Nuno Guedes

Introdução a Azure Arc para Kubernetes

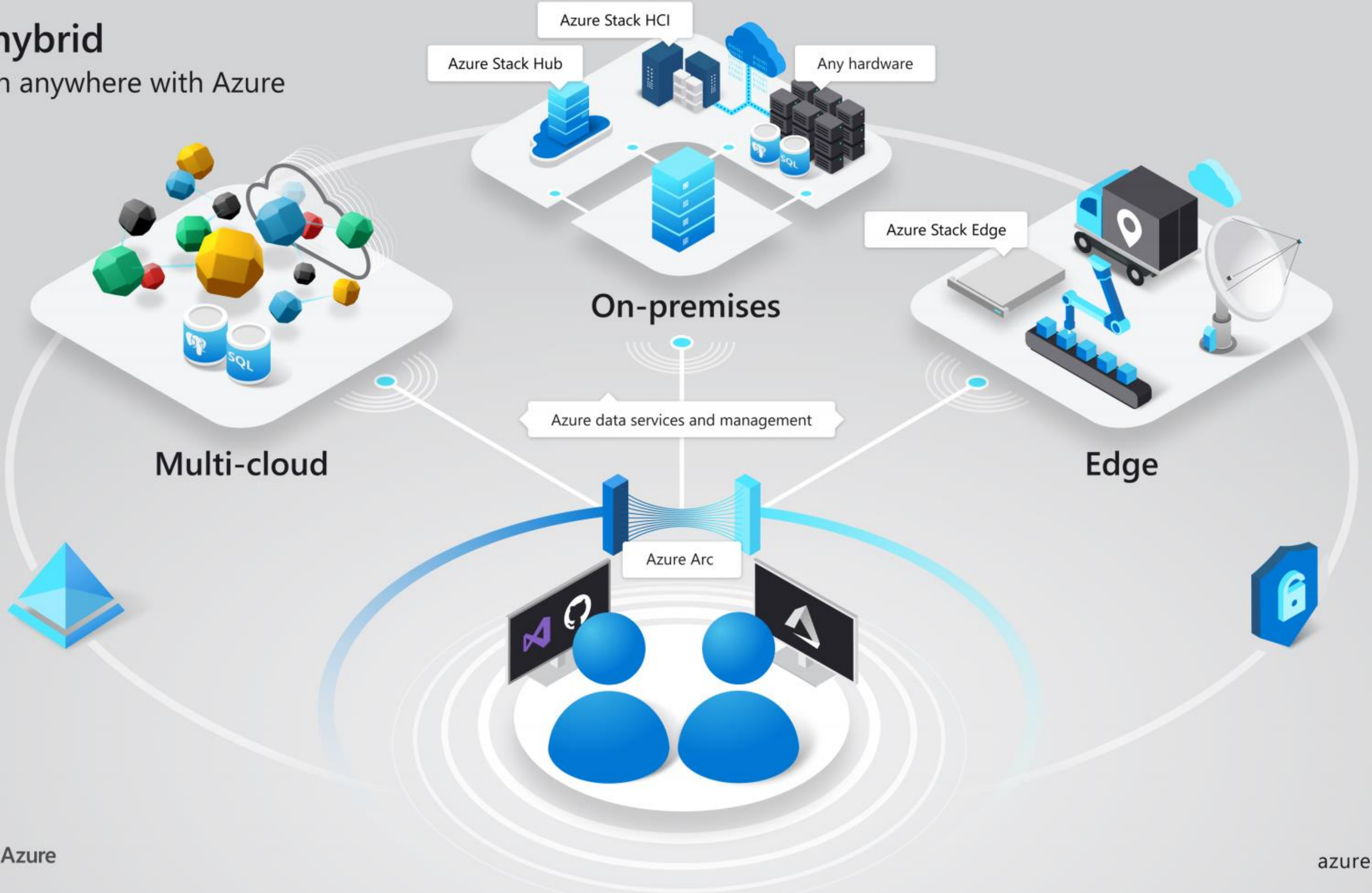
17 de Abril 2021
10:45

linkedin.com/in/nunoguedes
@infbase
github.com/infbase/GlobalAzure2021

Azure Arc

Azure hybrid

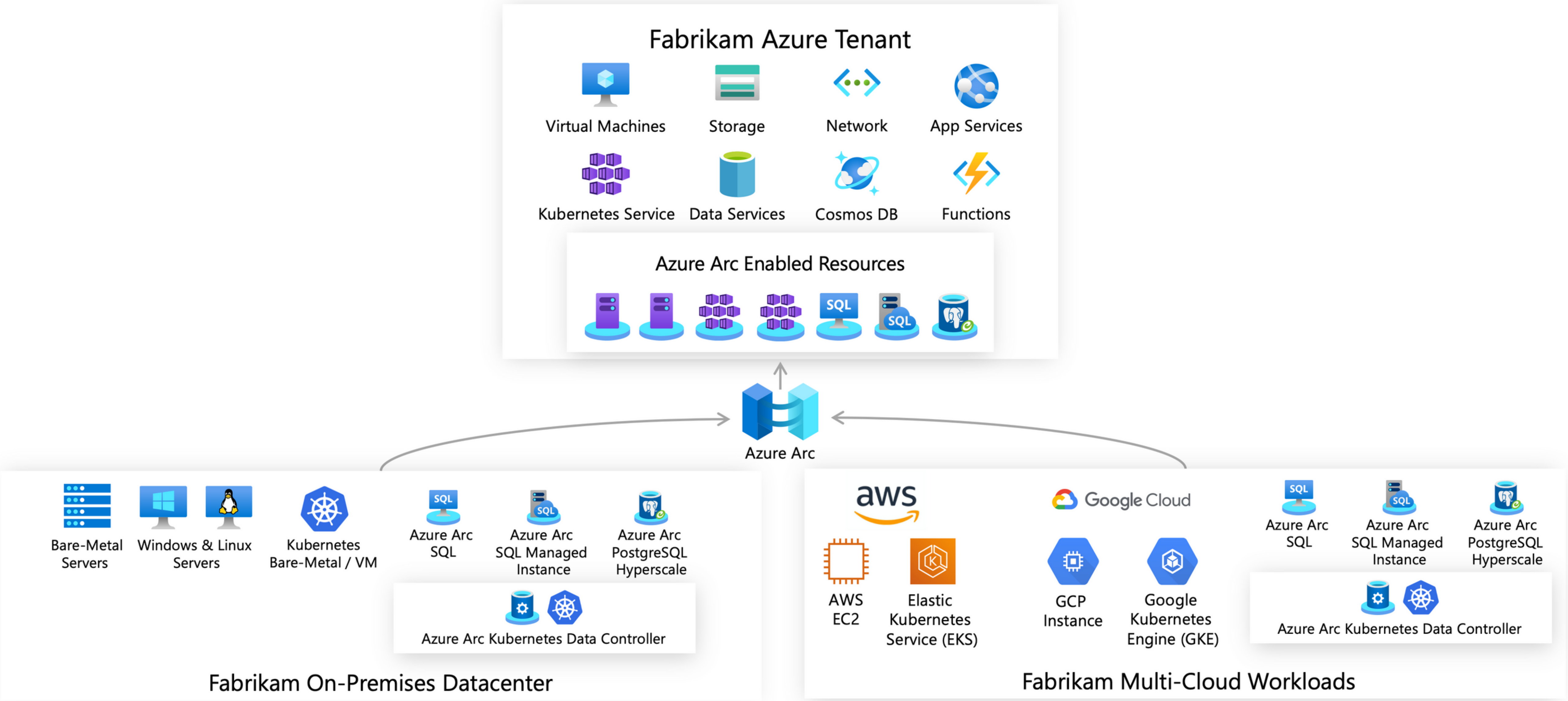
Innovation anywhere with Azure



Microsoft Azure

azure.com/hybrid

Azure Arc



Fabrikam Azure Tenant

Virtual Machines
Storage
Network
App Services
Kubernetes Service
Data Services
Cosmos DB
Functions

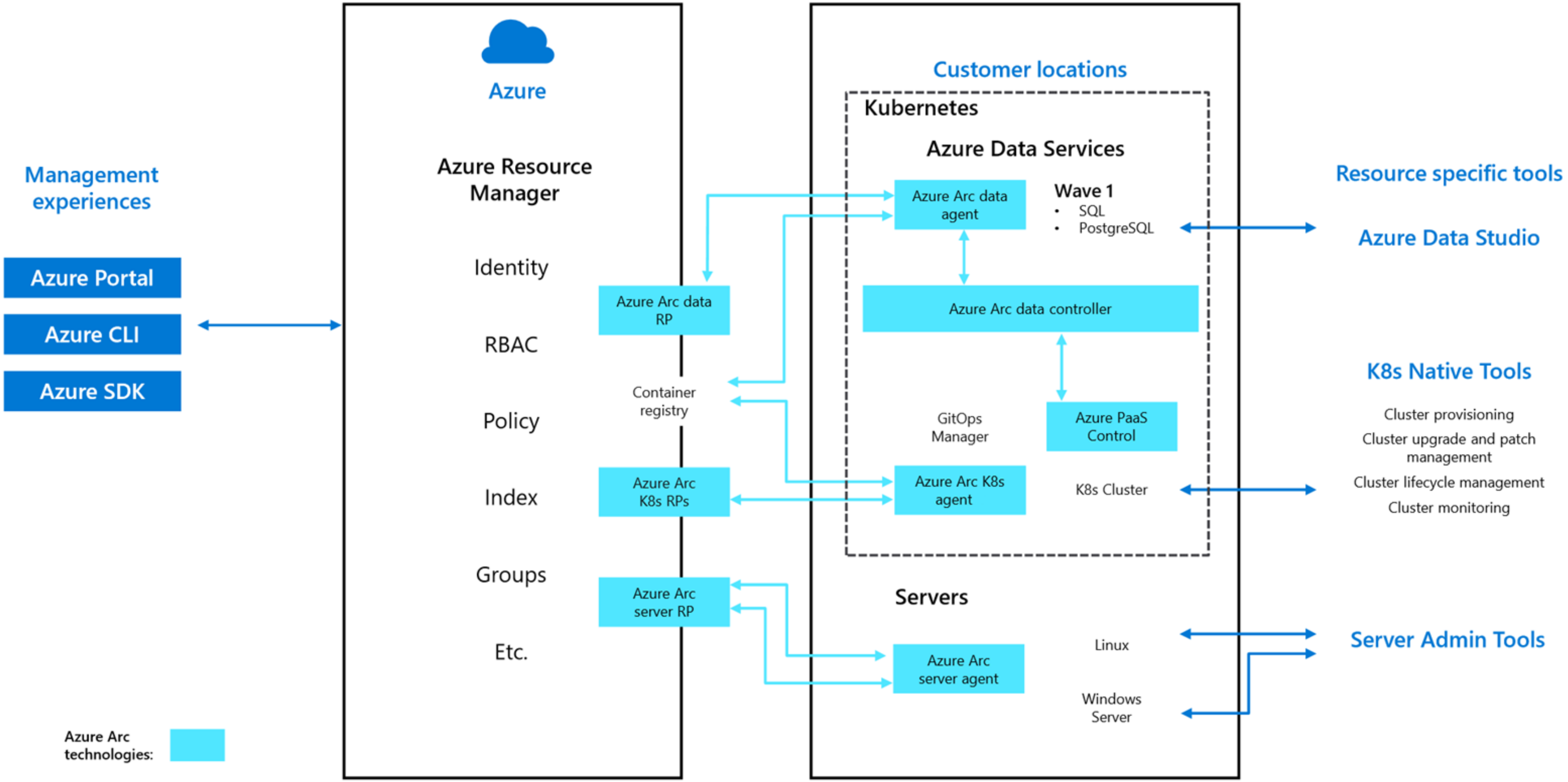
Azure Arc Enabled Resources

SQL
SQL
Azure Arc
Bare-Metal Servers
Windows & Linux Servers
Kubernetes Bare-Metal / VM
Azure Arc SQL
SQL
Azure Arc SQL Managed Instance
Azure Arc PostgreSQL Hyperscale
Azure Arc Kubernetes Data Controller
aws
AWS EC2
Elastic Kubernetes Service (EKS)
Google Cloud
GCP Instance
Google Kubernetes Engine (GKE)
SQL
Azure Arc SQL
SQL
Azure Arc SQL Managed Instance
Azure Arc PostgreSQL Hyperscale
Azure Arc Kubernetes Data Controller

Fabrikam On-Premises Datacenter

Fabrikam Multi-Cloud Workloads

Azure Arc



Management experiences

Azure Portal

Azure CLI

Azure SDK

Azure

Azure Resource Manager

Identity

RBAC

Policy

Index

Groups

Etc.

Azure Arc data RP

Container registry

Azure Arc K8s RPs

Azure Arc server RP

Customer locations

Kubernetes

Azure Data Services

Azure Arc data agent

Wave 1
- SQL
- PostgreSQL

Azure Arc data controller

GitOps Manager

Azure PaaS Control

Azure Arc K8s agent

K8s Cluster

Servers

Azure Arc server agent

Linux

Windows Server

Resource specific tools

Azure Data Studio

K8s Native Tools

Cluster provisioning

Cluster upgrade and patch management

Cluster lifecycle management

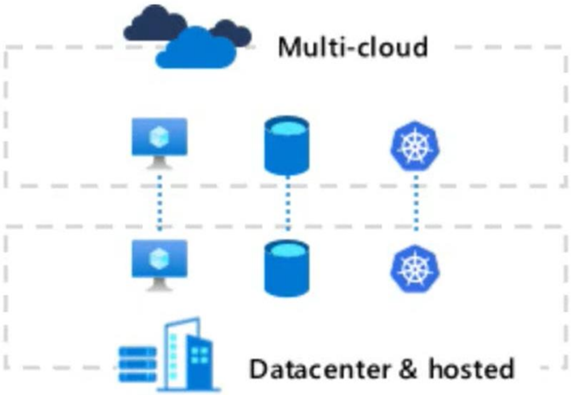
Cluster monitoring

Server Admin Tools

Azure Arc technologies: 🟦

Azure Arc enabled Kubernetes

Azure Arc enabled Kubernetes



Inventário único e gestão central de clusters

Todos os clusters de Kubernetes visíveis no portal de Azure independentemente da sua localização

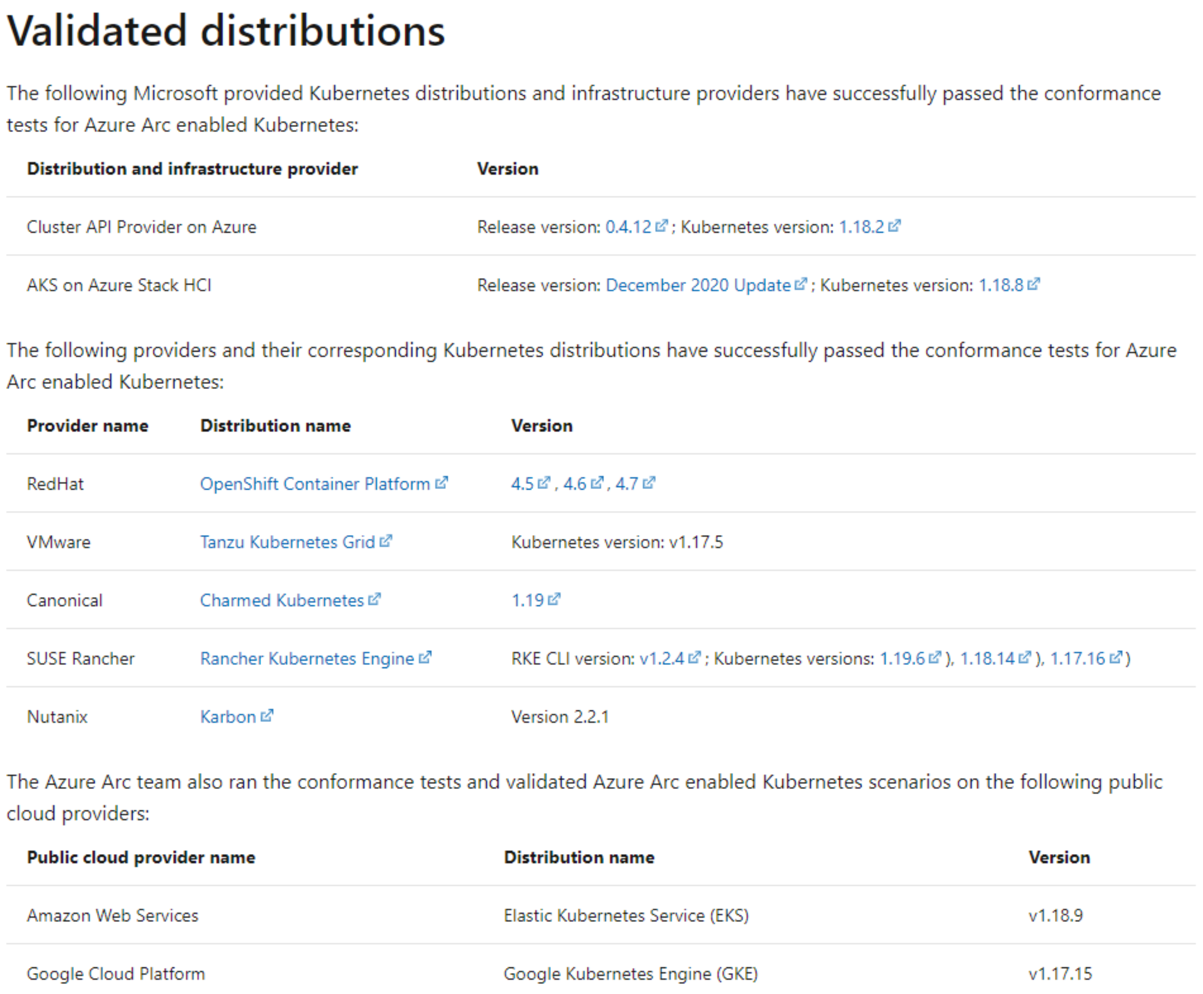
GitOps

Deploy centralizado de aplicações e configurações para todos os clusters

Policies centralizadas de audit e compliance

Ponto único para garantir audit e compliance em todos os clusters

Azure Arc enabled Kubernetes



Validated distributions

The following Microsoft provided Kubernetes distributions and infrastructure providers have successfully passed the conformance tests for Azure Arc enabled Kubernetes:

Distribution and infrastructure provider	Version
Cluster API Provider on Azure	Release version: 0.4.12 ; Kubernetes version: 1.18.2
AKS on Azure Stack HCI	Release version: December 2020 Update ; Kubernetes version: 1.18.8

The following providers and their corresponding Kubernetes distributions have successfully passed the conformance tests for Azure Arc enabled Kubernetes:

Provider name	Distribution name	Version
RedHat	OpenShift Container Platform	4.5 , 4.6 , 4.7
VMware	Tanzu Kubernetes Grid	Kubernetes version: v1.17.5
Canonical	Charmed Kubernetes	1.19
SUSE Rancher	Rancher Kubernetes Engine	RKE CLI version: v1.2.4 ; Kubernetes versions: 1.19.6), 1.18.14), 1.17.16)
Nutanix	Karbon	Version 2.2.1

The Azure Arc team also ran the conformance tests and validated Azure Arc enabled Kubernetes scenarios on the following public cloud providers:

Public cloud provider name	Distribution name	Version
Amazon Web Services	Elastic Kubernetes Service (EKS)	v1.18.9
Google Cloud Platform	Google Kubernetes Engine (GKE)	v1.17.15

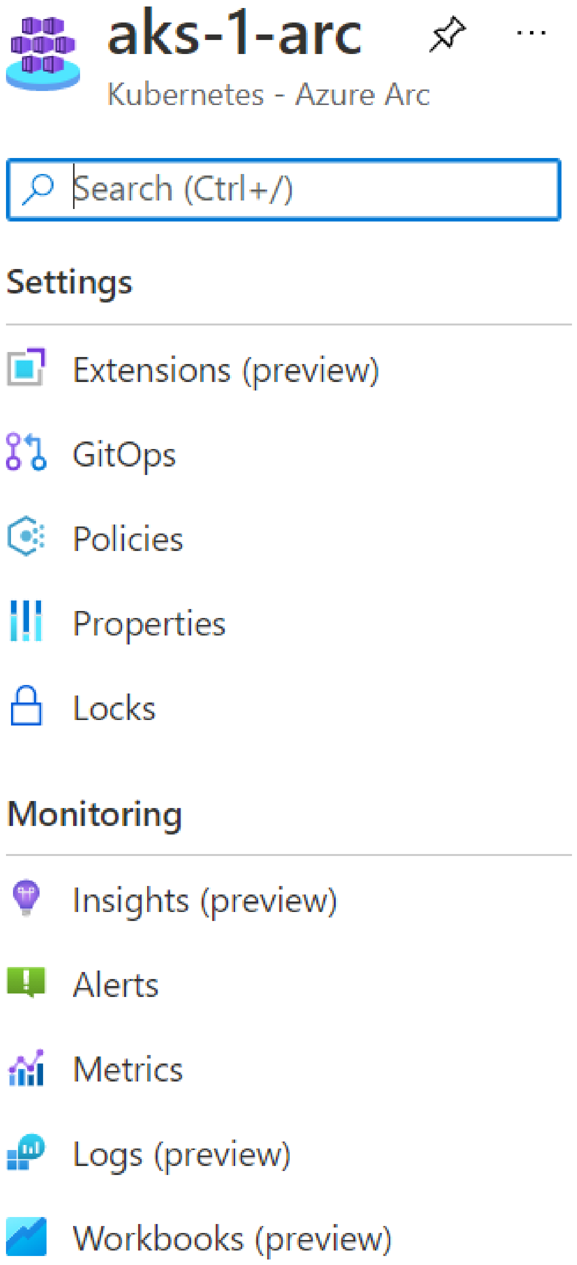
https://docs.microsoft.com/en-in/azure/azure-arc/kubernetes/validation-program

Azure Arc enabled Kubernetes

Onboarding

Onboarding

```
az connectedk8s connect
  --name aks-1-arc
  --resource-group GlobalAzure2021
```



Então e com Terraform?

Add-ons vs. Extensions

```
az aks enable-addons -n aks-1-arc -g GlobalAzure2021 -a monitoring
```

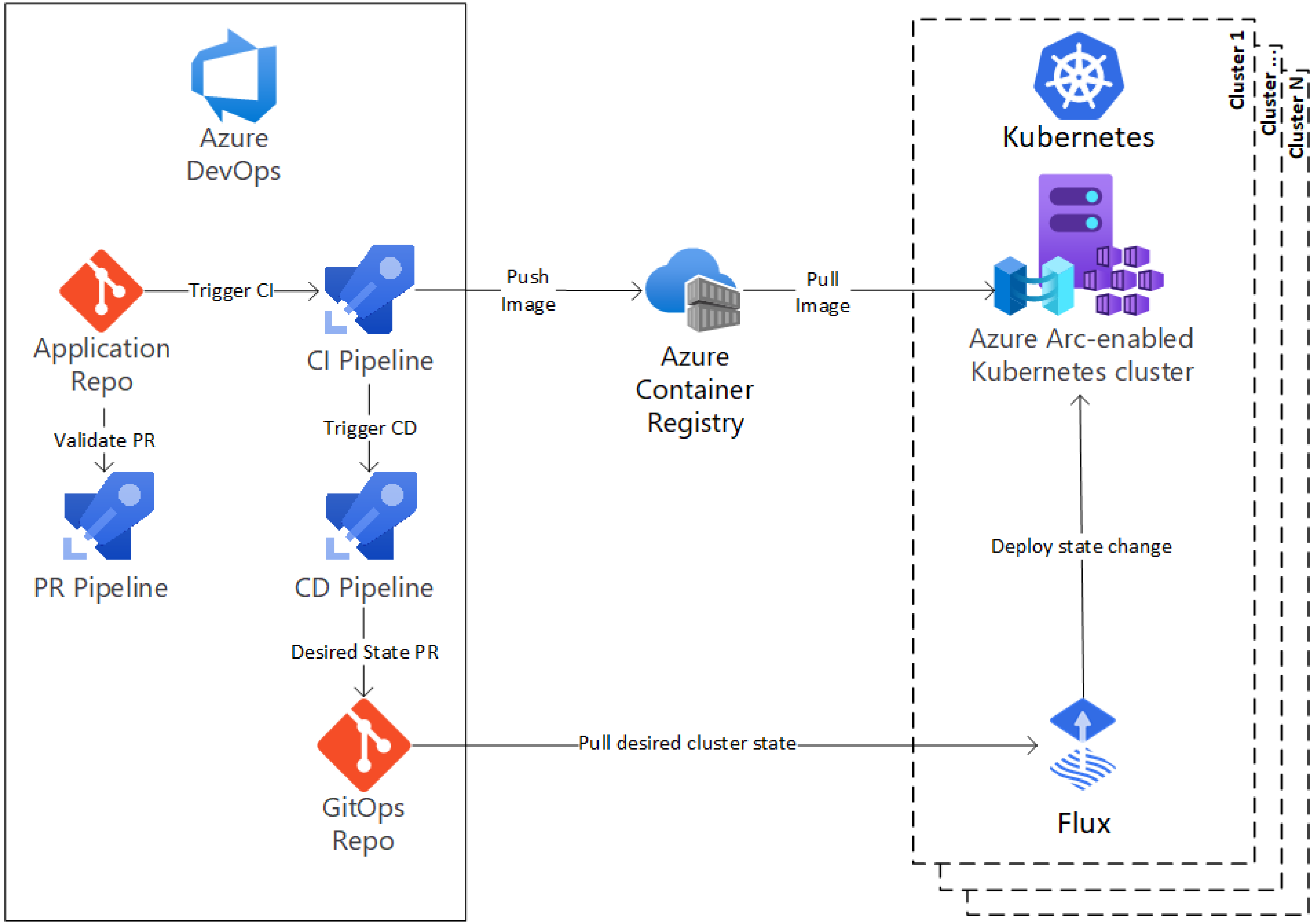
vs.

```
az k8s-extension create --name azuremonitor-containers  --extension-type
Microsoft.AzureMonitor.Containers --scope cluster --cluster-name aks-1-arc
--resource-group GlobalAzure2021 --cluster-type connectedClusters
```

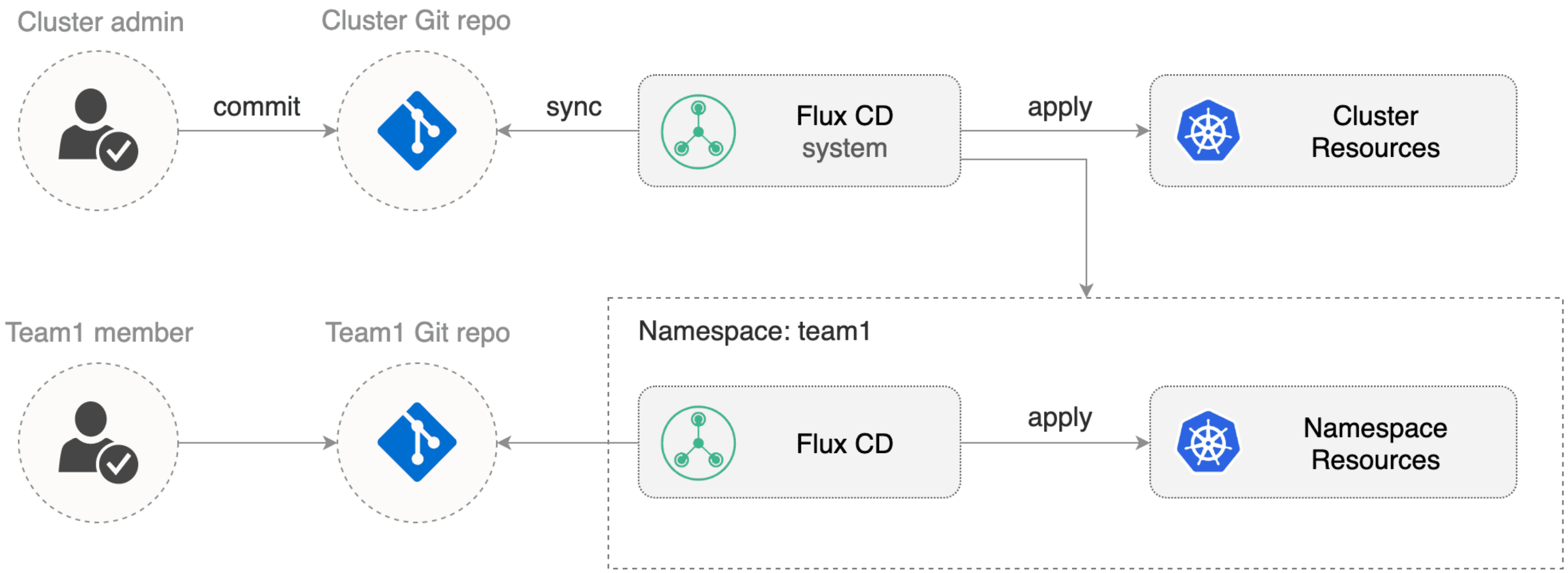
Azure Arc enabled Kubernetes

GitOps

GitOps

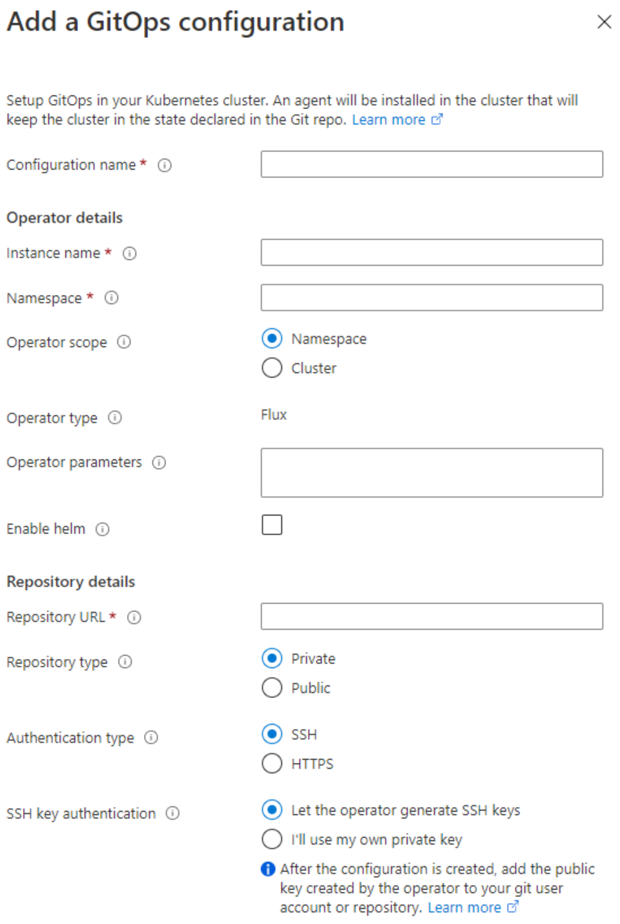

Azure
DevOps
Application
Repo
Trigger CI
CI Pipeline
Validate PR
Trigger CD
PR Pipeline
CD Pipeline
Desired State PR
GitOps
Repo
Push
Image
Azure
Container
Registry
Pull
Image
Pull desired cluster state
Kubernetes
Cluster 1
Cluster ...
Cluster N
Azure Arc-enabled
Kubernetes cluster
Deploy state change
Flux

GitOps multi-tenant



GitOps configurations

Az Portal



Add a GitOps configuration

Setup GitOps in your Kubernetes cluster. An agent will be installed in the cluster that will keep the cluster in the state declared in the Git repo. Learn more

Configuration name * ⓘ

Operator details

Instance name * ⓘ

Namespace * ⓘ

Operator scope ⓘ ● Namespace ○ Cluster

Operator type ⓘ Flux

Operator parameters ⓘ

Enable helm ⓘ □

Repository details

Repository URL * ⓘ

Repository type ⓘ ● Private ○ Public

Authentication type ⓘ ● SSH ○ HTTPS

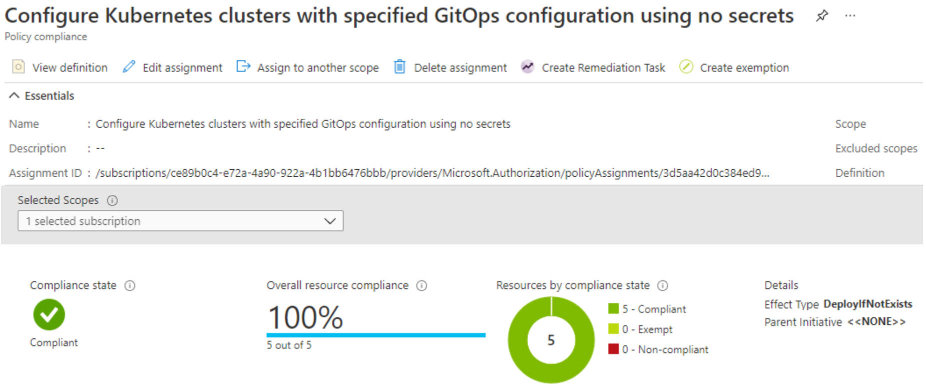
SSH key authentication ⓘ ● Let the operator generate SSH keys ○ I'll use my own private key

ⓘ After the configuration is created, add the public key created by the operator to your git user account or repository. Learn more

Az CLI

```
az k8sconfiguration create …
```

Az Policy



Configure Kubernetes clusters with specified GitOps configuration using no secrets

Policy compliance

Name : Configure Kubernetes clusters with specified GitOps configuration using no secrets

Description : --

Assignment ID : /subscriptions/ce89b0c4-e72a-4a90-922a-4b1bb6476bbb/providers/Microsoft.Authorization/policyAssignments/3d5aa42d0c384ed9...

Scope

Excluded scopes

Definition

Selected Scopes ⓘ 1 selected subscription

Compliance state ⓘ ✓ Compliant

Overall resource compliance ⓘ 100% 5 out of 5

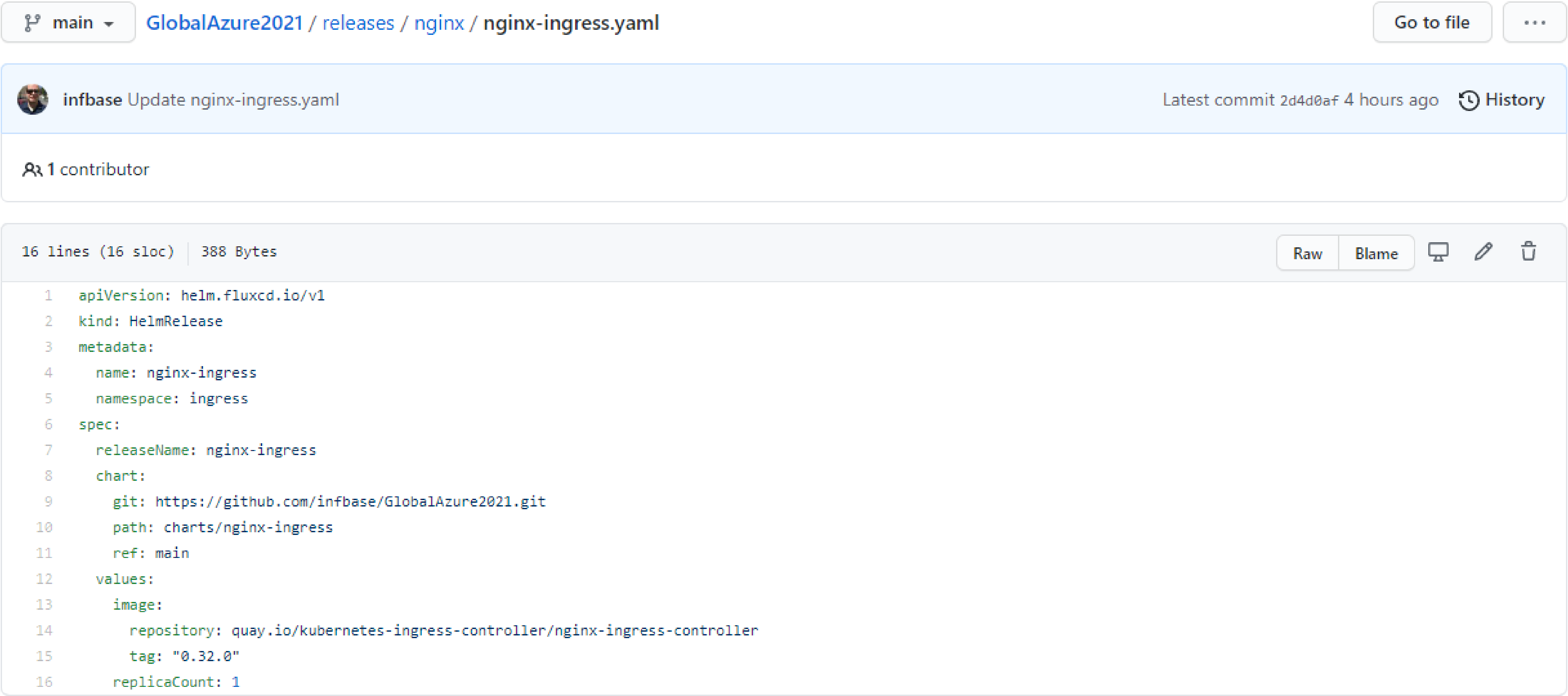
Resources by compliance state ⓘ

Details

Effect Type **DeployIfNotExists**

Parent Initiative **<<NONE>>**

GitOps repo



GlobalAzure2021 / releases / nginx / nginx-ingress.yaml

infbase Update nginx-ingress.yaml

Latest commit 2d4d0af 4 hours ago

1 contributor

16 lines (16 sloc) | 388 Bytes

```yaml
apiVersion: helm.fluxcd.io/v1
kind: HelmRelease
metadata:
  name: nginx-ingress
  namespace: ingress
spec:
  releaseName: nginx-ingress
  chart:
    git: https://github.com/infbase/GlobalAzure2021.git
    path: charts/nginx-ingress
    ref: main
  values:
    image:
      repository: quay.io/kubernetes-ingress-controller/nginx-ingress-controller
      tag: "0.32.0"
    replicaCount: 1
```

GitOps pains

- GitOps covers only a subset of the software lifecycle
- Splitting CI and CD with GitOps is not straightforward
- GitOps doesn’t address promotion of releases between environments
- There is no standard practice for modeling multi-environment configurations
- GitOps breaks down with auto-scaling and dynamic resources
- There is no standard practice for GitOps rollbacks
- Observability for GitOps (and Git) is immature
- Auditing is problematic despite having all information in Git
- Running GitOps at scale is difficult
- GitOps and Helm do not always work well together
- Continuous Deployment and GitOps do not mix together
- There is no standard practice for managing secrets

(acrescem as dores do Flux v1)

The pains of GitOps 1.0 - Codefresh

GitOps benefits

Declarativo vs. Imperativo

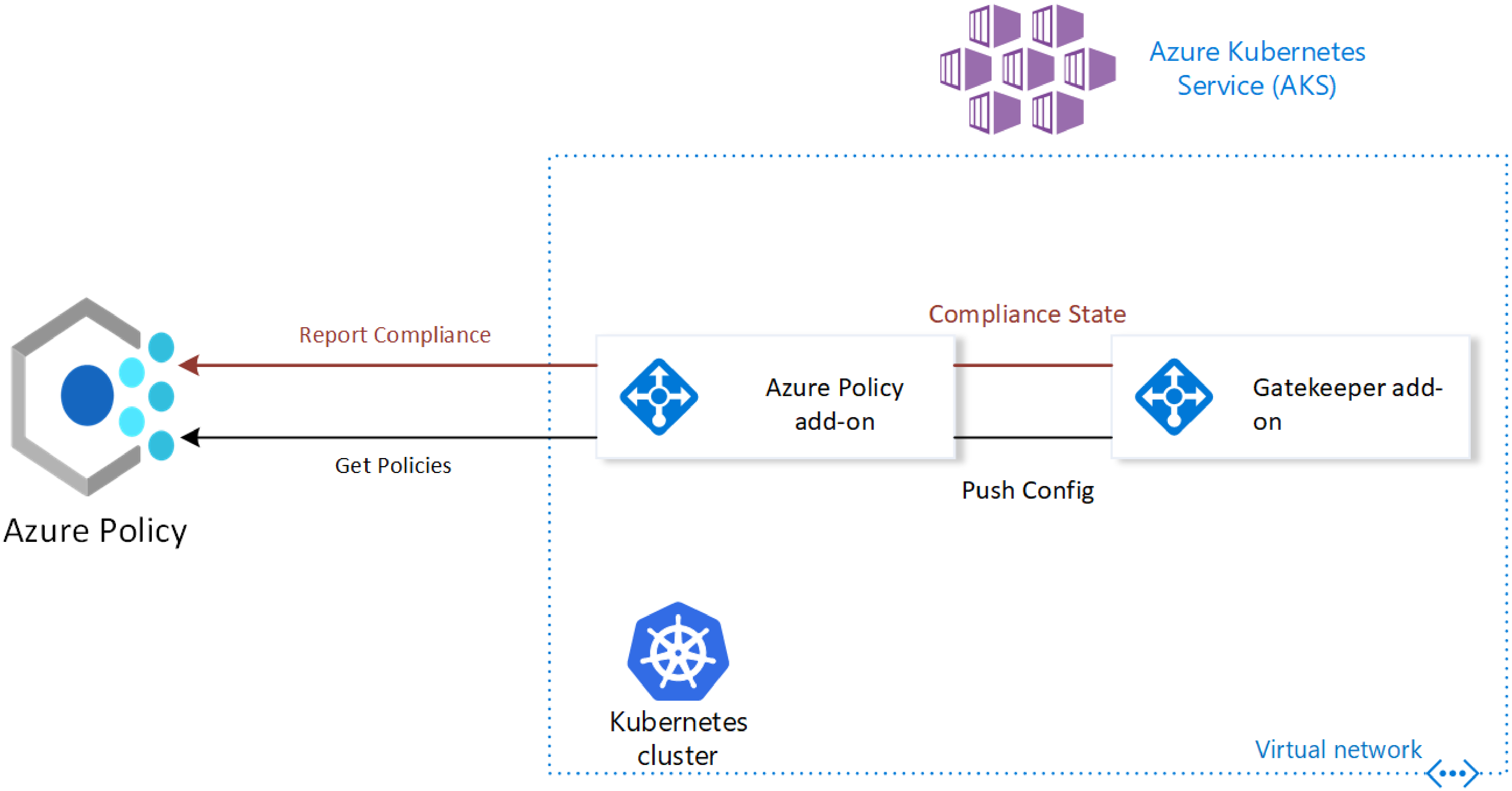
Azure Arc enabled Kubernetes

Policy

Policy for Kubernetes

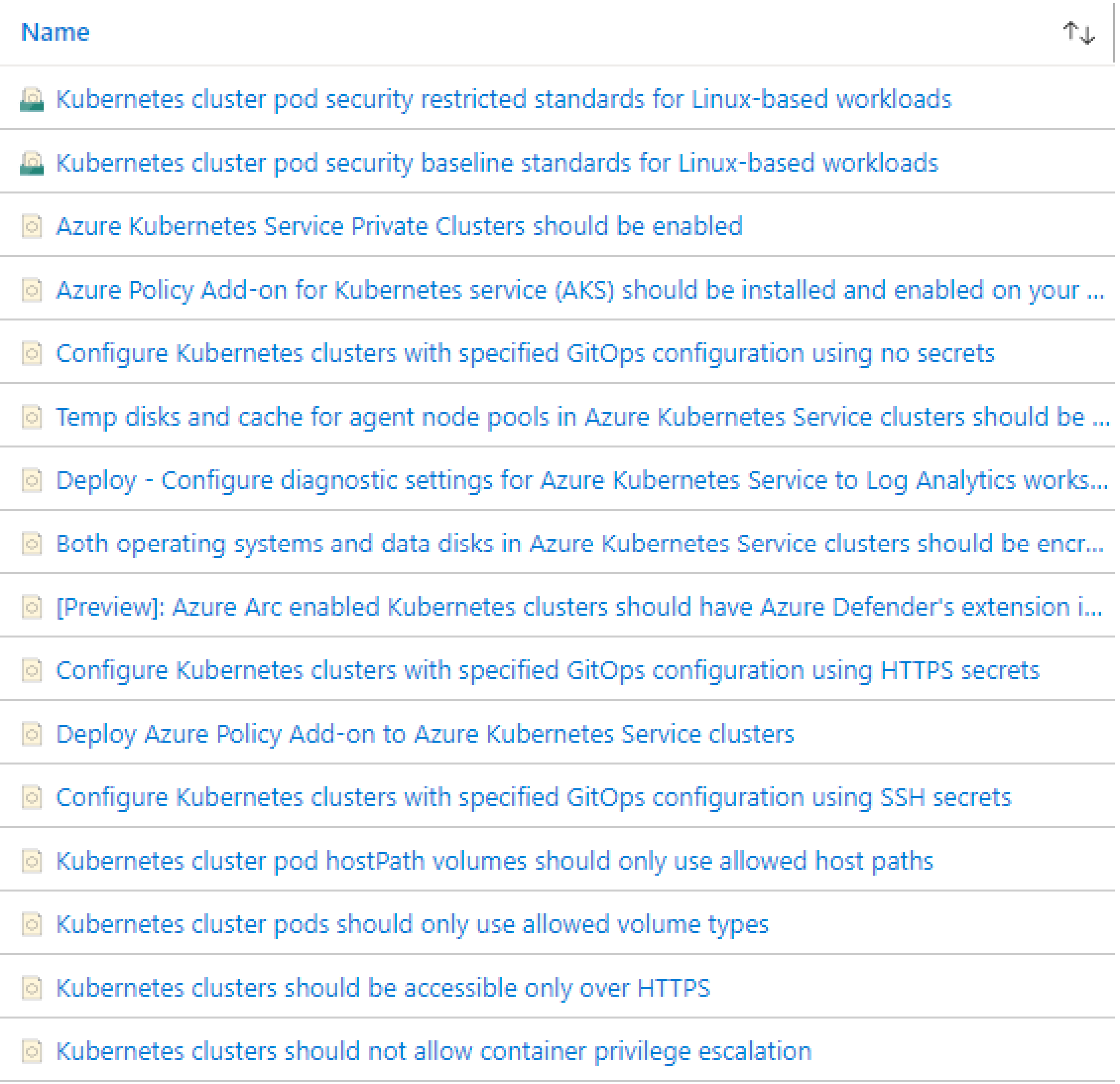
Governance!

Azure Policy



Azure Policy

Built-in policies



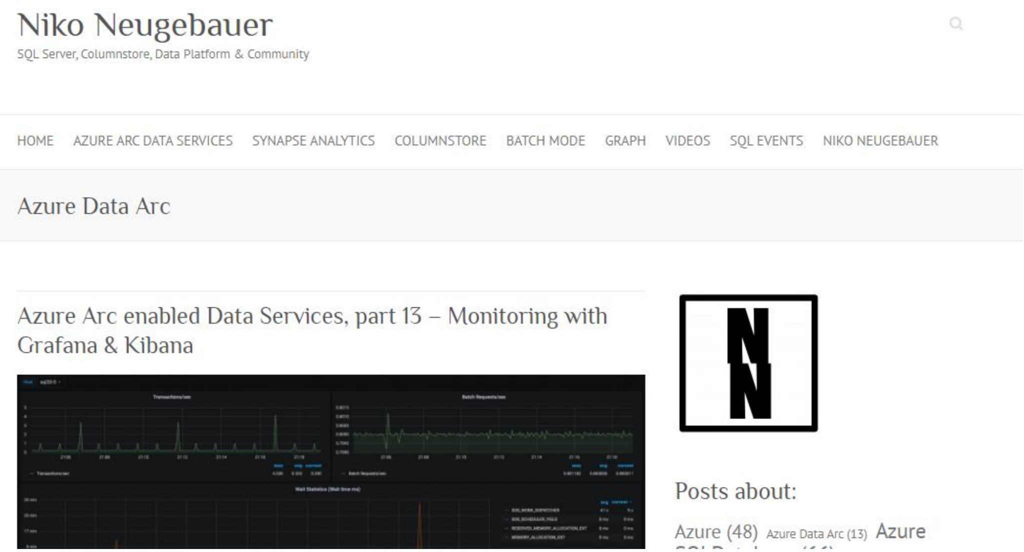
Name
Kubernetes cluster pod security restricted standards for Linux-based workloads
Kubernetes cluster pod security baseline standards for Linux-based workloads
Azure Kubernetes Service Private Clusters should be enabled
Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your ...
Configure Kubernetes clusters with specified GitOps configuration using no secrets
Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be ...
Deploy - Configure diagnostic settings for Azure Kubernetes Service to Log Analytics works...
Both operating systems and data disks in Azure Kubernetes Service clusters should be encr...
[Preview]: Azure Arc enabled Kubernetes clusters should have Azure Defender's extension i...
Configure Kubernetes clusters with specified GitOps configuration using HTTPS secrets
Deploy Azure Policy Add-on to Azure Kubernetes Service clusters
Configure Kubernetes clusters with specified GitOps configuration using SSH secrets
Kubernetes cluster pod hostPath volumes should only use allowed host paths
Kubernetes cluster pods should only use allowed volume types
Kubernetes clusters should be accessible only over HTTPS
Kubernetes clusters should not allow container privilege escalation

Custom policies

1. Author REGO and unit tests (e.g: src.rego and src_test.rego as in here)
    1. Here are details about policy testing: https://www.openpolicyagent.org/docs/latest/policy-testing/ (you can run this for testing regos in same folder: opa test . -v)
    2. Download opa binary here: https://github.com/open-policy-agent/opa/releases or from a package manager
2. Author Gatekeeper CRDs (constraint.yaml and template.yaml as in here)
3. Once constraint templates are authored, upload constraint templates and constraints to any public github repo (e.g. Azure community-policy repo)
4. Integrate the templates and constraint with Azure Policy (e.g. here)
5. Create custom definitions in whitelisted test subscriptions and apply the policies to cluster
6. Create good and bad YAMLs for testing policy on cluster (e.g. examples-good and examples-violations)
7. Test above YAMLs on cluster
8. In Azure Portal, verify compliance data is shown for the policy.

Azure Arc previews

Azure Arc enabled data services preview



Niko Neugebauer

SQL Server, Columnstore, Data Platform & Community

HOME AZURE ARC DATA SERVICES SYNAPSE ANALYTICS COLUMNSTORE BATCH MODE GRAPH VIDEOS SQL EVENTS NIKO NEUGEBAUER

Azure Data Arc

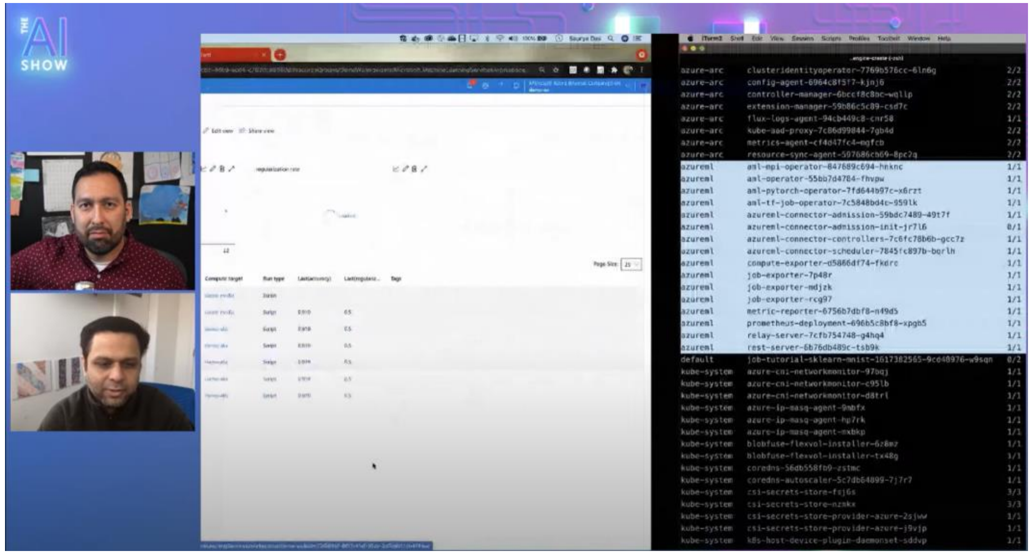
Azure Arc enabled Data Services, part 13 – Monitoring with Grafana & Kibana

Posts about:

Azure (48) Azure Data Arc (13) Azure

[Niko Neugebauer - Azure Data Arc](#)

Azure Arc enabled machine learning preview



```
azure-arc     clusteridentityoperator-7769b576cc-6ln6g              2/2
azure-arc     config-agent-6964c8f5f7-kjnj6                         2/2
azure-arc     controller-manager-6bccf8c8bc-wqllp                   2/2
azure-arc     extension-manager-59b86c5c89-csd7c                    2/2
azure-arc     flux-logs-agent-94cb449c8-cnr58                       1/1
azure-arc     kube-aad-proxy-7c86d99844-7gb4d                       2/2
azure-arc     metrics-agent-cf4d47fc4-mgfcb                         2/2
azure-arc     resource-sync-agent-597686cb69-8pc2q                  2/2
azureml       aml-mpi-operator-847689c694-hnknc                     1/1
azureml       aml-operator-55bb7d4784-fhvpw                         1/1
azureml       aml-pytorch-operator-7fd644b97c-x6rzt                 1/1
azureml       aml-tf-job-operator-7c5848bd4c-959lk                  1/1
azureml       azureml-connector-admission-59bdc7489-49t7f           1/1
azureml       azureml-connector-admission-init-jr7l6                0/1
azureml       azureml-connector-controllers-7c6fc78b6b-gcc7z        1/1
azureml       azureml-connector-scheduler-7845fc897b-bqrlh          1/1
azureml       compute-exporter-d5866df74-fkdrc                      1/1
azureml       job-exporter-7p48r                                    1/1
azureml       job-exporter-mdjzk                                    1/1
azureml       job-exporter-rcg97                                    1/1
azureml       metric-reporter-6756b7dbf8-n49d5                      1/1
azureml       prometheus-deployment-696b5c8bf8-xpgb5                1/1
azureml       relay-server-7cfb754748-g4hq4                         1/1
azureml       rest-server-6b76db489c-tsb9k                          1/1
default       job-tutorial-sklearn-mnist-1617382565-9cd48976-w9sqn  0/2
kube-system   azure-cni-networkmonitor-97bqj                        1/1
kube-system   azure-cni-networkmonitor-c95lb                        1/1
kube-system   azure-cni-networkmonitor-d8trl                        1/1
kube-system   azure-ip-masq-agent-9mbfx                             1/1
kube-system   azure-ip-masq-agent-hp7rk                             1/1
kube-system   azure-ip-masq-agent-mxbkp                             1/1
kube-system   blobfuse-flexvol-installer-6z8mz                      1/1
kube-system   blobfuse-flexvol-installer-tx48g                      1/1
kube-system   coredns-56db558fb9-zstmc                              1/1
kube-system   coredns-autoscaler-5c7db64899-7j7r7                   1/1
kube-system   csi-secrets-store-fsj6s                               3/3
kube-system   csi-secrets-store-nzmkx                               3/3
kube-system   csi-secrets-store-provider-azure-2sjww                1/1
kube-system   csi-secrets-store-provider-azure-j9vjp                1/1
kube-system   k8s-host-device-plugin-daemonset-sddvp                1/1
```

THE AI SHOW
iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help

[The AI Show - Run Azure Machine Learning anywhere](#)

BY COMMUNITY • FOR COMMUNITY

#GLOBALAZURE

2021

linkedin.com/in/nunoguedes
@infbase
github.com/infbase/GlobalAzure2021