Modern Azure Infrastructure as Code mit Bicep und Deployment Stacks

Agenda

1. Speaker
2. Azure Resource Manager (ARM)
3. From ARM to Bicep
4. ARM template - generated
5. From ARM to Bicep
6. Bicep
7. ARM template vs. Bicep
8. AVM - Azure Verified Modules
9. Deployment Stacks
10. Deployment
11. Deployment stacks limitations
12. Summary

Speaker

Jan-Henrik Damaschke

CTO, Senior Cloud Architect, Founder

@Visorian GmbH | Microsoft Azure MVP

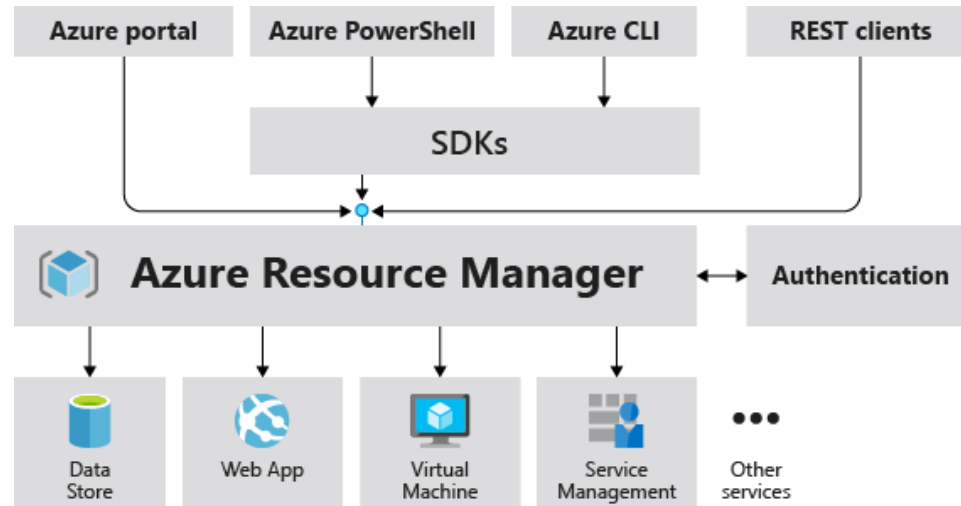
Socials

/jandamaschke

/in/jan-henrik-damaschke

Azure Resource Manager (ARM)

- Foundation for deploying and managing Azure resources.
- Consistent interface across all Azure tools
- Supports Infrastructure as Code (IaC) using declarative syntax
- Implements control plane and data plane



From ARM to Bicep

- 😀 **ARM templates are mapping natively to ARM APIs**
- 😮‍💨 **ARM templates are mapping natively to ARM APIs**

ARM

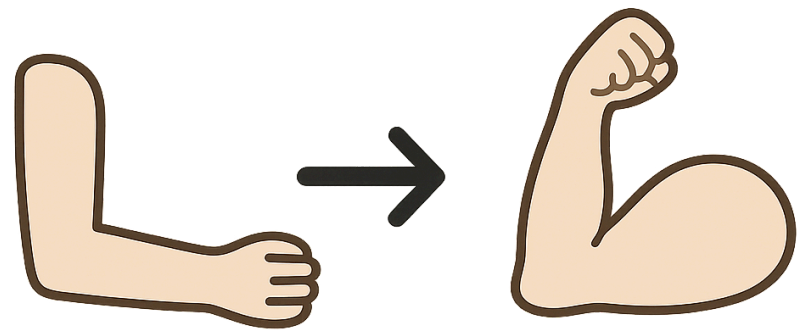
```
{
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2024-01-01",
      "name": "[parameters('storageAccounts_stgbicepde
      "location": "germanywestcentral",
      "sku": {
        "name": "Standard_LRS",
        "tier": "Standard"
      },
      "properties": {
        "dnsEndpointType": "Standard",
        "defaultToOAuthAuthentication": true,
        "publicNetworkAccess": "Enabled",
        "immutableStorageWithVersioning": {
          "enabled": true
        }
      }
    }
  ]
}
```

ARM template - generated

```
"variables": {
                        "copy": [
                            {
                                "name": "formattedRoleAssignments",
                                "count": "[length(coalesce(parameters('roleAssignments'), createArray()))]",
                                "input": "[union(coalesce(parameters('roleAssignments'), createArray())[copyIndex(
                            }
                        ],
                        "enableReferencedModulesTelemetry": false,
                        "supportsBlobService": "[or(or(or(equals(parameters('kind'), 'BlockBlobStorage'), equals(p
                        "supportsFileService": "[or(or(equals(parameters('kind'), 'FileStorage'), equals(parameter
                        "formattedUserAssignedIdentities": "[reduce(map(coalesce(tryGet(parameters('managedIdentit
                        "identity": "[if(not(empty(parameters('managedIdentities'))), createObject('type', if(coal
                        "builtInRoleNames": {
                            "Contributor": "[subscriptionResourceId('Microsoft.Authorization/roleDefinitions', 'b2
                            "Owner": "[subscriptionResourceId('Microsoft.Authorization/roleDefinitions', '8e3af657
                            "Reader": "[subscriptionResourceId('Microsoft.Authorization/roleDefinitions', 'acdd72a
                            "Reader and Data Access": "[subscriptionResourceId('Microsoft.Authorization/roleDefini
                            "Role Based Access Control Administrator": "[subscriptionResourceId('Microsoft.Authori
                            "Storage Account Backup Contributor": "[subscriptionResourceId('Microsoft.Authorizatio
                            "Storage Account Contributor": "[subscriptionResourceId('Microsoft.Authorization/roleD
                            "Storage Account Key Operator Service Role": "[subscriptionResourceId('Microsoft.Autho
```

From ARM to Bicep

- **Template Specs were introduced to share templates securely via RBAC**
- **Azure Blueprints introduced for better bundling**
- **Bicep as an abstraction for an improved authoring experience**



Bicep

- **Better readability & dx**
- **Implicit dependencies**
- **Compiled to ARM**
- **Modularization & code reuse**
- **Strongly typed & validated parameters**

ARM template vs. Bicep

ARM | Bicep

```
{
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2024-01-01",
      "name": "[parameters('storageAccounts_stgbicepdeploymentstack_name')]",
      "location": "germanywestcentral",
      "sku": {
        "name": "Standard_LRS",
        "tier": "Standard"
      },
      "properties": {
        "dnsEndpointType": "Standard",
        "defaultToOAuthAuthentication": true,
        "publicNetworkAccess": "Enabled",
        "immutableStorageWithVersioning": {
          "enabled": true
        }
      }
    }
  ]
}
```

AVM - Azure Verified Modules

- **Successor of CARML and other efforts**
- **Validated resource, pattern and utility modules**
- **Responsible person at Microsoft**
- **WAF aligned**
- **No preview versions**
- **No full parameter support**

Deployment Stacks

- **Stateful resource tracking**
- **Full lifecycle control**
- **Deny assignments**
- **Support for new ARM features**

Deployment

```
az deployment sub create
--name GUID
--location germanywestcentral
--template-file ./main.bicep
--parameters ./dev.bicepparam
```

```
az stack sub create
--name best-stack
--location germanywestcentral
--template-file ./main.bicep
--parameters ./dev.bicepparam
--action-on-unmanage detachAll
--deny-settings-mode denyDelete
# --what-if
```

Deployment stacks limitations

- **No what-if support (yet)**
- **Azure PowerShell issues**
- **Permissions not clearly explained, partially unclear**

Summary

ARM templates -> Bicep

Blueprints -> Deployment Stacks

AVM for standardization

Extensions, Developer Experience and Ecosystem

Thank you