

Building and Deploying a .NET 9 App Using Azure, Bicep, and GitHub Actions

Scott Sauber
Director of Engineering
Lean TECHniques
Level: Introductory



What you need

- .NET 9
- An Editor that supports .NET 9 and Bicep
 - Visual Studio 2022 Latest
 - Visual Studio Code (Bicep extension)
- Fork this repo:
 - <https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>
 - Slides in root under Slides.pdf
- Download the Azure CLI
- Azure will be provided for free
- Please let Scott know the following if you're participating:
 - Email you will use for Azure
 - Your GitHub username

What we all need

- Azure to not go down
- GitHub to not go down
- GitHub Actions to not go down
- The conference internet to not go down
- 🙏 🙏 🙏
- (I do have recordings if needed but that's no fun)

Audience

- Anyone interested in Azure, GitHub, or Bicep
- .NET Developers
- People interested in DevOps but never got to do it
- Already know Git
- If you have questions, ask them! If no one but me talks this is gonna be boring

Poll

- How many .NET Developers in the room?
- How many have used Azure?
- How many have used Bicep?
- How many have used GitHub Actions?
- Why are you here? What do you want to learn?

Agenda

- What is the final state of what we're building?
- What is Azure?
- What is Azure App Service? Plans?
- What is Bicep?
- What are GitHub Actions?
- Health Checks
- Azure Key Vault Integration
- Azure Application Insights Integration
- Hands on all throughout

Goals

- Learn GitHub Actions, Bicep, and Azure
- How they all integrate with a .NET app
- The feedback loop on this can be slow – especially if you typo!
- Take home a few things back to work, whether beginner or expert

Who am I?

- Director of Engineering at Lean TECHniques
- Microsoft MVP
- Dometrain author
- Redgate Community Ambassador
- Co-organizer of Iowa .NET User Group



What are we building?

- .NET 9 API
- Running on Azure App Service
- Configured using Infrastructure as Code with Bicep
- Deployed using a CI/CD Pipeline via GitHub Actions

Features of what we're building

- Zero Downtime Deployments
- Infrastructure managed by code, not clicking in the Azure Portal
- Automated Build and Deploys
- Follows Azure Naming Standards
- Versioning your app so you know what's deployed
- Health Checks
- Secrets in Key Vault, not Source Control
- Observability using Application Insights

Why is this important?

- <https://dora.dev/>
- DORA
- Continuous Delivery, Deployment Automation, Flexible Infrastructure, Continuous Integration, Version Control, Monitoring/Observability are all listed as 6 of the 18 capabilities listed for high performing teams.
- We will touch on all of these today



Scott Sauber

@scottsauber

Setting up a CI/CD pipeline for the first time be like



8:55 PM · Jan 25, 2022

||| View post engagements



15



17



128





GitHub Action Runner

- CI (artifacts)

Passes

- Deploy to Dev

Passes

- Deploy to Prod

Deploy

Deploy



Dev Environment



App Service



Prod Environment



App Service

Azure

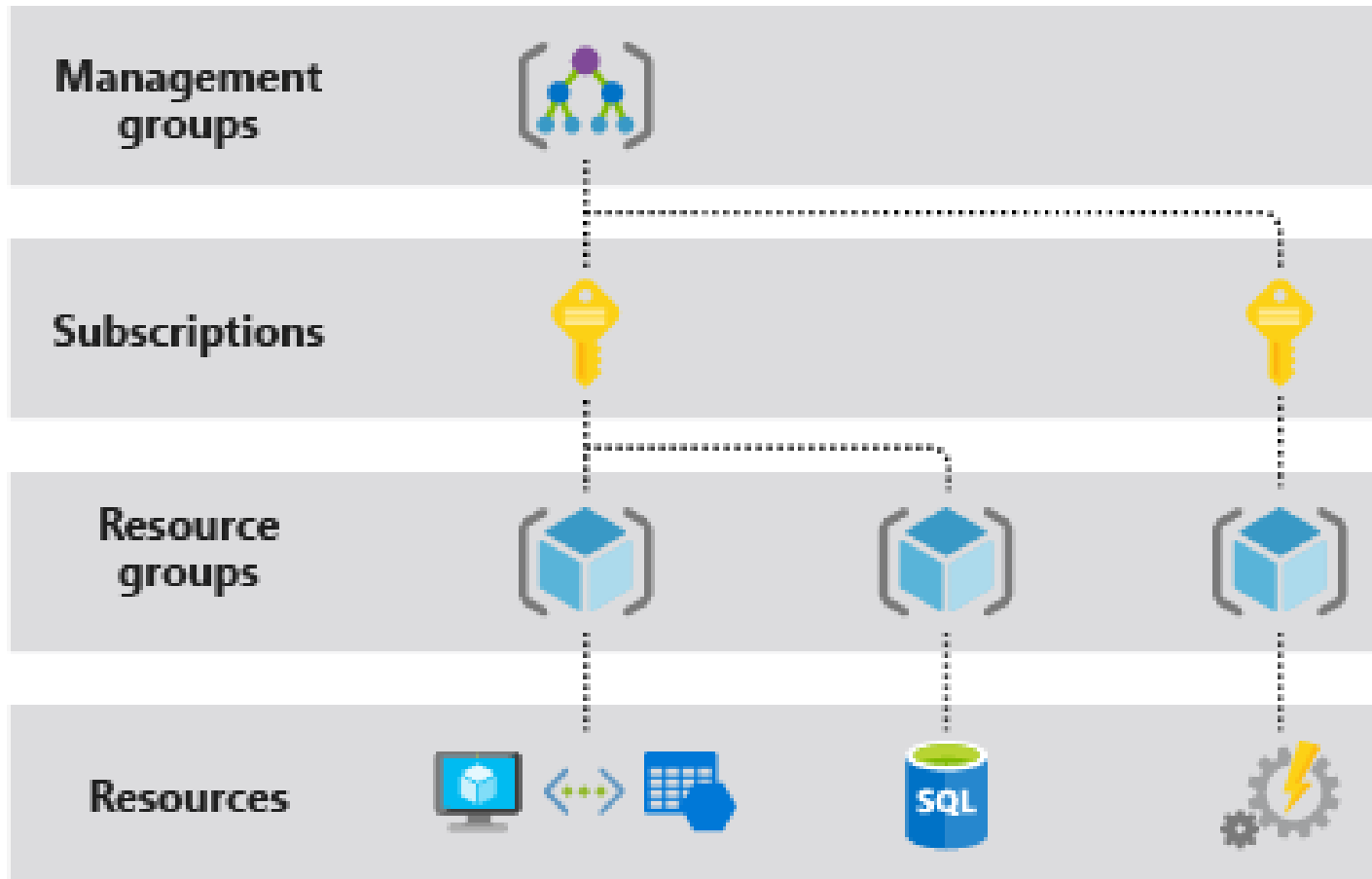


What is Azure?

- Microsoft offering for cloud hosting
- Offers many services from hosting web apps to databases to caching to messaging to...
- You should probably be picking PaaS offerings (i.e. not VMs)

On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

- You manage
- Service provider manages

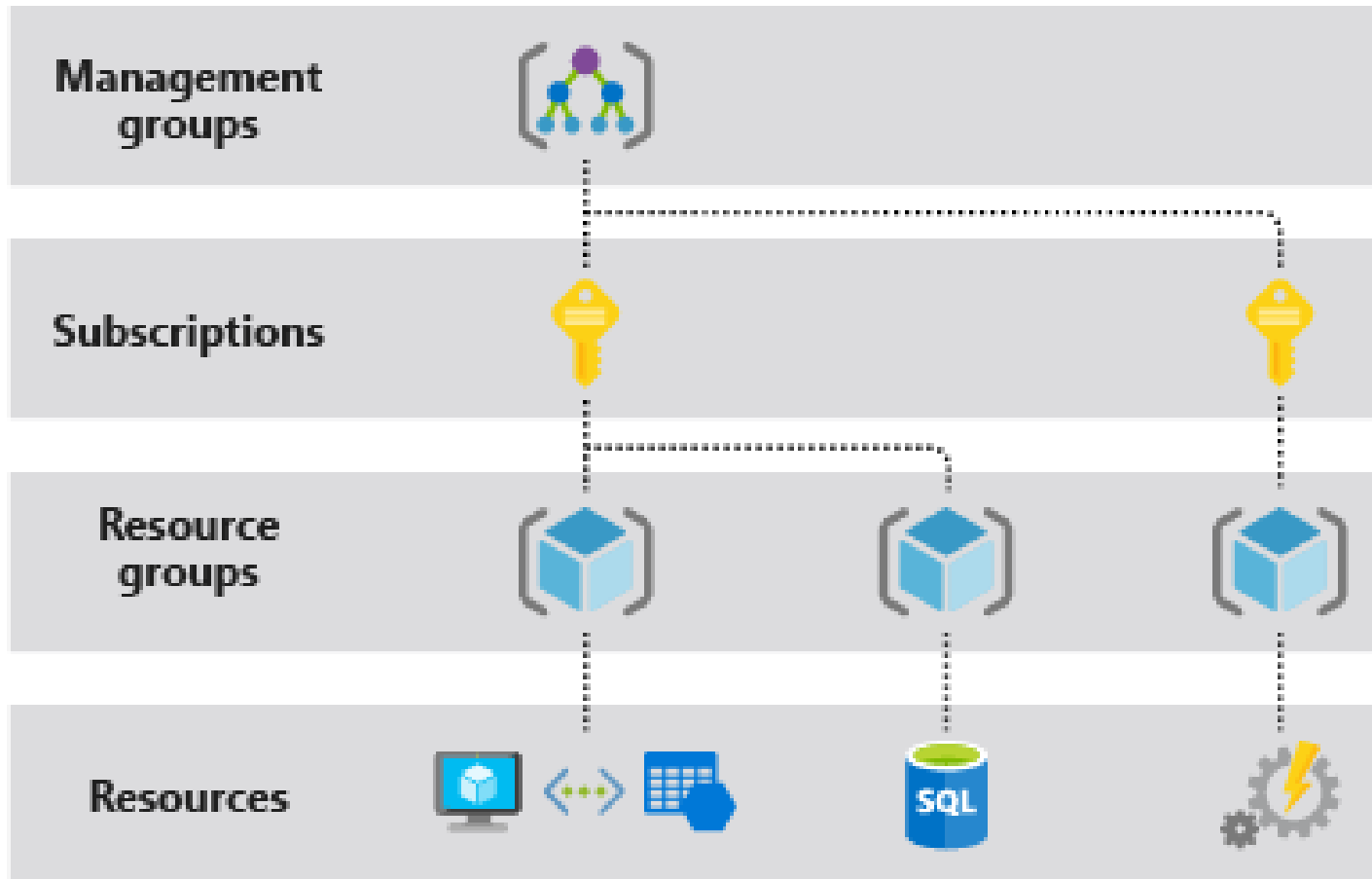


Subscriptions

- Top-ish level organization (ignoring Tenants, Management Groups)
- Recommended per team per env
- Naming convention: sub-<team>-<env>
 - Ex: sub-accounting-dev
- Role access separation
- Billing separation

Resource Groups

- Related groups of resources (ie web, db, key vault, etc)
- Quickly view all resources related to app
- RG = folder, Resources = files
- Recommended per app per env
- Naming convention: rg-<product>-<env>
 - Example: rg-fancyapp-dev
- May have many RG's in 1 subscription
- Role access separation
- Billing separation











Questions?



Azure App Service



App Service

- PaaS offering for hosting applications
-  Handles OS patches, Framework patches
-  Zero downtime deployments via Slots
-  SSL Certs
-  Custom domains
-  Autoscaling
-  Very simple
-  And more
-  Less control because PaaS

App Service Plan

- Kinda like VM for your App Service(s)
- Pick how much memory, storage, CPU
- Multiple app service on one ASP (should you?)
- Many apps can get away with P0V3 (\$62/mo for Linux)
- Need to be at least Standard to get Slots

\$ an issue?

- Savings Plan – commit to \$ amount
- Save 25% 1 yr, 45% 3 yrs
- Reservation – commit to compute tier
- Save 35% 1 yr, 55% 3 yrs



Visits
<https://app-workshop-dnazghbicep-scottsauer-dev.azurewebsites.net>

Dev Environment



App Service



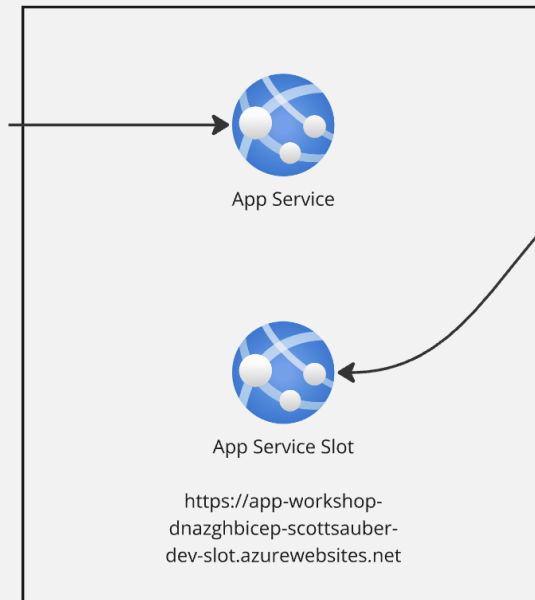
App Service Slot

<https://app-workshop-dnazghbicep-scottsauer-dev-slot.azurewebsites.net>



Visits
<https://app-workshop-dnazghbicep-scottsauer-dev.azurewebsites.net>

Dev Environment



GitHub Action Runner

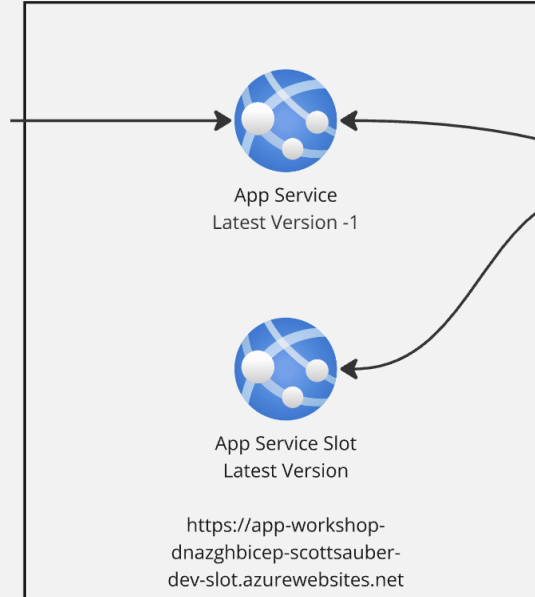
Deploy to Slot with latest

- Real App Service has latest -1 version
- Swap the Slot
- Real App Service has latest
- Slot now has latest -1 version



Visits
<https://app-workshop-dnazghbicep-scottsauer-dev.azurewebsites.net>

Dev Environment



GitHub Action Runner

- Deploy to Slot with latest
- Real App Service has latest -1 version
- Swap the Slot
- Real App Service has latest
- Slot now has latest -1 version



CUSTOMER

Visits
<https://app-workshop-dnazghbicep-scottsauer-dev.azurewebsites.net>

Dev Environment



App Service Slot
Latest Version -1

<https://app-workshop-dnazghbicep-scottsauer-dev-slot.azurewebsites.net>



App Service
Latest Version



GitHub Action Runner

- Deploy to Slot with latest
- Real App Service has latest -1 version
- Swap the Slot
- Real App Service has latest
- Slot now has latest -1 version

Live Demo



Questions?



Bicep



Infrastructure as Code (IAC)

- Source code defining what resources to provision
- Stored in version control
- Declarative – what resources to create, not how to create them
- Deployed via pipeline
- Need a new env? Few lines of code

Without IAC

- Clickety Clack Configuration™
- Repeat yourself for each environment
- “It worked in Dev/UAT/Staging, not Prod”
- “It works on my machine”

What is Azure Bicep?

- Used to configure Azure resources
- Built and maintained by Microsoft
- Domain-specific language (fancy word for custom)

What is Azure Bicep?

- Provides intellisense, error checking, “whatif,” and orders the resource creations
- Built on top of Azure Resource Manager (ARM) – don’t use ARM directly
- Can compose multiple files into “modules”
- Can pass data between modules via outputs
- No state file

What is Azure Bicep?

```
appservice.bicep
1 resource appServicePlan 'Microsoft.Web/serverfarms@2022-09-01' = {
2   name: 'asp-myapp-dev'
3   location: 'centralus'
4   sku: {
5     name: 'S1'
6   }
7   kind: 'linux'
8 }
```

`<>` appservice.bicep

```
1  resource appServicePlan 'Microsoft.Web/serverfarms@2022-09-01' = {  
2    name: 'asp-myapp-dev'  
3    kind: 'linux'  
4    location: 'centralus'  
5    sku: {  
6      name: 'S1'  
7    }  
8  }
```

Create Web App - Microsoft Az x +

https://portal.azure.com/#create/Microsoft.WebSite

Microsoft Azure Search resources, services, and docs (G+)

Home > App Services >

Create Web App ...

Name asp-myapp-dev ✓
.azurewebsites.net

Operating System * ☒ Linux ☐ Windows

Region * Central US

Pricing plan **Standard S1** (100 total ACU, 1.75 GB memory, 1 vCPU)

```
resource appServicePlan 'Microsoft.Web/serverfarms@2022-09-01' = {  
  name: 'asp-workshop-demo'  
  location: 'centralus'  
  sku: {  
    name: 'S1'  
  }  
  kind: 'linux'  
}
```

```
resource appService 'Microsoft.Web/sites@2022-09-01' = {  
  name: 'app-workshop-demo'  
  location: 'centralus'  
  properties: {  
    serverFarmId: appServicePlan.id  
    // others  
  }  
}
```

```
param appName string
@allowed(['dev', 'prod'])
param environment string
param location string
```

```
resource appServicePlan 'Microsoft.Web/serverfarms@2022-09-01' = {
  name: 'asp-${appName}-${environment}'
  location: location
  sku: {
    name: 'S1'
  }
  kind: 'linux'
}
```


dev.bicepparam file

```
using '../main.bicep'  
  
param environment = 'dev'
```

But how do I deploy it?

```
az deployment group create
  --name dev-deployment-1
  --template-file infrastructure/main.bicep
  --parameters infrastructure/environments/dev.bicepparam
  --resource-group rg-some-name-here
  --verbose
```

Key Concepts – Quiz time!

- Resources
- Modules
- Parameters
- .bicepparam
- Outputs
- --whatif

Benefits

- No manual work of configuring in the portal (and repeating for each env)
- Eliminate configuration drift
- Traceability of who, did what, and when
- Give Contributor access to the pipeline – not to individuals
- No more “it works in Dev, not Prod” bc they’re the same!

Additional Resources

- Documentation for various Bicep resources:
 - <https://learn.microsoft.com/en-us/azure/templates/microsoft.web/sites?pivots=deployment-language-bicep>

Live Demo



Questions?



First Hands On Lab coming up... ...how do you want to run these?

1. I give you time to do alone then move on
2. We “Do It Live™” together



Break then Hands On for 40 minutes

Module 4:

<https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>



CI/CD Pipelines



Continuous Integration

- Automated verification of your application that generates artifacts
- Compiles the app
- Runs the tests
- Independent witness - eliminates “works on my machine”

Continuous Delivery

- Takes the artifacts from CI and deploys them automatically
- Doesn't deploy all the way to Production
- Deploying to Production is a button click

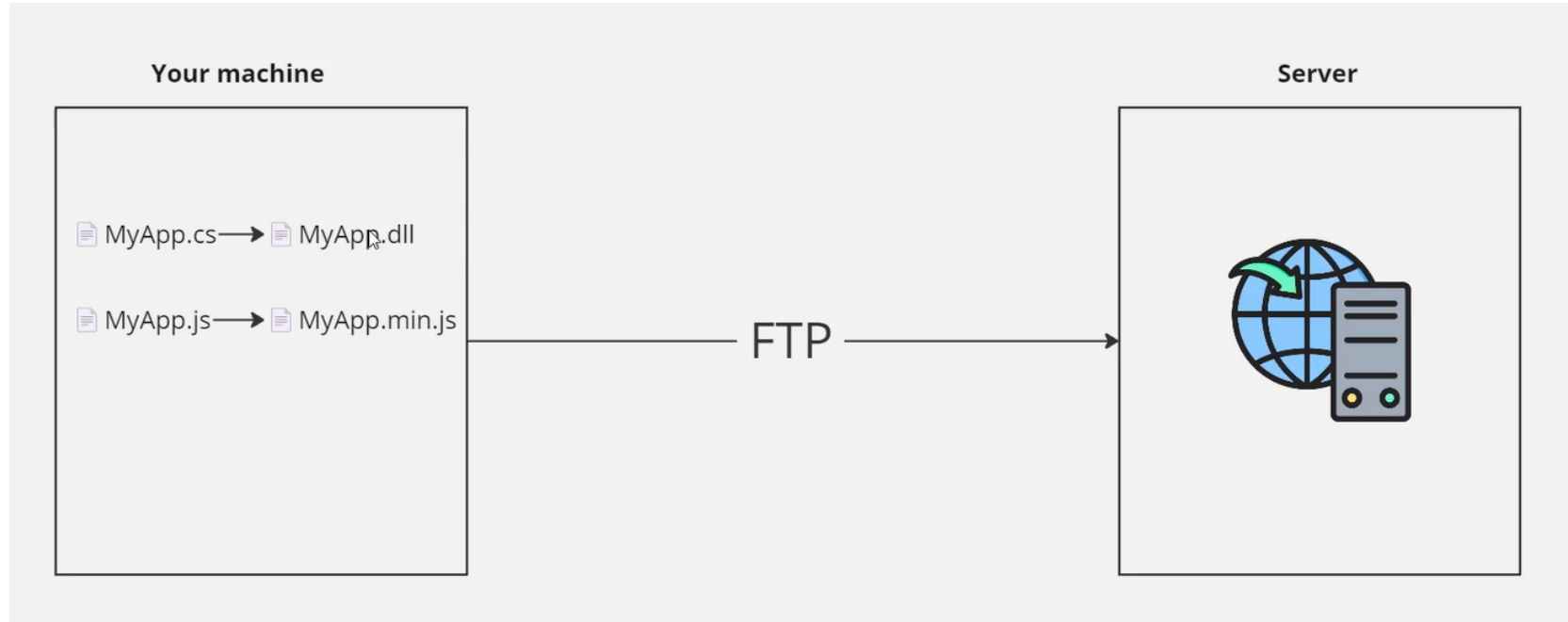
Continuous Deployment

- Deploys all the way to Production automatically
- If the pipeline is green, it's going to Production

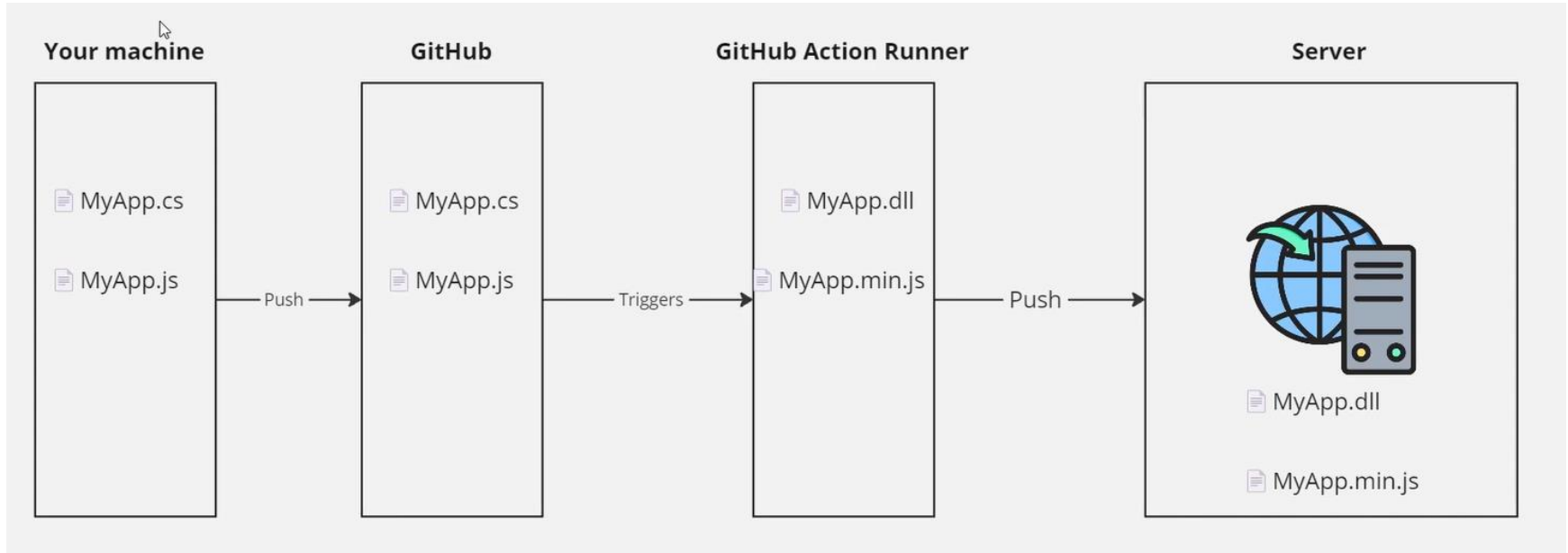
Confident Green

- If our build passes – why aren't we shipping to Production?
- Likely lack of confidence
- Likely missing automated tests or zero downtime deployments, let's fix that
- Ok now why?
- Repeat

Before CI/CD



After CI/CD



What's in a Pipeline?

Continuous Integration

- ✓ Restore Packages
- ✓ Compile
- ✓ Test
- ✓ Format
- ✓ Linting
- ✓ Security Scans
- ✓ Upload Artifacts
- ✓ Alerting on Failure

Continuous Delivery/Deployment

- ✓ Download Artifacts
- ✓ Deploy Artifacts
- ✓ Zero Downtime
- ✓ Deploy IAC
- ✓ Smoke Tests
- ✓ Alerting on Failure

Questions?



GitHub Actions



What is GitHub Actions?

- Thing doer on a trigger
- Trigger could be PR, push to main branch, open an issue, etc
- Automatically build and deploys your application
- Including the infrastructure (i.e. Bicep)

GitHub Actions Concepts

- Workflows
- Triggers
- Jobs
- Steps
- Inputs
- Secrets

Example

```
1  name: CI - Deploy App and Bicep
2
3  on:
4    push:
5      branches: [main]
6    workflow_dispatch:
7
8  jobs:
9    build_and_test:
10     runs-on: ubuntu-latest
11     name: Build, Test, Upload Artifact
12
13     steps:
14       - name: Checkout repo
15         uses: actions/checkout@v1
16
17       - name: Run dotnet test
18         run: |
19           dotnet test -c Release
20
```

How do I reuse workflows?

```
1  name: CI - Deploy App and Bicep
2
3  on:
4    push:
5      branches: [main]
6    workflow_dispatch:
7
8  jobs:
9    build_and_test:
10     runs-on: ubuntu-latest
11     name: Build, Test, Upload Artifact
12
13     steps:
14       - name: Checkout repo
15         uses: actions/checkout@v1
16
17       - name: Run dotnet test
18         run: |
19           dotnet test -c Release
20
21       - name: Run dotnet publish
22         run: |
23           dotnet publish ./src/WorkshopDemo/WorkshopDemo.csproj -c Release -o ./publish
```

How do I reuse workflows?

```
1  name: Step - Test and Publish
2
3  on:
4    workflow_call:
5      inputs:
6        project_path:
7          required: true
8          type: string
9
10 jobs:
11   build_and_test:
12     runs-on: ubuntu-latest
13     name: Build, Test, Upload Artifact
14
15     steps:
16       - name: Checkout repo
17         uses: actions/checkout@v1
18
19       - name: Run dotnet test
20         run: |
21           dotnet test -c Release
22
23       - name: Run dotnet publish
24         run: |
25           dotnet publish "${{ inputs.project_path }}" -c Release -o ./publish
```


Consume reusable workflow

```
1  name: CI - Test and Publish
2
3  on:
4    push:
5      branches: [main]
6    workflow_dispatch:
7
8  jobs:
9    build_and_test:
10      uses: ../.github/workflows/step-build-and-test.yml
11      with:
12        project_path: ./src/WorkshopDemo/WorkshopDemo.csproj
13
```

Consume from another repo

```
1  name: CI - Test and Publish
2
3  on:
4    push:
5      branches: [main]
6    workflow_dispatch:
7
8  jobs:
9    build and test:
10      uses: my-org-or-username/repo-name/step-build-and-test.yml
11      with:
12        project_path: ./src/WorkshopDemo/WorkshopDemo.csproj
13
```

Live Demo



Questions?



Break then Hands On for 40 minutes

Module 6:

<https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>



Health Checks

What are Health Checks?

- Health Checks check an app's status
- Might stop a rolling deployment
- Might restart the app on failure
- App Services allow configuring Health Check endpoint

What are Health Checks?

- /api/healthz
- Why z?
- Z-pages from Google

What do you check?

- Even “nothing” is useful. If it can’t get to the URL – the app didn’t boot
- Can I connect to dependencies? (ie DB, APIs, Secret Store, etc)
- Note: be careful here – if your DB goes down/blips, do you want your app to restart?

C#

```
var builder = WebApplication.CreateBuilder(args);
```

```
builder.Services.AddHealthChecks();
```

```
var app = builder.Build();
```

```
app.MapHealthChecks("/healthz");
```

```
app.Run();
```

Questions?

Hands On for 15 minutes

Module 8:

<https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>

Azure Key Vault



What is Azure Key Vault

- Secret Store for Azure
- Don't store secrets in Version Control
- Traceability
- Rotate Secrets
- \$0.03 per 10K requests

Best Practices

- Separate Key Vault per app per env
- 1 app * 3 envs = 3 key vaults
- 2 apps * 3 envs = 6 key vaults
- Don't leak keys across envs or apps
- Naming: kv-<appname>-<environment>
- ie kv-myapp-dev

.NET Integration

- Plugs into IConfiguration
- Loads keys on app boot (saves \$ and more performant)
- Azure.Security.KeyVault.Secrets
- `builder.Configuration.AddAzureKeyVault("url");`

Managed Identities

- Essentially the user (Service Principal) a service (ie App Service) runs as
- Allows you to say “this App Service can talk to this Key Vault/DB/etc”
- Microsoft handles the credentials for you behind the scenes

Access Policies for Key Vault

- Allows you to specify who can connect to Key Vault
- Could be a group (ie Developers), user, or application
- Applications usually just need Read not Write

Local Secret Management

- Local dev often requires secrets
- .NET User Secrets is incompatible with teams, especially large ones
- Everyone has their own file on their machine
- Then secrets get shared around when they're added/updated
- Recommendation: use Key Vault even for local

Key Vault for Local

- When someone adds/updates/deletes a secret, everyone gets it
- Very team friendly
- Only downside – heartbeat to an Azure service
- In practice – rarely a problem

Live Demo



Questions?



Hands On for 30 minutes

Module 9:

<https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>



DefaultAzureCredential



What is DefaultAzureCredential?

- Azure services need to be authenticated to
- There are lots of ways to do this – CLI, Environment Variables, ManagedIdentity, etc
- DefaultAzureCredential tries all these for you until one works

What order does it try?

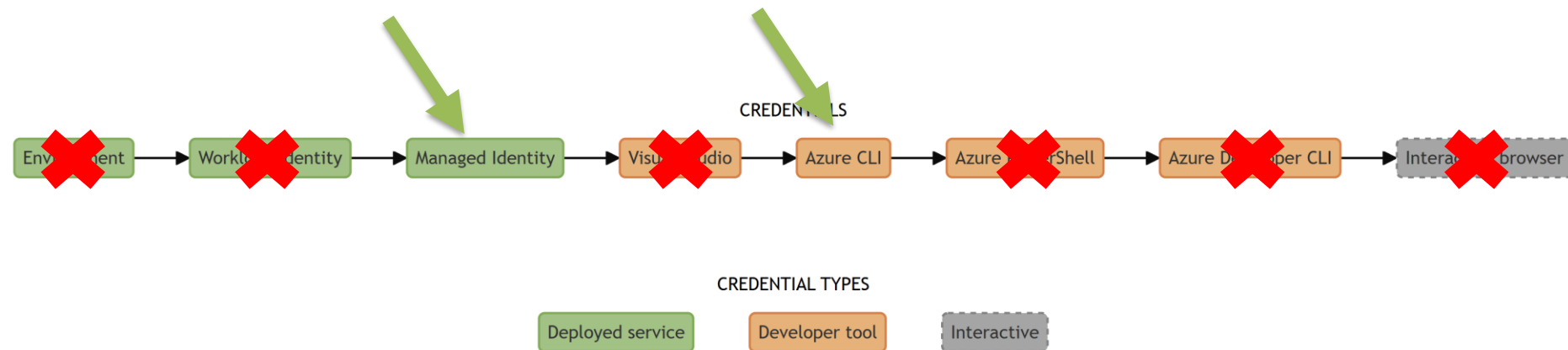
CREDENTIALS



CREDENTIAL TYPES



Which ones do we use?



What's the problem?

- Often need 1-2 ways of authing
- Local dev + deployed envs
- In our case, Azure CLI (Local) and Managed Identity (Dev + Prod)
- All other tries waste time
- I've seen 10+ seconds saved doing what I'm about to do

Solution

- DefaultAzureCredential has “Excludes”
- ChainedTokenCredential
- if local => CLI, else => ManagedIdentity

Live Demo



Questions?



Break?

Azure Log Analytics



What is Log Analytics?

- Part of Azure Monitor - observability platform
- Store Logs in central spot
- Not in Log Stream
- Query logs
- SQL like syntax
- Alert based on logs

New Query 1* +

Demo

Run

Time range : Last 12 hours

Save

Share

+ New alert rule

Export

Pin to

Tables

Queries

Functions

<<

Search

Filter

Group by: Solution

Collapse all

LogManagement

- AppDeliveryFailureLogs
- AGSGrafanaLoginEvents
- ALBHealthEvent
- Alert
- AppAvailabilityResults
- AppBrowserTimings
- AppDependencies
- AppEvents
- AppExceptions
- AppMetrics
- AppPageViews
- AppPerformanceCounters
- AppRequests
- AppServiceAntivirusScanAudit...
- AppServiceAppLogs
- AppServiceAuditLogs
- AppServiceAuthenticationLogs
- AppServiceConsoleLogs
- AppServiceFileAuditLogs
- AppServiceHTTPLogs
- AppServiceIPSecAuditLogs

1 AppRequests

Results Chart

Showing the first 30,000 results. [Learn more](#) on how to narrow down the result set.

Success	ResultCode	DurationMs	PerformanceBucket	Properties
true	200	9.7892	<250ms	{"_MS.ProcessedBy
true	200	102.1439	<250ms	{"_MS.ProcessedBy
false	404	2.6933	<250ms	{"_MS.ProcessedBy
false	0	5.6817	<250ms	{"LogLevel":"Error"
false	0	5.1909	<250ms	{"LogLevel":"Error"
true	200	3136.4451	3sec-7sec	{"_MS.ProcessedBy
true	200	103.5109	<250ms	{"_MS.ProcessedBy
true	200	100.8381	<250ms	{"_MS.ProcessedBy
true	200	6.6667	<250ms	{"_MS.ProcessedBy
false	404	1	<250ms	
false	404	0.8159	<250ms	{"_MS.ProcessedBy
true	200	8.8905	<250ms	{"_MS.ProcessedBy

7s 195ms

Display time (UTC+00:00)

[Query details](#)

1 - 13 of 30000



Run

Time range : Last 24 hours

Limit : 1000

KQL mode ▾

AppRequests

| where ResultCode in (``200`` , ``500`` , ``404`` , ``405``)

Results

Chart

TimeGenerated [UTC] ↑↓	Url	OperationName	Success	ResultCode	DurationMs
> 5/18/2024, 9:35:00.149 AM	http://ch...	GET Home/Index	true	200	79.2718
> 5/18/2024, 9:35:00.149 AM	http://ch...	GET Home/Index	true	200	79.2718
> 5/18/2024, 9:34:59.991 AM	http://fa...	POST /	false	500	101
> 5/18/2024, 9:34:59.991 AM	http://fa...	POST /	false	500	101

Columns

Questions?

Azure App Insights



What is Application Insights?

- Part of Azure Monitor
- Metrics
- Traces
- Application Maps
- Diagnose Performance Issues



Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Investigate

Application map

Smart detection

Live metrics

Transaction search

Availability

Failures

Performance

Troubleshooting guides

Monitoring

Alerts

Metrics

Diagnostic settings

Logs

Workbooks

Usage

Users

Sessions

Events

Funnels

User Flows

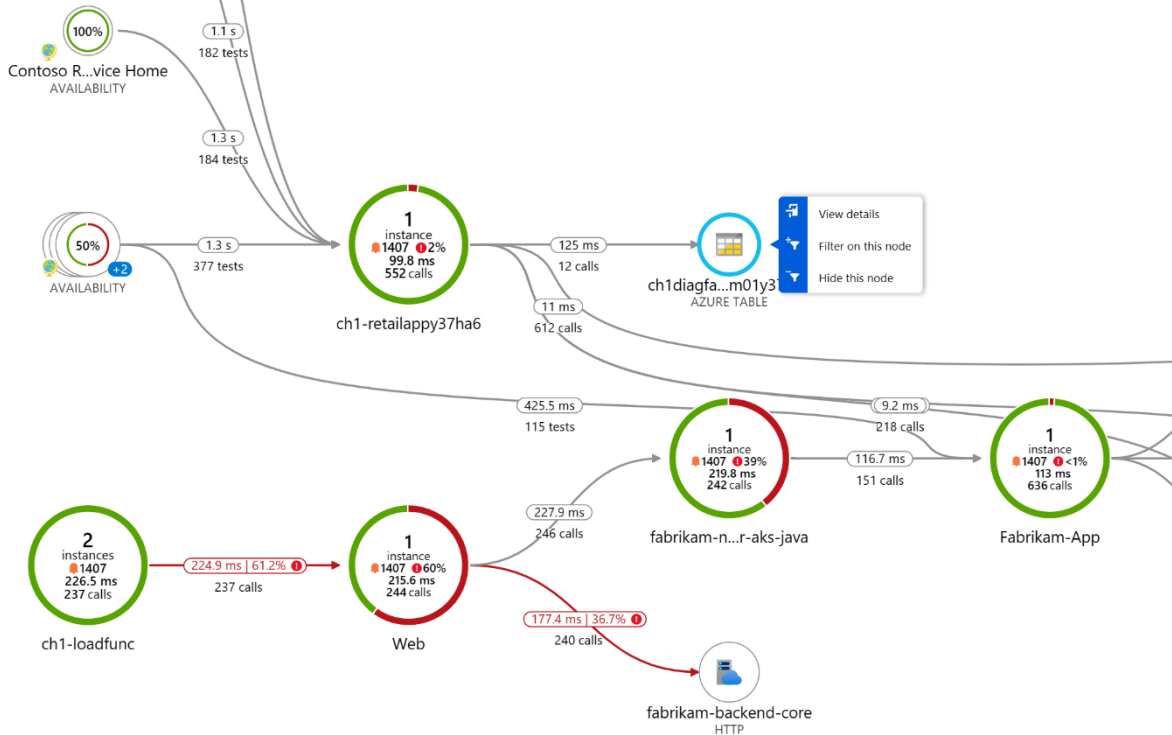
Cohorts

Last hour [Add filter](#)

Update map components

Intelligent view: [On](#) [Off](#)

Low Medium High

Exclude 4xx: [On](#) [Off](#)Layout: [On](#) [Off](#)

End-to-end transaction

Operation ID: b8e278fcd20456a88ab48ac9cde6476

Request (incoming)
Dependency (outgoing)
Exception
Profiler trace
Debug snapshot

EVENT	RES.	DURATION	0MS	200 MS	300 MS	400 MS	500 MS
<div> App Service Customer Details Central US </div>		557 ms	<div></div>				
<div> http://fabrikamfiberapp.azurewebsites.net/Customers/Details/8469 </div>		557 ms	<div></div>				
<div> fabrikamfiberapp GET Customers/Details </div>	500	430.3 ms	<div></div>				
<div> fabrikamxyz FabrikamISQL </div>		57 ms	<div></div>				
<div> fabrikamaccount POST fabrikamaccount/Tables </div>	409	112 ms	<div></div>				
<div> fabrikamaccount POST fabrikamaccount/fabrikamfiber </div>	409	111 ms	<div></div>				
<div> fabrikamaccount GET fabrikamaccount/fabrikamfiber </div>	200	48 ms	<div></div>				
<div> EXCEPTION System.FormatException </div>			<div></div>				
<div> Failed Central US </div>	0		<div></div>				

[Create work item](#)
[Open profiler traces](#)

fabrikamfiberapp
 GET Customers/Details

Request Properties

Show all

Event time	8/23/2018, 6:14:49 AM	...
Request name	GET Customers/Details	...
Response code	500	...
Successful request	False	...
Response time	430.3 ms	...
Request URL	http://fabrikamfiberapp.azurewebsites.net/Customers/Details/8469	...

Call Stack

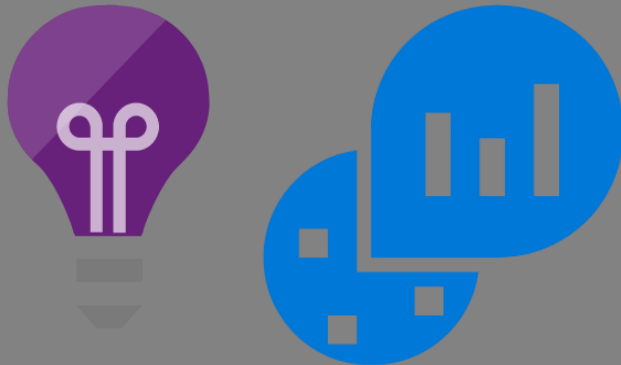
☐ Show Just My Code

```

System.FormatException:
  at System.Number.StringToNumber (mscorlib, Version=4.0.0.0, Cult
  at System.Number.ParseInt32 (mscorlib, Version=4.0.0.0, Culture=
  at System.Int32.Parse (mscorlib, Version=4.0.0.0, Culture=neutra
  at FabrikamFiber.DAL.Data.AddressValidator.ValidZipCode (Fabrika
  at FabrikamFiber.DAL.Models.Address.FullAddress (FabrikamFiber.D
  at ASP_Page_VIEWS_Customers_Details_cshtml.Execute (App_Web_sw4
  at System.Web.WebPages.WebPageBase.ExecutePageHierarchy (System.
  at System.Web.Mvc.WebViewPage.ExecutePageHierarchy (System.Web.M
  at System.Web.WebPages.StartPage.RunPage (System.Web.WebPages, V
  at System.Web.WebPages.StartPage.ExecutePageHierarchy (System.We
  at System.Web.WebPages.WebPageBase.ExecutePageHierarchy (System.
  at System.Web.Mvc.RazorView.RenderView (System.Web.Mvc, Version=
  at System.Web.Mvc.BuildManagerCompiledView.Render (System.Web.Mv
  at System.Web.Mvc.ViewResultBase.ExecuteResult (System.Web.Mvc, >
  at System.Web.Mvc.ControllerActionInvoker.InvokeActionResult />
  
```

Questions?

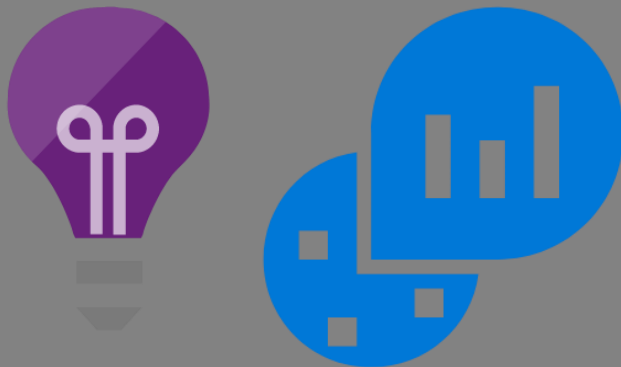
Live Demo



Hands On for 30 minutes

Module 13:

<https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>



Takeaways

- How to leverage Azure
- How to integrate Azure with .NET
- Why IAC is useful and how Bicep works
- How GitHub Actions fits into CI/CD Pipelines
- Some takeaway tips and tricks, even if you had prior experience with some of this

Resources

- This slide deck
- <https://github.com/scottsauber/workshop-dotnet-azure-github-bicep>
 - “final” branch has the final state of things

Live360 things to know

- 5:45 – 6:15 – Live360! First Timers Guide with Phil Japiske in
- 6:30 – 8:00 – Mix + Mingle Upstairs Patio HardRock Café City Walk

Any other Questions?

ssauber@leantechniques.com

@scottsauer on Twitter

@scottsauer.com on Bluesky

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!



THANK YOU!

If we have time...

Bonus: GitHub Environments

- GitHub natively has the concept of Environments
- These environments can have secrets
- You can also set up Protection Rules on environments
- Let's refactor our code to use Environments!

Bonus PR Checks for Infra

- When you change some Bicep it'd be nice to know what it's going to do
- --whatif for PR's
- Have the --whatif comment back on the PR what it's going to do
- Example

Bonus PR Checks for Infra

- Checkov security scanner
- Tells you if something is misconfigured
- ie TLS 1.2 is not the minimum TLS setting for an App Service
- Public Storage Accounts

```
→ bicep checkov -d /Users/maciejpoborca/Desktop/temp/bicep
[ bicep framework ]: 100%|██████████| [1/1], Current File Scanned=main.bicep
```



By bridgecrew.io | version: 2.1.75
Update available 2.1.75 -> 2.1.87
Run `pip3 install -U checkov` to update

bicep scan results:

Passed checks: 0, Failed checks: 6, Skipped checks: 0

Check: CKV_AZURE_132: "Ensure cosmosdb does not allow privileged escalation by restricting management plane changes"
FAILED for resource: Microsoft.DocumentDB/databaseAccounts.cosmosAccount
Severity: MEDIUM
File: /main.bicep:46-63
Guide: https://docs.bridgecrew.io/docs/bc_azr_storage_4

```
46 | resource cosmosAccount 'Microsoft.DocumentDB/databaseAccounts@2021-04-15' = {
47 |   name: cosmosAccountName
48 |   kind: 'GlobalDocumentDB'
49 |   location: location
50 |   properties: {
51 |     consistencyPolicy: {
52 |       defaultConsistencyLevel: 'Session'
53 |     }
54 |     locations: [
55 |       {
56 |         locationName: location
57 |         failoverPriority: 0
58 |         isZoneRedundant: false
59 |       }
60 |     ]
61 |     databaseAccountOfferType: 'Standard'
62 |   }
63 | }
```

Check: CKV_AZURE_15: "Ensure web app is using the latest version of TLS encryption"

THANK YOU!

(for real this time)