COALFIRE

Coalfire Technical Challenge

Before you begin, please note:

1. You must perform this challenge by yourself, no other persons may assist you.
2. Try to accomplish as many tasks as you can within the time period allotted. Quality of the implementation is an important factor.
3. You are strongly encouraged to search the web and use resources like Stack Overflow and GitHub. Please note in the write-up the URLs/sources you used for the final deliverable. The number of resources you use does not count negatively; we are interested in both the final product, as well as the process used to achieve said results.
4. If you are unsure on how to complete a task, or your implementation is not working, documenting the process you went through and what issues your ran into is also strongly encouraged as it highlights your thought process when posed with a challenge.
5. Do not post or share this Technical Challenge or information about it to the Internet. Each technical challenge has distinct differences and can be tied back to the individual who received it.

See scenario below and answer questions 1, 2 & 3 in relation to the scenario provided. Upon completing the challenge, please email your documentation and the link to your public GitHub repository to your technical recruiter. If you have further clarification questions, or issues, please notify us immediately.

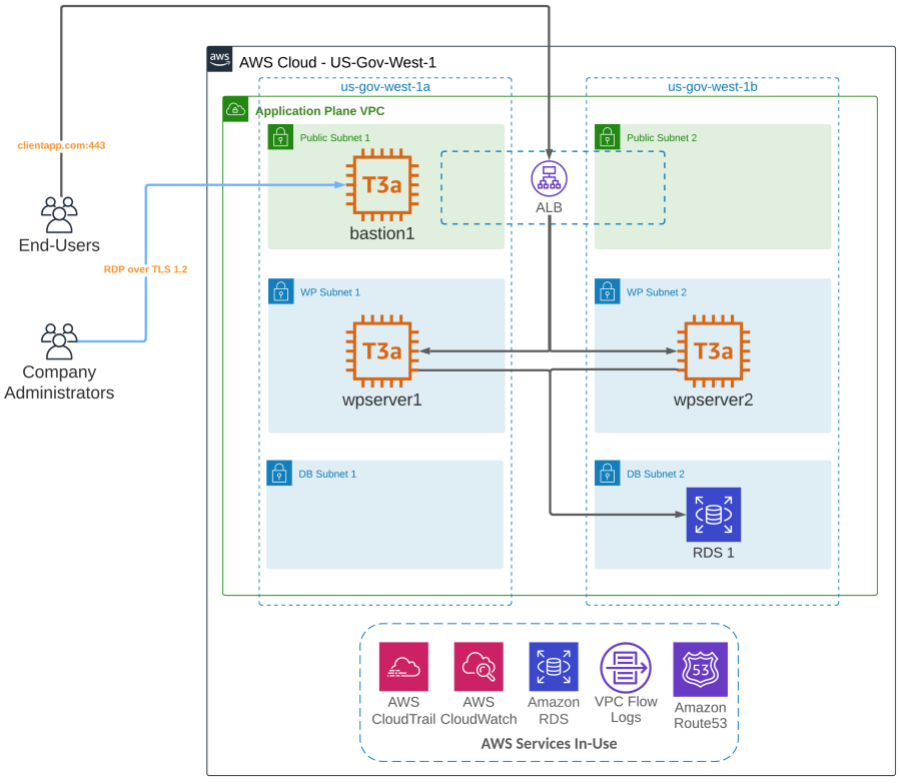
Scenario

A company has implemented the following Architecture to support one of their Applications in an AWS GovCloud environment.

The assumptions outlined below are assumed to be true, regarding the Cloud Infrastructure and Architecture.

- 1 VPC – 10.1.0.0/16
- 5 subnets (spread across two availability zones for high availability)
    - Public Subnet 1 – 10.1.0.0/24 (should be accessible from internet)
    - Public Subnet 2 – 10.1.1.0/24 (should be accessible from internet)
    - WP (Web Application) Subnet 1 – 10.1.2.0/24 (should NOT be accessible from internet)
    - WP (Web Application) Subnet 2 – 10.1.3.0/24 (should NOT be accessible from internet)
    - DB Subnet 1 – 10.1.4.0/24 (should NOT be accessible from internet)
    - DB Subnet 2 – 10.1.5.0/24 (should NOT be accessible from internet)
- 1 compute instance running Windows Server 2019 in subnet *Public Subnet 1*
    - 50 GB storage
    - t3a.medium
    - Hostname should “bastion1”
    - Public EIP associated (not reserved)
- 1 compute instance running RedHat in subnet *WP Subnet 1*
    - 20 GB storage
    - t3a.micro

    - Hostname should be “wpserver1”
- 1 compute instance running RedHat in subnet *WP Subnet 2*
    - 20 GB storage
    - t3a.micro
    - Hostname should be “wpserver2”
- 1 RDS PostgreSQL Databases running PostgreSQL 11 in subnet *DB Subnet 2*
    - db.t3.micro
    - DB Name should be “RDS1”
- 1 ALB that has listeners in subnets *Public Subnet 1 & 2*
    - listens on port 443/TCP
        - forwards traffic to the instance in subnet *WP Subnet 1*
- 1 CloudWatch Synthetics test is configured
    - "Web_Application_Alive" – This test attempts to access the web page from the external load balancer.
- Route53 is used to translate the company’s domain name to the ALB
- All Resources within the subnets have appropriate least-permissive Security Groups in place
- The company does not currently use any Infrastructure as Code (IaC) to manage their infrastructure via code
- The company has a SLA & SLO for the Application
    - SLA – 99.5% Availability
    - SLO – 99.9% Availability



Question 1

Assume now that you are an SRE who is responsible for maintaining the Availability & Uptime of the company's environment, which was described previously in the Scenario. At 4:35pm on Friday, there were reports of customers being unable to access the website coming in; at 4:35pm the "Web_Application_Alive" test began failing. Complete the following questions with a full, in-depth, and detailed write-up/response for each:

1. Describe the steps that you would take to begin debugging the problem, to determine what might be going on.
2. What metrics, monitoring, or other tooling/processes would you expect to have available within your monitoring system to identify and validate the infrastructure is performing in a functional, healthy state?
3. What changes or improvements could be made to the Architecture to reduce the risk of a similar incident?

Now that the issue was resolved, and the environment is back into a healthy state; complete the following:

1. Create an After-Action Report (Post-Mortem/Post-Incident Review). It should include, at minimum, the following sections (more is highly encouraged):
    a. High-level Summary
    b. Participants (include who would be invited to an After Action Report Discussion, as well other stakeholders who were involved in the incident)
    c. Timeline
    d. Root Cause Analysis

Question 2

Following the events that occurred, you've now been tasked additional SRE Tasks.

Document your solution – including any sources you used. You may be asked to walkthrough your solution as if presenting to a client.

Your final deliverables for this section will include: the codified solution, and your documentation. The structure, formatting, and language/tool used for the solution, as well as the structure and formatting of the documentation is up to you.

1. For example, after an audit, findings were published that identified several Compliance Controls were not implemented appropriately, nor were multiple Vulnerabilities remediated.

Create an appropriate solution that codifies and solves the issues and push the code to a public GitHub repository. Any detail that is not provided in the scenario is up to your discretion to include, or exclude. Use of Infrastructure as Code (Terraform), Scripts (PowerShell, BASH, Python, etc.), Playbooks (Ansible, Chef, Puppet, etc.), or Group Policy Objects (Windows), are preferred solutions.

Compliance Remediation (CIS Benchmark, Level 1 for: Windows Server 2019)

Host: bastion1 (Windows Server 2019)		
ID	**Name**	**Description**
1	2.2.21 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) - Guests, Local account and member of Administrators group	See CIS Benchmark Microsoft Windows Server 2019 L1 for more details: https://www.cisecurity.org/cis-benchmarks/#microsoft_windows_server
2	18.9.45.4.1.2 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured – '26190899-1602-49e8-8b27-eb1d0a1ce869	See CIS Benchmark Microsoft Windows Server 2019 L1 for more details: https://www.cisecurity.org/cis-benchmarks/#microsoft_windows_server

Question 3

The Client is interested in codifying their existing AWS infrastructure. As an SRE, you are well-positioned to assist the Client by developing the Terraform necessary to deploy the architecture described in the Scenario.

Document your solution – including any sources you used. You may be asked to walkthrough your solution as if presenting to a client.

Your final deliverables for this question will include: the codified solution, and your documentation. The structure, formatting, and language/tool used for the solution, as well as the structure and formatting of the documentation is up to you.

1. Create terraform code that creates the networking and compute constructs defined and push the code to a public GitHub repository. Any detail that isn't provided in the scenario is up to your discretion. Use of Terraform modules is highly encouraged.
2. Login to the web server instance in "WP Subnet 2" from the bastion host in "Public Subnet 1" and take a screenshot of the terminal logged in. Include this screenshot in your documentation.