F5 Essential App Protect - NGNIX Consolidation Documentation

F5 Networks, Inc.

Oct 08, 2020

F5 2020 Read The Docs Guide

F5 Read The Docs

F5 Networks, Inc.

1

1.1 Or, my limited attempt at it. . .

Welcome! This is a reference architecture document/site that shows the writers attempt at demostrating the use of Site Reliability Engineering techinical principals using a compination of F5/NGINX products and Open Source Software (OSS).

Thanks in advance dear reader for wandering into this corner of the ‘net and, hopefully, you’ll gleen something of use for yourself.

As always, this is just my attempt at a thought exercise on how things can be applied and is in no way reflective of the views, opinions or organisation ethos of F5 Networks.

So I will leave you dear reader, with the usual warning - do not attempt anything contained within on production networks or systems and that this is purely a theoretical techinical approach that can be referenced for insights into you own infrastructure.

Be well, always, and take care - now that we have the basics out of the way. Lets dive in shall we?

This is a holding page for code here: https://github.com/merps/f5devops/tree/f5-sre-demo/terraform/f5-sre-demo

2

2.1 Purpose

This design document/site provides details of the solution architecture of F5 Network products and platform deployment that aligns with the Centre for Internet (CIS) Security Level 1 Foundations and reference to F5 Secure Cloud Architecture (SCA).

Content of this document was collated, documented and built during Q3CY20 for the July 2020 Customer Experience Seminar webinar hosted in the ASEAN region.

Included within this document/site is all the information pertaining to the build and operation of the SRE Observability demonstration environment.

2.2 How to use this document

This SRE Solution Definition (SRE-SD) is to be used in conjunction with the relevant deployment guides and reference Concurrent Version System (CVS) repositories.

Throughout this SRE-SD there will be references to where additional detailed information can be found and this will also be provided within the References section of this document/site.

2.3 Intended Audience

This document/site is primarly written for the following:

- **Architects**
  - Enterprise
  - Security
  - Cloud
- Business Application stakeholders
- Operational & SRE Teams
- DevOps & NetOps leads

3

3.1 Customer Profile

A random name for a random organisation and ABC Co. is **truly** overused, this example customer operates in the Large SMB market that has an Public Internet precense for online training and marketting.

It is estatimated that MeBeFake has over 500 staff and are looking to begin their multi-cloud journey with a three (3) year plan of to have sixty (60) percent of workloads bursting to CSP environments.

3.2 Customer Objectives

In a galaxy far, far, away someone had a *terrible* idea of creating a php application called Customer Application Portal (CAP - *yes, I am a sadist*). Customer MeBeFake (MBF) currently hosts **'ne1MBF, CAP'**, Customer Portal Application, on-premises an the primary objects of this solution is to:

1) Provision Infrastucture as Code (IaC) for CSP's
2) Provide Integration of a Cloud Agnostic SaaS SRE solution
3) Reduce *'tool-sprawl'*, Infrastucture and management overheads through manual processes.

3.3 Scope of Services

MeBeFake has nominated the on-premises application *'ne1MBF'* as the Lighthouse application for the operational theoretical exercise as per previously listed objectives.

As such this document/site will be divided into two (2) distinct sections;

1) **On-premises**
    a) Production Workload Discovery
    b) Production Automation (IaC & CI/CD flows) of Lighthouse Application Stack
    c) SRE Solution Integration of On-premises
2) **AWS Deployment (CSP)**
    a) Production environment for hosting public facing workloads

b) Shared Services for hosting/deploying applications
c) NonProduction environments for Development/Testing
d) Management & Audit (SecOps) environment
e) Production Automation extension from on-premises to CSP
f) SRE Solution integration extension.

3.4 Scope of Exclusion

The following items are out-of-scope for SRE Observibility deployment:

1) Coffee, *there just isn't enough to go around*
2) Implimentation of CAP and supporting SSO/2FA integration
3) Implimentation of, yeah, something for later I guess.

3.5 Assumptions

The following assuptions have been made during the implimentation of the Lighthouse Application - *'ne1MBF'* - for this SRE Observibility project:

- the reader, yes - you, has an understanding of the following:
  a) Linux - SysOp experience
  b) **Automation;**
     1) Terraform
     2) AWS CLi
     3) GitLab/GitHub (CI/CD)
     4) Scripting languages
     5) Docker
  c) Network, specificlly F5/NGINX
  d) **Monitoring;**
     1) syslog-ng
     2) telegraf & influxdb
     3) telemetry streaming
- *ability to rtfm*

4

MeBeFake has currently has hosted infrastructure and application stacks in CoLo Data Centres at IBM Cumberland and FujiXerox Macquarie Park that is approaching capacity. SRE Observability of the current infrastructure and the expansion to Amazon Web Services will address the immediate resource constraints.

4.1 Solution Platform

The solution is a Self-Managed platform currently established On-premises using a mix of physical and virtualised infrastructure and the expansion to Amazon Web Services (AWS) Public Cloud will allow the flexibility to extend MeBeFake company security, continuity and scalability ethos.

MeBeFake SRE team develops, deploys and maintains the current On-premises *ne1MBF* application Stacks, this allows MeBeFake to have full control of the application stack providing best flexibility for the solution.

The SRE Managed On-premsise and AWS Platform provides infrastructure in a customisable multi-cloud environments.

4.1.1 AWS CSP Environment

MeBeFake Cloud environments consist will be a mix of the following covered in the scope of this or solution:

- Amazon Virtual Private Cloud (VPC) for virtual networks
- Amazon Elastic Cloud Compute (EC2) for virtual machines
- Amazon Elastic Block Storage (EBS) for block storage
- Amazon Simple Storage Service (S3) for object storage
- F5 BIGIP & NGINX for ADC & Security services.

4.1.2 On-premise Environment

MeBeFake environments consist will be a mix of the following covered in the scope of this solution:

- VMware vRealize Operations Cloud
- VMware vSphere 6.7

- NetApp FAS Storage Arrays
- F5 & Ubiquiti network appliances

4.1.3 F5aaS CloudServices (SaaS)

MeBeFake will leverage the following SaaS offerings to extend both On-premises and AWS Cloud environments;

- Beacon
- Essentials App Protect (EAP)
- DNS Services (DNS)
- DNS LoadBalancers (DNSLB)

The Platform will extend current on-premises environments to AWS and will consist of 4 VPCs for Production, Development, Shared Services and Security Operations Services. Each of these VPCs have high speed dedicated network connections to the AWS DirectConnect (DX) from both IBM Cumberland and FujiXerox Macquarie Park DC's.

The Platform subsequently has connectivity with the MeBeFake on-premise CoLo environments levering both PIPE networks and GlobalSwitch. Each of the VPCs span across three AWS Availability Zones (Data Centres) in the Sydney Region for high availability.

The solution includes a fully managed service consisting of:

- Incident Management
- Configuration Management
- Patch Management
- Monitoring
- Auditing and Logging
- Management of AWS Security Groups
- Backup as a Service

4.2 Systems and Solutions

MeBeFake SRE team will include supporting both On-Premise Cloud Infrastructure and Guest Server Operating Systems. This includes management tools for patch management, anti-virus management, monitoring and logging of the lighthouse application.

While the underlying Infrastructure. network and server Operating Systems of the OnPremises Systems to the existing Infrastructure teams the development of MeBeFake SRE team for SRE Observibility project journey will also assist in the transition for OnPremises Infrastructure development pipelines.

Systems that are outside of MeBeFake's SRE project scope are the following OnPremises systems:

- Oracle Business Objects
- SAP HR
- SharePoint
- Windows Infrastructure

5

This section of the *ne1MBF* MeBeFake's AWS deployment and is broken down into the following sections:

5.1 Network Overview

The MeBeFake SRE AWS Platform consists of four AWS VPCs (Virtual Private Clouds) for Production, Development, Shared Services and Security Operations Services each VPC has layer 3 interconnects (using AWS TransitGateway) to IBM Cumberland and FujiXerox Macquarie Park DC's.

5.2 VPCs

AWS Virtual Private Cloud (VPC) is an isolated virtual network in AWS. This virtual network enables MeBeFake to manage the resources allocation inside the established VPCs including implementing a secure access between MeBeFake and AWS data centres.

MeBeFake's strategy on VPC is to utilise the Multi-VPC approach. This approach enables MeBeFake to set isolated boundaries based on core services being provided. This effectively establishes VPC as a foundational platform in the MeBeFake SRE-Managed AWS platform of which workloads will be placed into.

The VPC structure is outlined as follows:

VPC Name	Description	TransitGateway Interconnect
Production **(PRD)**	A VPC containing the Visy production and UAT environments	Yes
Development (DEV)	A VPC containing MeBeFake's development and test environments	Yes
Shared Services (SHARE)	A VPC containing MeBeFake's SRE shared services that hosts MeBeFake's CI/CD framework and other services such as ActiveDirectory	Yes
Security Operations (SecOps)	A VPC that is used for SRE Management and Audit Operational Services. This VPC also provides centralised management services.	No

An AWS Virtual Private Cloud (VPC) allows an isolated virtual network created in AWS. The address range is allocated per RFC1918 with the largest address range for a VPC being a /16 subnet. Inside a VPC, subnets are deployed in multiple availability zones (AZs) to provide support for a highly available applications architecture. Multiple subnets are required to separate public, private and protected subnets.

The following table highlights the network allocation for each VPC in-scope for the MeBeFake SRE- Managed AWS Platform.

Region	VPC	Network	CIDR Mask	Usable IP's
Sydney	PRD	10.92.0.0	/18	16378
	DEV	10.92.64.0	/18	16378
	SHARE	10.92.128.0	/18	16378
	SecOps	10.92.192.0	/18	16378

5.3 Subnets

The following section defines the overall subnets placement for MeBeFake's SRE Managed AWS cloud platform. Subnets design is key to MeBeFake AWS implementation as it sets a foundation for MeBeFake's infrastructure on the AWS platform. Hence any modification should be minimised where possible to prevent additional costs to migrate workloads.

Further to this, MeBeFake is establishing a pattern for each VPC to simplify overall network architecture, ensure consistency and aid repeatability. Three logical tiers are proposed: public, private and protected as follows:

Tier	Description
Public tier	The Public tier will include Public subnets. This subnet type is targeted for instances that support inbound connections from the internet through an AWS Internet Gateway (for example, Web Application Firewall (WAF) servers). Public subnets have been provisioned in anticipation that internet facing workloads will be deployed to these subnets in the future
Private tier	The Private tier will include Private subnets. This subnet type is targeted for internal web servers and application servers that have private IP addresses. Instances in a Private subnet will not support inbound internet connections.
Protected tier	Instances in a Private subnet are accessible to MeBeFake on-premise networks. The Protected tier will include Protected subnets. This subnet type is designated for EC2 instances with database(s) and can only be accessed by servers in the Private tier.

For detailed Network Subnet definitions please refer to the Network Subnets tab in the *ne1MBF* Data spreadsheet.

5.4 ACL's

Network access control lists (ACL), are an optional layer of security within the VPC layer. They are stateless (return traffic must be allowed by rules) firewalls for controlling traffic entering and leaving the subnets. Security Groups provide much better security controls at a more granular level with better debug capabilities than Network ACLs and therefore ACLs will not be used beyond the default allow settings.

5.5 Security Groups

Security groups are a stateful firewall used to control traffic entering or leaving an instance or groups of instances. Outbound traffic for all EC2 instances will be allowed out without filtering, however for Inbound traffic connections will be restricted to improve instance security

MeBeFake Security Group Standards:

- **Instances will generally belong to the following security groups:**
  - Default security group (per tier) or a workload specific security group
  - Management security group – allows incoming traffic for management/shared services
- **Default security groups are as follows:**
  - Private Default security group – allows/filters incoming traffic from the Public
  - Default security group, allows/filters incoming traffic from on-premise networks
  - Protected Default security group – allows/filters incoming traffic from the Private security group
  - Within a default security group instances allow incoming traffic from all other instances in the same security group

Through SRE Service Requests custom security groups can be created and updates to existing security groups can be made.

For detailed Network Security Groups definitions please refer to the Security Groups tab in the *ne1MBF* Data spreadsheet.

6

6.1 Or, my limited attempt at it. . .

To Be Completed