Building and managing landing zones with Azure Blueprints and Azure DevOps

Azure Thursdays

Wesley Haakman

Lead Azure Architect @ Intercept

@whaakman

www.linkedin.com/in/wesleyhaakman

https://www.wesleyhaakman.org

Agenda

- Governance 101
- Azure Blueprints
- Shifting left with Azure Blueprints
- Implementing Guard Rails with Azure Blueprints
- Blueprints as Code

Governance

Governance

- Organizing resources
- Control Costs
- Role Based Access Control
- Consistency in code & infrastructure
- Regulatory requirements & Compliance
- Life cycle management

Governance & Compliance

"I'm concerned about data sovereignty; how can I ensure that my data and systems meet our regulatory requirements?"

"How do I know what each resource is supporting so I can account for it and bill it back accurately?"

"I want to make sure that everything we deploy or do in the public cloud starts with the mindset of security first, how do I help facilitate that?"

The challenges with governance

- Nobody wants to do it
- Governance can slow down a company’s ability to release new innovations
- Bad or no governance results in non-compliance, unforeseen costs and unmanageable environments

But… We do want consistency, predictable outcome and happy customers

This is an automation problem

Automation of Governance on Azure

- Implement governance early in the process (shift left)
- Enforce internal standards and guardrails
- Meet regulatory compliance requirements
- Consistent security management
- Setup environments faster
- Release compliant code faster
- Control costs

What do we need?

- Azure Policy
- Azure Blueprints
- Azure DevOps

Azure Policy

- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy

Enforcement & Compliance

- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale

- Real time remediation
- Remediation on existing resources

Remediation

Azure Policy

Enforcement

Real-time (on change & on creation):
Audit, Audit if not exists
Deny
Append
Deploy if not exist

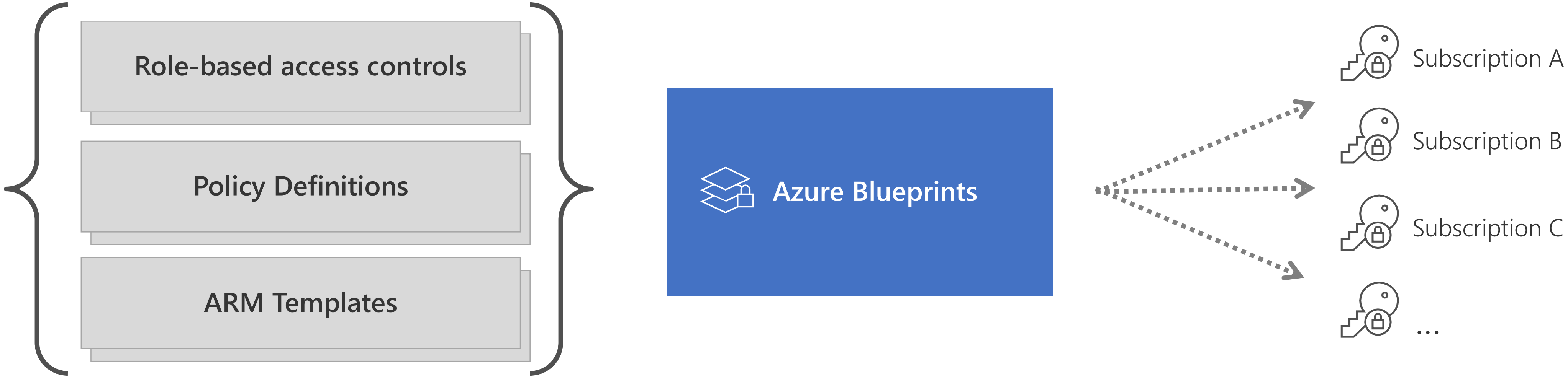
Compliance

Always On:
On Change
On Periodic Cadence
On Demand

Azure Blueprints

- Designed to help with environment setup
- Made of Artifacts
  - Resource Groups
  - ARM Templates
  - Azure Policy
  - Role Assignments (RBAC)
- Relationship between definition (what should be deployed) and assignment (what is deployed) is maintained
- Great for tracking and auditing deployments
- Blueprint Locks

Azure Blueprints



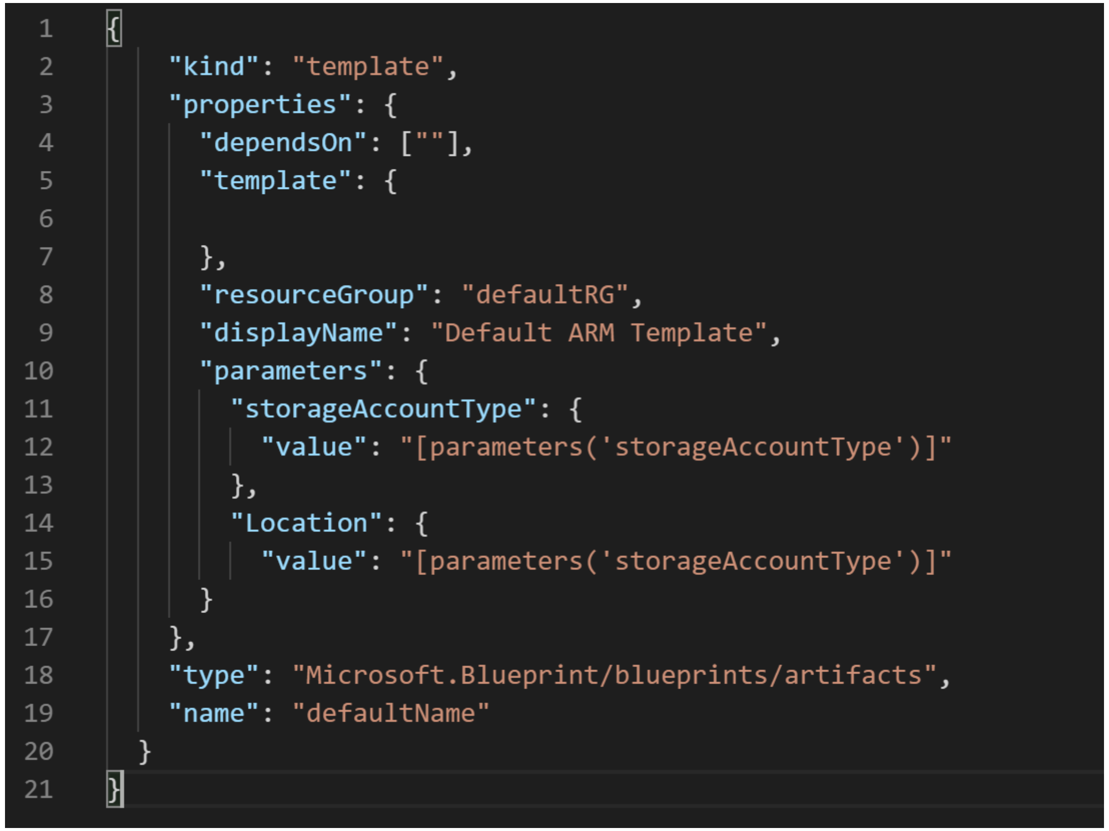
compose | manage | scale

The Blueprint process

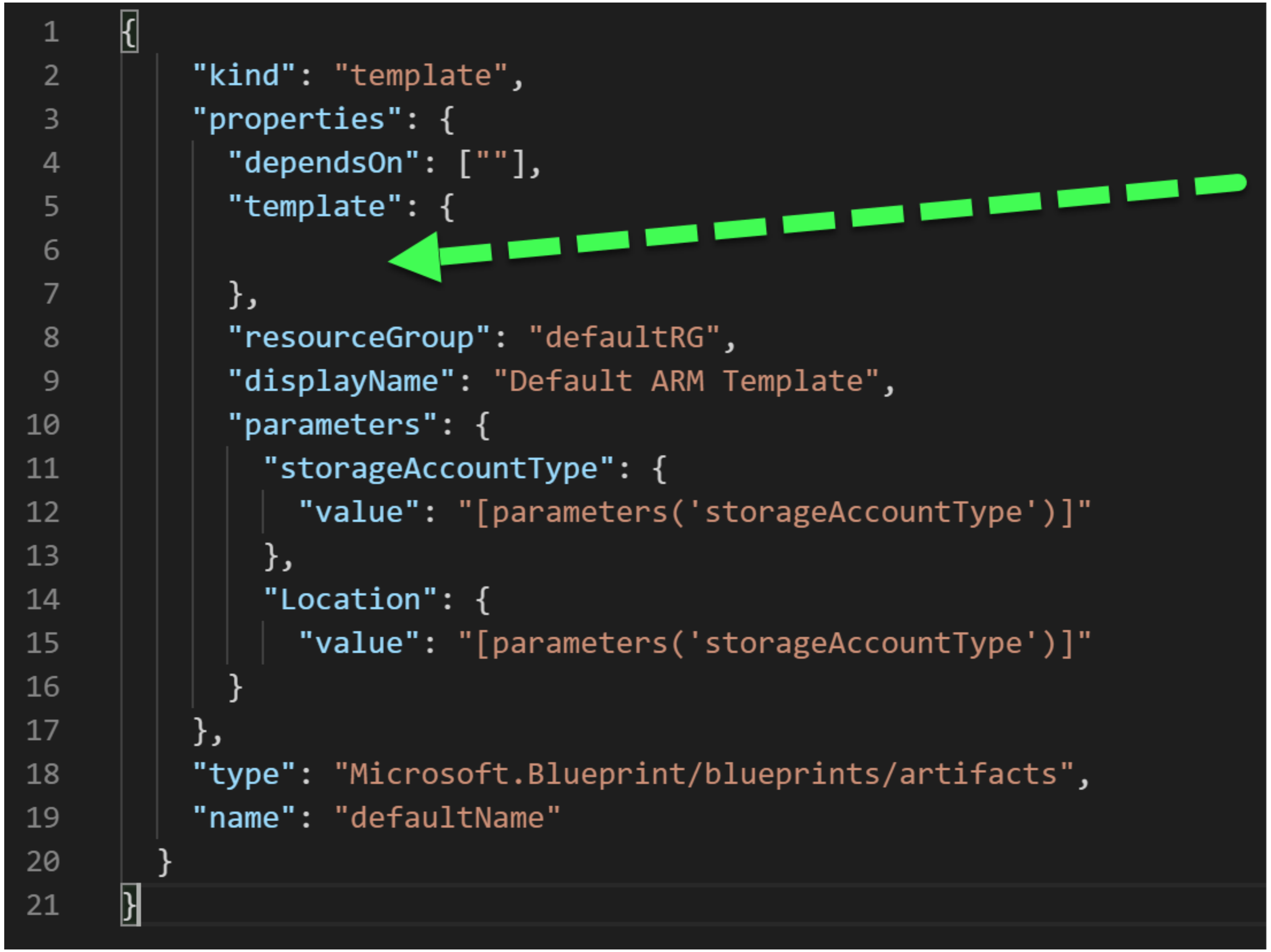
1. Create Blueprint Draft
2. Publish Blueprint Definition
3. Assign Blueprint
4. Repeat

From Azure Blueprints to Blueprints as Code

Artifacts and ARM Templates

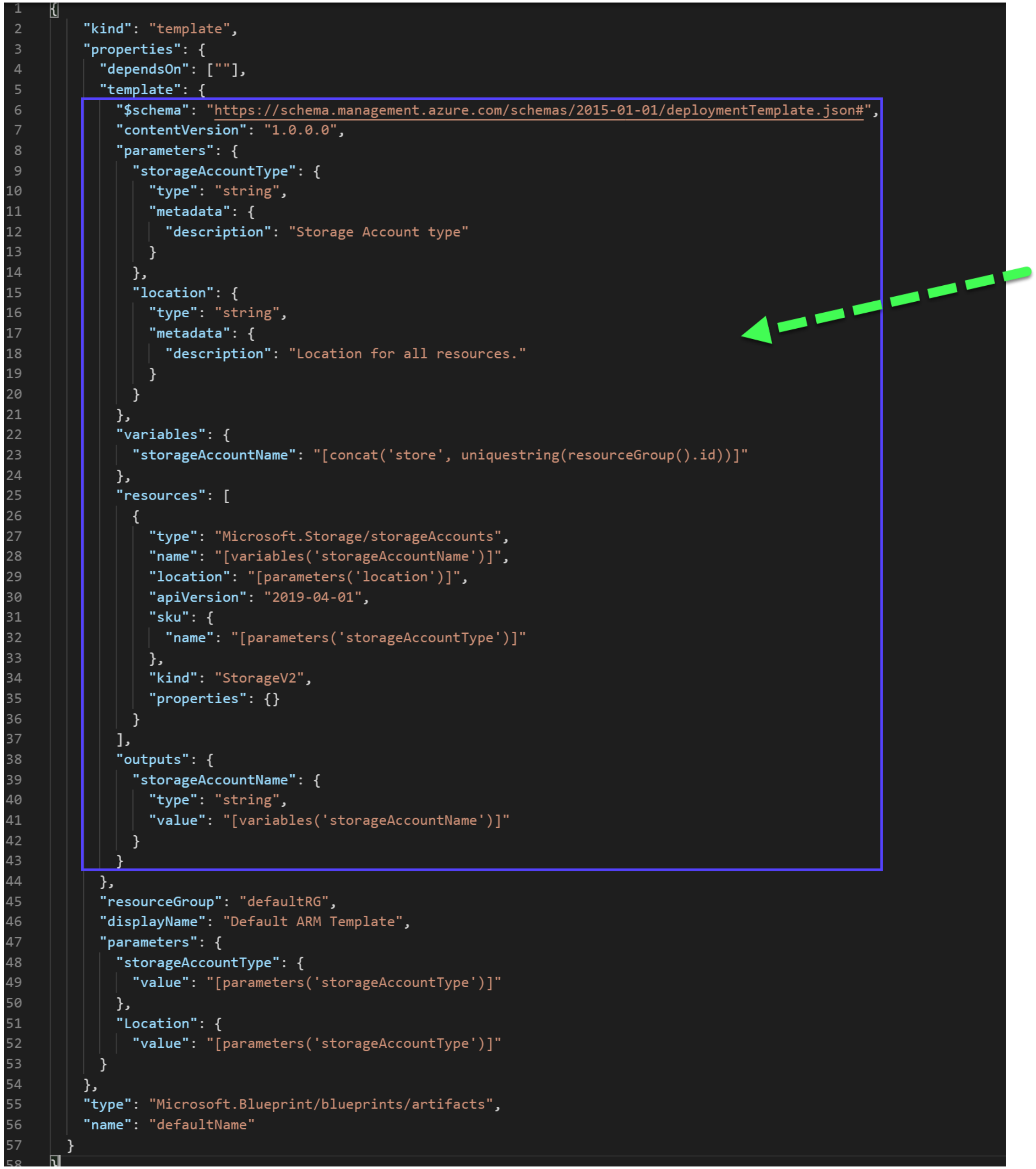


```
{
    "kind": "template",
    "properties": {
      "dependsOn": [""],
      "template": {

      },
      "resourceGroup": "defaultRG",
      "displayName": "Default ARM Template",
      "parameters": {
        "storageAccountType": {
          "value": "[parameters('storageAccountType')]"
        },
        "Location": {
          "value": "[parameters('storageAccountType')]"
        }
      }
    },
    "type": "Microsoft.Blueprint/blueprints/artifacts",
    "name": "defaultName"
  }
}
```



```
{
    "kind": "template",
    "properties": {
      "dependsOn": [""],
      "template": {

      },
      "resourceGroup": "defaultRG",
      "displayName": "Default ARM Template",
      "parameters": {
        "storageAccountType": {
          "value": "[parameters('storageAccountType')]"
        },
        "Location": {
          "value": "[parameters('storageAccountType')]"
        }
      }
    },
    "type": "Microsoft.Blueprint/blueprints/artifacts",
    "name": "defaultName"
  }
}
```

ARM Template goes here



```
{
    "kind": "template",
    "properties": {
      "dependsOn": [""],
      "template": {
        "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
        "contentVersion": "1.0.0.0",
        "parameters": {
          "storageAccountType": {
            "type": "string",
            "metadata": {
              "description": "Storage Account type"
            }
          },
          "location": {
            "type": "string",
            "metadata": {
              "description": "Location for all resources."
            }
          }
        },
        "variables": {
          "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
        },
        "resources": [
          {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[variables('storageAccountName')]",
            "location": "[parameters('location')]",
            "apiVersion": "2019-04-01",
            "sku": {
              "name": "[parameters('storageAccountType')]"
            },
            "kind": "StorageV2",
            "properties": {}
          }
        ],
        "outputs": {
          "storageAccountName": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
          }
        }
      },
      "resourceGroup": "defaultRG",
      "displayName": "Default ARM Template",
      "parameters": {
        "storageAccountType": {
          "value": "[parameters('storageAccountType')]"
        },
        "Location": {
          "value": "[parameters('storageAccountType')]"
        }
      }
    },
    "type": "Microsoft.Blueprint/blueprints/artifacts",
    "name": "defaultName"
  }
}
```

ARM Template

Drawbacks

- Manually entering the parameters for each assignment
- Version control of Blueprints is not the “version control” we need
- Managing multi deployments through the Azure Portal doesn’t scale well

Blueprints with Azure DevOps by example

Use Case

JJ Binks – CEO of Cloud Adventures, a software company that provides a solution to support manufacturers in optimizing their order picking process.

Cloud Adventures just landed a contract with 3 large manufacturers: *Incom-FreiTek*, *Sienar Fleet Systems* and *Astromech*.

The contract includes hosting their solutions on Microsoft Azure and implement guard rails to ensure the environments are conforming with applicable laws and regulations. Each customer has different requirements when it comes to Governance. JJ Binks would like to deploy the Cloud Adventures solution to each environment but maintain consistency and remain in control.

Additionally, each customer has their own requirements when it comes to the location of their environment:

- Incom-Freitek operates out of Europe and requires their data to remain within Europe
- Sienar Fleet Systems operates out of the United States, data needs to remain within the US
- Astromech requires their data to remain in the UK

As Cloud Adventures used to do single (manual) deployments, they are now looking at automating the process and deploy their solution from a single source of truth in an automated way.

Use Case

JJ Binks – CEO of Cloud Adventures, a software company that provides a solution to support manufacturers in optimizing their order picking process.

Cloud Adventures just landed a contract with 3 large manufacturers: *Incom-FreiTek*, *Sienar Fleet Systems* and *Astromech*.

The contract includes hosting their solutions on Microsoft Azure and implement guard rails to ensure the environments are conforming with applicable laws and regulations. Each customer has **different requirements** when it comes to Governance. JJ Binks would like to deploy the Cloud Adventures solution to each environment but **maintain consistency and remain in control**.

Additionally, each customer has their own requirements when it comes to the location of their environment:

- Incom-Freitek operates out of Europe and requires their **data to remain within Europe**
- Sienar Fleet Systems operates out of the United States, **data needs to remain within the US**
- Astromech requires their **data to remain in the UK**

As Cloud Adventures used to do single (manual) deployments, they are now looking at **automating the process** and deploy their solution from a **single source of truth** in an automated way.

Use Case

- Consistency
- Custom Configuration per customer
- Automated Deployment
- Single Source of Truth

What just happened?

- ~~3 large manufacturers~~
- ~~Implement guard rails~~
- ~~Nuances in the required guard rails~~
- ~~Managed from a single tenant~~
- Single source of truth.

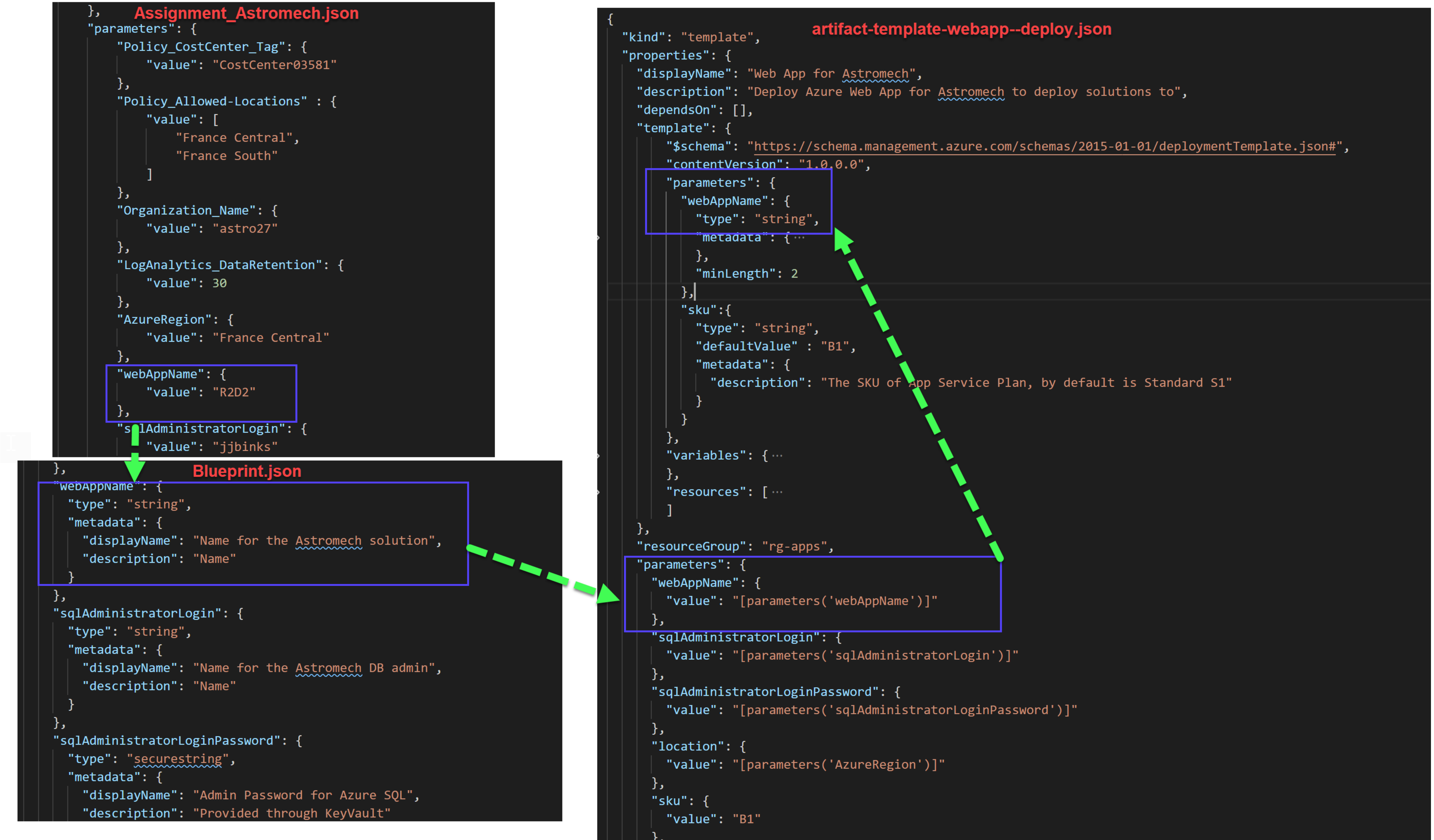
Drawbacks

- Managing through the portal is quite the "Point and click adventure"
- Managing parameters for each customer can be time-consuming
- Blueprints on a Management Group level is not suited for cross-tenant management
- Blueprints are incremental
- Manual versioning

Managing your Blueprints through Azure DevOps

What just happened?

- Single source of truth
- Source Control
- Versioning through Azure DevOps



Assignment_Astromech.json

```
    },
    "parameters": {
        "Policy_CostCenter_Tag": {
            "value": "CostCenter03581"
        },
        "Policy_Allowed-Locations" : {
            "value": [
                "France Central",
                "France South"
            ]
        },
        "Organization_Name": {
            "value": "astro27"
        },
        "LogAnalytics_DataRetention": {
            "value": 30
        },
        "AzureRegion": {
            "value": "France Central"
        },
        "webAppName": {
            "value": "R2D2"
        },
        "sqlAdministratorLogin": {
            "value": "jjbinks"
```

Blueprint.json

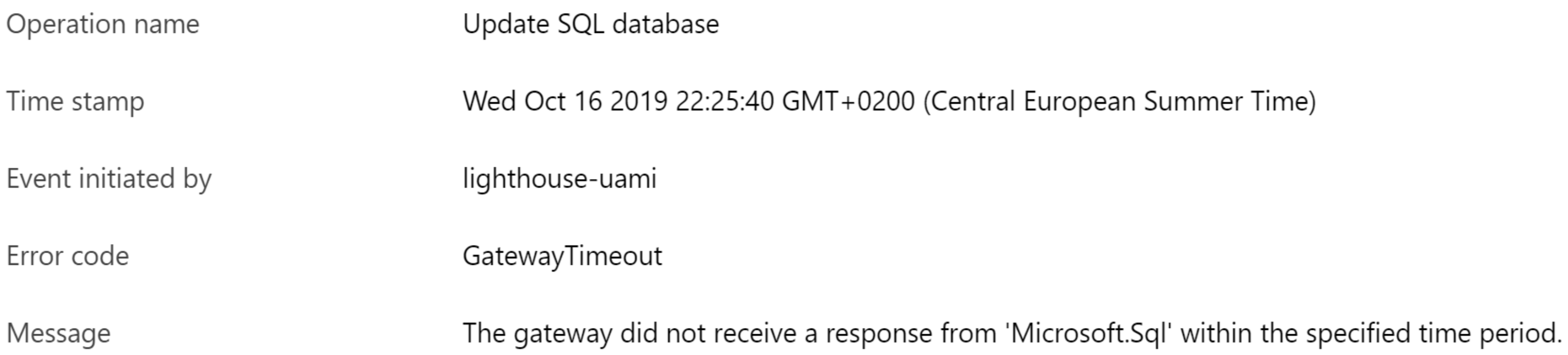
```
},
"webAppName": {
  "type": "string",
  "metadata": {
    "displayName": "Name for the Astromech solution",
    "description": "Name"
  }
},
"sqlAdministratorLogin": {
  "type": "string",
  "metadata": {
    "displayName": "Name for the Astromech DB admin",
    "description": "Name"
  }
},
"sqlAdministratorLoginPassword": {
  "type": "securestring",
  "metadata": {
    "displayName": "Admin Password for Azure SQL",
    "description": "Provided through KeyVault"
```

artifact-template-webapp--deploy.json

```
{
  "kind": "template",
  "properties": {
    "displayName": "Web App for Astromech",
    "description": "Deploy Azure Web App for Astromech to deploy solutions to",
    "dependsOn": [],
    "template": {
      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "contentVersion": "1.0.0.0",
      "parameters": {
        "webAppName": {
          "type": "string",
          "metadata": {···
          },
          "minLength": 2
        },
        "sku":{
          "type": "string",
          "defaultValue" : "B1",
          "metadata": {
            "description": "The SKU of App Service Plan, by default is Standard S1"
          }
        }
      },
      "variables": {···
      },
      "resources": [···
      ]
    },
    "resourceGroup": "rg-apps",
    "parameters": {
      "webAppName": {
        "value": "[parameters('webAppName')]"
      },
      "sqlAdministratorLogin": {
        "value": "[parameters('sqlAdministratorLogin')]"
      },
      "sqlAdministratorLoginPassword": {
        "value": "[parameters('sqlAdministratorLoginPassword')]"
      },
      "location": {
        "value": "[parameters('AzureRegion')]"
      },
      "sku": {
        "value": "B1"
      }
```

Drawbacks

- Learning Curve
- Azure Resource Manager time outs



Operation name	Update SQL database
Time stamp	Wed Oct 16 2019 22:25:40 GMT+0200 (Central European Summer Time)
Event initiated by	lighthouse-uami
Error code	GatewayTimeout
Message	The gateway did not receive a response from 'Microsoft.Sql' within the specified time period.

Wrap up

- Blueprints help with lifecycle management of your infrastructure
- Consistent and protected deployments
- Current ARM Templates can be added to artifacts with no additional configuration
- Blueprints scale well across subscriptions if you manage them as code
- Learning curve

But it’s still pretty awesome..

@whaakman

www.linkedin.com/in/wesleyhaakman

https://www.wesleyhaakman.org

Thank You