



# Responsibility Matrix

*This document does not plan to give an exhaustive matrix because the product is continuously evolving, and each Kubernetes project is different. Take it as a starting point for your context*

	Microsoft	Customer
SETUP		
Provision VMs	✓	
Select Network mode <a href="#">↗</a>		✓
Install Kubernetes	✓	
Select public / private mode <a href="#">↗</a>		✓
SECURITY		
Node hardening <a href="#">↗</a>	✓	
Egress lockdown <a href="#">↗</a>		✓
Protect API server (public cluster) <a href="#">↗</a>		✓
Container hardening		✓
Configure Policies <a href="#">↗</a>	✓	✓
OPERATION		
Keep a cluster up to date (=supported) <a href="#">↗</a>		✓
Trigger version upgrade <a href="#">↗</a>		✓
Perform Kubernetes components upgrade	✓	
Install security patch on Operating System	✓	
Reboot nodes to apply security patches <sup>1</sup> <a href="#">↗</a>		✓
Patch container runtime <sup>2</sup>	✓	
Update AKS layer <sup>2</sup>	✓	
Scale pods (manual)		✓

Scale pods (HPA / VPA / KEDA) <a href="#">↗</a>		✓
Scale nodes (manual)		✓
Scale nodes (cluster autoscaler) <a href="#">↗</a>		✓

## DISASTER RECOVERY

Activate availability zones for VMs <a href="#">↗</a>		✓
Auto repair nodes <a href="#">↗</a>	✓	
Configure storage backup / restore <a href="#">↗</a>		✓
Configure traffic management between clusters <a href="#">↗</a>		✓

## MONITORING

Enable monitoring <a href="#">↗</a>		✓
Capture metrics	✓	
Configure captured metrics (Prometheus) <a href="#">↗</a>		✓
Configure capture metrics (host + containers) <a href="#">↗</a>		✓

<sup>1</sup> Some patches require host reboot. Azure cannot decide when reboot them (could cause application disruption). Customer can either watch for [reboot\\_required.txt file presence or use KURED](#).

<sup>2</sup> container runtime and AKS layer are only upgraded during Kubernetes upgrade (=a new node is created). To ensure to stay up to date in terms of runtime and AKS (security & bugs fixes), either you should upgrade the version of Kubernetes or you can use "[node image upgrade](#)"

For any remark / issue / question, do not hesitate to  
contact me on GitHub

<https://github.com/lgmorand/aks-responsability-matrix>

## THE AKS checklist

Start!  
Check  
Generate  
**ENJOY**

ON  GitHub

- ☐ **Logically isolate cluster:** Use logical isolation to separate teams and projects. Try to deploy clusters you deploy to isolate teams or applications

- ☐ **Physically isolate cluster:** Minimize the use of physical isolation for each separate team

## DISASTER RECOVERY

0 %

Disaster Recovery items are ✓

- ☐ **Enable geo-replication for container images:** Use logical isolation to separate teams and projects. Try to deploy clusters you deploy to isolate teams or applications

## SECURITY

66 %

Security items are ✓

- ☒ **IP Range authorization:** The API-server is the central way to interact with and manage the cluster. To ensure security and minimize attacks, the API-server should only be accessible from a limited set of IP addresses. Because the api-server has a private address, it means that to access it for administrative tasks, you need to establish a private connection, like using a 'jumpbox' (i.e.: Azure Bastion)

- ☒ **AAD Integration:** Azure Kubernetes Service (AKS) can be configured to use Azure Active Directory (AAD) for authentication and authorization

META TAG

[www.the-aks-checklist.com](http://www.the-aks-checklist.com)