AGILITY
Best Practices for Deploying F5 in Azure

PRESENTED BY:
Jeff Stathatos: Cloud Solution Architect
Gary Lu: Cloud System Engineer
Overview

• Why F5 in Azure
• F5 Products in Azure
• VE Sizing for the Right Instance
• Deployment Tools
• More resources
• Q and A
WHY F5 IN AZURE
Technical Leadership

Figure 1. Magic Quadrant for Application Delivery Controllers

Figure 2. Magic Quadrant for Web Application Firewalls

Source: Gartner (August 2016)

Source: Gartner (August 2017)

- F5 is one of the Gold Cloud Platform Partners
- F5 is one of the Intelligent Security Partners
Platforms: IaaS vs PaaS vs SaaS

On-Premises
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

You manage

Infrastructure (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Other manages

Platform (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Other manages

Software (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Other manages

Source: https://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/
# Azure Shared Responsibility

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td>LTM</td>
<td>LTM</td>
<td>LTM</td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td>LTM</td>
<td>LTM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- **Cloud Customer**
- **Cloud Provider**

© F5 Networks
# Azure Shared Responsibility

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
<tr>
<td>Application level controls</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
<tr>
<td>Network controls</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
<tr>
<td>Host infrastructure</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
<tr>
<td>Physical security</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
<td>🟦</td>
</tr>
</tbody>
</table>

- Cloud Customer: 🟦
- Cloud Provider: 🟦

- DNS

---

*F5 Networks*
# Azure Shared Responsibility

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td></td>
<td>ASM</td>
<td>ASM</td>
<td>ASM</td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td></td>
<td>ASM</td>
<td>ASM</td>
<td>ASM</td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td>APM</td>
<td>APM</td>
<td>APM</td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td>DNS</td>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td>AFM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Cloud Customer**: Blue
- **Cloud Provider**: Grey

© F5 Networks
F5 PRODUCTS IN AZURE
BIG-IP Solutions

“Enterprise Grade ADC that leverages the same user interface, management, and breadth of features as on BIG-IP Hardware”

- Advanced Global Server Load Balancing
- Remote Access, Pre-Authentication, SSO, and Multi-Factor Authentication
- SAML 2.0 Federation IdP/SP
- ICSA Certified Web Application Firewall / WAF
- ICSA Certified L3/4 Network Firewall
- Traffic Optimization and Acceleration
- Intelligent L7 Load Balancing
F5 | BIG-IP Modules | Good

PERFORMANCE | AVAILABILITY | SECURITY

LTM | Local Traffic Manager
- Intelligent L4-L7 Load Balancing
- Traffic Optimization - (Caching & Compression)
- Deep Packet Inspection
- Intelligent Traffic Steering
- Full-Proxy Architecture

TMOS

BIG-IP Virtual Edition
F5 | BIG-IP Modules | Better

**AFM** Advanced Firewall Manager
- ICSA Labs Certified
- Stateful firewall
- Processes 8x more traffic than closest competitor
- Access rules applied at multiple levels, (virtual server, VLAN, route domain)

**DNS** Global Traffic Manager
- Global Server Load Balancing (GSLB)
- Application availability Awareness
- Geolocation
- DNS services
- DNSSEC
F5 | BIG-IP Modules | Best

**APM** Access Policy Manager
- Strategic Point of Control for Application Delivery
- Multi-Factor = Integrates with RSA, SecurID, RADIUS, OTP, certificates, etc.
- Device-based access controls
- Single Sign-On (SSO)

**ASM** Application Security Manager
- ICSA Labs Certified Layer 7 firewall
- Web Application Firewall
- Positive and Negative Security Models
- Mitigate Layer 7 attacks – DDoS, SQL injection, OWASP Top Ten

Performance

Availability

Security

APM

ASM

AFM

DNS

LTM

TMOS

BIG-IP Virtual Edition
F5 | BIG-IP Modules | WAF

**LOCAL TRAFFIC MANAGER (LTM)**
- Intelligent L4-L7 Load Balancing
- Traffic Optimization - (Caching & Compression)
- Deep Packet Inspection
- Intelligent Traffic Steering
- Full-Proxy Architecture

**APPLICATION SECURITY MANAGER (ASM)**
- ICSA Labs Certified Layer 7 firewall
- Web Application Firewall
- Positive and Negative Security Models
- Mitigate Layer 7 attacks – DDoS, SQL injection, OWASP Top Ten

**BIG-IP VIRTUAL EDITION (VE)**

---

Performance | Availability | Security
F5 Preconfigured WAF with Azure Security Center

- Simple deployment experience integrated with Azure workflow and services
- Deploys 2 clustered WAF’s for increased redundancy
- Out-of-the-box choice of security settings preconfigured by F5 experts, plus ability to make more customized settings/policies
- Comprehensive application security with advanced L7 protections
- Guaranteed compliance with all leading regulatory standards
- BYOL/PAYG deployment, inside ASC (Azure Security Centre)
- WAF Solution for ASC has Integration with Azure dashboard and alert/visualization services

Azure Security Center

Marketplace Offering
BIG-IP VE on Microsoft Azure Stack

• VE is available from Azure Marketplace in Good, Better & Best bundles, as well as more specific integrated solutions.

• Throughput and licensing options for BIG-IP VE’s include BYOL
  • BYOL: Lab, 25M, 200M, 1G, 3G
  • Subscription Supported – BIG-IQ outside of Azure Required

• Supports Single-NIC configuration & Configuration sync

• Supports all core BIG-IP modules including LTM, DNS, ASM, AFM & APM

• **Key Use Cases:**
  • Office 365 Identity Federation and Single Sign On
  • Preconfigured WAF in Azure Security Center
  • First PIP – Compliant Secure Proxy for ADFS
Licensing and Throughput Offering

What is Available

Licensing Offerings

Good
Better
Best

GBB Offering

WAF
ELA
Per-App

Custom Offering

Virtual Editions

VE
VE
VE
VE

PayGo

25M
200M
1G
3G

Big-IQ*

Per-App

BYOL
F5 Azure Marketplace Offerings
F5 WAF Solution in Azure Marketplace

- Simple deployment experience integrated with Azure workflow and services
- Deploys 2 clustered WAF’s for increased redundancy
- Out-of-the-box choice of security settings preconfigured by F5 experts
- Comprehensive application security with advanced L7 protections
- Guaranteed compliance with all leading regulatory standards
- Choice of pay-as-you go and BYOL to best fit business scenario, deployable outside of ASC (Azure Security Centre)
- ASC service is not required to implement this solution

Manual Deployment ~ 9 hours
Marketplace Deployment ~ 30 mins

Marketplace Offering
F5 O365 SAML IDP Solution In Marketplace

- Deploys an F5 built, pre-configured VE with BIG-IP APM provisioned
- Leverage an existing active directory and SAML 2.0 to provide federated access to O365 applications
- Extend security with other APM features including MFA, geo-location based control and device checks.
- Simple deployment experience direct from marketplace and integration with Azure workflow and services
- Choice of PAYG and BYOL deployments to best fit business scenario

Manual Deployment ~ 4 hours
Marketplace Deployment ~ 30 mins
LTM Autoscale Solution in Marketplace

Deploys BIG-IP VE with LTM provisioned in an Azure VM Scale Set that has been configured for auto scaling, to consistently provide intelligent traffic management services to applications under varying traffic loads.

- As traffic increases/decreases and crosses pre-defined ‘network out’ throughput thresholds, BIG-IP LTM instances are either spun up or spun down, accordingly.
- The BIG-IP VE instance operates with 1 network interface used for both management and data plane traffic.
- Deployed directly from Azure marketplace via a fully integrated Azure Resource Manager template for increased agility
- Azure resources required include: Azure load balancer and VM Scale Set

Manual Deployment ~ 7 hours
Templated Deployment ~ 30 mins

PAYG Marketplace Offering
Deploys VE instances with BIG-IP LTM and BIG-IP ASM provisioned in an Azure VM Scale Set that has been configured for auto scaling, to provide intelligent traffic management and application security services to applications under varying traffic loads. Instances scale up or down depending on traffic throughput, ensuring application security and operational expenditure are optimized. As traffic passes pre-defined thresholds, BIG-IP VE instances are spun up or down. Thresholds are based on ‘network out’ throughput.

- Comprehensive, layer 7 application protection and guaranteed compliance with all major regulatory standards. Out-of-the-box deployment using pre-built, F5 developed, security policies – which can be customized further for more advanced policy creation
- Deployed directly from Azure marketplace via a fully integrated Azure Resource Manager template for increased agility
- Azure resources required include: Azure load balancer and VM Scale Set

Manual Deployment ~ 7 hours
Templated Deployment ~ 30 mins

Marketplace Offering
F5 AZURE VE SIZING
F5 Recommended VE Instances

**Microsoft Azure**

F5 recommends these instance types for BIG-IP VE on Microsoft Azure.

F5 also supports instance types with similar vCPU and memory.

**Important**: Only the latest version of BIG-IP VE is available in the Azure Marketplace. For older versions, see [http://downloads.f5.com](http://downloads.f5.com).

<table>
<thead>
<tr>
<th>BIG-IP VE VERSION</th>
<th>GOOD</th>
<th>BETTER</th>
<th>BEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1.0.2, 13.0.0, 12.1.2, 12.1.1, 12.1.0, 12.0.0</td>
<td>Standard_A1</td>
<td>Standard_A4</td>
<td>Standard_A7</td>
</tr>
<tr>
<td></td>
<td>Standard_D11</td>
<td>Standard_A6</td>
<td>Standard_DS4_v2</td>
</tr>
<tr>
<td></td>
<td>Standard_DS1_v2</td>
<td>Standard_D4</td>
<td>Standard_DS3_v2</td>
</tr>
<tr>
<td></td>
<td>Standard_DS2_v2</td>
<td>Standard_DS3</td>
<td>Standard_DS13_v2</td>
</tr>
<tr>
<td></td>
<td>Standard_DS11_v2</td>
<td>Standard_DS12_v2</td>
<td></td>
</tr>
</tbody>
</table>

- Production licenses support throughput speeds of up to 3 Gbps, 1 Gbps, 200 Mbps, or 25 Mbps.

BIG-IP VE 13.1.0.2 with a BYOL license is supported in Azure Stack.
Deploy From Azure Marketplace and Template

Azure Market place automatically suggest VE instance types

Azure ARM Template also provides a list of suggested VE instance types
DEPLOYMENT TOOLS
F5 Cloud Solution Template

Tested & Validated
- Cloud solution templates deploy app services in minutes
- Designed, tested and supported by F5 experts following cloud best practices.
- Manual configuration - time consuming and prone to error

Simple & Automated
- Improve efficiency while reducing cost, variability & deployment risk
- Automation & orchestration is table stakes as infrastructure complexity increases
- Templated app services can be integrated with 3rd party tools

Solutions Across Clouds
- Multi-cloud is becoming the norm
- F5 provides standard app services to deploy across all Public Clouds
- Enables fast, simple and the same security posture for the multi-cloud world
Azure Resource Manager Templates for quickly deploying BIG-IP services in Azure

- 29 commits
- 2 branches
- 27 releases
- 1 contributor

Commit for 3.3.0.0:
- 4 months ago

Commit for 4.1.0.0:
- 4 months ago

Commit for 3.0.0.0:
- 4 months ago

Commit for 3.3.0.0:
- 4 months ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago

View release notes for v5.2.0.0:
- 3 days ago
F5 Cloud Solution Templates

What are they?

- **Automatically** lay down virtual infrastructure such as VM’s and subnets within a virtual cloud network

- **Spin up** and configure cloud resources autonomously on top of this infrastructure including BIG-IP VE and any necessary cloud native services

- **Designed and Tested** by F5 engineers using cloud native resource management services:
  - CloudFormation for AWS
  - Azure Resource Manager for Azure
  - Google Deployment Manager for Google

- **F5 support** is available for any ‘supported’ template up on GitHub

---

### Cloud Solution Templates in Azure

- 1NIC Architecture
- 2NIC Architecture
- 3NIC Architecture
- n-NIC Architecture
- 2 Clustered BIG-IP’s (Active/Active, Active/Standby 3NICs)
- HA API Failover (Active/Standby 3NICs or N-NICs)
- Auto Scale Cloud WAF
- Auto Scale Cloud LTM
Single NIC ARM Template

Deploys a standalone BIG-IP VE in a new or pre-existing Azure virtual network, where traffic automatically flows via the VE to the application servers. The BIG-IP instance operates with 1 network interface, processing both management and data plane traffic from the internet. This is the set-up most cloud native developers are accustom to and is best for single tenant or ‘per app’ services.

- BYOL and PAYG templates available

Pre-requisites to this template can be found [here](#).

Manual Deployment ~ 3+ hours
Templated Deployment ~ 40 mins

[Link to GitHub](#)
Deploys BIG-IP LTM in an Auto Scaling group, to consistently provide intelligent traffic management services to applications under varying traffic loads. As traffic increases/decreases and crosses pre-defined network throughput thresholds, BIG-IP LTM instances are either spun up or spun down, accordingly.

- The BIG-IP VE instance operates with 1 network interface used for both management and data plane traffic.
- Only available with PAYG instances
- Requires use of an Azure Load Balancer (ALB)

Post-deployment tasks

- Add a Health Probe and Load balancing rule to ALB
- Modify network security group (NSG) inbound rules

Manual Deployment: 6+ hours
Templated Deployment: 40 mins

Link to GitHub
WAF Autoscale ARM Template

Launches a PAYG BIG-IP VE instance with LTM and ASM provisioned for intelligent traffic management and application security. As traffic fluctuates, VE instances are automatically spun up or down to provide the optimal solution for processing application traffic.

- This solution is deployed into a new networking stack which is created along with the solution.
- The BIG-IP VE instance operates with 1 network interface used for both management and data plane traffic.
- Only available with PAYG instances
- Requires use of an Azure Load Balancer (ALB)

Post-deployment tasks

- Add a Health Probe and Load balancing rule to ALB
- Modify network security group (NSG) inbound rules

Manual Deployment ~ 6+ hours
Templatd Deployment ~ 40 mins

Link to GitHub
Deploys two BIG-IP VE’s across an Azure availability set in an Active-Active configuration for enhanced availability. The BIG-IP’s are configured in front of pre-existing application servers, and thus traffic traverses the BIG-IP’s to these servers.

- The BIG-IP VE instance operates with 3 network interfaces used for both management and data plane traffic
- Can be configured as Active/Standby or Active/Active cluster
- Requires use of an Azure Load Balancer(basic) or Internal Load Balancer
- BYOL and PAYG templates available

Manual Deployment: 8+ hours
Templated Deployment: 40 mins
HA Failover API ARM template

Deploys two BIG-IP VE’s in an Active-Standby configuration to ensuring high availability in both cases. The VE’s are within an Azure availability set allowing them to be spread across different update and fault domains. The VE’s can be added to an existing Azure stack or can be deployed into a new stack.

- Each VE has 3 Network interfaces, and is most similar to an ‘on-premise’ deployment, with one interface for management, one for front-end application traffic and one for back end application traffic. Also has an option to create additional NICs if needed
- UDRs can be part of the failover action
- Does not require use of an Azure Load Balancer
- PAYG & BYOL templates available

Pre-requisites to this template can be found [here]

Manual Deployment ~ 8+ hours
Templated Deployment ~ 40 mins

Link to GitHub
Deploys BIG-IP VE(s) in either Standalone or Active-Standby Firewall Sandwich configuration. The BIG-IP VE are in multi-NICs setup depending on how many Firewalls being LB the traffic to. User Defined Routes (UDRs) are needed for the redirecting the traffic to the Firewall(s).

- Each VE's interface is in its own subnet, and each subnet has a UDR for forwarding the traffic to the FW(s)
- In this architecture, the Inbound VE is for reverse proxy use case; while the Outbound VE is for the forward proxy use case
- Does not require use of an Azure Load Balancer
- Standalone or Failover-API templates can be used for this use case
F5 Programmability

• Programmable Management, Control & Data planes

iControl (REST & SOAP)
Allows light weight, rapid interaction between user, script & F5 devices

iApps
Services-based, template-driven configurations on BIG-IP

iRule
Allows complete programmatic access to application traffic in real time
BIG-IQ Centralized Management

- BIG-IQ can be provisioned as Licensing Manager to activating and revoking licenses across multiple BIG-IP VEs.
- BIG-IQ can also help you to manage BIG-IPs and their services such as LTM, AFM, ASM, and APM.
- A data collection device (DCD) is a specially provisioned BIG-IQ system that you use to manage and store alerts, events, and statistical data from one or more BIG-IP systems.
F5 Ansible Solution

1. Ansible Versions 2.3 +
2. bigsuds, f5-sdk

Playbooks

REST/SOAP API calls

Private cloud
- LTM
- DNS
- F5 Virtual Editions
- BIG-IP Platform
- F5 V1PRION

Public cloud
- LTM
- DNS
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

3. TMOS v12.X +

www.ansible.com/f5
## Ansible F5 Modules

### BIG-IP device features
- bigip_device_dns
- bigip_device_ntp
- bigip_device_sshd
- bigip_hostname
- bigip_routedomain
- bigip_selfip
- bigip_sys_db
- bigip_sys_global
- bigip_vlan
- bigip_user
- bigip_provision
- bigip_qkview
- bigip_snmp
- bigip_snmp_trap
- bigip_configsync_actions

### BIG-IP LTM Features
- bigip_irule
- bigip_monitor_tcp_echo
- bigip_monitor_tcp_half_open
- bigip_monitor_http
- bigip_monitor_tcp
- bigip_node
- bigip_pool
- bigip_pool_member
- bigip_snat_pool
- bigip_ssl_certificate
- bigip_virtual_server
- bigip_virtual_address

### BIG-IP DNS features
- bigip_gtm_datacenter
- bigip_gtm_facts
- bigip_gtm_virtual_server
- bigip_gtm_wide_ip
- bigip_gtm_pool

---

**38 Modules + Active Development!!!**
Cloud Logging in Azure
With F5’s ‘Cloud-Logger’ iApp

• Automatically exports logs via json to cloud services including Azure OMS
• All ARM templates deploy BIG-IP VE’s with the iApp pre-loaded
• iApp manages logging profiles for various BIG-IP services (request logging for virtual services, ASM policies, system logs, etc.)

Cloud Logger iApp on GitHub

Example - BIG-IP ASM Logs in Azure OMS
MORE RESOURCES
More Helpful links

**Getting Started:**

**F5 VM Sizing:**

**Blogs:**

F5 in Azure Part 1 – Integrate Azure MFA with BIGIP
https://devcentral.f5.com/articles/heres-how-i-did-it-integrating-azure-mfa-with-the-big-ip-19634

F5 in Azure Part 2 – Assigning Multiple Public IPs to an Azure Hosted BIG-IP

F5 in Azure Part 3 – Integrate Azure MFA with O365 Federation

**Azure ARM Templates:**
https://github.com/F5Networks/f5-azure-arm-templates/tree/master/support
(Official Supported template)
https://github.com/F5Networks/f5-azure-arm-templates/tree/master/experimental
Thank You