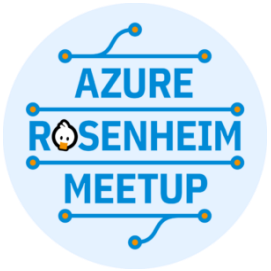
white duck

Neuigkeiten zu Containern und Kubernetes auf Azure

Azure Rosenheim Meetup, 29.11.2021



Microsoft Partner

Microsoft

Gold Cloud Platform
Gold DevOps
Silver Application Development
Silver Security
Silver Application Integration

GitHub

Wer sind wir?

Martin Brandl (white duck GmbH, Cloud Solution Architect & Azure MVP)
Twitter: @martin_jib
LinkedIn: linkedin.com/in/mbrandl/

Nico Meisenzahl (Senior Cloud & DevOps Consultant & Cloud & Data Management MVP)
Twitter: @nmeisenzahl
LinkedIn: https://www.linkedin.com/in/nicomeisenzahl/

Philip Welz (Senior Kubernetes & DevOps Engineer & CKA, CKAD & CKS)
Twitter: @philip_welz
LinkedIn: https://www.linkedin.com/in/philip-welz

white duck

twitter.com/whiteduck_gmbh

AZURE ROSENHEIM MEETUP

twitter.com/AzureMeetup

CLOUD NATIVE ROSENHEIM MEET UP

twitter.com/CloudNative_Ro

Azure Meetup STUTTGART

twitter.com/AzureStuttgart

© white duck GmbH 2021

Housekeeping

- Wir streamen dieses Meetup auf YouTube!
- Du hörst über YouTube zu?
  - Die Zoom Meeting URL gibt's im Meetup
    - https://www.meetup.com/Azure-Meetup-Rosenheim
  - Wir beobachten auch die Kommentare auf YouTube
- Unser nächstes Event
  - Azure Developer Community Day 2021 (07.12.)
    - https://www.meetup.com/Azure-Meetup-Rosenheim/events/282093556

© white duck GmbH 2021

Agenda

- Container auf Azure
- Azure Container Apps
- Container & Azure Kubernetes Service News
- Fragen / Networking

© white duck GmbH 2021

white duck

CONTAINER AUF AZURE

© white duck GmbH 2021

Container auf Azure

Kundenbetreute Infrastruktur → Plattformgesteuerte Infrastruktur

Orchestrierung durch den Nutzer

- Azure Kubernetes Service
- Azure Red Hat OpenShift

Orchestrierung durch die Plattform

Fokus auf Infrastruktur

- Azure Container Instances

Fokus auf Anwendungsentwicklung

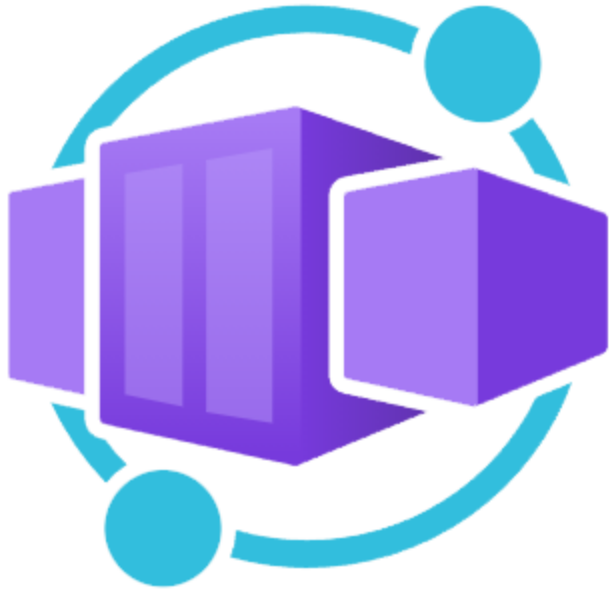
- Azure App Services *
- Azure Container Apps
- Azure Functions *
- Azure Spring Cloud

* bei Verwendung mit Containern

© white duck GmbH 2021

white duck

AZURE CONTAINER APPS



© white duck GmbH 2021

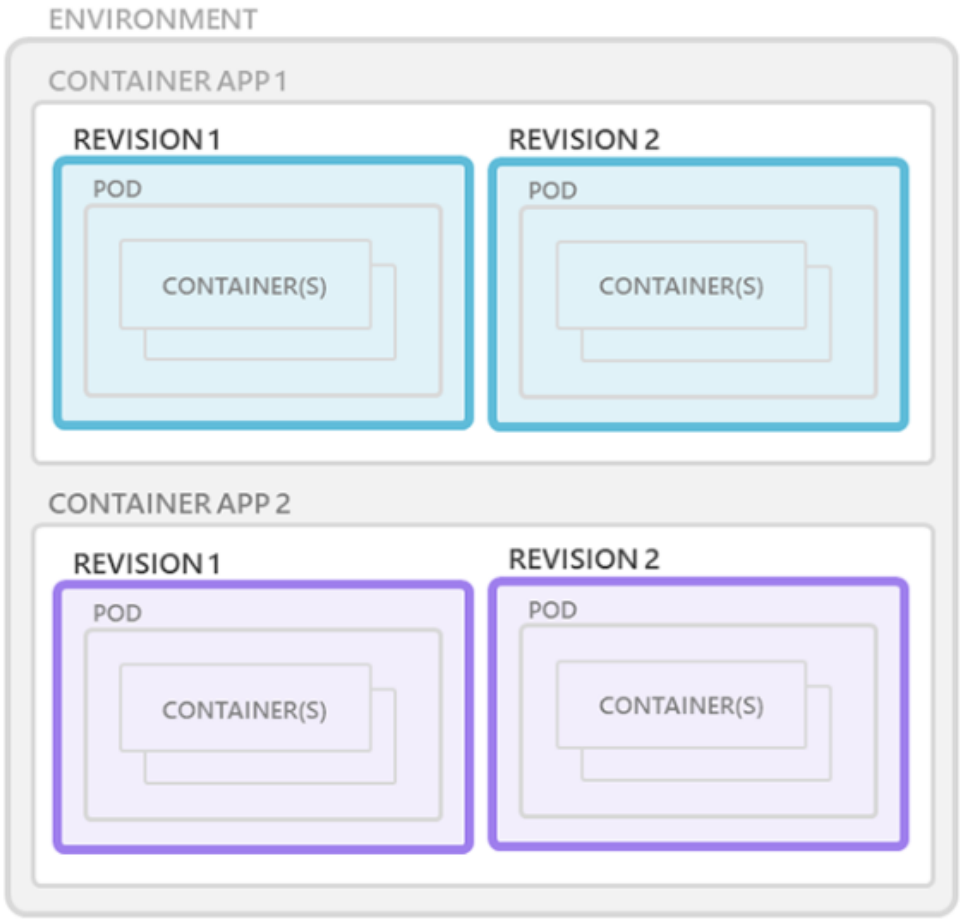
About Azure Container Apps

- announced during Microsoft Ignite 2021
- fully managed serverless container runtime
- Optimized for running general purpose containers, especially for applications that span many microservices
- Based on Kubernetes

© white duck GmbH 2021

Core Components

- **Environment**
  - secure boundary around groups of container apps
  - container apps inside share the same virtual network
  - write logs to the same Log Analytic workspace
- **Containers**
  - Grouped together in pods inside revision snapshots
  - Linux-based containers only
- **Revisions**
  - Immutable snapshots of a pod
  - Automatically created when a container configuration changes (Change types)
  - Can be used to split traffic (e. g. A/B testing or Blue/Green deployment)



© white duck GmbH 2021

Highlights

- Scaling with Kubernetes Event-driven Autoscaling (KEDA)
- Built in Distributed Application Runtime (dapr) support
- Built in Ingress with traffic splitting (Envoy proxy)

© white duck GmbH 2021

Azure Container Apps – Example scenarios

Azure Container Apps: Example scenarios

PUBLIC API ENDPOINTS

HTTP requests are split between two versions of the container app where the first revision gets 80% of the traffic, while a new revision receives the remaining 20%.

AUTO-SCALE CRITERIA

Scaling is determined by the number of concurrent HTTP requests.

BACKGROUND PROCESSING

A continuously-running background process that transforms data in a database.

AUTO-SCALE CRITERIA

Scaling is determined by the level of CPU or memory load.

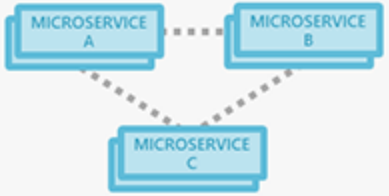
EVENT-DRIVEN PROCESSING

A queue reader application that processes messages as they arrive in a queue.

AUTO-SCALE CRITERIA

Scaling is determined by the number of messages in the queue.

MICROSERVICES



Deploy and manage a microservices architecture with the option to integrate with Dapr.

AUTO-SCALE CRITERIA

Individual microservices can scale according to any KEDA scale triggers.

Pricing

Requests

Container Apps are billed based on total number of requests executed each month. Executions are counted each time a app is executed in response to an HTTP request or an event. The first two million requests are included free each month.

Meter	Price	Free Grant (Per Month)
Requests	€0.483 per million	2 Million

Resource consumption

Container Apps are billed based on resource consumption measured in vCPU seconds and gi
month are free. Active usage occurs while your container is starting or while there is at least c
You can also configure Container Apps with a minimum number of instances to be always ru
processing any requests.

Meter	Active Usage Price	Idle Usage Price*	Free Grant (Per Month)
vCPU (seconds)	€0.0000294 per second	€0.0000035 per second	180,000 vCPU-seconds
Memory (GiB-Seconds)	€0.0000035 per second	€0.0000035 per second	360,000 GiB-seconds

2 CPU ~ 4,6€ / day ~ 138€ / month (18€ full idle)
4 GiB ~ 1,2€ / day ~ 36€ / month (same idle price)
= ~174€ / month

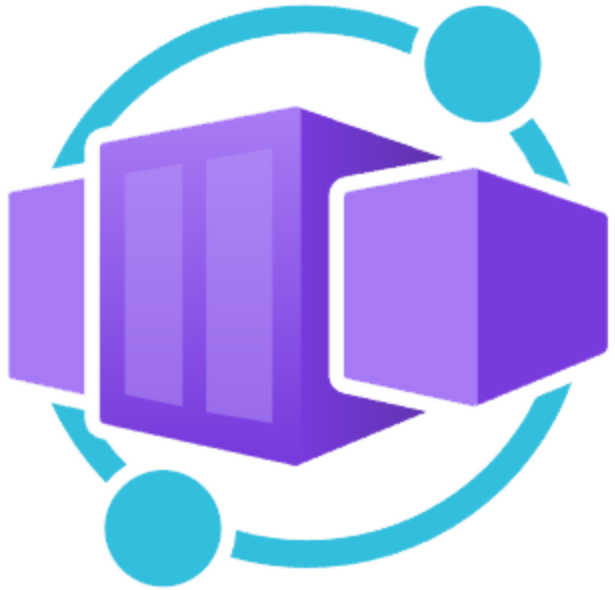
D2v3 (2vCPU + 8GB RAM) ~ 67 € / month

© white duck GmbH 2021

white duck

Azure container apps

DEMO



© white duck GmbH 2021

Azure CLI

az extension add --source https://workerappscliextension.blob.core.windows.net/azure-cli-extension/containerapp-0.2.0-py2.py3-none-any.whl

az containerapp env (create|delete|list…)

az containerapp (create|delete|list…)

az containerapp revision (activate|deactivate|list|restart)

© white duck GmbH 2021

Missing

- More sizing options
- Configuration Management
- Managed Identity support (coming soon)
- Additional examples / description of the YAML schema
- Support for more than 2 Environments within a subscription
- Availability in more than 2 region…
- Enterprise Features (Custom DNS, Private Link, …)

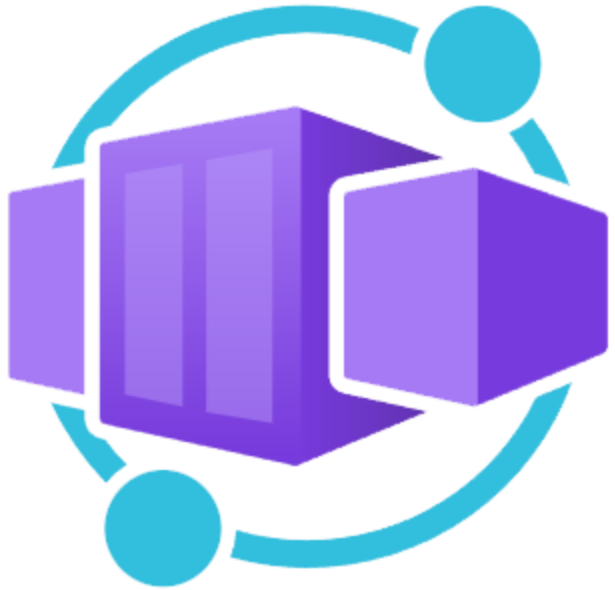
….but: GA planned for Spring 2022

© white duck GmbH 2021

white duck

Azure Container Apps

SHOULD I USE IT NOW?



© white duck GmbH 2021

white duck

NEWS: AZURE CONTAINER REGISTRY

© white duck GmbH 2021

Zonenredundanz

- Noch in Preview
- Bietet Ausfallsicherheit und Hochverfügbarkeit für die Registry in einer bestimmten Region
- Verbessert sowohl die Zuverlässigkeit als auch die Leistung
- Limitierungen
  - ACR Tasks unterstützt noch keine Verfügbarkeitszonen
- https://docs.microsoft.com/azure/container-registry/zone-redundancy

© white duck GmbH 2021

Availability Zones

© white duck GmbH 2021

Anonymer Pull-Zugriff

- Noch in Preview
- Aktiviert anonymen (nicht authentifizierten) Pull-Zugriff auf die ACR
- Kann jederzeit de- oder aktiviert werden
- Limitierungen
  - gilt für alle Repositories in der ACR
- https://docs.microsoft.com/azure/container-registry/anonymous-pull-access

© white duck GmbH 2021

Connected Registry

- Noch in Preview (Asia East, EU North & West und US East)
- Synchronisiert regelmäßig Inhalte mit einer Cloud-basierten Azure Container Registry
- Betriebsarten: ReadWrite (standard) & ReadOnly
- Hierarchische IoT Edge-Bereitstellung
  - in dieser Architektur sind die auf jeder Ebene bereitgestellten verbundenen Registrierungen so konfiguriert, dass die Images mit der verbundenen Registrierung auf der darüber liegenden Ebene synchronisiert werden
- https://docs.microsoft.com/azure/container-registry/intro-connected-registry

© white duck GmbH 2021

white duck

NEWS: AZURE KUBERNETES SERVICE

© white duck GmbH 2021

Run Command

- Generell verfügbar
- Befehle in einem AKS-Cluster über die AKS-API remote aufrufen und gleichzeitig die Vorzüge von RBAC und private cluster nutzen
- Just-in-Time-Befehle werden als Pods im Namespace "aks-command" ausgeführt
- Beispiel:
  - az aks command invoke -g <resourceGroup> -n <clusterName> -c "kubectl get pods -A"
- https://docs.microsoft.com/azure/aks/private-clusters#aks-run-command

© white duck GmbH 2021

Auto-Upgrade

- Generell verfügbar
- Automatisches Upgrade auf neuere AKS-Versionen
- Optionen: none, patch, stable, rapid & node-image
- https://docs.microsoft.com/azure/aks/upgrade-cluster#set-auto-upgrade-channel

© white duck GmbH 2021

Public DNS für private Cluster

- Generell verfügbar
- Ermöglicht die Erstellung eines privaten Clusters mit einem öffentlichen FQDN
- Kann das Routing vereinfachen
- https://docs.microsoft.com/azure/aks/private-clusters#create-a-private-aks-cluster-with-a-public-fqdn

© white duck GmbH 2021

Open Service Mesh Add-On

- Generell verfügbar
- Cloudbasiertes Service-Mesh basieren auf dem Service Mesh Interface (SMI)
- Verfügbar als AKS Add-On
- https://docs.microsoft.com/azure/aks/open-service-mesh-about

© white duck GmbH 2021

Node pool Snapshots

- Preview
- Momentaufnahme des Node pools vor einem Update etc.
- Erstellen von Node pools aus Snapshots
- Beispiele:
  - az aks snapshot create --name MySnapshot --resource-group MyResourceGroup --nodepool-id $NODEPOOL_ID --location eastus
  - az aks nodepool add --name np2 --cluster-name myAKSCluster --resource-group myResourceGroup --snapshot-id $SNAPSHOT_ID
- https://docs.microsoft.com/azure/aks/node-pool-snapshot

© white duck GmbH 2021

CSI Storage Driver

- Generell verfügbar
- Ermöglicht die Kubernetes-native Anbindung von
  - Azure Disks
    - Unterstützt nun ReadWriteMany, ZRS, Snapshots, Resizing, Cloning
  - Azure Files
- Ab der Kubernetes-Version 1.21 werden von Kubernetes standardmäßig nur noch CSI-Treiber verwendet
- https://docs.microsoft.com/azure/aks/csi-storage-drivers

© white duck GmbH 2021

Secrets Store CSI Driver

- Generell verfügbar
- Erweitert das offizielle Kubernetes-SIGS Projekt "Secrets Store CSI-Treiber"
- Ermöglicht das einbinden von Secrets, Keys und Zertifikaten mithilfe eines CSI-Volumes
- Eigenes CRD = SecretProviderClass
- Als AKS Add-On oder Helm-Chart verfügbar
- https://docs.microsoft.com/azure/aks/csi-secrets-store-driver

© white duck GmbH 2021

Scale-down Mode

- Es kann nun der bevozugte Scale-down Mode gewählt werden
  - “delete”
  - “deallocated”
- Mehrwerte von “Deallocated”
  - Bewahrt angehängten Storage und lokale Container Images
  - Schnelleres skalieren und starten von Containern
- Noch in Preview
- https://docs.microsoft.com/azure/aks/scale-down-mode

© white duck GmbH 2021

Deaktivieren lokaler User Accounts

- Per Default wird im AKS (auch bei AAD Anbindung) ein lokaler User mit „cluster-admin“ Berechtigung erstellt
  - Dies ist aus Sicherheitsgründen nicht zu empfehlen!
- Es ist nun möglich diesen lokalen Nutzer zu deaktivieren
- Noch in Preview
- Wichtig: Bei bestehenden Cluster müssen die Zertifikate manuell rotiert werden
- https://docs.microsoft.com/azure/aks/managed-aad#disable-local-accounts

© white duck GmbH 2021

Node Pool start/stop Command

- Node Pools können mit einem Command gestoppt und gestartet werden
  - Vorher mussten diese hierfür auf 0 Instanzen skaliert werden
- Erlaubt es Kosten und re-deployments zu sparen
- Beispiel:
  - az aks nodepool [start/stop] --nodepool-name <nodePoolName> --resource-group <resourceGroup> --cluster-name <clusterName>
- Noch in Preview
- https://docs.microsoft.com/azure/aks/start-stop-nodepools

© white duck GmbH 2021

NAT Gateway Integration

- Erlaubt es den ausgehenden Cluster Traffic auf bis zu 16 IP Adressen mit 64000 gleichzeitige Verbindungen zu skalieren
- Noch in Preview
- https://docs.microsoft.com/azure/aks/nat-gateway

© white duck GmbH 2021

WASM/WASI Node Support

- Ermöglicht das Betreiben von WebAssembly Modulen in AKS
  - Über das WASI (WebAssembly System Interface) der Krustlet Implementierung
- WebAssembly (Wasm)?
  - „…is a binary instruction format for a stack-based virtual machine. Wasm is designed as a portable compilation target for programming languages, enabling deployment on the web for client and server applications.“
- Noch in Preview (Early stage)
- https://docs.microsoft.com/azure/aks/use-wasi-node-pools

© white duck GmbH 2021

HTTP Proxy Support

- AKS unterstützt nun HTTP(S) Proxies für ausgehende Verbindungen
- Noch in Preview
- https://docs.microsoft.com/azure/aks/http-proxy

© white duck GmbH 2021

Kubernetes 1.22 Support

- Kubernetes 1.22 bringt viele neue Funktionen
  - Aber auch einige Deprecations & API Removals
    - Mehr Infos im Replay unseres Meetups zu Kubernetes 1.22 (EN)
    - https://www.youtube.com/watch?v=YmGiIRj9tdM
- Noch in Preview
- Info: Kubernetes 1.19 geht am 31.01.22 aus dem Support
  - https://github.com/Azure/AKS/releases/tag/2021-11-18

© white duck GmbH 2021

white duck

NEWS: AZURE CONTAINER INSTANCE

© white duck GmbH 2021

Support für Availability Zones

- Höhere Verfügbarkeit durch Availability Zones
- Noch in Preview
- Limitierungen
  - Ist noch nicht über das Azure Portal verfügbar
  - Noch kein Support für GPUs & vNet Integration
- https://docs.microsoft.com/azure/container-instances/availability-zones

© white duck GmbH 2021

FAQ / NETWORKING

© white duck GmbH 2021

FAQ / Networking

- Gibt es Fragen?

© white duck GmbH 2021