F5 Cloud Recommendations - UWA Documentation

F5 Networks, Inc.

May 26, 2020

F5 2020 Read The Docs Guide

F5 Read The Docs

F5 Networks, Inc.

1

1.1 UWA - Ingest VNET.

The approach, BIG-IP VE HA pair load balancing for the transit VNET, deployed with HA Failover via LB template can easily fit into existing infrastructure without asking the customer to re-architect the entire infrastructure. Of course, the main requirement of this use case is that SNAT is allowed when traffic reaches the F5 BIG-IP VE's.

1.1.1 Benefits

- This solution works for both Reverse and Forward proxies use cases
- Minimal affect to the customer's existing setup
- All the same benefits as HA failover-via LB solution

1.1.2 Requirements:

- SNAT is required
- Azure Native Internal load balancer

Following these deployment patterns it enables native Azure functionality, this includes the integration into Azure Security Center and consolidation logging framework that aligns the previously mentioned Cloud Security posture.

1.2 Application Deployment Lifecycle.

As with all Cloud Journeys this document will outline the each stage and how F5's vision of Code-To-Customer, it will be broken down into the following stages:

- *Provisioning*
- *Configuration*
- *Monitoring & Analytics*
- *Backup and Restoration*

With each stage outlined and tools details recommendations will be made of the Code-To-Customer approach.

1.3 Provisioning

1.3.1 ARM Templates

Using Azure ARM templates it is possible to create a high availability (active-active/active-standby) pair of BIG-IP VE instances in Microsoft Azure. F5 Networks have grouped the available templates into the following categories:

Standalone

These templates are used to deploy a single BIG-IP VE, these are primarily used for development testing or replacing/upgrading instances that form part of traditional fail-over clusters.

Failover

These templates are designed for the deployment of more that one BIG-IP VE in a ScaleN cluster, this would be similar to UWA existing, traditional, deployment methodologies. These clusters are primary deployed in replication of traditional Active/Standby BIG-IP deployments, in the case of UWA the nominated deployment pattern is from active/active.

Autoscale

These template types deploy a group of BIG-IP VE's that scale in and out based on thresholds nominated, BIG-IP VE's are all deployed as Active and are primarily used to scale out an individual L7 service on a single wildcard virtual. Addition services can be provisioned using port remapping for these, these types of deployments rely upstream service to distribute traffic like DNS/GSLB or a platform's built-in load balancer.

With the recommended configuration of Active/Active, **SourceNAT** is needed to ensure the egress traffic traverse the same ingress BIG-IP. Another, more advanced, alternative is to use Direct Server Return (DSR) in Azure LB that means that the Azure LB will not perform *Destination* NAT on the traffic which will arrive at the backend pool with the correct *destination* IP address, this is commonly used in scenarios that require 1 VIP per application within BIG-IP Cluster.

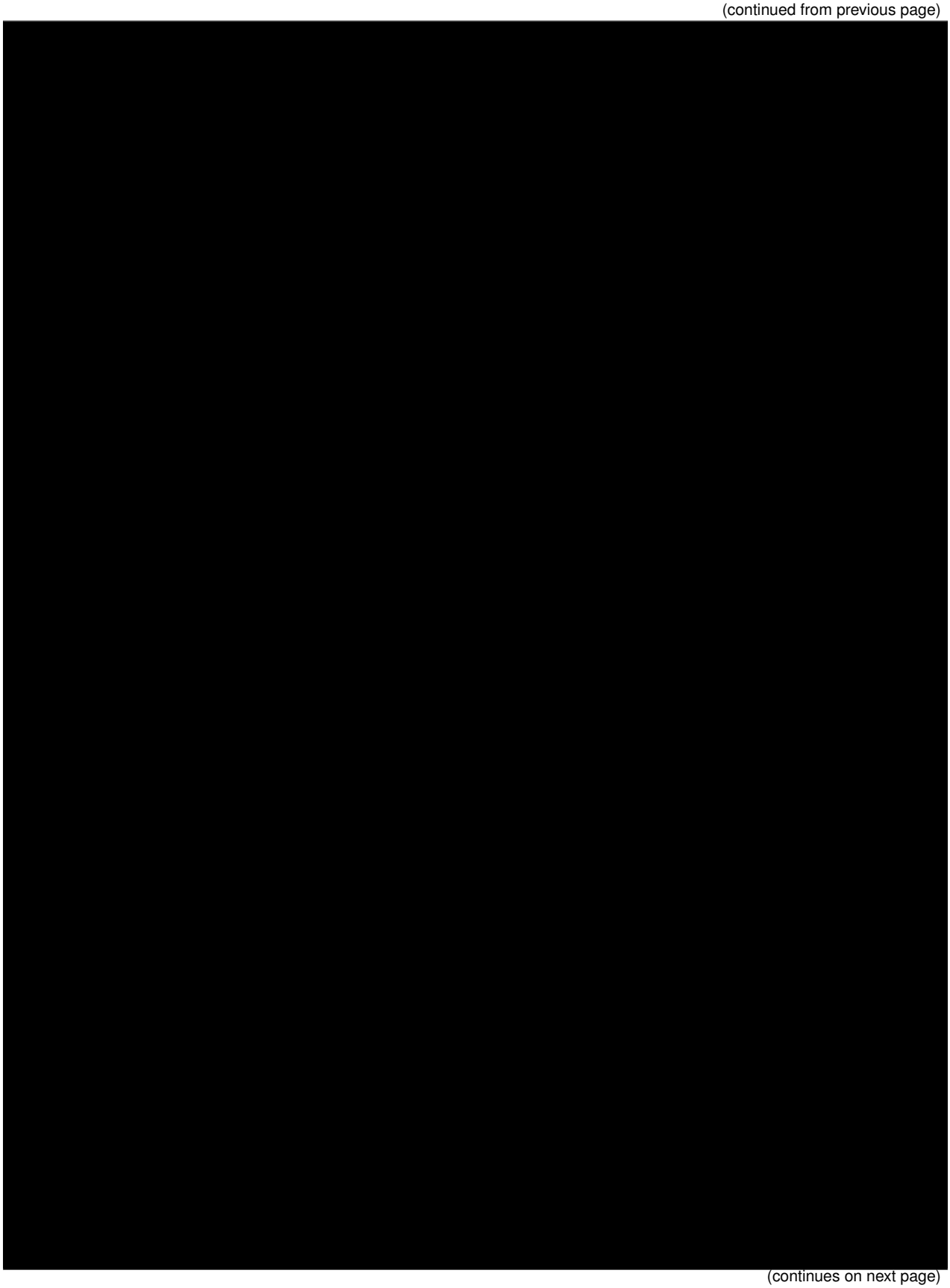
1.3.2 Declarative Onboarding (DO)

F5 Declarative Onboarding (DO)?is an F5 offering that provides a framework to automate BIG-IP onboarding?via Declarative REST APIs. Similar to AS3, DO?provides a foundation to enable F5's Infrastructure as Code (IaC) deployment methodologies.

DO automates L1-L3 on-boarding for BIG-IP, making BIG-IP available on the network and ready to accept L4-L7 Application Services configurations. The following example declaration on-boards a clustered BIG-IP system, further explanation of this can be found locate at Composing a Declarative Onboarding declaration for a cluster of BIG-IPs.

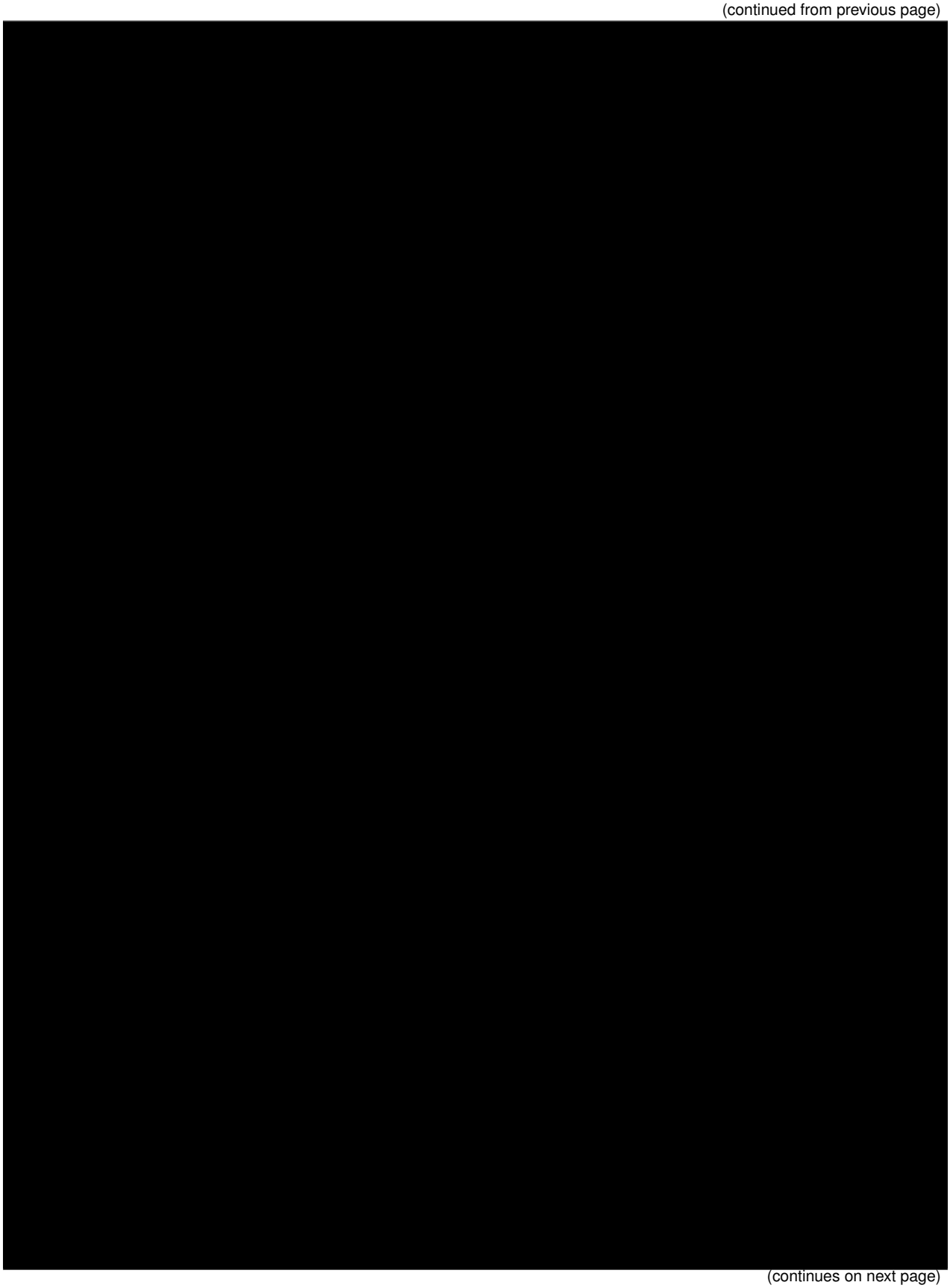
(continues on next page)

(continued from previous page)



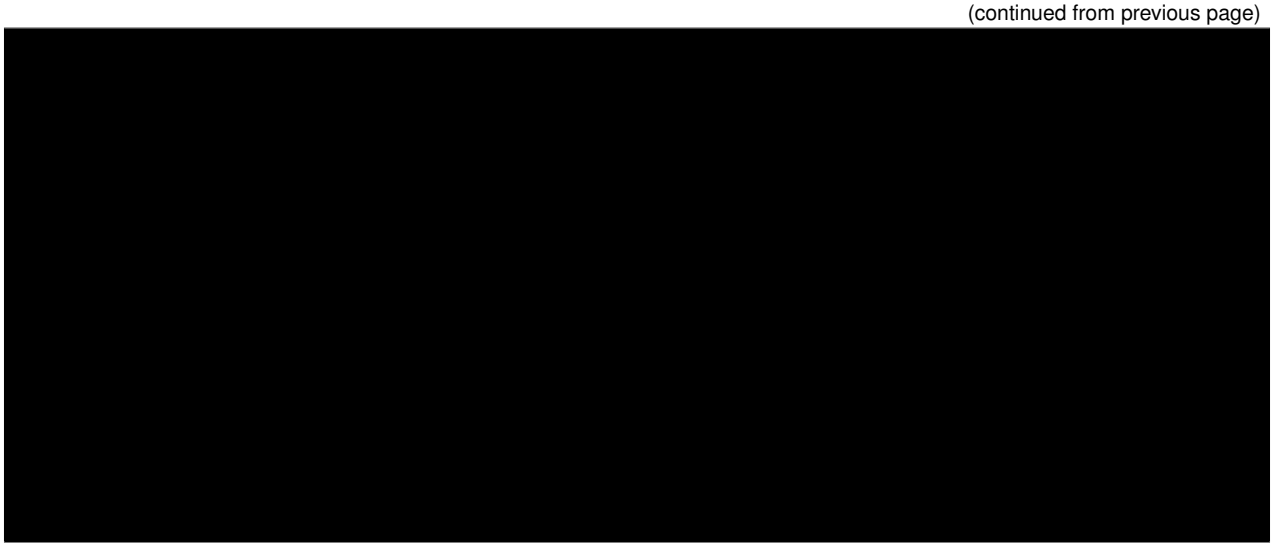
(continues on next page)

(continued from previous page)



(continues on next page)

(continued from previous page)



1.4 Configuration

F5 BIG-IP VE's, once deployed, may be configured to either suit UWA DevOps methodology levering Azure DevOps or in-house deployment pipelines. As with the variations of provisioning of BIG-IP VE's, the same variety exists to suit the provisioning of application services such as;

- *F5 Application Services Templates (FAST)*
- *Application Services 3 Extension (AS3)*
- *Ansible*
- *HashiCorp*

1.4.1 F5 Application Services Templates (FAST)

F5 FAST, provides a way to streamline deployment of AS3 applications onto BIG-IP using AS3 deployment patterns, or templates. FAST is the next phase of evolution for F5, unlocking new capabilities, aligning to multi-cloud, injecting automation, and empowering customers with our best-in-class application services.

This allows, through the use of a tabbed gui within the BIG-IP console, the construction of Virtual Server configuration that produces a AS3 declaration that can be copied, committed to source or templates to be set as AS3 payloads on REST API operations.

Further information, how-to's and additional examples are located at the FAST documentation site.

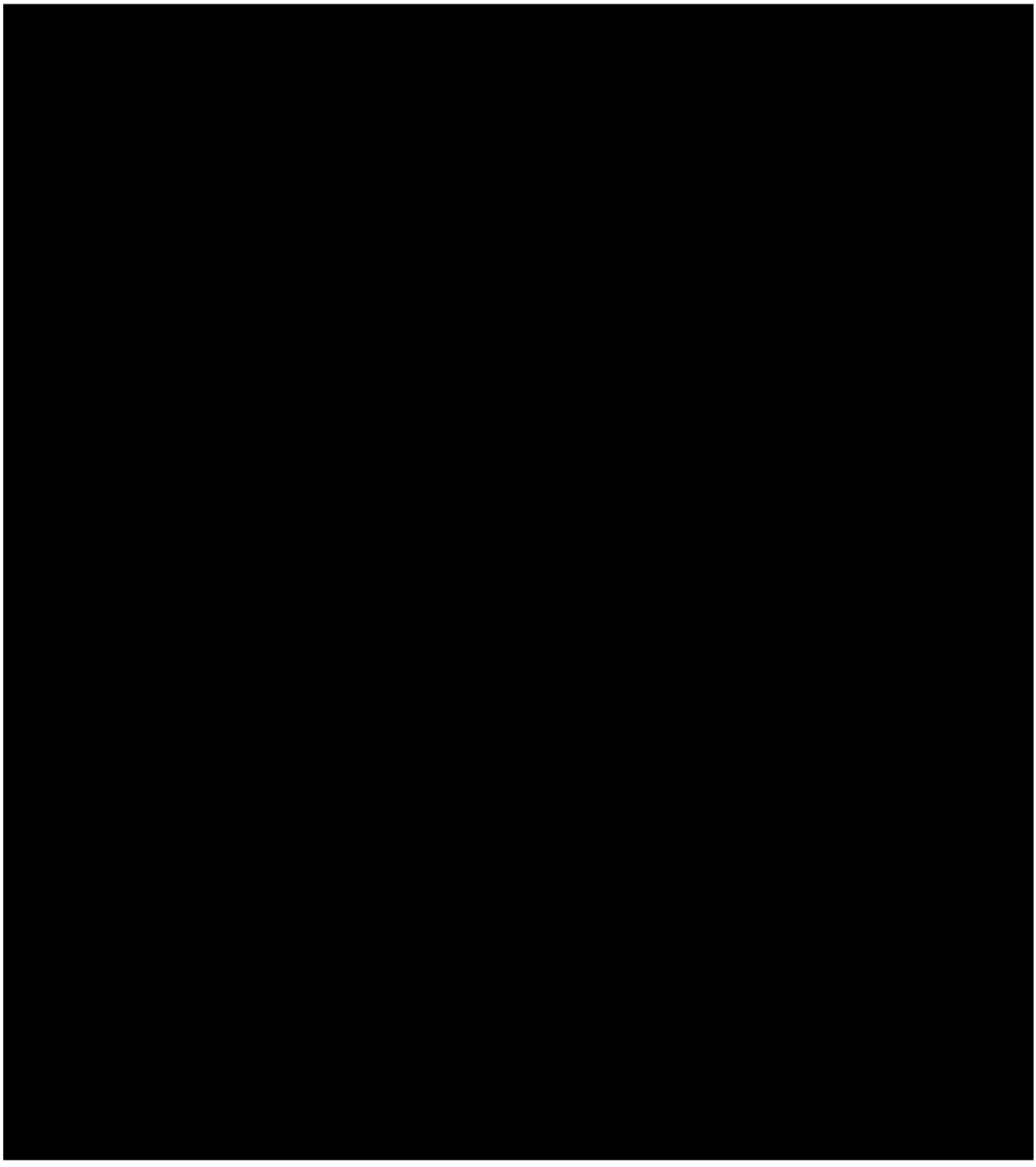
1.4.2 Application Services 3 Extension (AS3)

Application Services 3 Extension is a flexible, low-overhead mechanism for managing application-specific configurations on a BIG-IP system. AS3 uses a declarative model, meaning you provide a JSON declaration rather than a set of imperative commands.

The declaration represents the configuration which AS3 creates on a BIG-IP system. AS3 is well-defined according to the rules of JSON Schema, and declarations validate according to JSON Schema. AS3 accepts declaration updates via REST (push), reference (pull), or CLI (flat file editing).

An example AS3 is as follows, this contains;

- Partition (Tenant) named *Sample_http_01*
- HTTP VIP called *servceMain*
- A pool named *web_pool*
- Persistence provide based on JSESSIONID cookie



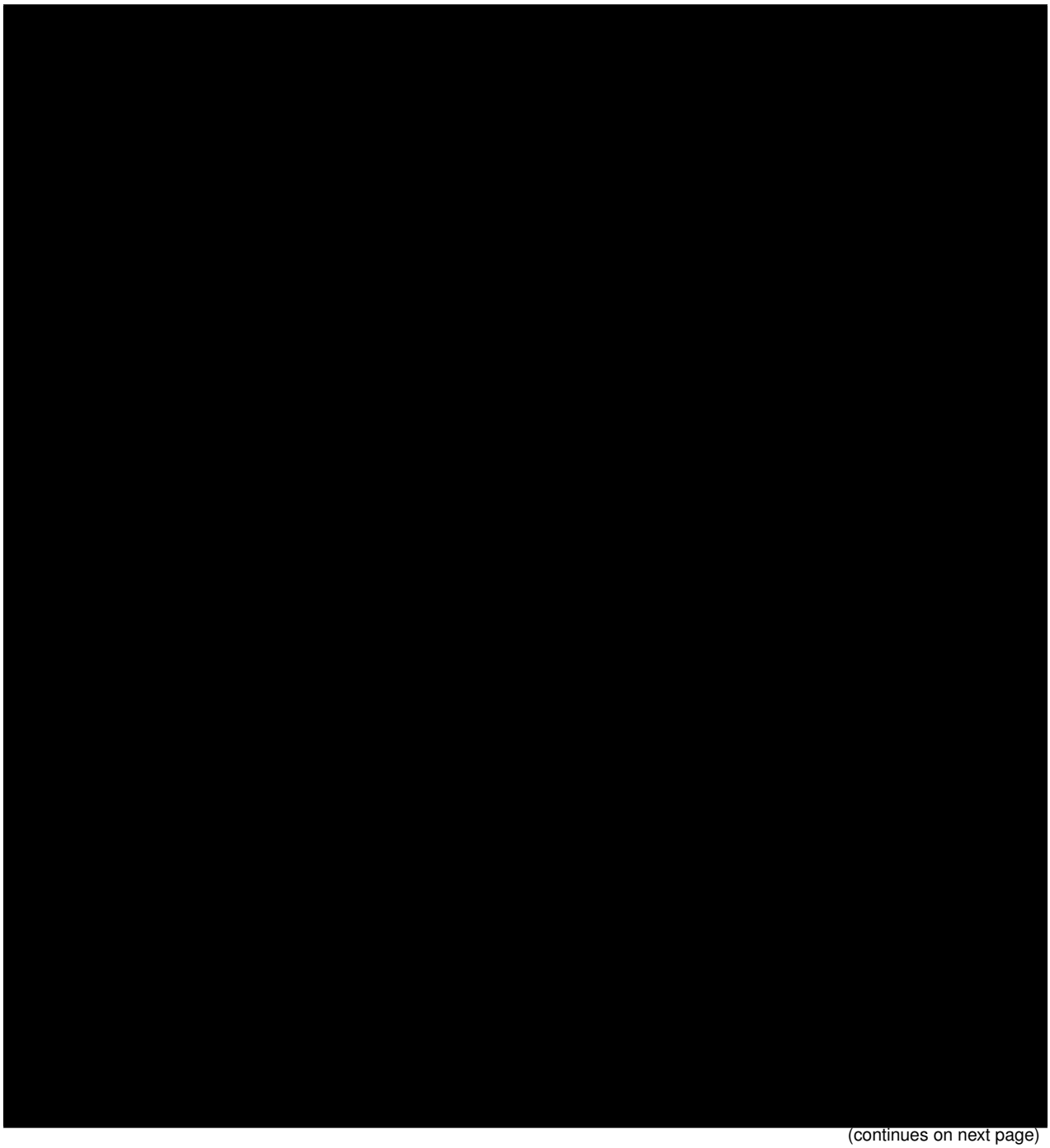
Further information, along with VSCode Schema validation, is currently located at Application Services 3

Extension Documentation

1.4.3 Ansible

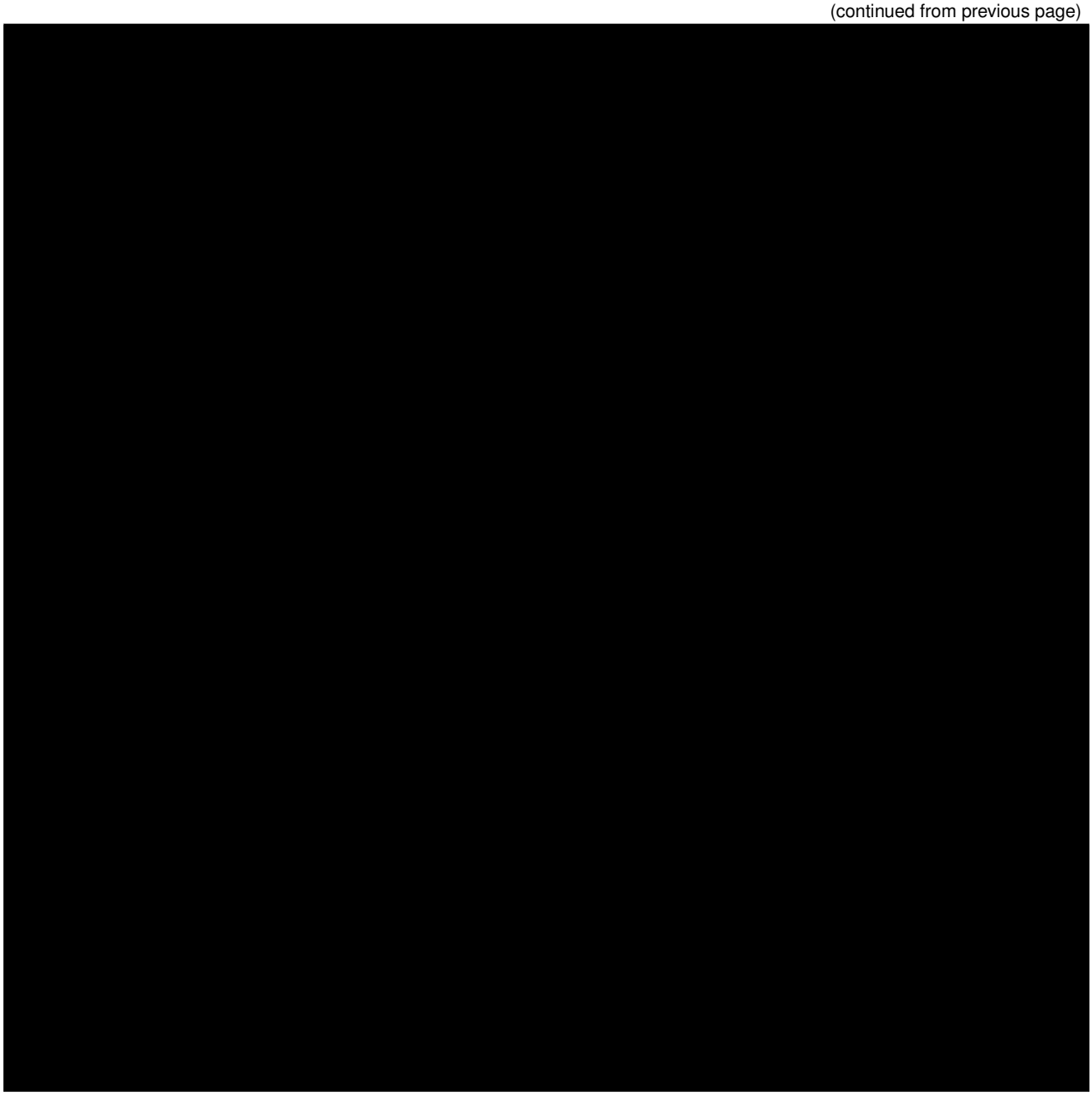
BIP-IP's, both physical and virtual appliances, can also be provisioned, configured and managed with the application-deployment tool Anisble. From Ansible 2.9+ BIG-IP and BIG-IQ supports Ansible Galaxy, a website - Galaxy - where users can obtain collection of roles that also support F5 Ansible Galaxy Modules

An example Ansible playbook declaration for configuration HA Pair of BIG-IP's, Ansible templates - as below - using Jinja2



(continues on next page)

(continued from previous page)



Further information, along with further references are located;

- Ansible Playbooks
- Ansible Tower
- AWX

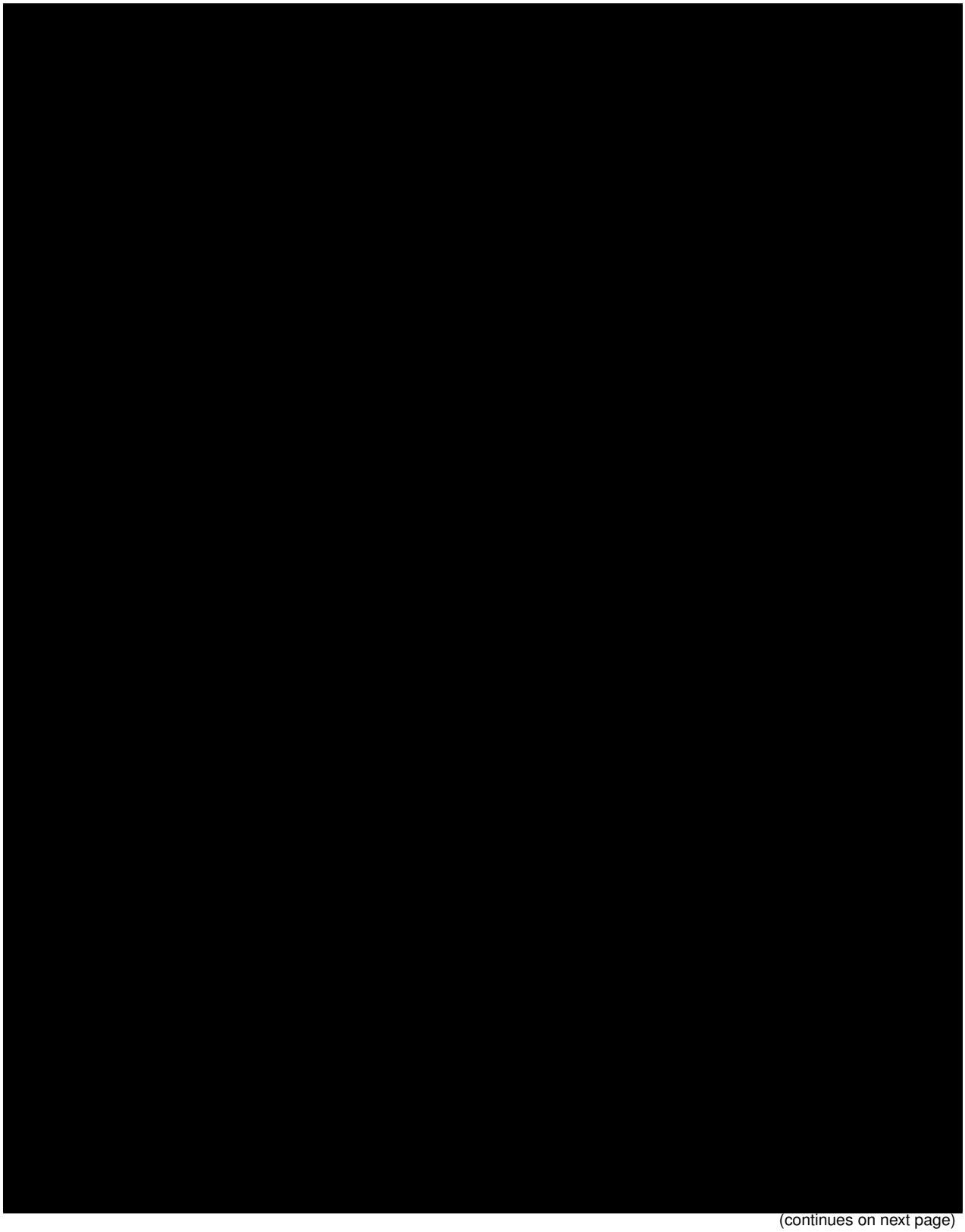
Or how to run F5 Ansible Playbooks for Tower and AWX.

1.4.4 HashiCorp

HashiCorp, the creators of Terraform OpenSource IaC, also have Terraform Cloud, the enterprise offering that supports divisions along with MFA and SSO, that incorporates Sentinel that enables the shift to multi-

cloud infrastructure. Like DO, AS3 and Ansible Terraform also support DevOps pipelines and GitFlow.

An example Terraform Plan, *main.tf*, is defined as follows;



(continues on next page)

(continued from previous page)

Further information on the use of Terraform;

- Modules
- Providers

along with F5 Terraform Resources that can also be found on F5 CloudDocs.

1.5 Monitoring & Analytics

1.5.1 F5 Automation Tool Chain - Telemetry Streaming (TS)

Consistent with IaC, Telemetry Streaming (TS) is F5 Networks JSON declarative model of streaming events and statistics to the customers preferred data visualization, it also supports native integration with both Microsoft Azure Log Analytics and Azure Application Insights along with other known logging solutions.

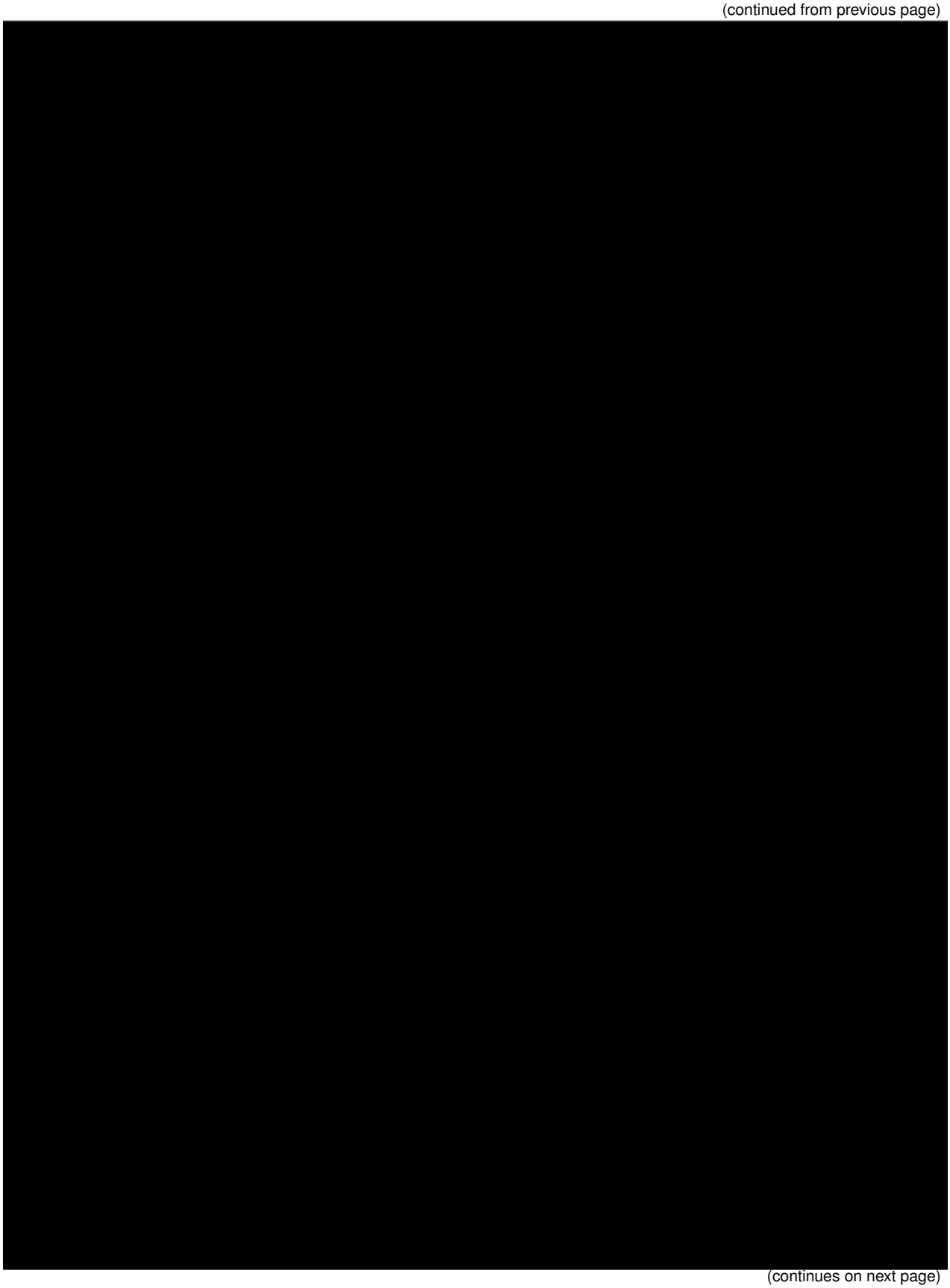
For complete visibility BIG-IP and TS also integrate with Azure Sentinel.

F5 Telemetry Streaming also provides metrics and analytics to F5-aaS Cloud Offers along with rich application insights and understanding when deployed alongside BIG-IQ Centralised Management (CM).

An example stanza for the configuration and declaration of TS is as follows:

(continues on next page)

(continued from previous page)



(continues on next page)

(continued from previous page)

The previous TS example creates a Virtual Server (VS) local listener on the BIG-IP appliance, port 6517, then a system poller with an interval of 60 seconds on port 8100 then finally configures three consumers of TS:

- F5a-aaS Beacon
- StatsD local listener
- ElasticSearch Indexes.

BIG-IP High Speed Logging (HSL) shares a similar framework to that of Telemetry Streaming, this enables an ease of upgrade from HSL deployment. Telemetry Streaming also support the redaction/masking of information on instance.

1.6 Backup and Restoration

As with all Cloud Journeys the requirements for the backup and restoration of configuration is nullified to align with Cloud Native Immutable Infrastructure Principals.

> _"The gold standard for cloud infrastructure is for it be able to be provisioned without any assistance. The tools that provision that infrastructure should accept declarative configuration as inputs."_

F5 Automated Tool Chain combined with Azure ARM templates enables the ease of secure deployments in an agile manner, if the both the workload and data classification require it F5 Networks Secure Cloud Architecture (SCA) Solutions.

As with migrations, workload components need configuration up-lifted or refreshed and understanding this F5 offers assistance through both professional services and community channels within Slack or GitHub.

1.7 Recommendations

With cloud to align with the elasticity and immutability I believe that operating in the cloud requires automation, therefore one should not shy away from automated updates to User Defined Routing (UDR's) given that tools such as F5's Cloud Failover Extension (CFE) to be native with mature cloud operations.

The use of BIG-IP v15.1.x also brings support for Accelerated Networking on Azure that has support for SR-IOV, also improvements to cloud-init both an upgrade to version 18.5 and additional support two custom modules, Set password and TMOS Declared. Using these modules you can change the built-in TMOS admin and root passwords and leverage F5 Automation Toolchain (including, Declarative Onboarding and F5 Application Services Extension) respectively.

BIG-IP v15.1.x also brings support for the previously mention *F5 Application Services Templates (FAST)* that allows the creation application templates for virtual server configuration and for these to be deployed as AS3 applications.

With outbound traffic traversing the BIG-IP as per the 3nic deployment pattern, it allows for the inspection, analysis, securing, etc - not only because it allows apps to see the true source IP.

Finally, best practices to follow when on the early stages of a cloud journey;

- use of GitFlow or Git Branching DevOps
- use CI/CD tools, Azure DevOps, for speed of deployments
- template based deployments both non-prod and prod (IaC)
- use of DO and AS3 to keep configuration off box
- App & Dev teams configuring partitioned BIG-IP using declarative deployments.

1.8 Conclusion

As it has been touched on there is multiple ways to deploy and dictate the architectural requirements of individual workloads, in a immutable declarative way that removes the need for break-glass and ClickOps configuration steps.

By framing the application flows/workloads as a series of objects rather than a single blob/entity it allows this flow, Code to Customer, to be simplified in all stages of the applications life-cycle.