# Pre-requisites

* A computer with Chrome
* Optional - git

# Lab Prep – Launch Cloudformation Stacks Setup

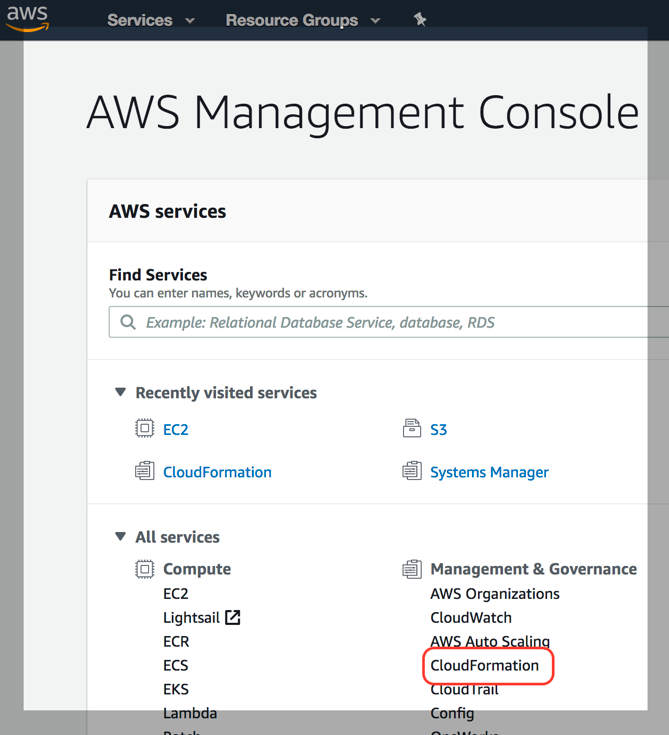
(Estimated completion time – 35 minutes)

Lab preparation will take some time to complete, so we recommend that you initiate this and let it complete in the background.

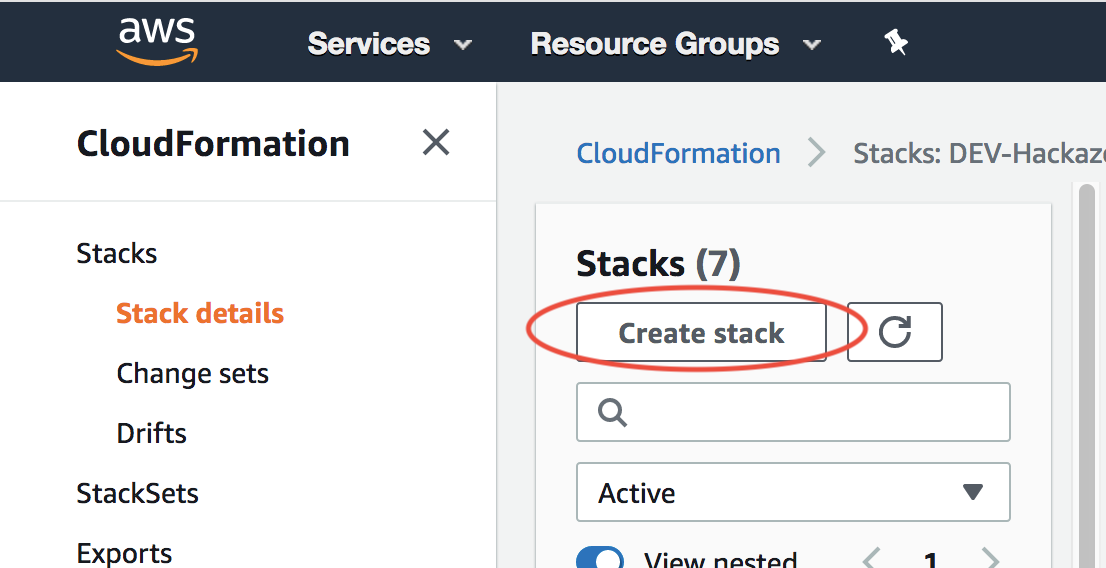
## WAF Automation And Dashboard Setup

This Cloudformation stack will stand up the automation for managing WAF and the dashboards.

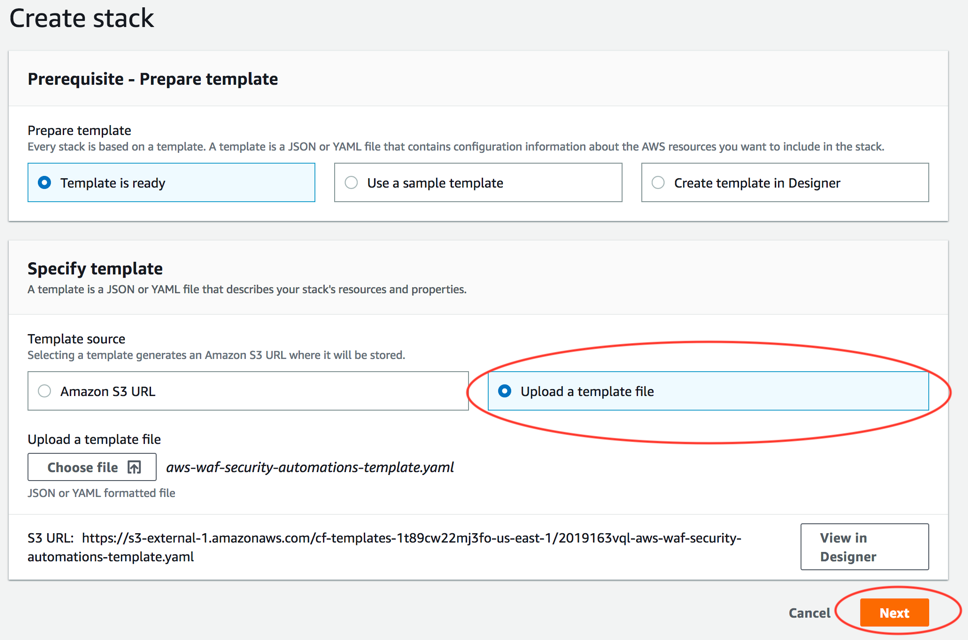
1. Open the CloudFormation console



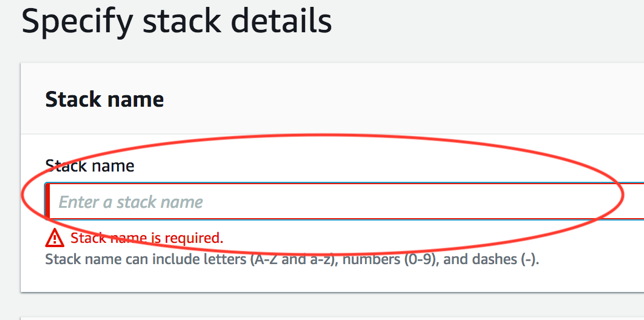
1. Create a new stack



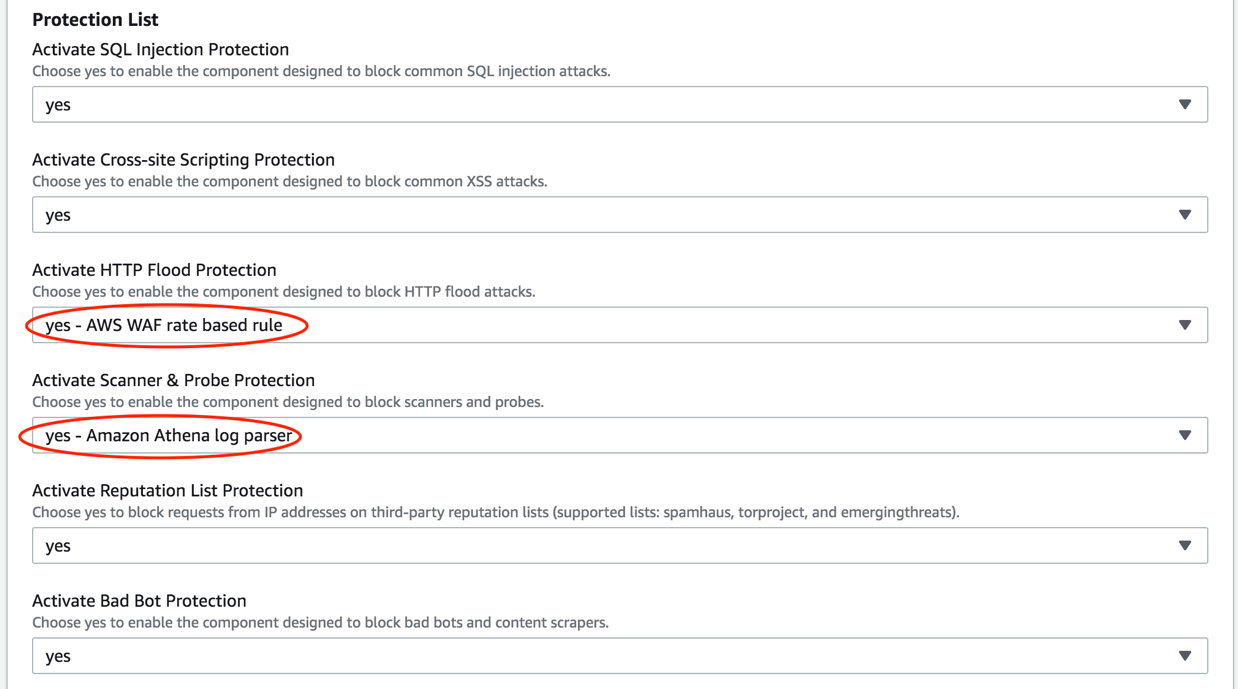
1. Upload the template template/aws-waf-security-automations-template.yaml



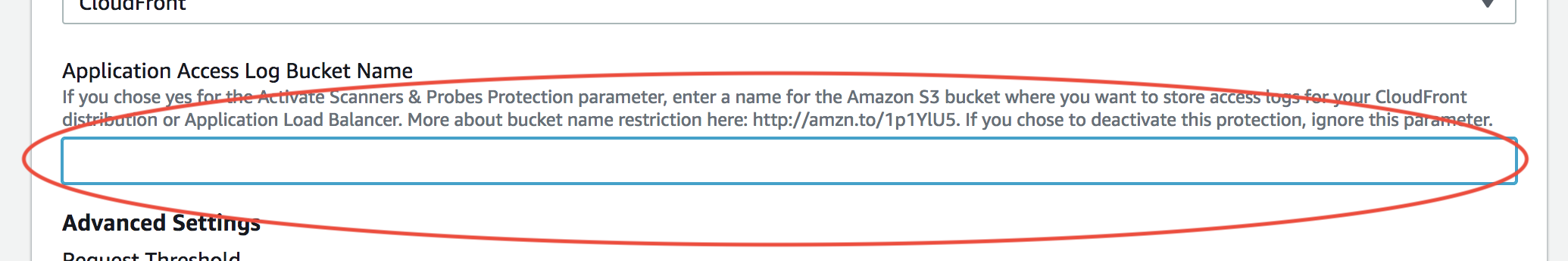
1. Enter a new stack name in **all lowercase** – e.g. waf-lab



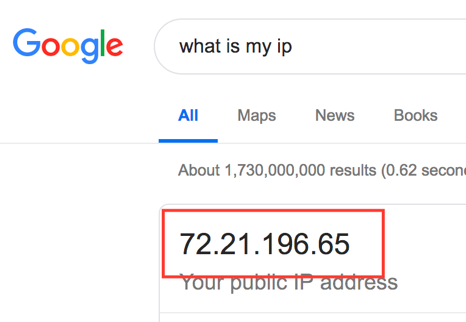
1. Update Scanner & Probe Protection to “yes – Amazon Athena log parser” and “Activate HTTP Flood Protection” to ““yes – AWS WAF rate based rule”:



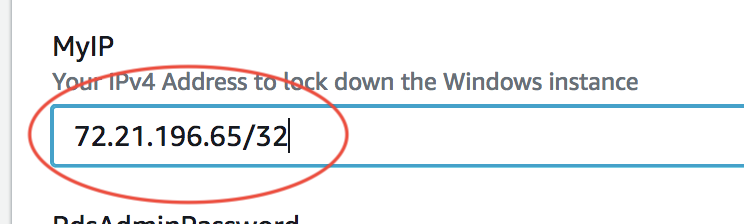
1. Enter a new S3 bucket to collect access logs for WAF



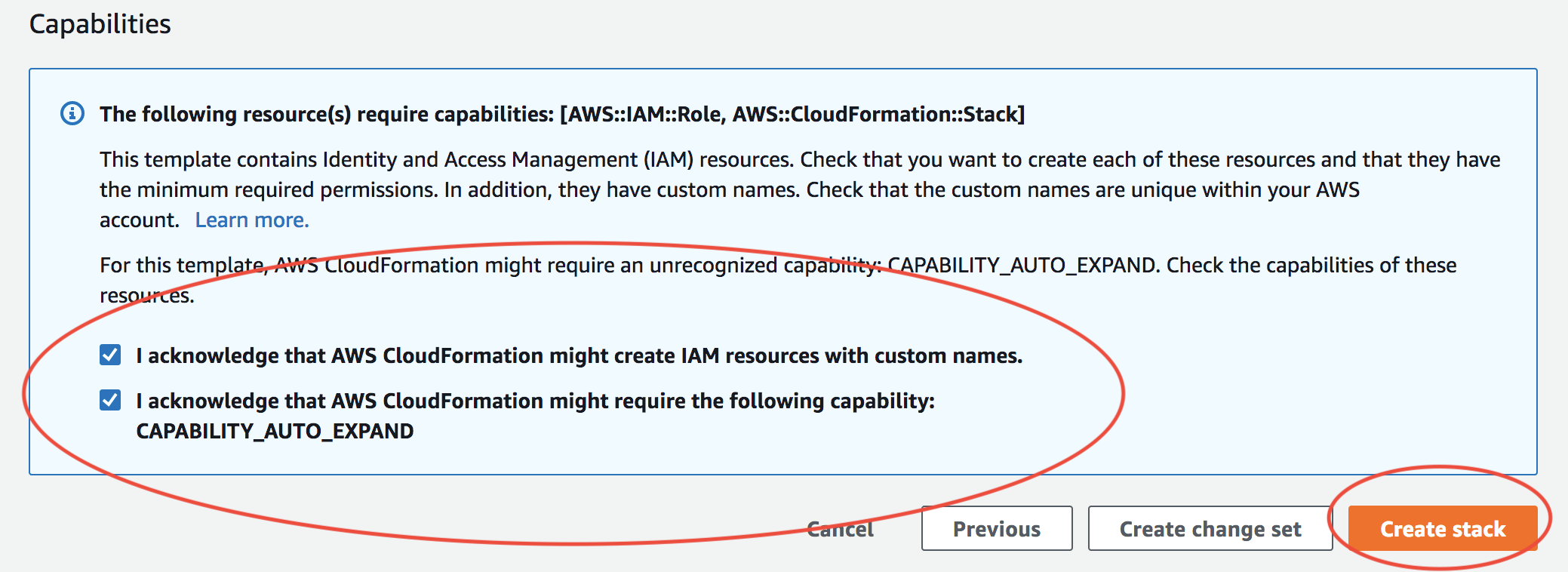
1. Get your IP from Google with “what is my ip”.



1. Enter your IP + “/32” for the attacker’s allowed ingress IP address in the Cloudformation form. Please replace 72.21.196.65 in these instructions with your IP address:



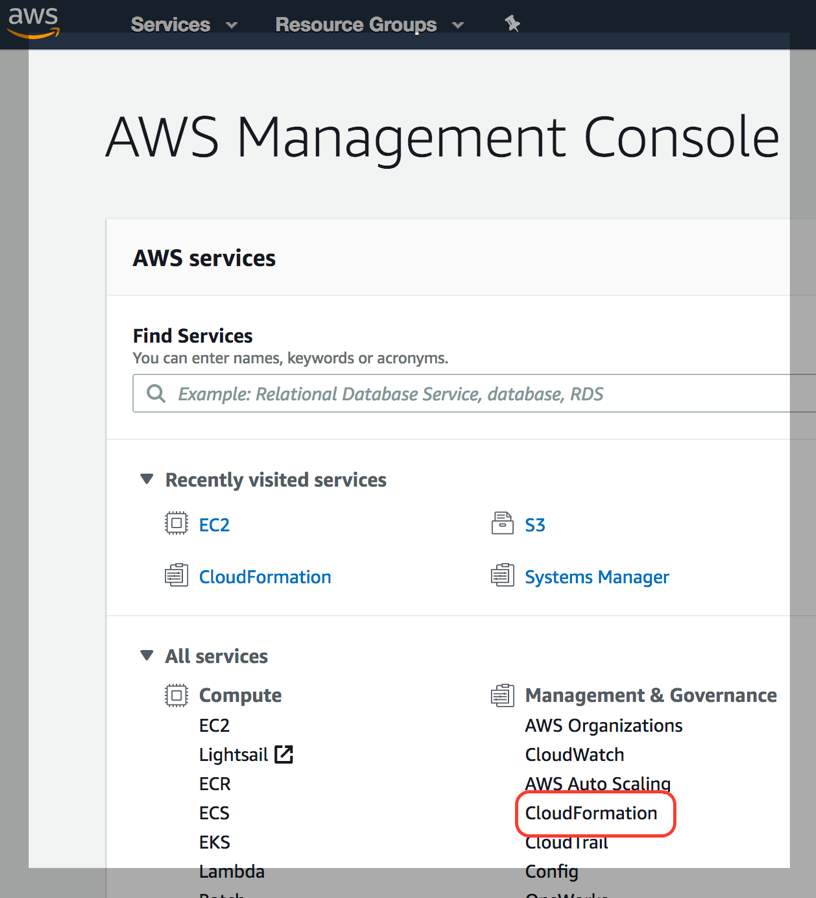
1. Scroll to the bottom of the page and hit **Next**.
2. Hit **Next** on “Configure stack options”
3. Scroll to the bottom of the page. Check **I acknowledge that AWS CloudFormation might create IAM resources with custom names.** and **I acknowledge that AWS Cloudformation might require the following capability: CAPABILITY\_AUTO\_EXPAND**, then click “Create”



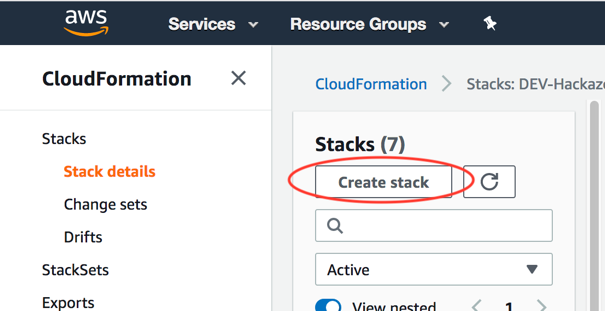
1. While you’re waiting for the stack turns to CREATE\_COMPLETE, let’s start on the next stack.

## Web Carter & Attacker workstation setup

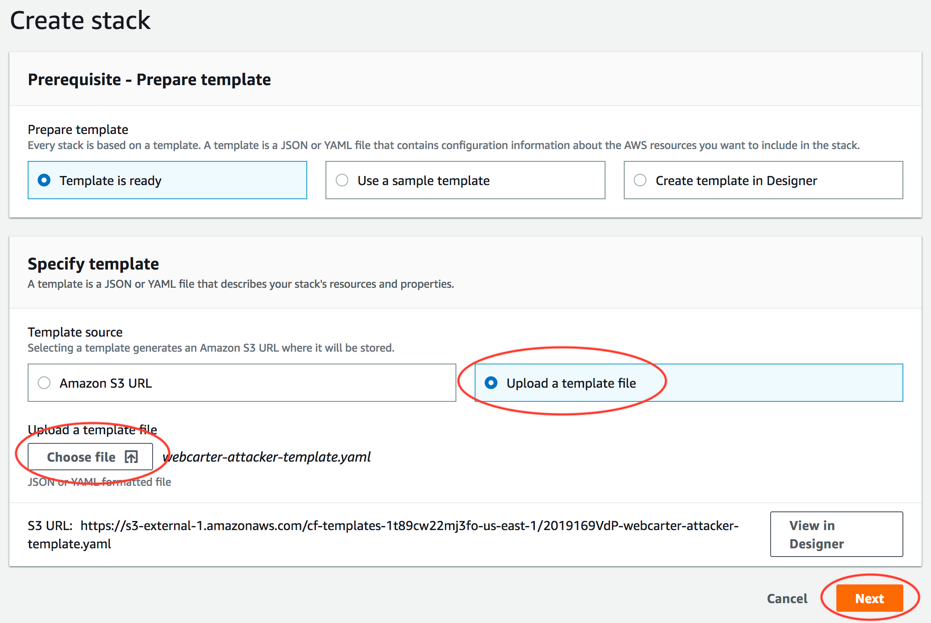
1. Open the Cloudformation console



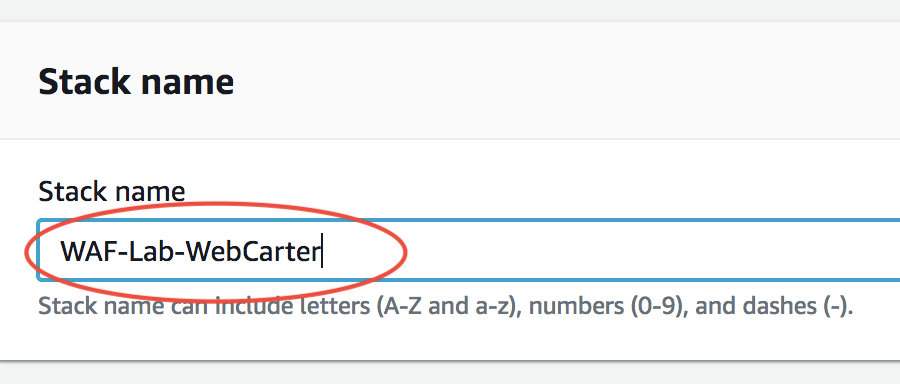
1. Create a new stack



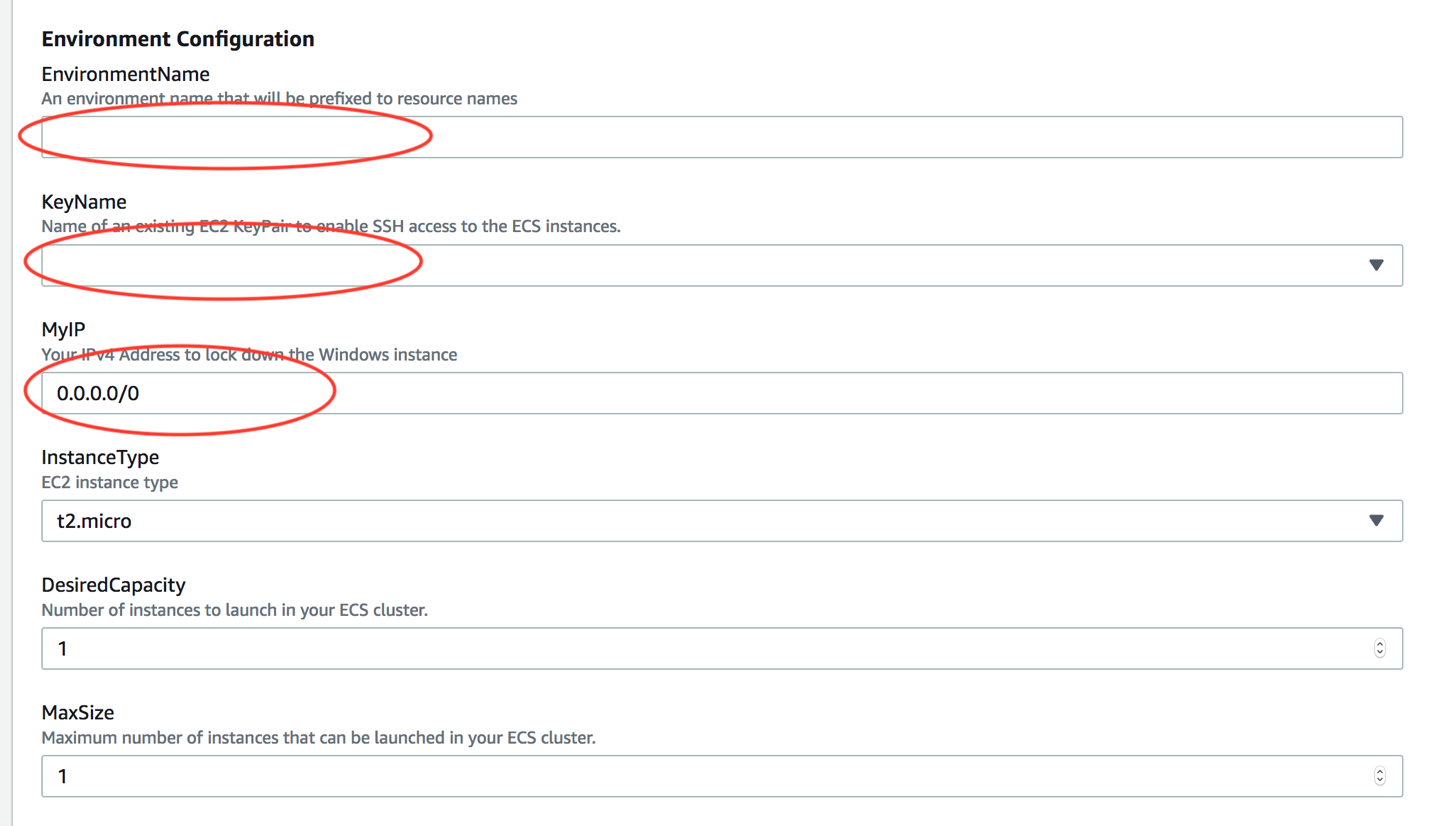
1. Upload stack template **template/webcarter-attacker-template.yaml**



1. Enter a stack name – e.g. “WAF-Lab-WebCarter”

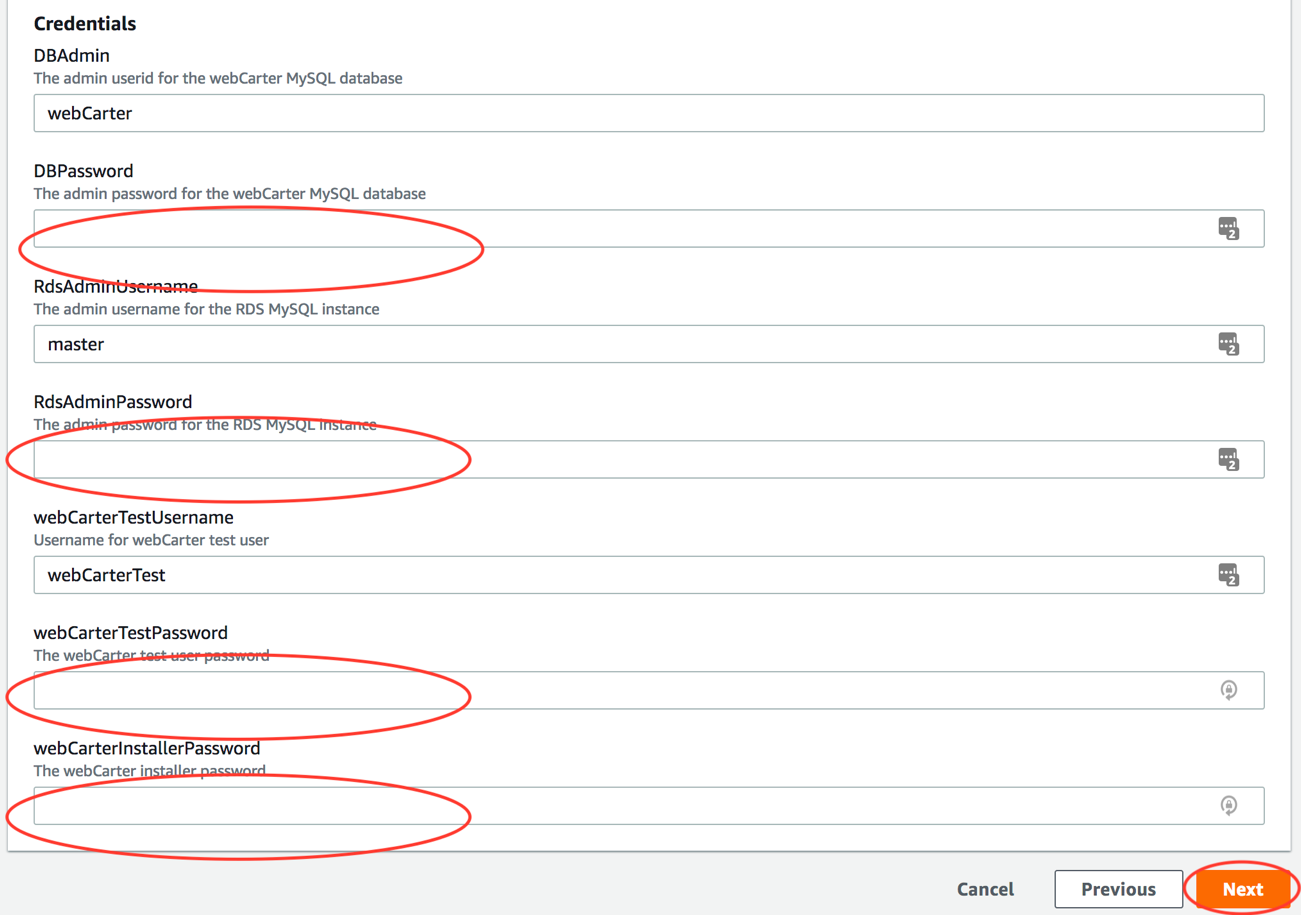


1. Enter the environmental configurations for the stack
   1. Your IP address from above
   2. An SSH in your inventory from EC2
   3. An environment tag (e.g. DEV or TEST or PROD)

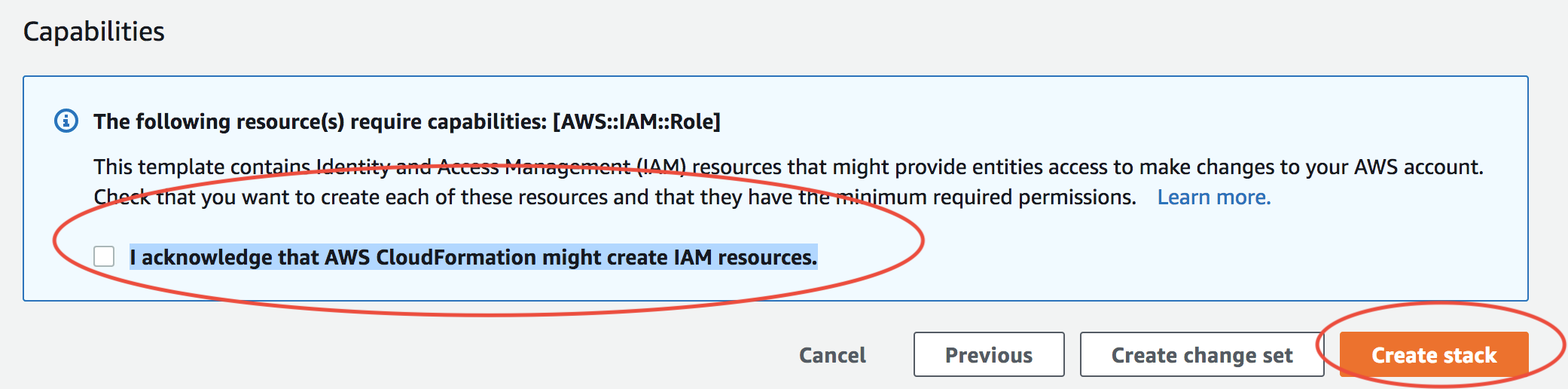


1. Enter passwords for the following credentials:
   1. RDS instance master password
   2. RDS database password
   3. Admin password
   4. Test user password

Scroll to the bottom of the page and hit **Next**



1. Scroll to the bottom of the page and hit **Next** on *Configure stack options* page
2. Scroll to the bottom of the page and check **I acknowledge that AWS CloudFormation might create IAM resources.**, the click **Create**



1. The stack will eventually turn to CREATE\_COMPLETE.