Private DNS resolution in your Azure environment.

Azure Platform Engineering

Mark Scholman

CA8
Part of Codeinceps Group

“We can’t link private DNS zones directly to the Vwan/Vhub?”

Many customers that seek integration on private DNS

“Do we need to link Private DNS Zones to each Spoke VNET when using Azure VWAN?”

Many customers that seek integration on private DNS

CA8

“How does registration work for PaaS services when we use ALZ?”

Many customers that seek integration on private DNS

CA8

Mark Scholman

Co-founder / Director CA8 – Microsoft Azure MVP

X /markscholman

LinkedIn /markscholman

Blog markscholman.com

GitHub /markscholman

Agenda

- Introduction
- Private DNS for PaaS Services
- Enterprise scale | Hub / Spoke models
- Enterprise scale | VWAN / VHUB
- Private DNS resolution for IaaS & PaaS
- Private DNS Resolver and DNS Rulesets

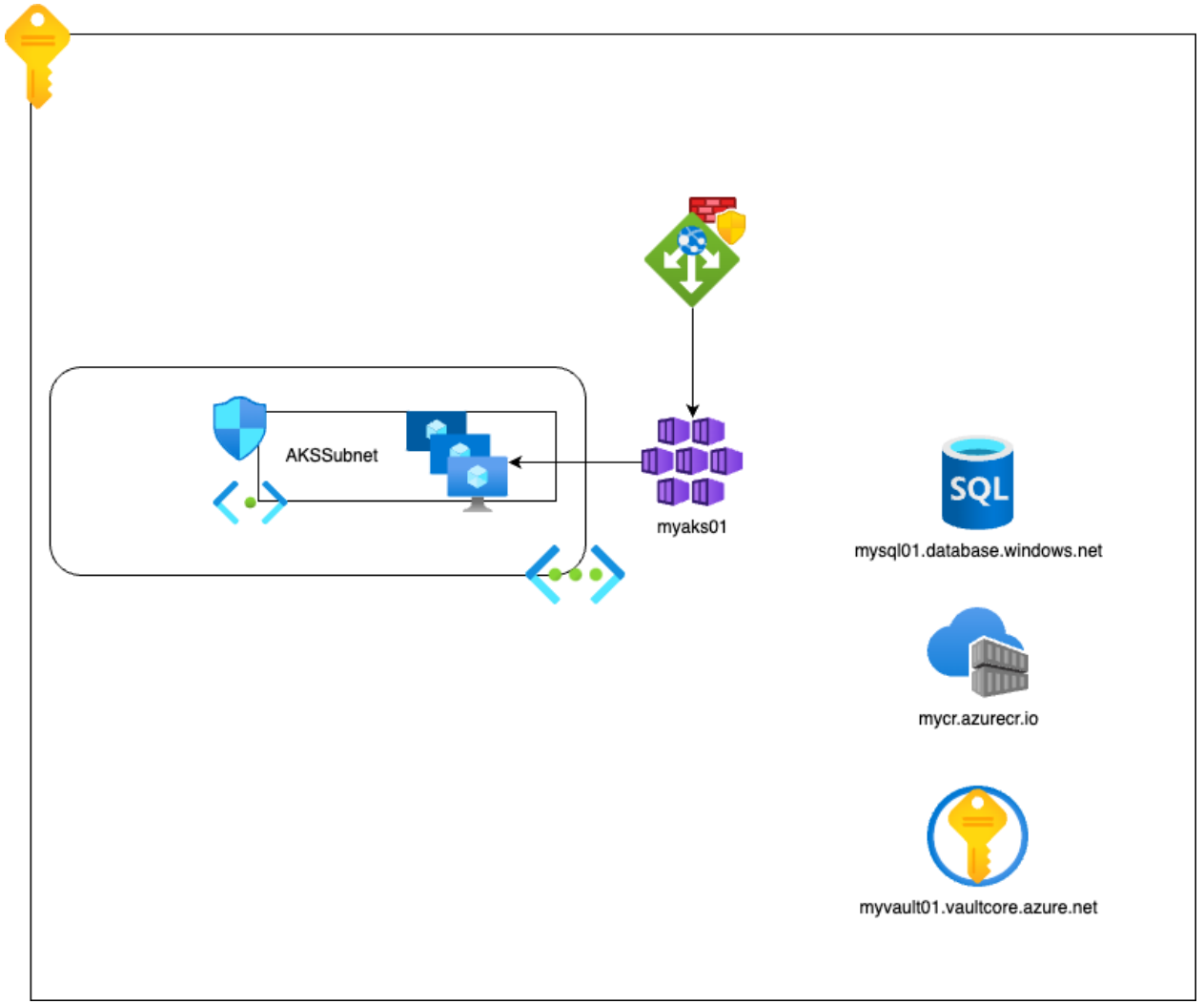
Part of Codeinceps Group

Simple example:

AKS needs to pull image from ACR

Starting a pod with a connection-string to connect an app to SQL DB

Connection string is retrieved from Keyvault



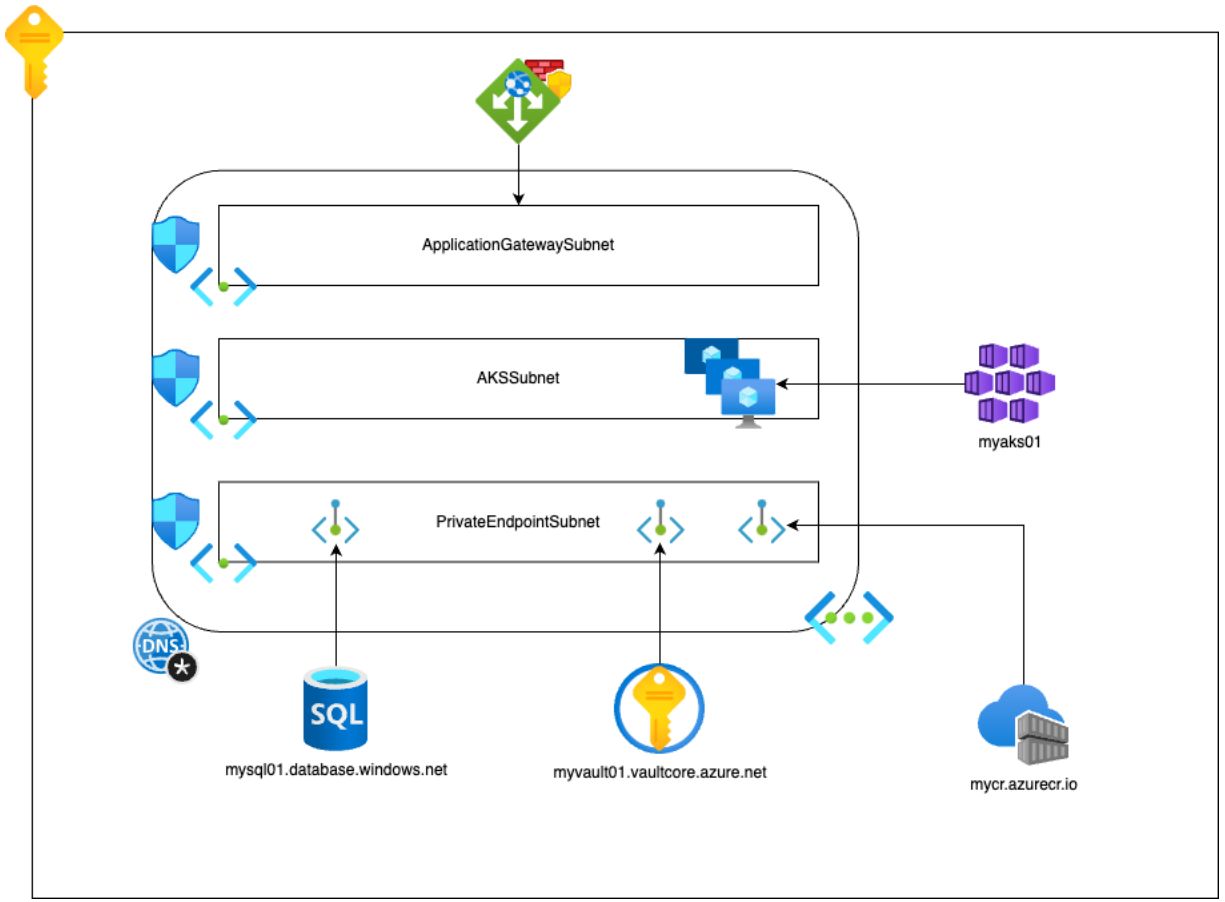
Simple example:

AKS needs to pull image from ACR

Starting a pod with a connection-string to connect an app to SQL DB

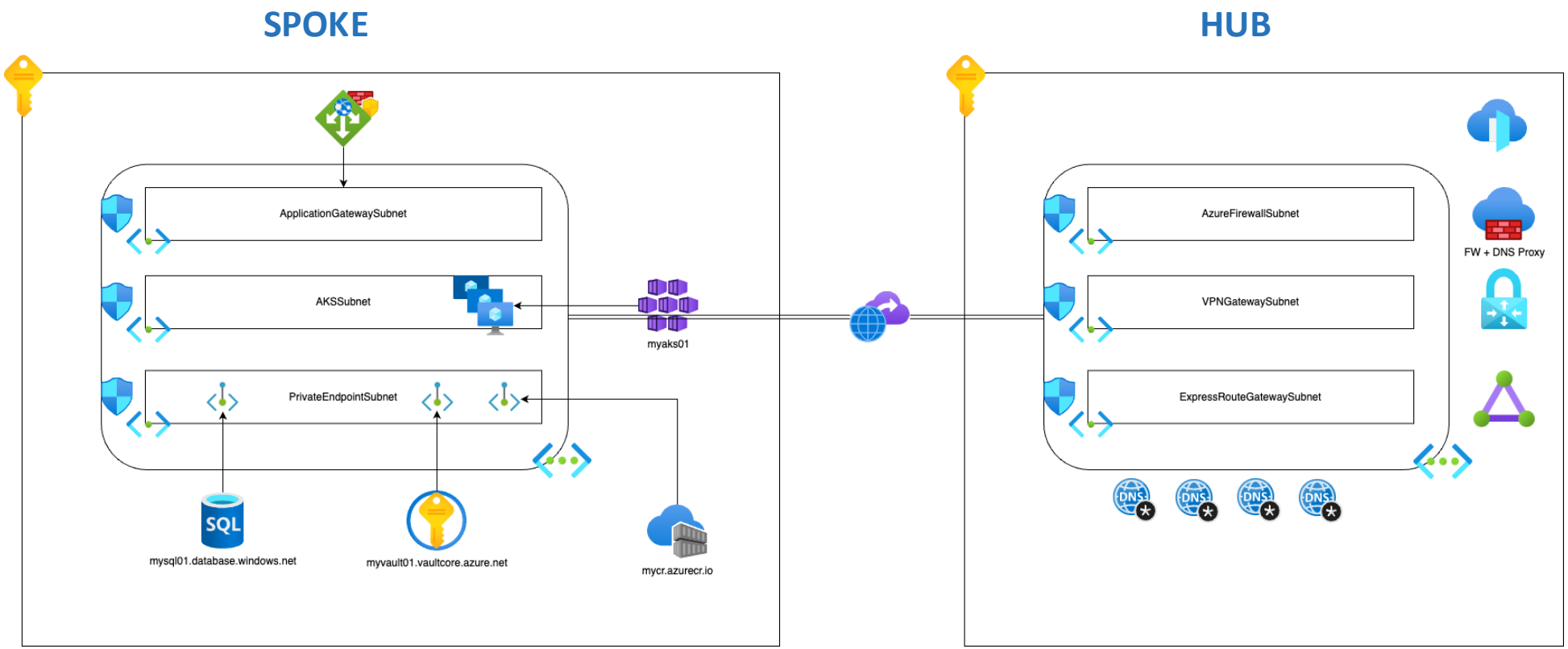
Connection string is retrieved from Keyvault

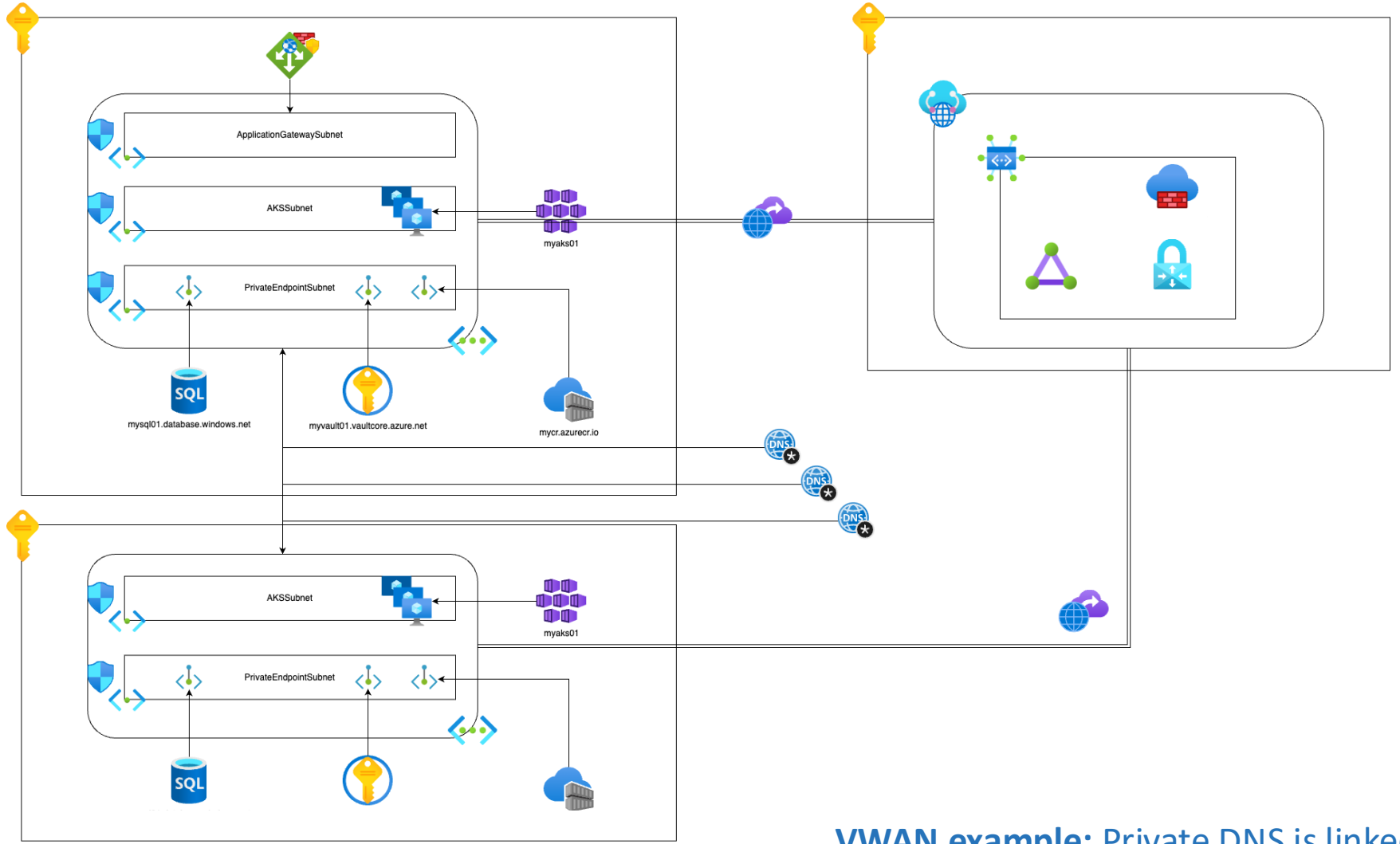
PaaS resources are private endpoint integrated. A private DNS zone prefixed with privatelink. is deployed*



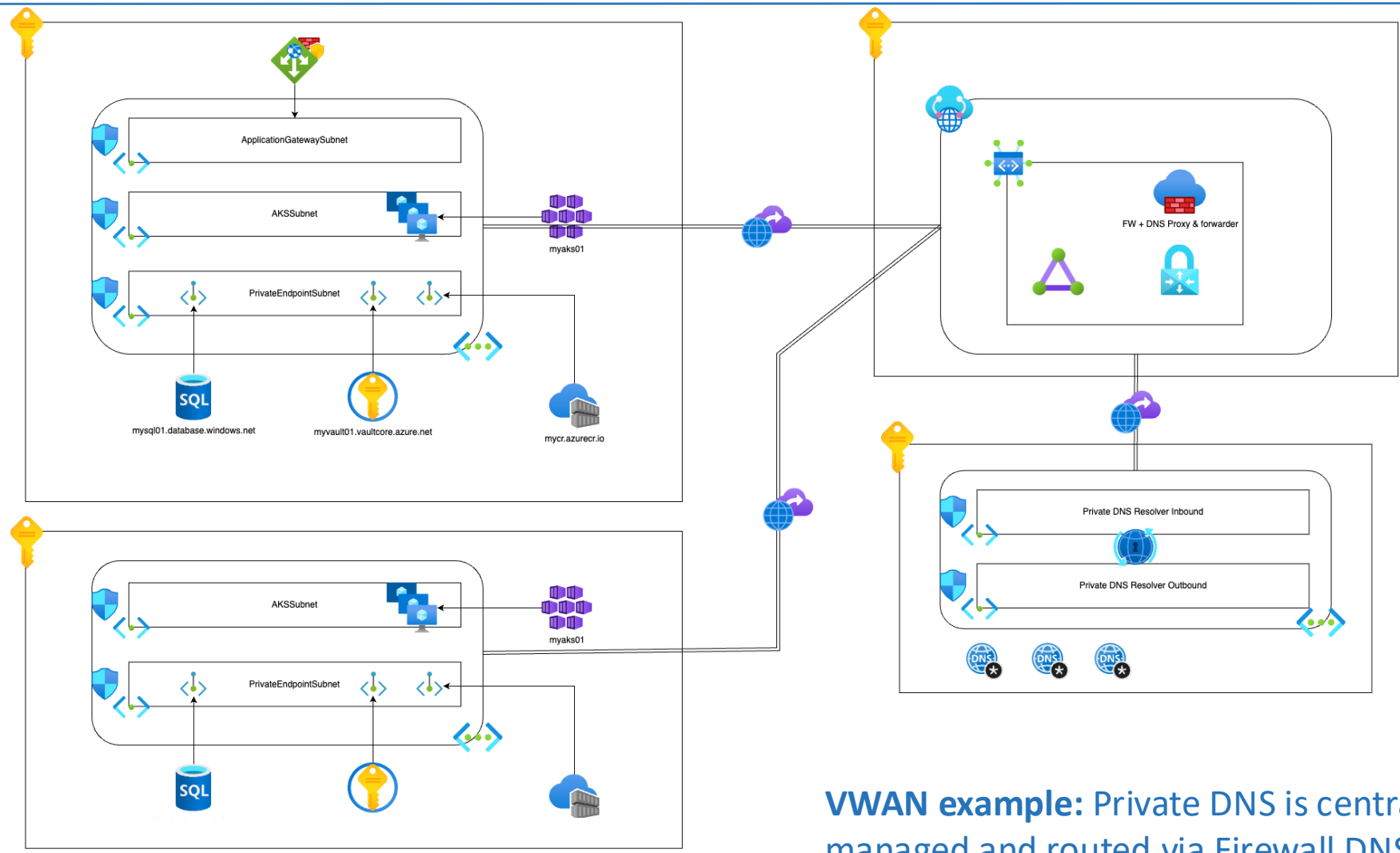
- Enables the VM Agent to communicate with the Azure platform to signal that it is in a "Ready" state.
- Enables communication with the DNS virtual server to provide filtered name resolution to the resources that don't have a custom DNS server.
- Enables health probes from Azure Load Balancer to determine the health state of VMs
- Enables the VM to obtain a dynamic IP address from the DHCP service in Azure.
- Enables Guest Agent heartbeat messages for the PaaS role.

HUB / Spoke example: Private DNS is moved to the network hub and registration is done in the zone in the network hub subscription

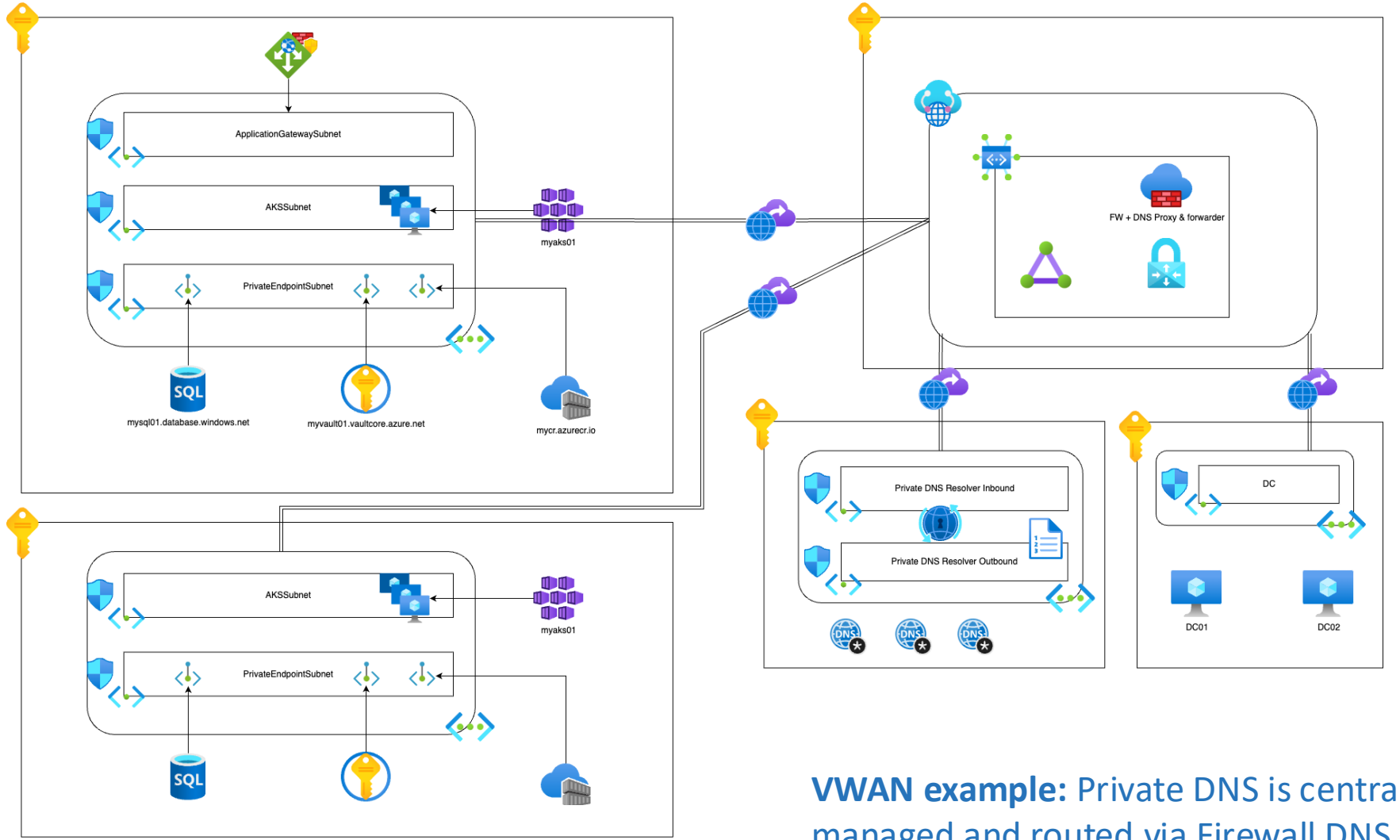




VWAN example: Private DNS is linked to the spoke networks



VWAN example: Private DNS is centrally managed and routed via Firewall DNS Proxy



VWAN example: Private DNS is centrally managed and routed via Firewall DNS Proxy

“DEMO”

- New private DNS created and linked to a VNet. On that VNet custom DNS servers are specified so name resolution is not working.
- Multiple private DNS zones with the same name are created and linked in different VNets and registrations is eventually a mess.
- Trying to create and link an already existing private DNS zone to an VNet

Questions?

CA8
Part of Codeinceps Group