F5 and Ansible: Automate, Scale, and Secure

Matt Quill
Sr. Strategic Business Development Manager
Enabling ecosystems

ECOSYSTEM INTEGRATIONS

NGINX Controller
BIG-IQ
PLATFORM CONTROL PLANES

Ecosystems

App / Web server
Ingress controller
API gateway
Load balancer
App security
DNS
DDoS
CDN

Software as a Service
Containers
Public cloud
Virtual machines
Commodity hardware
Purpose-built hardware

Customer

BIG-IP
NGINX
F5 & Ansible

F5 Networks
- De-facto platform for load balancing and L4-L7 application provisioning / security
- One of the first adopters of automation enablement esp. Ansible
- Committed to open source (see: NGINX)

Ansible
- De-facto automation platform for network automation
- Automation for all F5 users
- Developers using BIG-IP, BIG-IQ, and AS3 modules in Playbooks
- Operations using certified F5 Ansible Roles

Competitive edge
- F5 Information / Inventory Retrieval and Configuration
  - Ad hoc or bulk
  - Iteration over specific network segments, VIPs, pools
  - Credential management with Tower Vault
- State Checking and Validation
  - Compare running F5 configs to desired F5 configs
- Execute F5 playbooks with flexibility
  - Invoke manually, API via Tower, Scheduled via Tower
- Continuous Compliance
  - Combine stateful validation with schedules
  - Logging and Aggregation
- Integrations
  - ZTP post-install NOS handoff to Ansible
Ansible Modules for F5
170+ Modules Currently Available as of Release 2.9.x

Ansible Module Information
https://clouddocs.f5.com/products/orchestration/ansible/devel/modules/module_index.html

Ansible Module/Collections Support
https://github.com/F5Networks/f5-ansible/issues
Ansible Collections for F5
Ansible Collections 2.10+ contains Collections v1.5 (Native)

Installing Collections
Both the official or daily build are placed in this folder structure: ./collections/ansible_collections/f5_modules

Official Releases
- View the F5 Collection releases: https://galaxy.ansible.com/f5networks/f5_modules
- Install the most recent release:
  ansible-galaxy collection install f5networks.f5_modules

Referencing a Collection in a playbook
There are two options for referencing a Collection in a playbook:
1. Preface each module, role, or resource with the collection name:

```yaml
- name: Use Collections
  hosts: f5
  connection: local

  tasks:
  - f5networks.f5_modules.bigip_pool:
      name: my-pool
      partition: Common
```

2. Specify the collection for the entire play (any module found in the collection will be used before core):

```yaml
- name: Use Collections
  hosts: f5
  connection: local

  collections:
  - f5networks.f5_modules

  tasks:
  - bigip_pool:
```

Make Sure to Upgrade Collections to Latest Version
https://galaxy.ansible.com/f5networks/f5_modules

Ansible Collection Information

Ansible Module/Collections Support
https://github.com/F5Networks/f5-ansible/issues
Use Cases
Ansible Solution for F5 BIG-IP & BIG-IQ

Use Cases

- BIG-IP Licensing
- Deploying L4-L7 application services
- BIG-IP onboarding, including high availability
- Drive Infrastructure as Code migrations

Ansible Host

Playbooks

App Templates

Private Cloud

Public Cloud

REST API calls

BIG-IQ

Amazon Web Services

Microsoft Azure

Google Cloud Platform
Use Cases
Automate, Continuous Delivery, Operational Agility, Consistent Reliability & Security in Any Cloud!

Policy (AFM/WAF)
Source Code Repo - IAC
Revision Control
Webhook

Logging & Reporting
RBAC
Job Scheduling
Deployment Playbooks

GitHub
SCM

F5 BIG-IP & BIG-IQ
Ansible Modules & Collections

F5 Application Services 3 (AS3)

Environments
Development
Test
Production

Public Clouds
(AWS/GCP/AZURE)
Private Clouds

Blue Green deployments
Canary deployments
...

Physical Appliance/Chassis
Virtual Edition
Cloud Edition

Jenkins

Logging & Reporting
RBAC
Job Scheduling
Deployment Playbooks

F5 Infrastructure
Security Automation
Why Security Automation?

SOLVING THE SECURITY OPERATIONS CHALLENGE

Streamline Repeatable Tasks
Automate repeatable tasks

Eliminate Inefficient Investigations
Avoid managing hundreds of point solutions

Accelerate Response
Minimizing the risk with the prompt remediation

Optimize ROI / TCO
Enhance performance of SOC analysts
Why Ansible security automation?

- **5%**
  - Portion of alerts coming in that the average security team examines every day

- **57%**
  - Said the time to resolve an incident has grown

- **65%**
  - Reported increased Severity of attacks

- **29%**
  - Have their ideal security-skilled staffing level, making it the #2 barrier to Cyber resilience

Source:
1. The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)
Security Automation Process

HOW IT WORKS?

1. F5 AWAF monitoring all legal and illegal web requests for the application servers.
   - F5 AWAF exports detailed network telemetry data to external Elasticsearch system.

2. If any of AWAF alerts meet below conditions, ‘ELK Watcher’ will execute the pre-configured ‘Ansible Playbook’.
   - Conditions
     - If ‘Alert’ is NOT blocked by AWAF … AND
     - If the source geolocation of the ‘Alert’ is ‘North Korea’ OR ‘China’ OR ‘Russia’ … AND
     - If the alert severity is ‘Error’ OR ‘Critical’ … THEN
     - execute the ‘Ansible Playbook’.

3. Ansible playbook updates existing AWAF policy enforcement setting from ‘Transparent’ to ‘Blocking’.
Security Automation Process

HOW IT WORKS?

1. Export network telemetry data to 'logstash' which includes:
   - IP Bytes In/Out
   - HTTP Info
   - WAF Info
   - IP Reputation Info
   - Geolocation Info
   - Network-level info

2. Processing/modifying data and forwards them to Elasticsearch

3. Indexing data

4. Visualize the data
   Monitoring the data through the 'Watcher'

5. If any data meets the condition of the 'Watcher', 'Kibana' sends a HTTP POST to logstash.

6. Once 'logstash' receives the POST message from the 'Watcher' of Kibana, it executes the 'Ansible Playbook'.

7. Ansible will update the policy of F5 AWAF.
F5/Ansible Solution Resources

- Webinar recordings + Q&A blogs
- Whitepaper (needs updating)
- Solution overview (needs updating)

Pre-built F5 roles for
- BIG-IP Onboarding
- GSLB Configuration
- Device Backup
Customer Enablement Resources

- F5/Ansible Tower Linklight Workshop
  - https://ansible.github.io/workshops/exercises/ansible_f5/

- Red Hat Ansible Automation Platform F5 Workshops Self-Paced Training
  - https://clouddocs.f5.com/training/automation-sandbox/

- NetOps meets DevOps report
Red Hat Ansible Automates

THANK YOU

youtube.com/AnsibleAutomation
facebook.com/ansibleautomation
linkedin.com/company/Red-Hat
twitter.com/ansible