Jan Vanuytrecht
jan.vanuytrecht@kapuani.be

+32 3 375 26 03
info@kapuani.be

kapuani

Let Bicep do the heavy lifting

Haha.. Ha.. Ha..

kapuani

About 3.640.000.000 results (0,30 seconds)

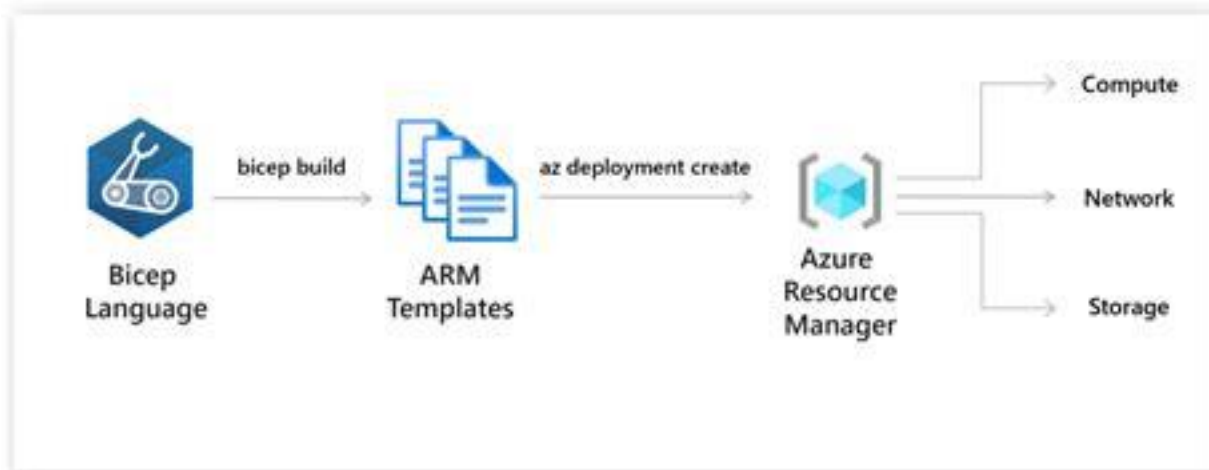| Māori – detected ▼	⇄	English ▼
kapua ✕		cloud

Jan Vanuytrecht - Toon Van Deuren

IAC?

Desired state configuration

What you describe is what you get

Caveat example: arrays, at some places..

Bicep > no statefile like in Terraform!!

- IaC > Bicep/Terraform
  - Desired State

ARM?

ARM?

```
          }
        },
        "copy": [
          {
            "name": "dataDisks",
            "count": "[parameters('numberOfDisks')]",
            "input": {
              "diskSizeGB": "[parameters('sizeOfEachDataDiskInGB')]",
              "lun": "[copyIndex('dataDisks')]",
              "name": "[concat(variables('vmName'), '_DataDisk', copyIndex('dataDisks'))]",
              "createOption": "Empty",
              "managedDisk": {
                "storageAccountType": "[parameters('storageType')]"
              }
            }
          }
        ]
      },
      "networkProfile": {
        "networkInterfaces": [
          {
            "id": "[resourceId('Microsoft.Network/networkInterfaces', variables('nicName'))]"
          }
        ]
      }
    }
  },
  {
    "type": "Microsoft.Compute/virtualMachines/extensions",
    "name": "[concat(variables('vmName'),'/', variables('DscExtensionName'))]",
    "apiVersion": "2017-03-30",
    "location": "[parameters('location')]",
    "dependsOn": [
      "[variables('vmName')]"
    ],
    "properties": {
      "publisher": "Microsoft.Powershell",
      "type": "DSC",
      "typeHandlerVersion": "2.19",
      "autoUpgradeMinorVersion": true,
      "settings": {
        "ModulesUrl": "[variables('modulesUrl')]",
        "SasToken": "[parameters('_artifactsLocationSasToken')]",
        "ConfigurationFunction": "[variables('configurationFunction')]",
        "Properties": {
          "MachineName": "[variables('vmName')]"
        }
      }
    }
  }
],
"outputs": {
  "fqdn": {
    "type": "string",
    "value": "[reference(variables('publicIPAddressName')).dnsSettings.fqdn]"
  }
}
```

```
1   @description('The email address of the owner of the service')
2   @minLength(1)
3   param publisherEmail string
4
5   @description('The name of the owner of the service')
6   @minLength(1)
7   param publisherName string
8
9   @description('The pricing tier of this API Management service')
10  @allowed([
11    'Basic'
12    'Consumption'
13    'Developer'
14    'Standard'
15    'Premium'
16  ])
17  param sku string = 'Developer'
18
19  @description('The instance size of this API Management service.')
20  param skuCount int = 1
21
22  @description('Location for all resources.')
23  param location string = resourceGroup().location
24
25  resource apiManagement 'Microsoft.ApiManagement/service@2021-08-01' = {
26    name: 'apiservice${uniqueString(resourceGroup().id)}'
27    location: location
28    sku: {
29      name: sku
30      capacity: skuCount
31    }
32    properties: {
33      publisherEmail: publisherEmail
34      publisherName: publisherName
35    }
36    identity: {
37      type: 'SystemAssigned'
38    }
39  }
40
```

```
1   {
2     "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3     "contentVersion": "1.0.0.0",
4     "metadata": {
5       "_generator": {
6         "name": "bicep",
7         "version": "0.34.44.8038",
8         "templateHash": "8070384426886005230"
9       }
10    },
11    "parameters": {
12      "publisherEmail": {
13        "type": "string",
14        "minLength": 1,
15        "metadata": {
16          "description": "The email address of the owner of the service"
17        }
18      },
19      "publisherName": {
20        "type": "string",
21        "minLength": 1,
22        "metadata": {
23          "description": "The name of the owner of the service"
24        }
25      },
26      "sku": {
27        "type": "string",
28        "defaultValue": "Developer",
29        "allowedValues": [
30          "Basic",
31          "Consumption",
32          "Developer",
33          "Standard",
34          "Premium"
35        ],
36        "metadata": {
37          "description": "The pricing tier of this API Management service"
38        }
39      },
40      "skuCount": {
41        "type": "int",
42        "defaultValue": 1,
43        "metadata": {
44          "description": "The instance size of this API Management service."
45        }
46      },
47      "location": {
48        "type": "string",
49        "defaultValue": "[resourceGroup().location]",
50        "metadata": {
51          "description": "Location for all resources."
52        }
53      }
54    },
55    "resources": [
56      {
57        "type": "Microsoft.ApiManagement/service",
58        "apiVersion": "2021-08-01",
59        "name": "[format('apiservice{0}', uniqueString(resourceGroup().id))]",
60        "location": "[parameters('location')]",
61        "sku": {
62          "name": "[parameters('sku')]",
63          "capacity": "[parameters('skuCount')]"
64        },
65        "properties": {
66          "publisherEmail": "[parameters('publisherEmail')]",
```

```bicep
@description('Required. Name of the Container App.')          You, 13 months ago • add bicep modules
param name string

@description('Optional. Location for all Resources.')
param location string = resourceGroup().location

@description('Optional. Bool indicating if app exposes an external http endpoint.')
param ingressExternal bool = true

@allowed([
  'auto'
  'http'
  'http2'
  'tcp'
])
@description('Optional. Ingress transport protocol.')
param ingressTransport string = 'auto'

@description('Optional. Bool indicating if HTTP connections to is allowed. If set to false HTTP con
param ingressAllowInsecure bool = true

@description('Optional. Target Port in containers for traffic from ingress.')
param ingressTargetPort int = 80

@description('Optional. Maximum number of container replicas. Defaults to 10 if not set.')
param scaleMaxReplicas int = 1

@description('Optional. Minimum number of container replicas.')
```

- Params/variables
- Resources
- Modules
- Existing/loops

```bicep
116    resource sqlConnectionStringSecret 'Microsoft.KeyVault/vaults/secrets@2021-06-01-preview' existing = {
117      parent: sharedKeyVault
118      name: sqlConnectionStringName
119    }
120
121    // We don't set the default properties appInsightsId and storageAccountId, as this would set app setti
       You, 3 weeks ago | 1 author (You)
122    module appServiceModule 'modules/Microsoft.Web/sites/deploy.bicep' = {
123      name: '${affix}-app'
124      scope: gppModuleRG
125      params: {
126        location: location
127        name: appServiceName
128        kind: 'app'
129        serverFarmResourceId: servicePlan.id
130        clientAffinityEnabled: false
131        httpsOnly: true
132        systemAssignedIdentity: true
133        appSettingsKeyValuePairs: {
134          APPINSIGHTS_INSTRUMENTATIONKEY: '@Microsoft.KeyVault(SecretUri=${appInsightsKeySecret.properties
135          APPLICATIONINSIGHTS_CONNECTION_STRING: '@Microsoft.KeyVault(SecretUri=${appInsightsConnectionStr
```

File explorer:
- devops
  - templates
    - pipeline.yml
  - azure-pipelines.develop.yml
  - azure-pipelines.main.yml
  - infrastructure / bicep
    - modules
    - project-modules
    - secrets.bicep
  - main.acc.parameters.json
  - main.bicep
  - main.dev.parameters.json   M
  - main.prd.parameters.json
  - main.tst.parameters.json
  - .gitignore
  - README.md

```json
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "sqlSkuTier": {
            "value": "Standard"
        },
        "sqlSkuName": {
            "value": "S1"
        },
        "sqlDtu": {
            "value": 20
        },
        "sqlDbSizeBytes": {
            "value": 5368709120
        },
        "appServiceSku":{
            "value": { "name": "B1"}
        },
        "serviceBusSkuName": {
```

You, 13 months ago • init project bicep

Alternative or additional?

az cli

Cases:
- Delete resources
- Update specific properties

```
Write-Host "Executing: az network vnet peering update --resource-group $spokeRg --vnet-name $spokeVnetName --name $spokePeering.name --set useRemoteGateways=
az network vnet peering update --resource-group $spokeRg --vnet-name $spokeVnetName --name $spokePeering.name --set useRemoteGateways=true
}
```

Or: deployment scripts

What can bicep deploy?

Resources

Policies

- Compliance
- Audit, then
  - deny/ modify/ deploy
- Examples
  - VM sizes
  - Regions
  - Tag organization

```bicep
targetScope = 'managementGroup'

@description('Target Management Group')
param targetMG string

@description('An array of the allowed locations, all other locations will be denied by the created policy.')
param allowedLocations array = [
  'australiaeast'
  'australiasoutheast'
  'australiacentral'
]

var mgScope = tenantResourceId('Microsoft.Management/managementGroups', targetMG)
var policyDefinitionName = 'LocationRestriction'

resource policyDefinition 'Microsoft.Authorization/policyDefinitions@2020-03-01' = {
  name: policyDefinitionName
  properties: {
    policyType: 'Custom'
    mode: 'All'
    parameters: {}
    policyRule: {
      if: {
        not: {
          field: 'location'
          in: allowedLocations
        }
      }
      then: {
        effect: 'deny'
      }
    }
  }
}

resource policyAssignment 'Microsoft.Authorization/policyAssignments@2020-03-01' = {
  name: 'location-lock'
  properties: {
    scope: mgScope
    policyDefinitionId: extensionResourceId(mgScope, 'Microsoft.Authorization/policyDefinitions', policyDefinition.name)
  }
}
```

Policies

Add role assignment

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more ⧉

Job function roles | Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

🔍 key vault ✕ | Type : **All** | Category : **All**

Name ↑↓	Description ↑↓
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Cannot manage key vaul
Key Vault Certificate User	Read certificate contents. Only works for key vaults that use the 'Azure role-based access control' permission model.
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-ba
Key Vault Contributor	Lets you manage key vaults, but not access to them.
Key Vault Crypto Officer	Perform any action on the keys of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based a
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the 'Azure role-based access control
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the 'Azure role-based access control' permission model.
Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key vaults that use the 'Azure role-based access control' permission mo
Key Vault Data Access Administrator	Manage access to Azure Key Vault by adding or removing role assignments for the Key Vault Administrator, Key Vault Certificates Off
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key materia
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based
Key Vault Secrets User	Read secret contents. Only works for key vaults that use the 'Azure role-based access control' permission model.
Operator Nexus Key Vault Writer Service Role (Preview)	(Preview) Provides Azure Operator Nexus services the ability to write to a Key Vault. This role is in preview and subject to change.

Showing 1 - 13 of 13 results.

- RBAC

```
resource keyVault_roleAssignments 'Microsoft.Authorization/roleAssignments@2022-04-01' = [
  for (roleAssignment, index) in (roleAssignments ?? []): {
    name: guid(keyVault.id, roleAssignment.principalId, roleAssignment.roleDefinitionIdOrName)
    properties: {
      roleDefinitionId: contains(builtInRoleNames, roleAssignment.roleDefinitionIdOrName)
        ? builtInRoleNames[roleAssignment.roleDefinitionIdOrName]
        : contains(roleAssignment.roleDefinitionIdOrName, '/providers/Microsoft.Authorization/roleDefinitions/')
            ? roleAssignment.roleDefinitionIdOrName
            : subscriptionResourceId('Microsoft.Authorization/roleDefinitions', roleAssignment.roleDefinitionIdOrName)
      principalId: roleAssignment.principalId
      description: roleAssignment.?description
      principalType: roleAssignment.?principalType
      condition: roleAssignment.?condition
      conditionVersion: !empty(roleAssignment.?condition) ? (roleAssignment.?conditionVersion ?? '2.0') : null // Must only be set if condtion is set
      delegatedManagedIdentityResourceId: roleAssignment.?delegatedManagedIdentityResourceId
    }
    scope: keyVault
  }
]
```

- RBAC

Alerts

```bicep
module dataLostAlert '../../../../../ms-modules/avm/res/insights/scheduled-query-rule/main.bicep' = {
  name: 'hub-management-ar-log-data-lost-${deployId}'
  scope: resourceGroup(managementSubscriptionId,logRGName)
  params: {
    location: location
    name: 'Log analytics Data is being capped'
    alertDescription: 'Exceptional amount of data, which means something is wrong, check the logs to get more insights.'
    severity: 0
    enabled: true
    evaluationFrequency: 'PT5M'
    scopes: [
      logAnalyticsWorkspace.id
    ]
    targetResourceTypes: [
      'Microsoft.OperationalInsights/workspaces'
    ]
    windowSize: 'PT5M'
    criterias: {
      allOf: [
        {
          query: '\t_LogOperation | where Category =~ "Ingestion" | where Detail contains "OverQuota"\n'
          timeAggregation: 'Count'
          dimensions: []
          resourceIdColumn: '_ResourceId'
          operator: 'GreaterThan'
          threshold: 0
          failingPeriods: {
            numberOfEvaluationPeriods: 1
            minFailingPeriodsToAlert: 1
          }
        }
      ]
    }
    actions: [
      supportActionGroup.id
    ]
  }
}
```

Alerts
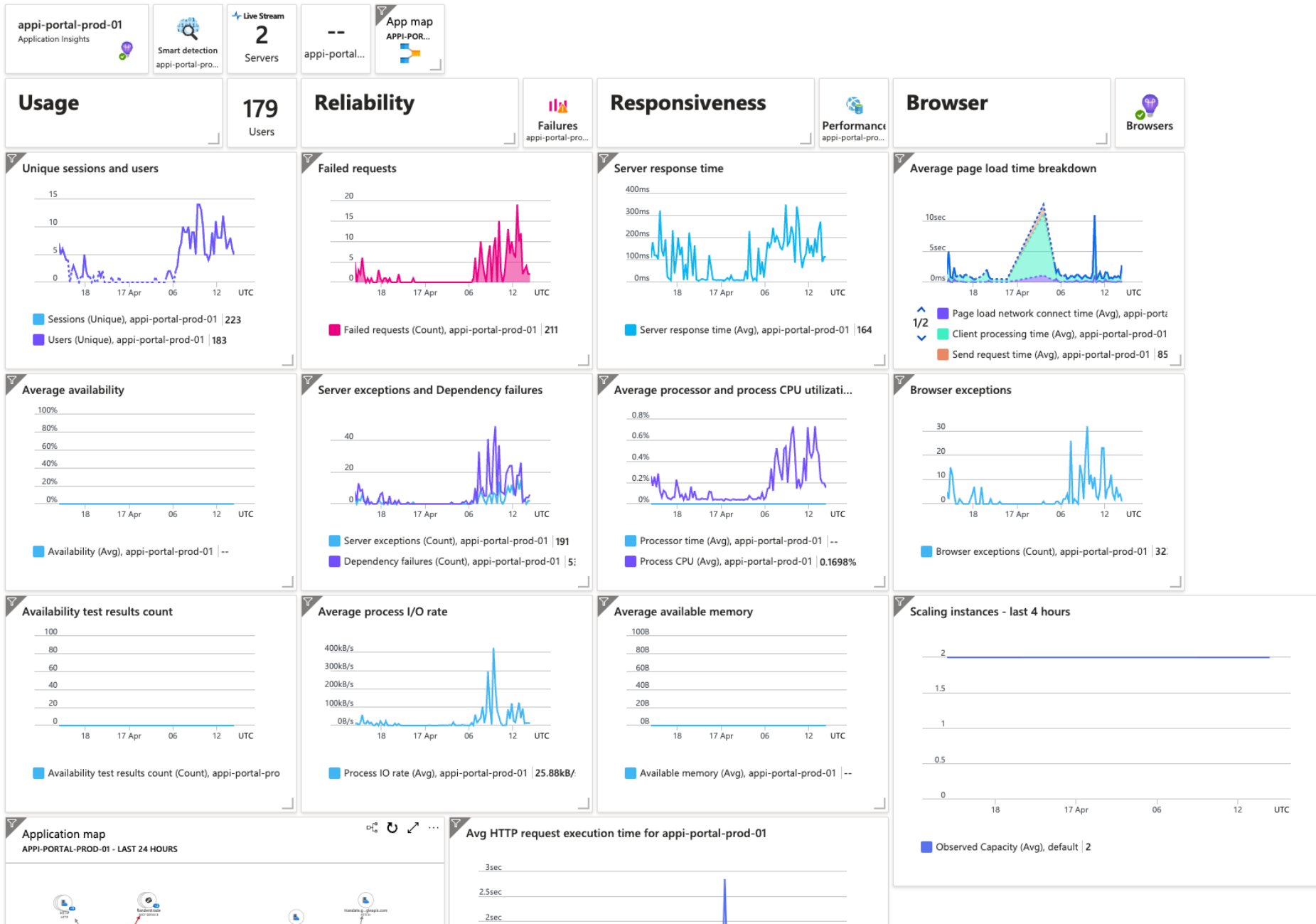
Dashboards

UNLIMITED POWER!!!

1.Azure AD Resources
- Users
- Groups
- Service Principals
- App Registrations
- Role Assignments at Management Group level
- Custom RBAC roles

2.Resource Provider Registration
- Cannot register new resource providers
- Must be done via Azure CLI/PowerShell/Portal

3.Subscription Management
- Cannot create new subscriptions
- Cannot change subscription billing
- Cannot transfer subscriptions

4.Management Group Structure
- Cannot create management group hierarchy
- Cannot move subscriptions between management groups

5.Cross-Tenant Operations
- Cannot create resources across tenants
- Cannot manage guest users
- Cannot set up cross-tenant access

What not?

6.Preview Features
- Some preview features are not available in ARM
- Must use Azure CLI/PowerShell/Portal

7.Resource Graph Operations
- Cannot query resources across subscriptions
- Cannot perform bulk operations

8.Support Tickets
- Cannot create or manage support tickets
- Cannot manage service health alerts

9.Marketplace Items
- Cannot publish to marketplace
- Cannot manage marketplace subscriptions

10.Some Network Operations
- Cannot create ExpressRoute circuits
- Cannot manage peering relationships
- Cannot create cross-region virtual network peering

These limitations often require using Azure CLI, PowerShell, or the Azure Portal for management.

What not?

Bicep magic wizard is you?

- Pipelines - Bicep
  - Build bicep
  - Validate bicep
  - What-if

Bicep build (az bicep build) only:Converts Bicep to ARM JSON
- Checks syntax
- Validates basic structure

Validation (az deployment group validate) does:

All of the above
- Checks resource provider registration
- Validates resource properties against API
- Verifies resource dependencies
- Validates parameter values
- Checks resource quotas
- Validates RBAC permissions
- Verifies resource naming rules
- Checks resource availability in region
- Validates SKU availability
- Checks resource limits

Key difference: Build is just syntax check, validation is full deployment simulation without actually deploying.

- Pipelines - Bicep
  - Build bicep
  - Validate bicep
  - What-if

- Dekt niet alles
  - Bvb.: key vault name die al in gebruik is

Fix typo casesensitive sql migration path

Completed   !2929   JV   Jan Vanuytrecht proposes to merge feature/17505-pipeline-gpp into develop

Overview   Files   Updates   Commits

Jan Vanuytrecht completed this pull request   29 Mar

Cherry-pick   Revert

Merged PR 2929: Fix typo casesensitive sql migration path
965bb7e7   Jan Vanuytrecht   29 Mar at 17:58

Show details

✓ All required checks succeeded

View 3 checks ⓘ

✓ 1 reviewer approved

✓ No merge conflicts
Last checked 29 Mar

Description

Fix typo casesensitive sql migration path

Reviewers   Add ⌄

Required

No required reviewers

Optional

✓ JV Jan Vanuytrecht
Approved

Tags   +

No tags

Work items   +

Product Backlog Item 17505: Nieuwe
Updated 19m ago, ● Done   ✕

- Pipelines
  - PR (branch policies)

- Deployments in Azure
  - Opvolging
  - Error output

- Resource providers

- Microsoft Learn - Bicep Documentation
- Bicep GitHub Repository
- Azure Verified Modules (AVM)
- Azure rest api reference

ARM Quickstarts

> Bicep decompile
az bicep decompile --file main.json

Useful resources

kapuani

Jan Vanuytrecht
jan.vanuytrecht@kapuani.be

+32 3 375 26 03
info@kapuani.be

linktr.ee/kapuani2025

Contact
Feel free to reach out