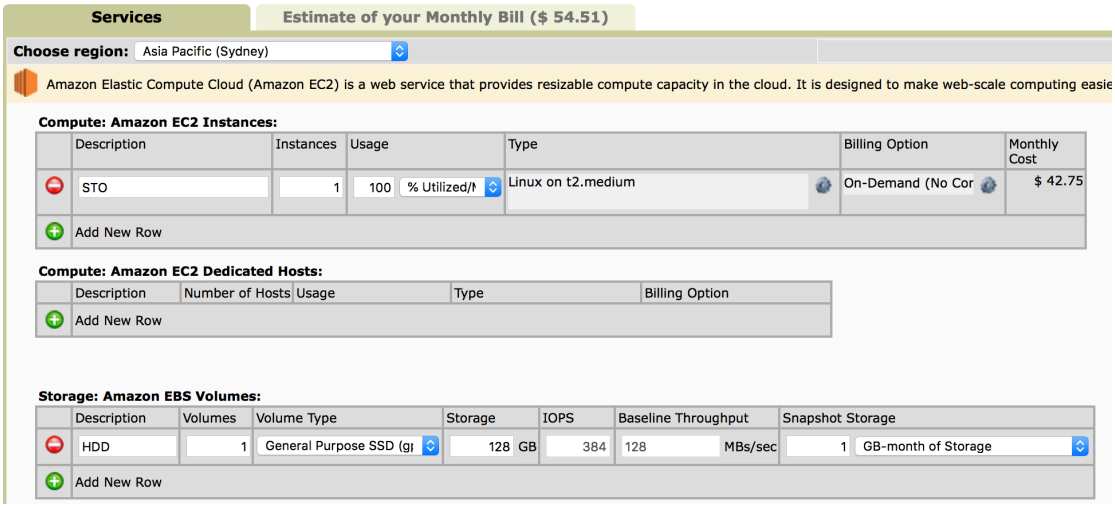
# Requirements for Installing SafeToOpen (STO)

Here is the list of requirements needed to Install SafeToOpen:

- An AWS account:
  - An EC2 to set up STO. We install it on an Ubuntu 16.04 LTS Virtual Machine in Sydney.
  - A static public IP address
  - Please refer to this link to get the pricing from AWS. For <= 3000 users a Linux medium-t2 should be enough
  - 128 GB Hard drive




- DNS Changes:
  - A DNS 'A' record to point to an EC2 public IP address. E.g., sto.org_name.co.nz
  - An MX record to point to STO Mail Server. E.g., sto.org_name.co.nz
- Mail Server Changes:
  - Write a rule to duplicate/copy (no header/content change) any emails from phishing@org_name.co.nz to isit@sto.org_name.co.nz
  - Write a rule in email security gateway to ignore emails to/from isit@sto.org_name.co.nz.
- EC2 Allowing Inbound Traffic:
  - A Web proxy IP address(es)
  - An Outgoing Mail Server IP address(es)
- Active Directory Changes:
  - An AD user account for SafeToOpen to access customer environment
  - A VPN access for SafeToOpen to access customer environment
  - A codesign certificate from Active Directory to sign the Outlook Add_in
  - A GPO policy to deploy Outlook Add_in
  - Adding the sto.org_name.co.nz in AD trusted domains
  - Adding the STO Add-in to the list of Outlook trusted applications
  - An SSL Certificate for accessing https://sto.org_name.co.nz.
- SIEM Changes:
  - An alert to be generated in SIEM to email all HTTP_Referer logs to isit@sto.org_name.co.nz every 2 hour
  - A SIEM account is required for SafeToOpen integration
  - Firewall changes to integrate STO with other security products (such as SIEM, WebProxy, Mail Gateway, etc)
- Automation via SafeToOpen (if required):
  - An admin access to Web Proxy API to blacklist malicious URLs via the STO dashboard
  - An admin access to Office 365 API to act on a malicious sender/email subject, etc
- SOC:
  - An email address to report the malicious emails (detected by STO) to the SOC team
- SafeToOpen Settings:
  - List of all domain named owned by the business (to whitelist)
  - List of all key people (full name) to detect Business Email Compromise
  - High-resolution logos in PNG