



21 May 2020

Automation & Orchestration

F5 Automation Toolchain

PRESENTED BY:

Saad Khalid, Solutions Engineer, F5

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

Agenda

- Introduction
- Challenges in DoD
- F5 Automation Toolchain
 - Declarative Onboarding (DO)
 - Application Services 3 Extension (AS3)
 - Telemetry Streaming (TS)
- Ecosystem Integrations
- Demo

Software is a Critical Component of the DoD mission

- Need for updating software rapidly (agile)
 - ...in a secure fashion
 - ...knowing things won't break
- Need to establish Secure Application Development Capabilities
- Bake-in & enforce cybersecurity from inception through operations
- Enhance enterprise visibility



Challenges in DoD

- **Lack of test automation**
- **Legacy Systems**
- **App Complexity**
- **Tool Sprawl**
- **Managing Environments (disconnected, classified, etc...)**
- **Skillset / Self-service training**
- **Culture**

F5 Automation Toolchain

Bootstrap



Cloud Templates

Configure and deploy F5 BIG-IP VEs into public and private clouds.

Device Onboard



Declarative Onboarding

Provision initial configuration of BIG-IP devices through a declarative API.

Deploy App Services



Application Services 3 Extension

Configuration of L4-L7 via declarative APIs.

Monitor



Telemetry Streaming

Stream BIG-IP telemetry for analytics and automation.

Telemetry Streaming is an iControl LX extension and will send client/server stats from the BIG-IP via HTTP(S), Statsd or Kafka formats.

Change



Change

Use telemetry data to track health, security and performance of applications

Use thresholds and triggers to scale app services

Imperative vs Declarative

Imperative

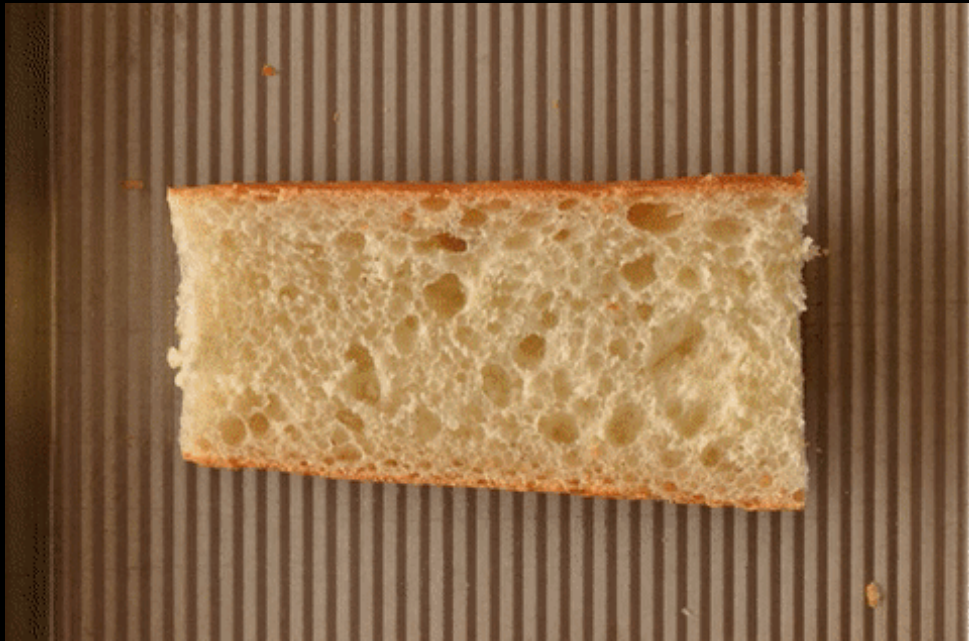
Tell the system **HOW** to do something - every step of the way

Declarative

Tell the system **WHAT** you want, and let it figure out **HOW** to do it

**Declarative API - you define the desired end-state
– it fills in the details on “how to get there”**

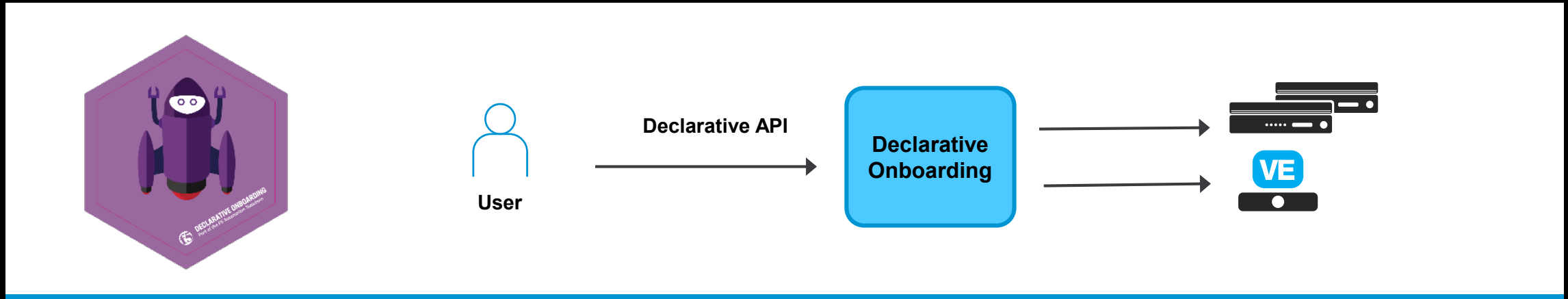
Imperative



Declarative



Automate Device Onboarding with Declarative Onboarding (DO)



What is it?

- F5 BIG-IP API Extension (Node.js)
- Provides declarative interface for L1-L3 device onboarding
- Deployments via a single REST API endpoint
- JSON-based document



What are the Benefits?

- Minimizes need for BIG-IP domain specific knowledge
- Minimizes onboarding errors
- Maximizes onboarding consistency
- TMOS-independent RPM package

Standalone Declaration – Declarative Onboarding

```
{
  "schemaVersion": "1.9.0",
  "class": "Device",
  "async": true,
  "label": "Declarative Onboarding Simple Standalone Example"
  "Common": {
    "class": "Tenant",
    "hostname": "bigip01.f5gov.com",
    "myLicense": {
      "class": "License",
      "licenseType": "regKey",
      "regKey": "RXUGL-HOTFC-WCICJ-NZGWY-PXZTNTQ",
      "overwrite": false
    },
    "myDns": {
      "class": "DNS",
      "nameServers": [
        "8.8.8.8",
        "2001:4860:4860::8844"
      ],
      "search": [
        "f5.com"
      ]
    },
    "myNtp": {
      "class": "NTP",
      "servers": [
        "0.pool.ntp.org",
        "1.pool.ntp.org",
        "2.pool.ntp.org"
      ],
      "timezone": "UTC"
    }
  },
  "guestUser": {
    "class": "User",
    "userType": "regular",
    "password": "mrpurple123!",
    "partitionAccess": {
      "Common": {
        "role": "guest"
      }
    }
  },
  "anotherUser": {
    "class": "User",
    "userType": "regular",
    "password": "mrpurple123!",
    "shell": "none",
    "partitionAccess": {
      "all-partitions": {
        "role": "guest"
      }
    }
  },
  "myProvisioning": {
    "class": "Provision",
    "ltm": "nominal",
    "gtm": "minimum",
    "asm": "nominal"
  },
  "internal": {
    "class": "VLAN",
    "tag": 4093,
    "mtu": 1500,
    "interfaces": [
      {
        "name": "1.1",
        "tagged": false
      }
    ]
  },
  "internal-self": {
    "class": "SelfIp",
    "address": "10.1.10.100/24",
    "vlan": "internal",
    "allowService": "default",
    "trafficGroup": "traffic-group-local-only"
  },
  "internal-floating": {
    "class": "SelfIp",
    "address": "10.1.10.120/24",
    "vlan": "internal",
    "allowService": "default",
    "trafficGroup": "traffic-group-1"
  },
  "external": {
    "class": "VLAN",
    "tag": 4094,
    "mtu": 1500,
    "interfaces": [
      {
        "name": "1.2",
        "tagged": false
      }
    ]
  }
}
```

```
},
"guestUser": {
  "class": "User",
  "userType": "regular",
  "password": "mrpurple123!",
  "partitionAccess": {
    "Common": {
      "role": "guest"
    }
  }
},
"anotherUser": {
  "class": "User",
  "userType": "regular",
  "password": "mrpurple123!",
  "shell": "none",
  "partitionAccess": {
    "all-partitions": {
      "role": "guest"
    }
  }
},
"myProvisioning": {
  "class": "Provision",
  "ltm": "nominal",
  "gtm": "minimum",
  "asm": "nominal"
},
"internal": {
  "class": "VLAN",
  "tag": 4093,
  "mtu": 1500,
  "interfaces": [
    {
      "name": "1.1",
      "tagged": false
    }
  ]
},
"internal-self": {
  "class": "SelfIp",
  "address": "10.1.10.100/24",
  "vlan": "internal",
  "allowService": "default",
  "trafficGroup": "traffic-group-local-only"
},
"internal-floating": {
  "class": "SelfIp",
  "address": "10.1.10.120/24",
  "vlan": "internal",
  "allowService": "default",
  "trafficGroup": "traffic-group-1"
},
"external": {
  "class": "VLAN",
  "tag": 4094,
  "mtu": 1500,
  "interfaces": [
    {
      "name": "1.2",
      "tagged": false
    }
  ]
}
```

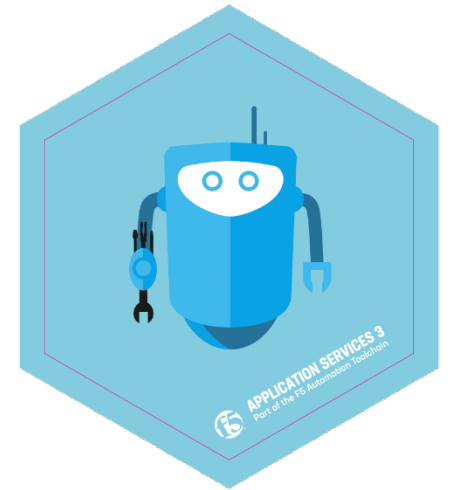
```
"internal": {
  "class": "VLAN",
  "tag": 4093,
  "mtu": 1500,
  "interfaces": [
    {
      "name": "1.1",
      "tagged": false
    }
  ]
},
"internal-self": {
  "class": "SelfIp",
  "address": "10.1.10.100/24",
  "vlan": "internal",
  "allowService": "default",
  "trafficGroup": "traffic-group-local-only"
},
"internal-floating": {
  "class": "SelfIp",
  "address": "10.1.10.120/24",
  "vlan": "internal",
  "allowService": "default",
  "trafficGroup": "traffic-group-1"
},
"external": {
  "class": "VLAN",
  "tag": 4094,
  "mtu": 1500,
  "interfaces": [
    {
      "name": "1.2",
      "tagged": false
    }
  ]
}
```

Standalone Declaration via BIG-IQ – Declarative Onboarding

```
{
  "class": "DO",
  "declaration": {
    "schemaVersion": "1.5.0",
    "class": "Device",
    "async": true,
    "Common": {
      "class": "Tenant",
      "hostname": "bigip01.f5gov.com",
      "myLicense": {
        "class": "License",
        "licensePool": "demo-licenses",
        "licenseType": "licensePool",
        "bigIpUsername": "admin",
        "bigIpPassword": "{{bigippassword}}"
      },
      "myProvisioning": {
        "class": "Provision",
        "ltm": "nominal",
        "gtm": "minimum",
        "afm": "nominal",
        "asm": "nominal"
      }
    },
    "myDns": {
      "class": "DNS",
      "nameServers": [
        "8.8.8.8",
        "2001:4860:4860::8844"
      ],
      "search": [
        "f5.com"
      ]
    },
    "myNtp": {
      "class": "NTP",
      "servers": [
        "0.pool.ntp.org",
        "1.pool.ntp.org",
        "2.pool.ntp.org"
      ],
      "timezone": "UTC"
    },
    "external": {
      "class": "VLAN",
      "interfaces": [
        {
          "name": "1.1",
          "tagged": false
        }
      ]
    },
    "internal": {
      "class": "VLAN",
      "interfaces": [
        {
          "name": "1.2",
          "tagged": false
        }
      ]
    },
    "external-floating": {
      "vlan": "external",
      "class": "SelfIp",
      "address": "10.1.10.240/24",
      "trafficGroup": "traffic-group-1"
    },
    "internal-floating": {
      "vlan": "internal",
      "class": "SelfIp",
      "address": "10.1.20.240/24",
      "trafficGroup": "traffic-group-1"
    },
    "external-self": {
      "vlan": "external",
      "class": "SelfIp",
      "address": "10.1.10.241/24",
      "allowService": "none"
    },
    "internal-self": {
      "vlan": "internal",
      "class": "SelfIp",
      "address": "10.1.20.241/24"
    },
    "default": {
      "gw": "10.1.10.1",
      "class": "Route"
    }
  },
  "targetUsername": "admin",
  "targetHost": "10.1.1.8",
  "targetPort": 443,
  "targetPassphrase": "{{bigippassword}}",
}
```

Automate Application Deployments with AS3

- Application Services 3 Extension – BIG-IP API extension that accepts a declarative API call
- Configures BIG-IP L4-7 services
- Minimizes need for BIG-IP domain specific knowledge
- Minimizes deployment errors
- Makes it easy to integrate F5 automation into orchestration systems
- Runs on BIG-IP & BIG-IQ
- Create application dashboards for monitoring & alerts when used with BIG-IQ



HTTP Example Declaration – AS3

```
{  
  "class":"AS3",  
  "action":"deploy",  
  "persist":true,  
  "declaration":{  
    "class":"ADC",  
    "schemaVersion":"3.7.0",  
    "id":"http-example-declaration",  
    "label":"Task1",  
    "remark":"Task 1 - HTTP Application Service",  
    "http_tenant":{  
      "class":"Tenant",  
      "http_app_1":{  
        "class":"Application",  
        "template":"generic",  
        "http_vs_1":{  
          "http_vs_1":{  
            "class":"Service_Generic",  
            "virtualPort":80,  
            "virtualAddresses":[  
              "10.1.10.111"  
            ],  
            "pool":"http_pool",  
            "profileHTTP":{  
              "use":"http"  
            }  
          },  
          "http_pool":{  
            "class":"Pool",  
            "monitors":[  
              "tcp"  
            ],  
            "members":[  
              {  
                "servicePort":80,  
                "serverAddresses":[  
                  "10.1.20.110",  
                  "10.1.20.111"  
                ]  
              }  
            ]  
          }  
        }  
      }  
    }  
  }  
}
```

```
"http_vs_1":{  
  "class":"Service_Generic",  
  "virtualPort":80,  
  "virtualAddresses":[  
    "10.1.10.111"  
  ],  
  "pool":"http_pool",  
  "profileHTTP":{  
    "use":"http"  
  }  
},  
"http_pool":{  
  "class":"Pool",  
  "monitors":[  
    "tcp"  
  ],  
  "members":[  
    {  
      "servicePort":80,  
      "serverAddresses":[  
        "10.1.20.110",  
        "10.1.20.111"  
      ]  
    }  
  ]  
}
```

A

```

{
  "class": "AS3",
  "action": "deploy",
  "persist": true,
  "declaration": {
    "class": "ADC",
    "schemaVersion": "3.7.0",
    "id": "http-example-declaration",
    "label": "Task2",
    "remark": "Task 2 - Add-HTTP Application Service",
    "http_tenant": {
      "class": "Tenant",
      "http_app_1": {
        "class": "Application",
        "template": "generic",
        "http_vs_1": {
          "class": "Service_Generic",
          "virtualPort": 80,
          "virtualAddresses": [
            "10.1.10.111"
          ],
          "pool": "http_pool",
          "profileHTTP": {
            "use": "http"
          }
        },
        "http_pool": {
          "class": "Pool",
          "monitors": [
            "tcp"
          ],
          "members": [
            {
              "servicePort": 80,
              "serverAddresses": [
                "10.1.20.110",
                "10.1.20.111"
              ]
            }
          ]
        }
      }
    }
  }
}

```

m

```

},
"http_app_2": {
  "class": "Application",
  "template": "generic",
  "http_vs_2": {
    "class": "Service_Generic",
    "virtualPort": 80,
    "virtualAddresses": [
      "10.1.10.113"
    ],
    "pool": "http_pool_2",
    "profileHTTP": {
      "use": "http"
    }
  },
  "http_pool_2": {
    "class": "Pool",
    "monitors": [
      "tcp"
    ],
    "members": [
      {
        "servicePort": 8082,
        "serverAddresses": [
          "10.1.20.112",
          "10.1.20.113"
        ]
      }
    ]
  }
}

```

3

```
{
  "class": "AS3",
  "action": "deploy",
  "persist": true,
  "declaration": {
    "class": "ADC",
    "schemaVersion": "3.7.0",
    "id": "http-example-declaration",
    "label": "Task2",
    "remark": "Task 2 - Add HTTP Application Service",
    "http_tenant": {
      "class": "Tenant",
      "http_app_1": {
        "class": "Application",
        "template": "generic",
        "http_vs_1": {
          "class": "Service_Generic",
          "virtualPort": 80,
          "virtualAddresses": [
            "10.1.10.111"
          ],
          "pool": "http_pool",
          "profileHTTP": {
            "use": "http"
          }
        },
        "http_pool": {
          "class": "Pool",
          "monitors": [
            "tcp"
          ],
          "members": [
            {
              "servicePort": 80,
              "serverAddresses": [
                "10.1.20.110",
                "10.1.20.111"
              ]
            }
          ]
        }
      }
    }
  }
}
```

```
},
  "waf_https": {
    "class": "Tenant",
    "waf_app": {
      "class": "Application",
      "template": "https",
      "statsProfile": {
        "class": "Analytics_Profile",
        "collectClientSideStatistics": true,
        "collectOsAndBrowser": false,
        "collectMethod": false
      },
      "serviceMain": {
        "class": "Service_HTTPS",
        "virtualAddresses": [
          "10.1.10.129"
        ],
        "pool": "web_pool",
        "profileAnalytics": {
          "use": "statsProfile"
        },
        "serverTLS": "webtls",
        "policyWAF": {
          "bigip": "/Common/templates-default"
        },
        "securityLogProfiles": [
          {
            "bigip": "/Common/templates-default"
          }
        ]
      }
    }
  }
}
```

```
},
  "web_pool": {
    "class": "Pool",
    "monitors": [
      "http"
    ],
    "members": [
      {
        "servicePort": 80,
        "serverAddresses": [
          "10.1.20.122",
          "10.1.20.123"
        ]
      }
    ]
  },
  "webtls": {
    "class": "TLS_Server",
    "certificates": [
      {
        "certificate": "webcert"
      }
    ]
  },
  "webcert": {
    "class": "Certificate",
    "certificate": {
      "bigip": "/Common/default.crt"
    },
    "privateKey": {
      "bigip": "/Common/default.key"
    }
  }
}
```

Deleting Configuration Objects with AS3

```
{
  "class": "AS3",
  "action": "deploy",
  "declaration": {
    "class": "ADC",
    "schemaVersion": "3.12.0",
    "waf_https": { ←
      "class": "Tenant"
    },
    "http_tenant": { ←
      "class": "Tenant"
    }
  }
}
```

Real-Time Analytics with Telemetry Streaming



- Provides stats on: Device, LTM, tenants and apps, TLS Cert Inventory, and event log (all sources)
- Declarative
- Streams from BIG-IP to a data store
- Validated 3rd party consumers: Splunk, Azure Log Analytics, AWS CloudWatch, AWS S3, Graphite, ElasticSearch and more

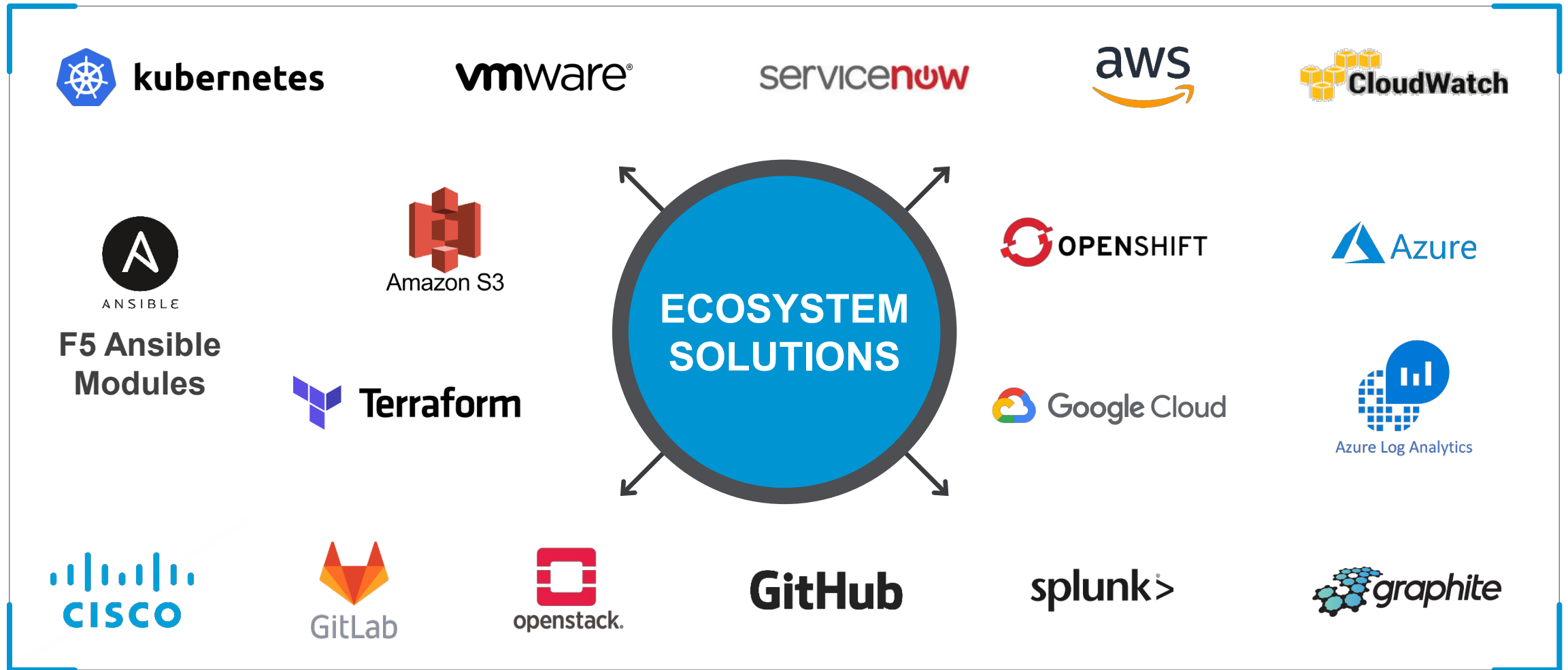
AWS CloudWatch Example Declaration – Telemetry Streaming

```
{
  "class": "Telemetry",
  "My_System": {
    "class": "Telemetry_System",
    "systemPoller": {
      "interval": 60
    }
  },
  "My_Listener": {
    "class": "Telemetry_Listener",
    "port": 6514
  },
  "My_Consumer": {
    "class": "Telemetry_Consumer",
    "type": "AWS_CloudWatch",
    "region": "us-east-1",
    "logGroup": "test_group",
    "logStream": "automation_demo",
    "username": "{{AWS_ACCESS_KEY}}",
    "passphrase": {
      "cipherText": "{{AWS_SECRET_KEY}}"
    }
  }
}
```

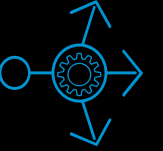
Automation Orchestration Toolchain Benefits

- Minimizes
 - Need for BIG-IP domain specific knowledge
 - Onboarding errors & deployment errors
- Maximizes
 - Onboarding & deployment consistency
 - Reusability
- Easy Integration
 - Enables developers to extend F5 app services & integrate with CI/CD toolchains, orchestration systems & 3rd-party ecosystems
- Helps drive an organizations' adoption of Infrastructure as Code (IaC) & DevOps

Ecosystem Integrations



Automate BIG-IP with Ansible



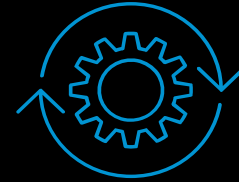
Simple

- Agentless solution: No new software to install on BIG-IP
- Use Ansible to license a BIG-IP for application deployment



Powerful

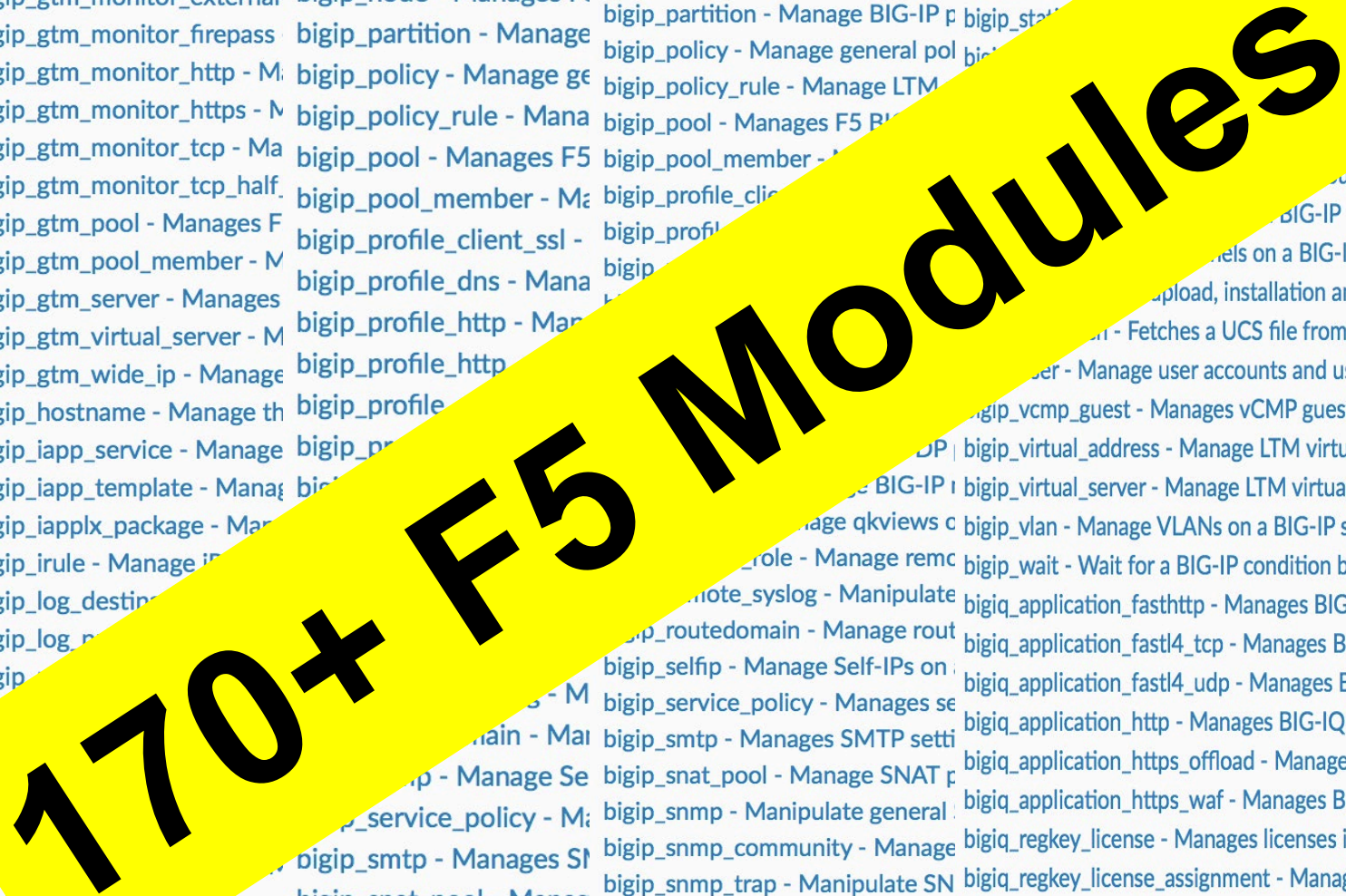
- Ansible integrates to make use of the native APIs of BIG-IP
- Ansible F5 modules follow best practice and enable compliance



Automated

- Automate the initial configurations on BIG-IP and deploy HTTP(S) apps
- Automate to Network the BIG-IP (VLANs, Self-IPs)

F5 Ansible BIG-IP Modules Now Available (Release 2.9.x)



170+ F5 Modules

bigip_gtm_monitor_firepass - Manage BIG-IP partition - Manage BIG-IP partition
 bigip_gtm_monitor_http - Manage BIG-IP policy - Manage general policy
 bigip_gtm_monitor_https - Manage BIG-IP policy_rule - Manage LTM policy rule
 bigip_gtm_monitor_tcp - Manage BIG-IP pool - Manages F5 pool
 bigip_gtm_monitor_tcp_half - Manage BIG-IP pool_member - Manage F5 pool member
 bigip_gtm_pool - Manages F5 BIG-IP profile_client - Manage BIG-IP profile client
 bigip_gtm_pool_member - Manage BIG-IP profile_client_ssl - Manage BIG-IP profile client SSL
 bigip_gtm_server - Manages BIG-IP profile_dns - Manage BIG-IP profile DNS
 bigip_gtm_virtual_server - Manage BIG-IP profile_http - Manage BIG-IP profile HTTP
 bigip_gtm_wide_ip - Manage BIG-IP profile_http - Manage BIG-IP profile HTTP
 bigip_hostname - Manage BIG-IP profile - Manage BIG-IP profile
 bigip_iapp_service - Manage BIG-IP vcmpp_guest - Manage vCMP guest
 bigip_iapp_template - Manage BIG-IP virtual_address - Manage LTM virtual address
 bigip_iapplx_package - Manage BIG-IP virtual_server - Manage LTM virtual server
 bigip_irule - Manage BIG-IP vlan - Manage VLANs on a BIG-IP system
 bigip_log_destino - Manage BIG-IP wait - Wait for a BIG-IP condition
 bigip_log_n - Manage BIG-IP application_fasthttp - Manages BIG-IP application fasthttp
 bigip_log_n - Manage BIG-IP application_fastl4_tcp - Manages BIG-IP application fastl4_tcp
 bigip_log_n - Manage BIG-IP application_fastl4_udp - Manages BIG-IP application fastl4_udp
 bigip_log_n - Manage BIG-IP application_http - Manages BIG-IP application HTTP
 bigip_log_n - Manage BIG-IP application_https_offload - Manages BIG-IP application https offload
 bigip_log_n - Manage BIG-IP application_https_waf - Manages BIG-IP application https waf
 bigip_log_n - Manage BIG-IP regkey_license - Manages licenses
 bigip_log_n - Manage BIG-IP regkey_license_assignment - Manages licenses assignment

Conclusion

- Software is a Critical Component of every aspect of the DoD mission
- Challenges in DoD
- F5 Automation Toolchain
 - DO, AS3, TS
- Ecosystem Integrations
 - Ansible F5 Modules
- F5 Automation Toolchain + Ansible Demo
 - Near real-time insights w/ Telemetry Streaming
 - Grafana Dashboard (visualization tool)

Getting Started Resources

- **Declarative Onboarding (DO)**

- <https://clouddocs.f5.com/products/extensions/f5-declarative-onboarding/latest/>

- **Application Services Extension (AS3)**

- <https://clouddocs.f5.com/products/extensions/f5-appsvcs-extension/latest/>

- **Telemetry Streaming (TS)**

- <https://clouddocs.f5.com/products/extensions/f5-telemetry-streaming/latest/>

- **F5 Ansible Modules & Integration**

- <https://clouddocs.f5.com/products/orchestration/ansible/devel/>

- **BIG-IQ API**

- <https://clouddocs.f5.com/products/big-iq/mgmt-api/v7.0.0/>

- **F5 Container Connector (OpenShift)**

- <https://clouddocs.f5.com/containers/v2/openshift/>

- **F5 Container Ingress Services (Kubernetes)**







- <https://clouddocs.f5.com/containers/v2/kubernetes/>

- **General Cloud Docs**

- <https://clouddocs.f5.com/>

F5 DoD Account Team



Air Force		AE / East	Eddie Augustine	e.augustine@f5.com	301-717-4131
		AE / West	Dustin Purkey	D.Purkey@F5.com	714-501-4815
		SE / East	Arnulfo Hernandez	A.Hernandez@f5.com	202-360-1984
		SE / West	Paul Deakin	p.deakin@f5.com	949-395-0051
DISA		AE	David Thomas	d.thomas@f5.com	703-930-9623
		AE	Thomas Ries	T.Ries@f5.com	703-850-4654
		SE	Anthony Graber	anthony.graber@f5.com	443-987-6487
Navy Marine Corps	 	AE / East	John Manning	j.manning@f5.com	703-898-4135
		AE / West	Archie Newell	a.newell@f5.com	858-922-2654
		SE / East	Paul Simmons	p.simmons@f5.com	843-300-7392
		SE / West	Jimmy Jennings	j.jennings@f5.com	951-334-8558
Pentagon Defense Agencies		AE	Mark Oldknow	m.oldknow@f5.com	512-410-9462
		SE	August Weinerstein	a.winterstein@f5.com	301-660-9644
Army		MAM / West	Brig Lambert	B.Lambert@f5.com	801-319-1221
		MAM / East	Todd Favakeh	t.favakeh@f5.com	847-334-5610
		SE / East	Shaun Simmons	s.simmons@f5.com	412-329-8366
		SE / West	Michael Slavinsky	M.Slavinsky@f5.com	206-637-2056

Thank You



F5 DoD Virtual User Group (DoDVUG) Schedule

Date	Title	F5 DoDVUG Topic
Apr 9th Thursday@ 1500	F5 DoD Virtual User Group #1	F5 Access Policy Manager with remote access, network tunneling, and CAC/PIV Authentication.
April 23rd Thursday@ 1500	F5 DoD Virtual User Group #2	Get Your SaaS in Gear Enterprise Application Strategy
May 7th Thursday@ 1500	F5 DoD Virtual User Group #3	Ghastly Wealth Compliance using F5 ASM
May 21st Thursday@ 1500	F5 DoD Virtual User Group #4	Automation/Orchestration - F5 A/O Toolchain
June 4th Thursday@ 1500	F5 DoD Virtual User Group #5	SCCA / SACA
June 18th Thursday@ 1500	F5 DoD Virtual User Group #6	SSLO Orchestrator