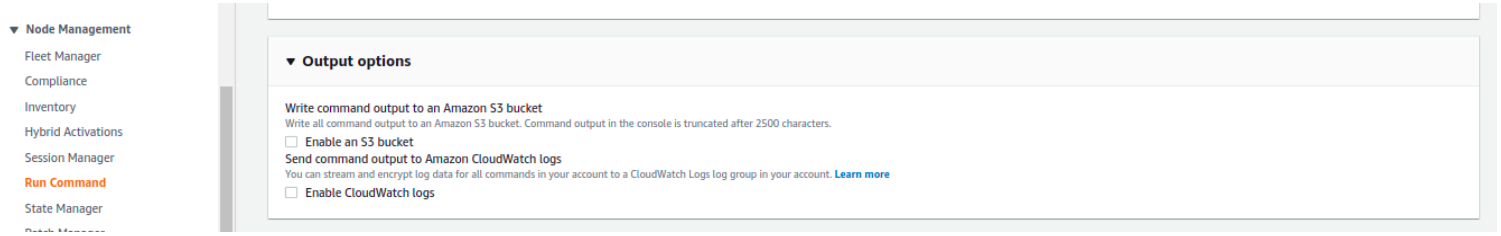
Abaixo em Command parameters insira o scripit

sudo wget -q https://bootcamp-aws.s3.amazonaws.com/install_security_agent.sh -P /tmp
sudo chmod +x /tmp/install_security_agent.sh
sudo /tmp/install_security_agent.sh
ls -ltr /usr/bin/security_agent

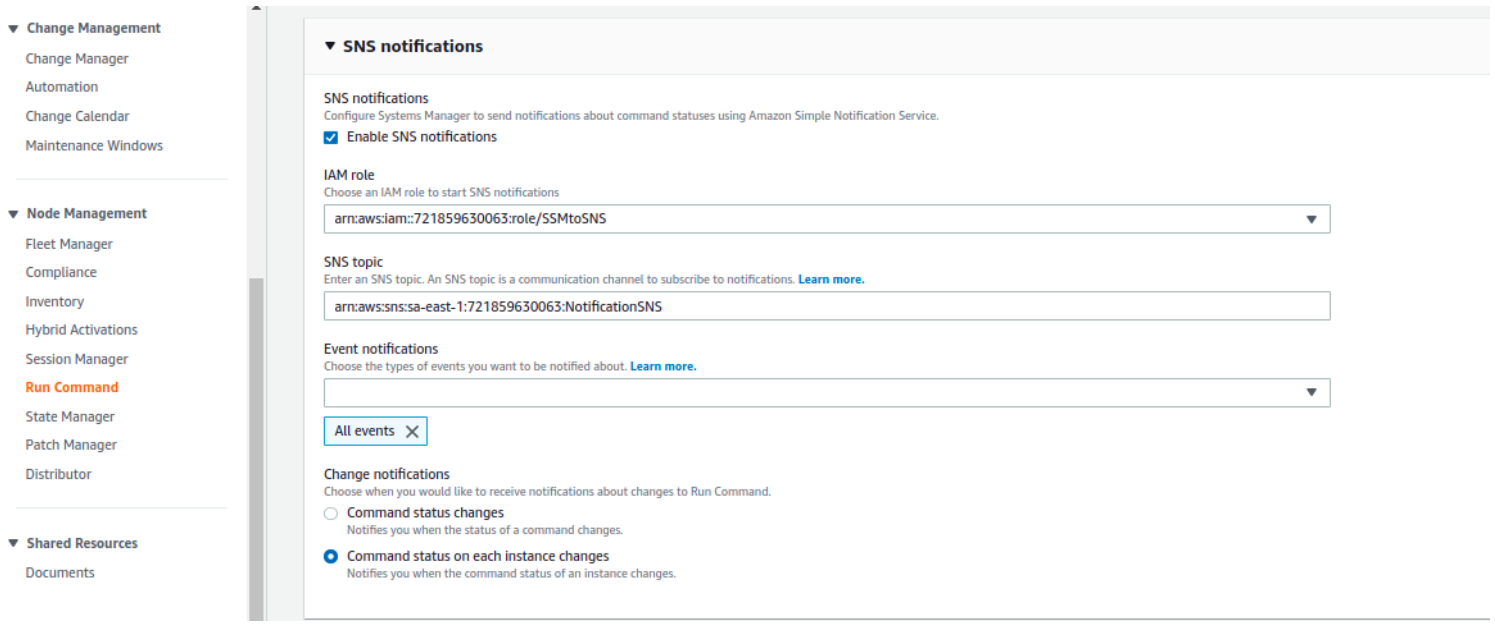
Na seção targets marque a opção Choose instances manually e selecione as instâncias



Na seção Output options desmarque a opção de S3



Na Seção SNS notifications em IAMrole selecione a role SSMtoSNS cole a arn do SNS topic e clique em RUN



Após retorne a sua instância e rode comando ls -ltr /usr/bin/security_agent
Você vai ver que o agente de segurança foi copiado para as Instâncias, em casos de muitas instâncias essa solução é perfeita para cópia e instalação