Azure Spring Cloud - VNET Injection

Asir Selvasingh

Principal PM Architect --- Java on Azure

June 2020

Purpose

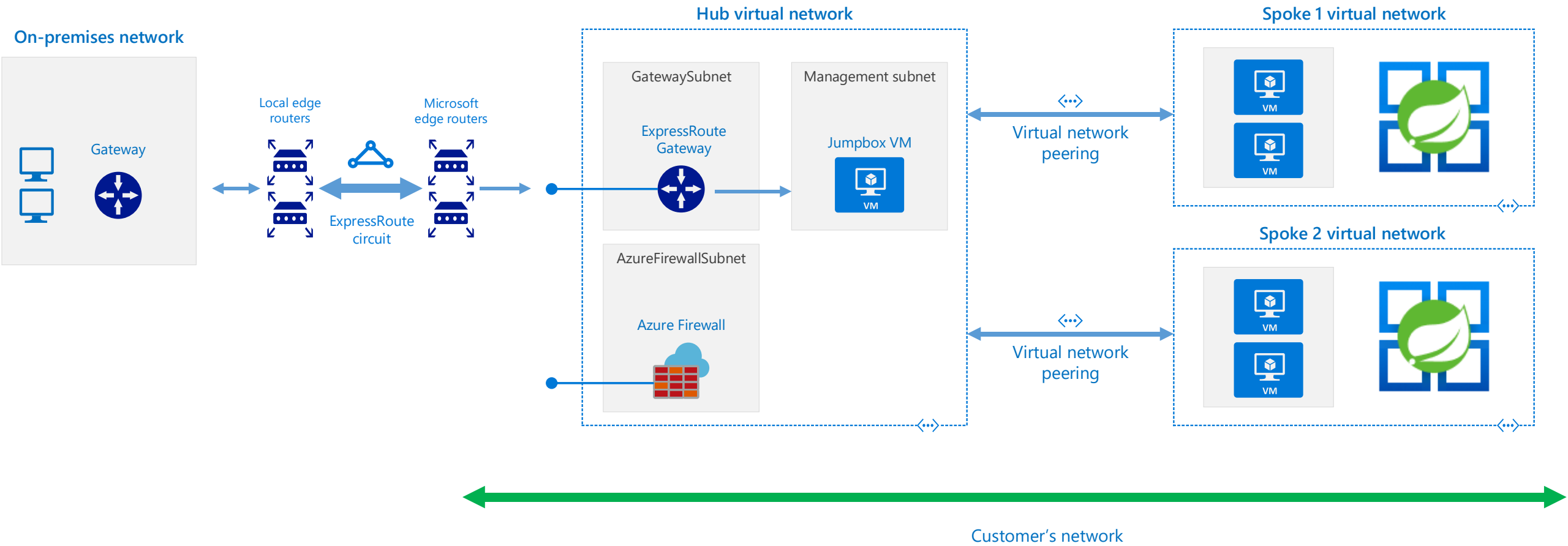
- **Isolate** Azure Spring Cloud (apps and service runtime) from Internet
  - Place it on customers' corporate networks

- Enable Azure Spring Cloud to **interact** with systems in
  - On premises data centers
  - Azure services in other VNETs

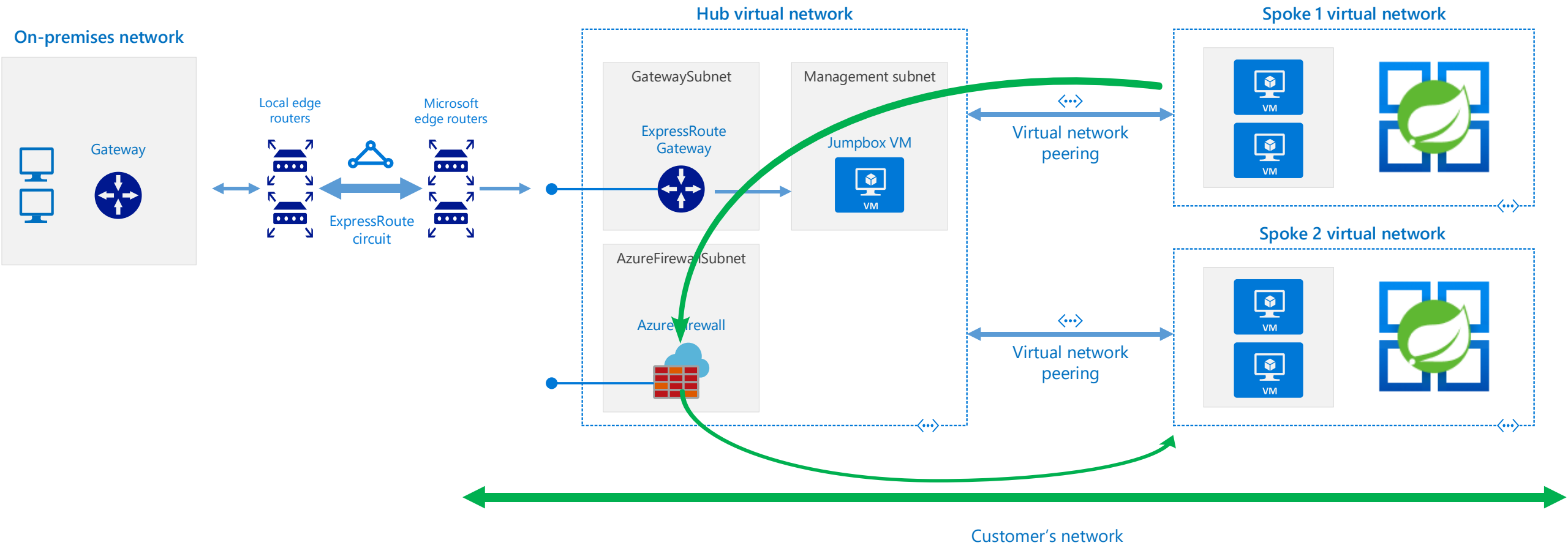
  Example - database, messaging, directory, FTP and mail systems

- Empower customers to **control** inbound and outbound network communications for Azure Spring Cloud

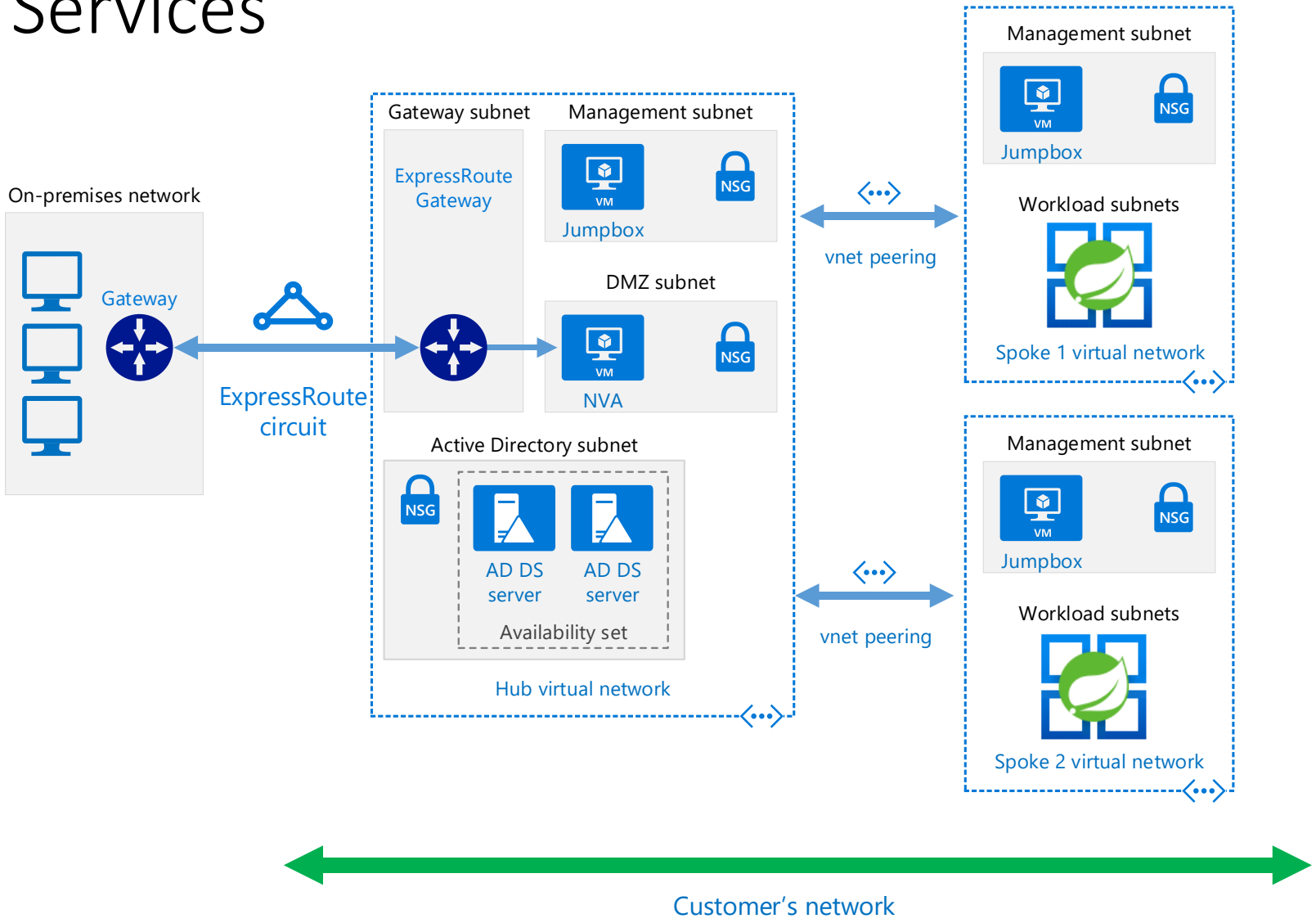
Example - Azure Spring Cloud in Hub + Spoke Topology



Example - Azure Spring Cloud in Hub + Spoke Topology



Example - Azure Spring Cloud in Hub + Spoke Topology with Shared Services

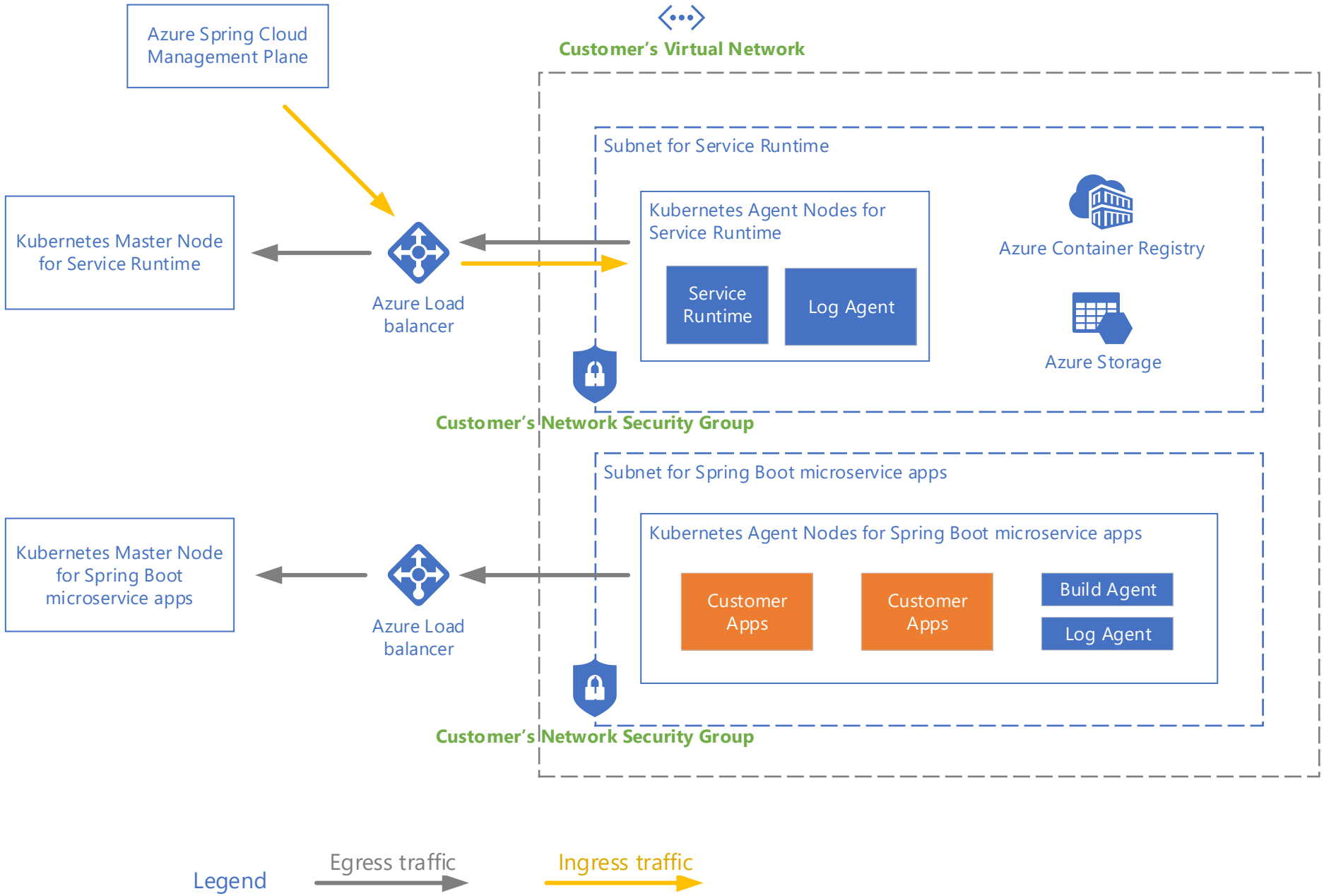


Concept – Azure Spring Cloud in VNET

Deploy Azure Spring Cloud resources in customer's own virtual network (sometimes called *VNet injection*) using:

- **Subnet for service runtime** - to host Spring Cloud Registry, Config Server, Storage, Azure Container Registry, log streaming, etc.
- **Subnet for Spring Boot microservice apps** - to host these apps
- **Resource Groups** – to host related Azure resources

VNET Layout for Azure Spring Cloud



Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

Azure Spring Cloud

Create service

Basics | Diagnostic setting | Tracing | Networking | Tags | Review and create

Deploy Azure Spring Cloud in your own virtual network (VNet). Two new subnets will be created in your virtual network.
Implicit delegation of both subnets will be done to Azure Spring Cloud on your behalf.

Deploy in your own virtual network ⓘ  No

Review + create | < Previous | Next : Tags > | Download a template for automation

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

Azure Spring Cloud

Create service

Basics | Diagnostic setting | Tracing | Networking | Tags | Review and create

Deploy Azure Spring Cloud in your own virtual network (VNet). Two new subnets will be created in your virtual network.
Implicit delegation of both subnets will be done to Azure Spring Cloud on your behalf.

Deploy in your own virtual network ⓘ Yes

Virtual network * ⓘ Placeholder

Create new

Service runtime subnet

Subnet name * service-runtime-subnet

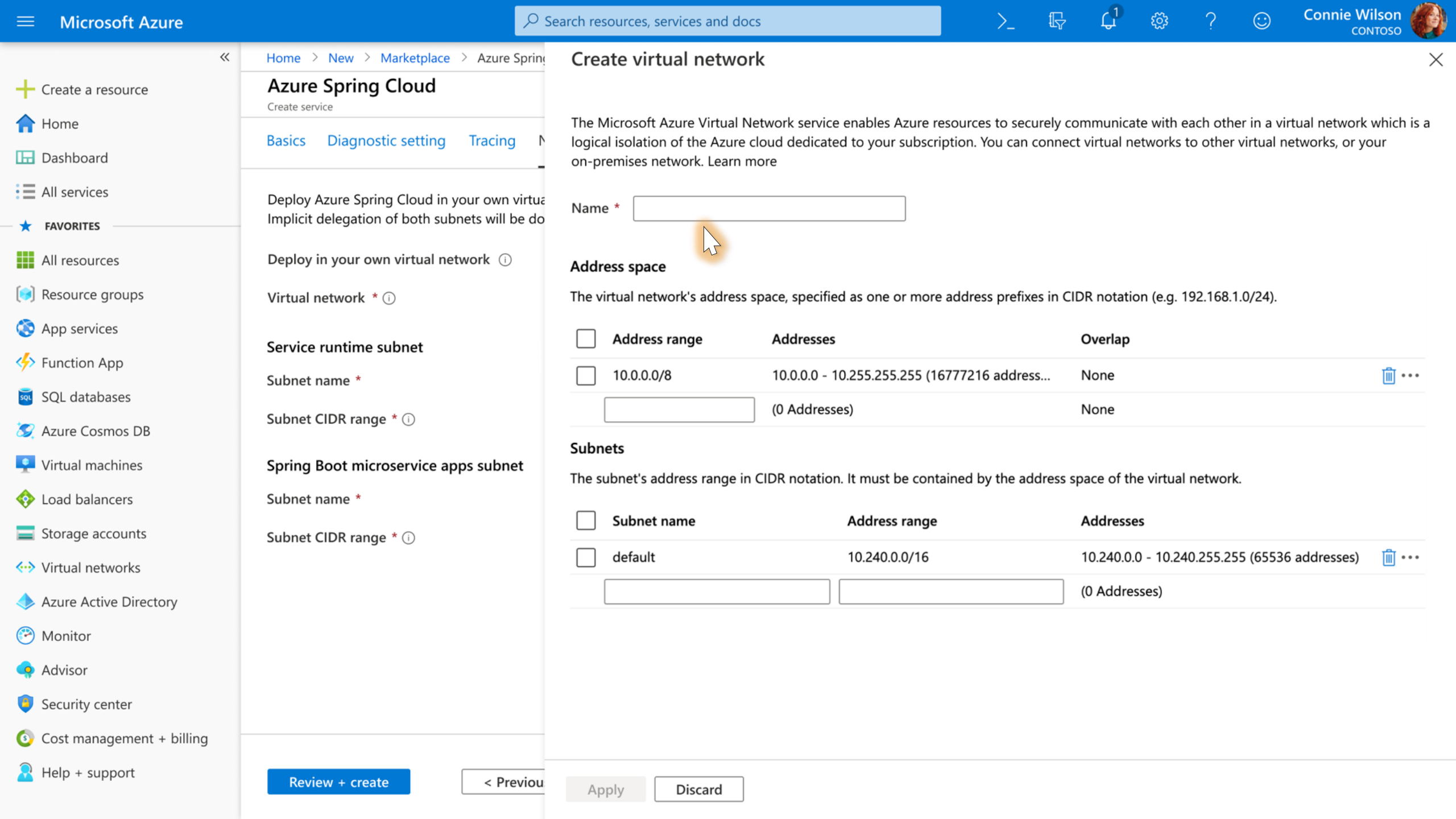
Subnet CIDR range * ⓘ ex. 10.0.3.0/24

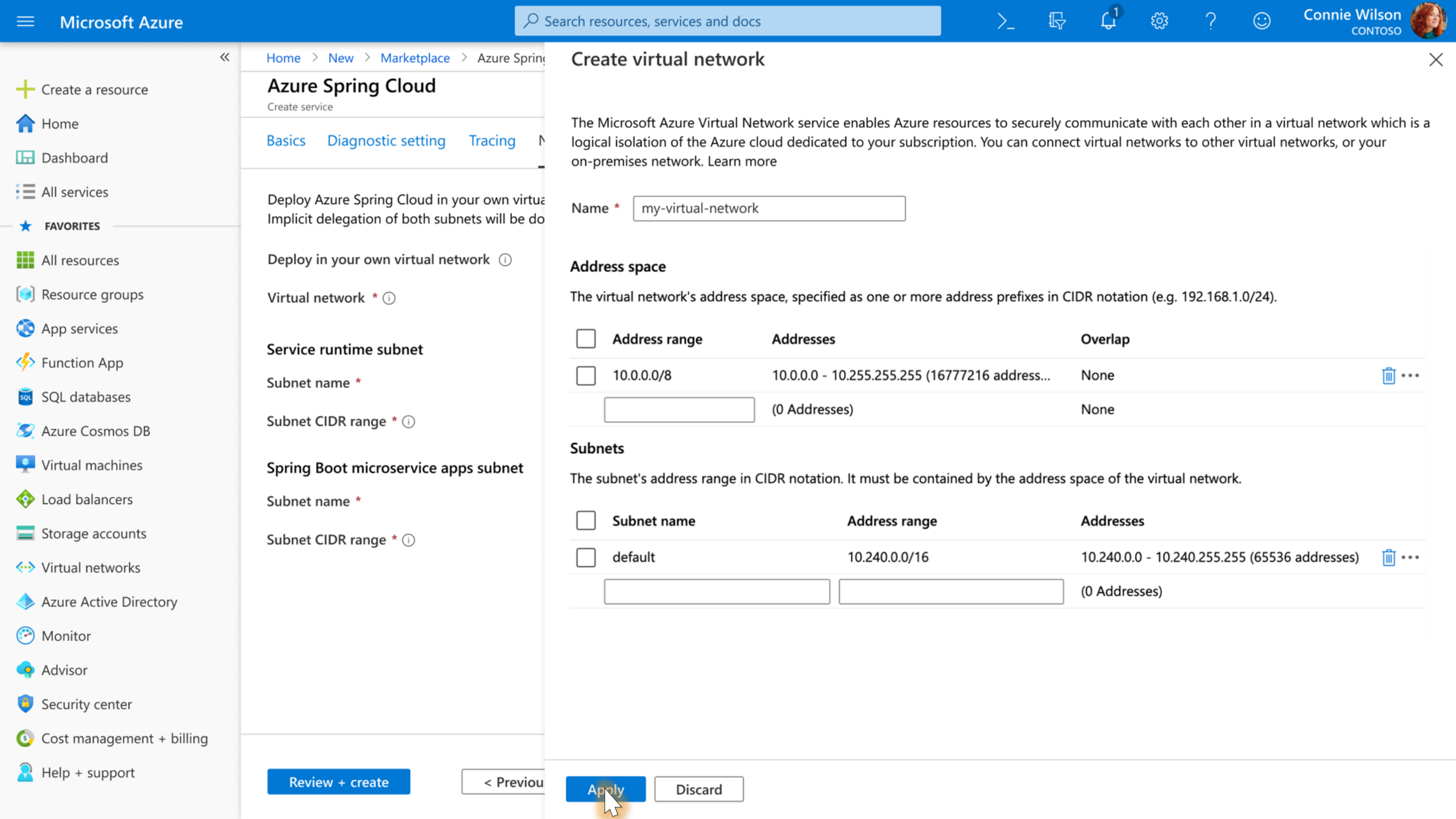
Spring Boot microservice apps subnet

Subnet name * apps-subnet

Subnet CIDR range * ⓘ ex. 10.0.4.0/24

Review + create | < Previous | Next : Tags > | Download a template for automation


Microsoft Azure
Search resources, services and docs
Connie Wilson
CONTOSO
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support
Home > New > Marketplace > Azure Spring
Azure Spring Cloud
Create service
Basics
Diagnostic setting
Tracing
Deploy Azure Spring Cloud in your own virtua
Implicit delegation of both subnets will be do
Deploy in your own virtual network
Virtual network *
Service runtime subnet
Subnet name *
Subnet CIDR range *
Spring Boot microservice apps subnet
Subnet name *
Subnet CIDR range *
Review + create
< Previou
Create virtual network
The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more
Name *
Address space
The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).
Address range
Addresses
Overlap
10.0.0.0/8
10.0.0.0 - 10.255.255.255 (16777216 address...
None
(0 Addresses)
None
Subnets
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.
Subnet name
Address range
Addresses
default
10.240.0.0/16
10.240.0.0 - 10.240.255.255 (65536 addresses)
(0 Addresses)
Apply
Discard


Microsoft Azure
Search resources, services and docs
Connie Wilson
CONTOSO
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support
Home > New > Marketplace > Azure Spring
Azure Spring Cloud
Create service
Basics
Diagnostic setting
Tracing
Deploy Azure Spring Cloud in your own virtua
Implicit delegation of both subnets will be do
Deploy in your own virtual network
Virtual network *
Service runtime subnet
Subnet name *
Subnet CIDR range *
Spring Boot microservice apps subnet
Subnet name *
Subnet CIDR range *
Review + create
< Previou
Create virtual network
The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more
Name *
my-virtual-network
Address space
The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).
Address range
Addresses
Overlap
10.0.0.0/8
10.0.0.0 - 10.255.255.255 (16777216 address...
None
(0 Addresses)
None
Subnets
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.
Subnet name
Address range
Addresses
default
10.240.0.0/16
10.240.0.0 - 10.240.255.255 (65536 addresses)
(0 Addresses)
Apply
Discard

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

Azure Spring Cloud

Create service

Basics | Diagnostic setting | Tracing | Networking | Tags | Review and create

Deploy Azure Spring Cloud in your own virtual network (VNet). Two new subnets will be created in your virtual network.
Implicit delegation of both subnets will be done to Azure Spring Cloud on your behalf.

Deploy in your own virtual network ⓘ — Yes

Virtual network * ⓘ — my-virtual-network

Create new

Service runtime subnet

Subnet name * — service-runtime-subnet

Subnet CIDR range * ⓘ — 10.0.3.0/24

Spring Boot microservice apps subnet

Subnet name * — apps-subnet

Subnet CIDR range * ⓘ — 10.0.4.0/24

Review + create | < Previous | Next : Tags > | Download a template for automation

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

Azure Spring Cloud

Create service

Basics | Diagnostic setting | Tracing | Networking | Tags | Review and create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value
Department	Finance
Environment	Pre-Production

Review + create | < Previous | Next : Review + create > | Download a template for automation

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

Azure Spring Cloud

Create service

Basics | Diagnostic setting | Tracing | Networking | Tags | Review and create

Product details

Azure Spring Cloud
by Microsoft
Terms of use | Privacy policy

Pricing for Azure Spring Cloud

Terms

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. For additional details see Azure Marketplace Terms.

Basics

Service name	piggymetrics
Subscription	Lorem ipsum
Resource group	lorem ipsum
Pegion	(US) East US

Monitoring

Enable logs	Yes
Log Analytics workspace	abc-e2e-test-20200309-2c-la
Enable tracing	Yes

Create | < Previous | Next > | Download a template for automation

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

Azure Spring Cloud

Create service

Service name	piggymetrics
Subscription	Azure Spring Cloud Team
Resource group	lorem ipsum
Pegion	(US) East US

Monitoring

Enable logs	Yes
Log Analytics workspace	abc-e2e-test-20200309-2c-la
Enable tracing	Yes
App insights	piggymetrics-1031

Networking

Deploy in your own virtual network	Yes
Virtual network	my-virtual-network
Service runtime subnet name	service-runtime-subnet
Service runtime subnet CIDR range	10.0.3.0/24
Spring Boot microservice apps subnet name	apps-subnet
Spring Boot microservice apps subnet CIDR range	10.0.4.0/24

Create < Previous Next > Download a template for automation

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

piggymetrics

Azure Spring Cloud | Directory: Microsoft

Search in the menu

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Apps
Config Server
Deployments
Networking
Test endpoint keys
Properties
Locks
Export template

Monitoring
Metrics
Diagnostics settings
Logs

Refresh Delete

Resource group
lorem ipsum

Subscription name
Lorem ipsum

Location
West Europe

Subscription ID
685ba99728-2138-sbshd-sbnbj-jknsjkwhjekkajk

Status
Succeeded

Tags (change)
Department: Finance | Environment: Pre-Production

Simplify Spring Boot app development and management

Use Spring Cloud to bring modern microservice patterns to Spring Boot apps, eliminating boilerplate code to quickly develop robust Java apps. Easily deploy, operate, and scale your apps in a fully managed environment.

Config Server
Connect and manage externalized config settings with Spring Config Server.

Create app
Create apps in simple steps.

Distributed tracing
Spot performance bottlenecks or fai hotspots across components apps.

Timespan : **Lsat 1 hour**

Header

Header

Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support

piggymetrics | Networking

Azure Spring Cloud | Directory: Microsoft

Search in the menu

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Apps
Config Server
Deployments
Networking
Test endpoint keys
Properties
Locks
Export template

Monitoring

Metrics
Diagnostics settings
Logs

Deploy in your own virtual network	Yes
Virtual network	my-virtual-network
Azure Spring Cloud reserved CIDR range	10.244.0.0/14

Service runtime subnet

Subnet name	service-runtime-subnet
Subnet CIDR range	10.0.3.0/24

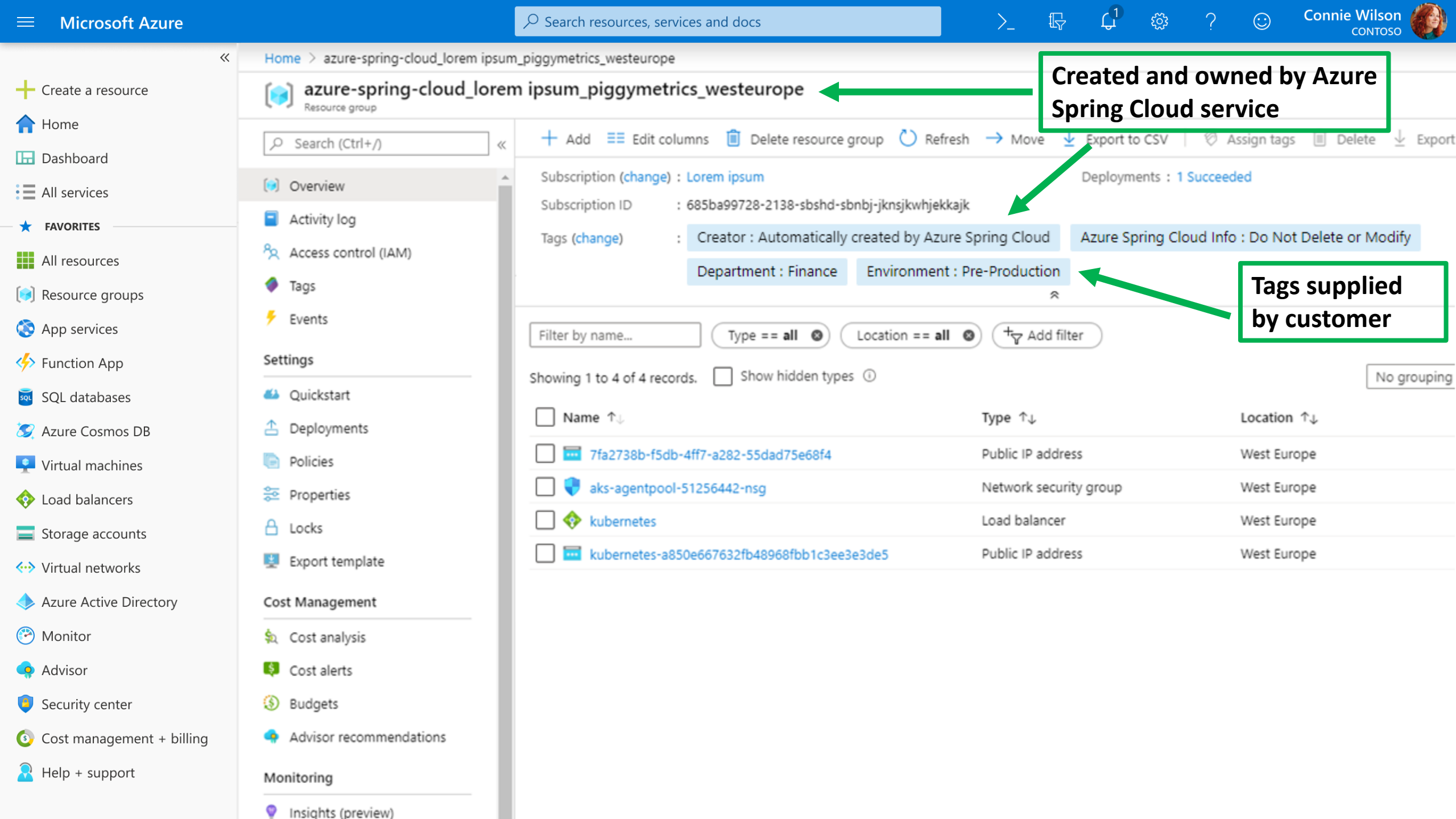
Spring Boot microservice apps subnet

Subnet name	apps-subnet
Subnet CIDR range	10.0.4.0/24

What happens when Azure Spring Cloud is placed in VNET?

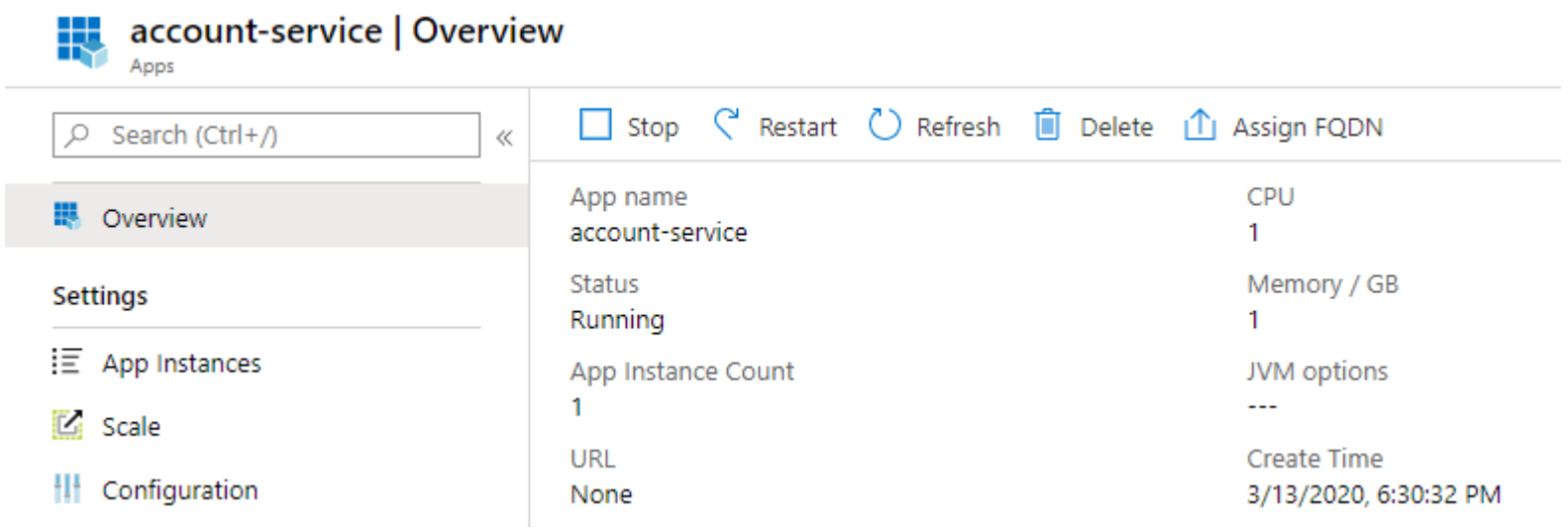
- Service runtime components are injected into "**subnet for service runtime"** in customer's VNET
- Microservice apps are injected into **"subnet for Spring Boot microservice apps"** in customer's VNET
- **Resource Groups** are created in customer's subscription to host network resources (Load Balancer, Public IP, etc.) owned by the Azure Spring Cloud service instance. The resource group is fully managed by Azure Spring Cloud service.
  - One RG for service runtime and another RG for microservice apps – network resources
  - Resources in this resource group are charged to customer's subscription.

"azure_spring_cloud_[SUBSCRIPTION-ID]_[SERVICE-NAME]_[REGION]_[RANDOMID]" – ***Resource Group name***


Microsoft Azure
Search resources, services and docs
Connie Wilson
CONTOSO
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security center
Cost management + billing
Help + support
Home > azure-spring-cloud_lorem ipsum_piggymetrics_westeurope
azure-spring-cloud_lorem ipsum_piggymetrics_westeurope
Resource group
Created and owned by Azure Spring Cloud service
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Events
Settings
Quickstart
Deployments
Policies
Properties
Locks
Export template
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Monitoring
Insights (preview)
Add
Edit columns
Delete resource group
Refresh
Move
Export to CSV
Assign tags
Delete
Export
Subscription (change) : Lorem ipsum
Deployments : 1 Succeeded
Subscription ID : 685ba99728-2138-sbshd-sbnbj-jknsjkwhjekkajk
Tags (change) :
Creator : Automatically created by Azure Spring Cloud
Azure Spring Cloud Info : Do Not Delete or Modify
Department : Finance
Environment : Pre-Production
Tags supplied by customer
Filter by name...
Type == all
Location == all
Add filter
Showing 1 to 4 of 4 records.
Show hidden types
No grouping
Name
Type
Location
7fa2738b-f5db-4ff7-a282-55dad75e68f4
Public IP address
West Europe
aks-agentpool-51256442-nsg
Network security group
West Europe
kubernetes
Load balancer
West Europe
kubernetes-a850e667632fb48968fbb1c3ee3e3de5
Public IP address
West Europe

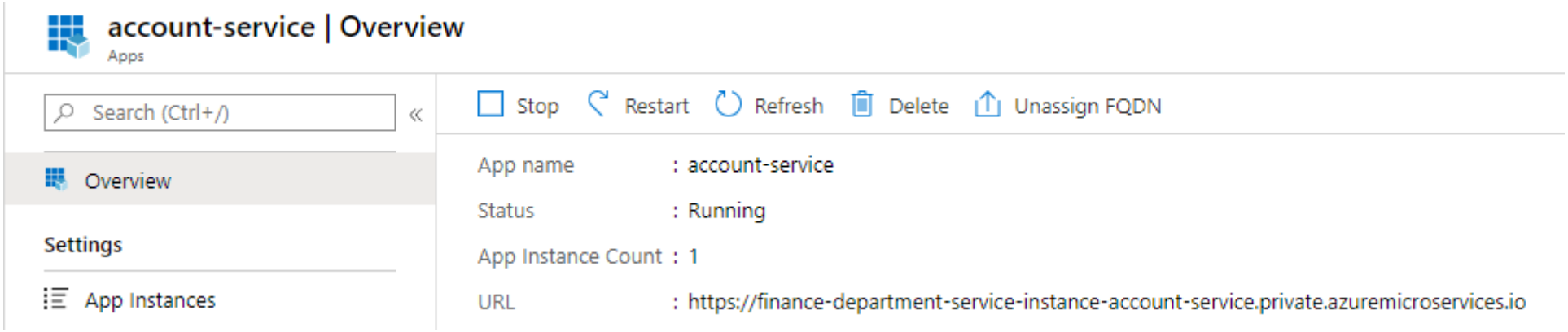
Endpoints - Azure Spring Cloud …

- Reserves 256 + 256 IP addresses from the two supplied subnets
- By default, apps are not bound to IP addresses



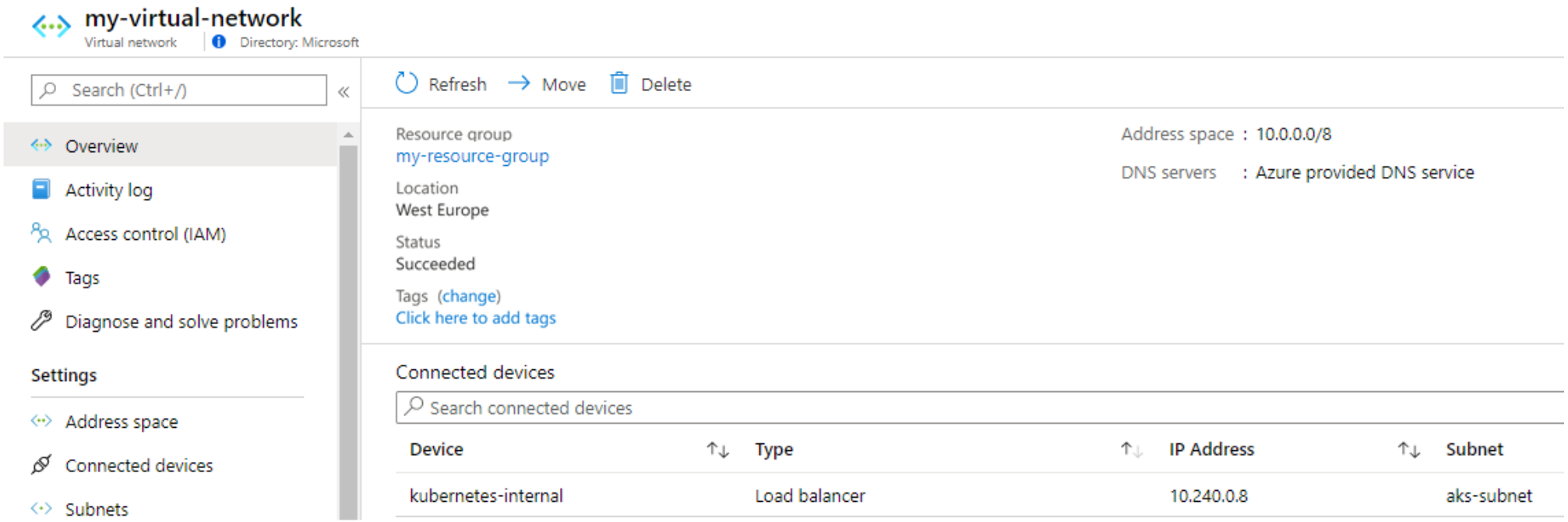
Endpoints - Azure Spring Cloud …

- On request, supplies default names for app and test endpoints
  - App Private FQDN
    - [service-instance-name]-[app-name].private.azuremicroservices.io
- Assigns app FQDN with random IP addresses from the customer subnet



Endpoints - Azure Spring Cloud …

- Customers can create and manage their own DNS, by creating a private DNS zone *private.azuremicroservices.io* and put into the same VNET as the one used for Azure Spring Cloud service instance
- Customers can create an A record to map [service-instance-name]-[app-name].private.azuremicroservices.io (or *.private.azuremicroservices.io if needed) to the ILB IP address



Endpoints - Azure Spring Cloud …

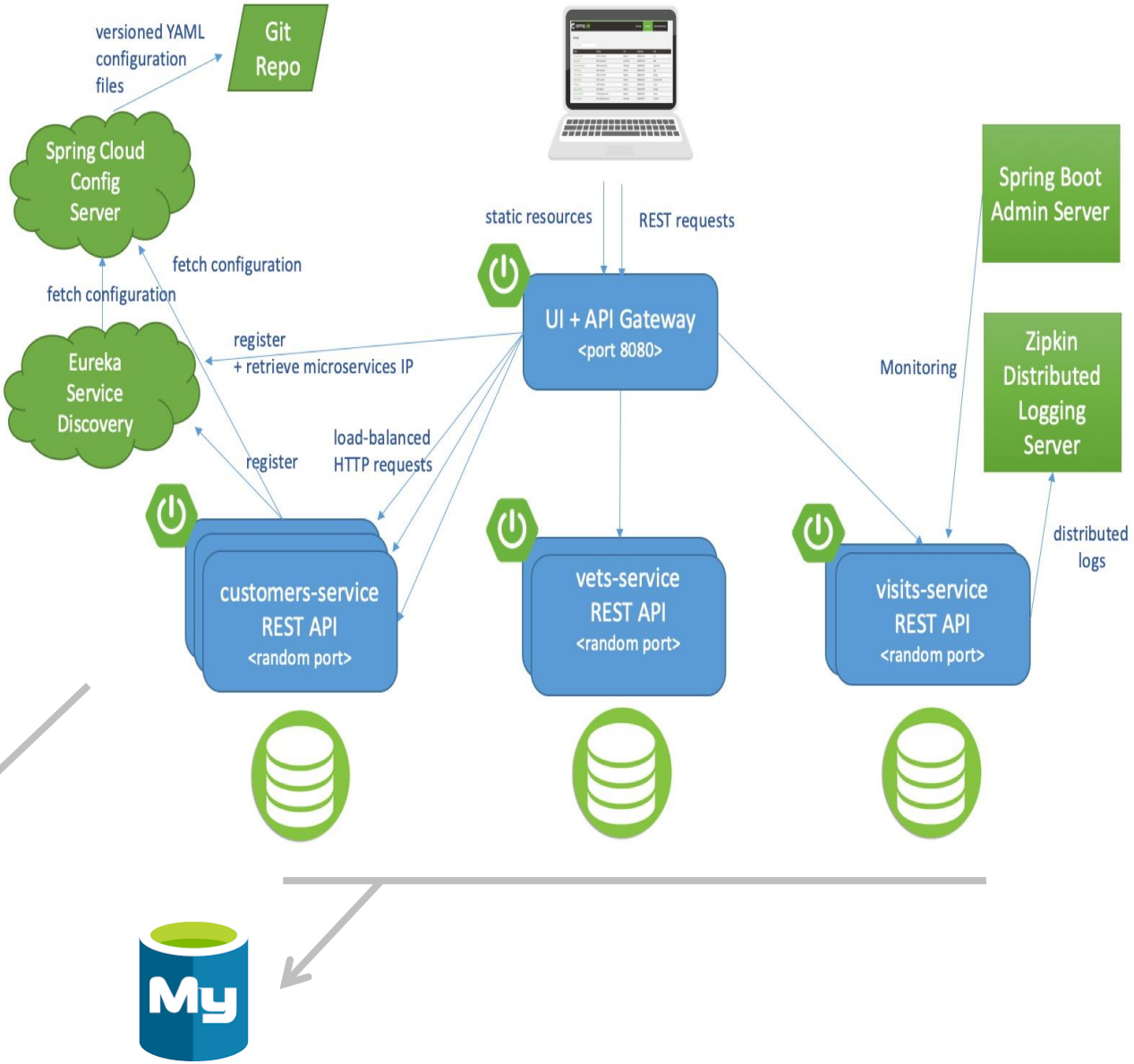
Test endpoints – can be disabled

[name]:[password]@[service-instance-name].test.**private**.azuremicroservices.io/[app-name]/[deployment-name]/

Demo

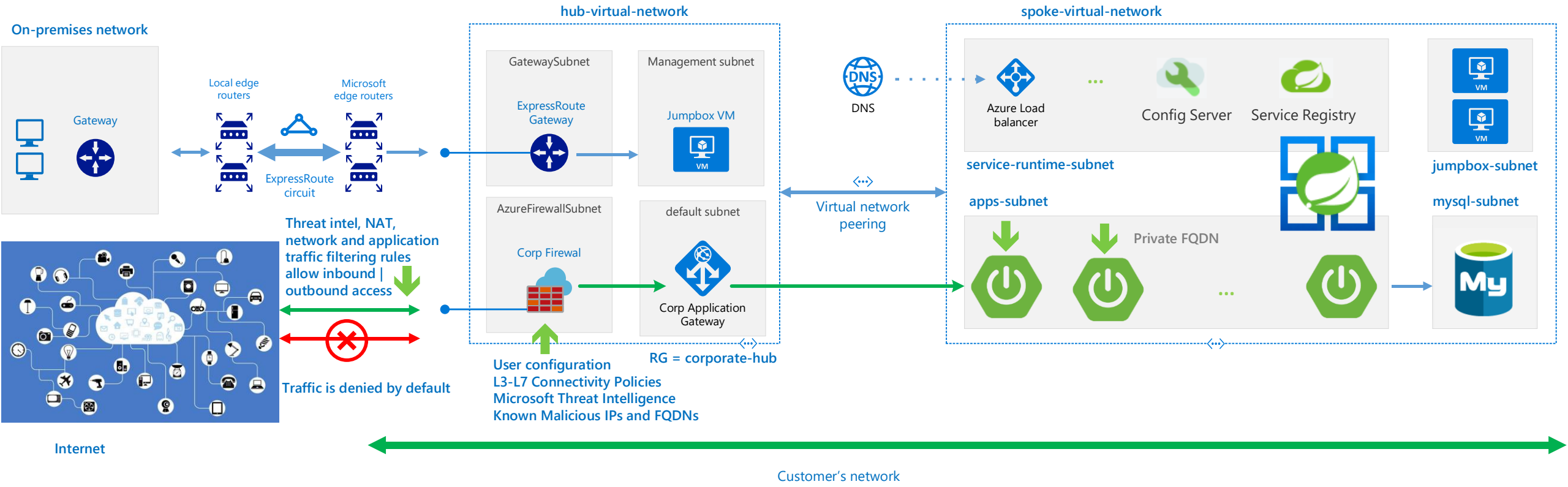
Deploy Spring Cloud app to Azure without worrying about:

- Infrastructure and scaling
- Spring Cloud middleware – config, registry, tracing and gateway, or
- Monitoring



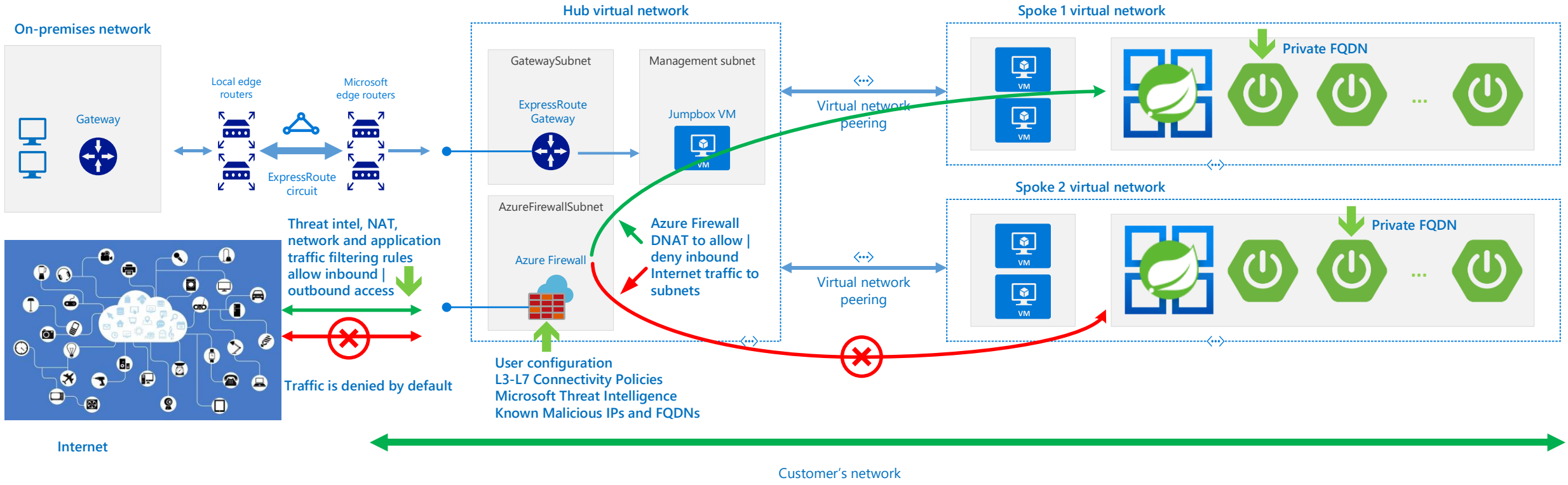
Demo – isolate apps and expose apps to Internet

Integrate with Azure Firewall & App Gateway to allow | deny traffic to FQDNs



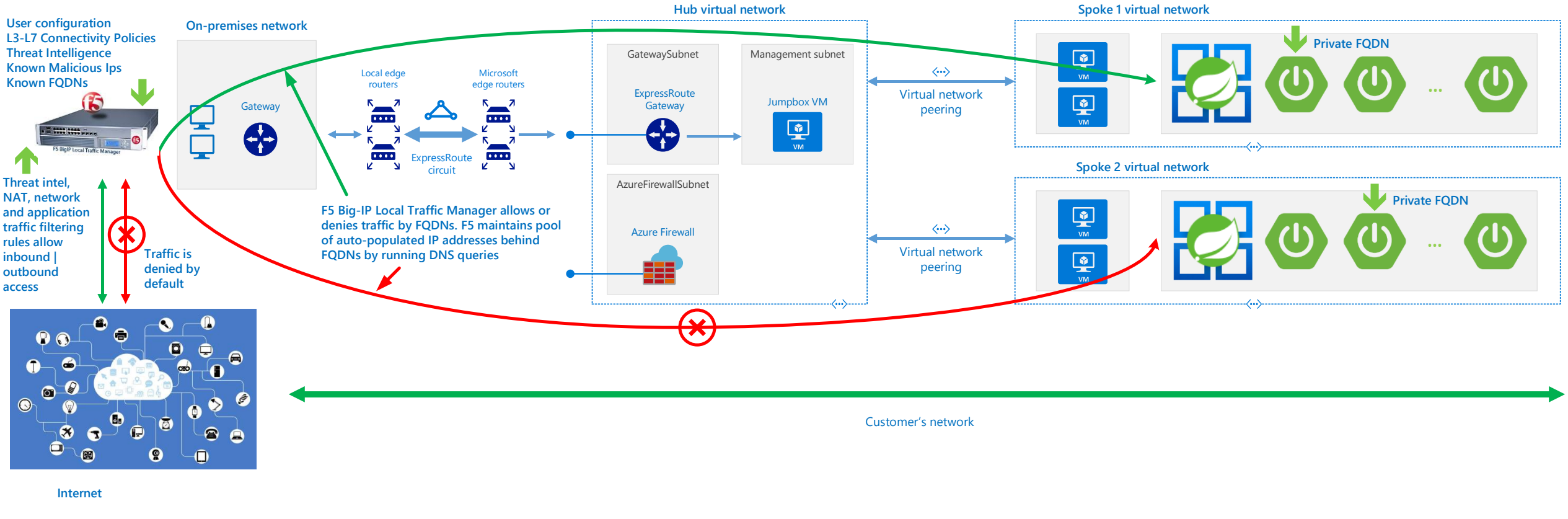
Expose apps to Internet – Example 1

Integrate with Azure Firewall in App Gateway to allow | deny traffic to subnets



Expose apps to Internet – Example 2

Integrate with F5 Big-IP Solution to allow | deny traffic to FQDNs



Customer can …

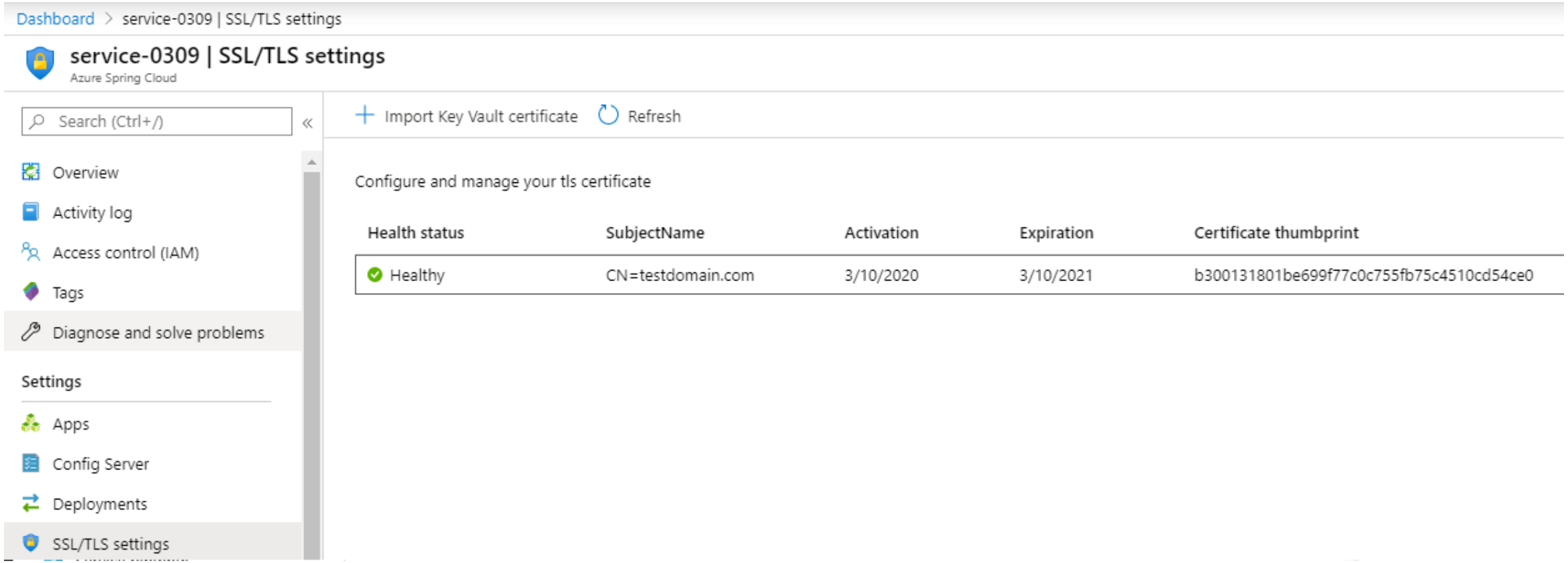
- **Control ingress and egress** traffic for VNET
  - Force tunnel Internet traffic (use UDR to define)
  - Define UDR for VNET
- **Assign Private FQDN** to apps
- **Compose with Azure Network** resources
  - Express Route
  - VPN
  - VNET Peering
  - Traffic Manager
  - Application Gateway
  - Azure Front Door
  - Azure Firewall

Customer can …

- Rely on **service-level diagnostic check** to continuously validate if VNET Injection is operational
  - Ingress, egress, resource health, subnet health, etc.

- Upload **certs**, bind **custom domains** to apps, and use certs for **TLS** communications
- Bring your own certs from **any Certificate Authority**
- **Deploy** apps and apply config – just like they do without VNET
  - Using Azure CLI, Maven, IntelliJ, Azure Pipelines, GitHub Actions, Jenkins Pipelines, etc.
- Enable **apps to interact** with Azure Services
  - Using Private Endpoints or Service Endpoints

Upload certs – bind custom domains to apps, use certs for TLS



Don’t do list for customers …

- **Don’t modify** Resource Group created and owned by Azure Spring Cloud

  “azure_spring_cloud_[SERVICE-NAME]_[REGION]” – *Resource Group name*

- **Don’t modify subnets** used by Azure Spring Cloud

- **Don’t create more than one Azure Spring Cloud service instance** in the same subnet

Don’t do list for customers …

- **Don’t block egress** traffic to Azure Spring Cloud components for operating, maintaining and supporting the service instance

Azure Spring Cloud required network rules

Destination Endpoint	Port	Use
*:1194 *Or* ServiceTag – AzureCloud:1194	UDP:1194	Underlying Kubernetes Cluster management.
*:443 *Or* ServiceTag – AzureCloud:443	TCP:443	Azure Spring Cloud service management.
*:9000 *Or* ServiceTag – AzureCloud:9000	TCP:9000	Underlying Kubernetes Cluster management.
*:123 *Or* ntp.ubuntu.com:123	UDP:123	NTP time synchronization on Linux nodes.
*.azurecr.io:443 *Or* ServiceTag – AzureContainerRegistry:443	TCP:443	Azure Container Registry.
*.file.core.windows.net:445 *Or* ServiceTag – Storage:445	TCP:445	Azure File Storage.

Don’t do list for customers …

Azure Spring Cloud required FQDN / application rules

- Azure Firewall provides a FQDN Tag “AzureKubernetesService” to simplify all following configurations.

Destination FQDN	Port	Use
*.azmk8s.io	HTTPS:443	Underlying Kubernetes Cluster API Server.
mcr.microsoft.com	HTTPS:443	Microsoft Container Registry (MCR).
*.cdn.mscr.io	HTTPS:443	MCR storage backed by the Azure CDN.
*.data.mcr.microsoft.com	HTTPS:443	MCR storage backed by the Azure CDN.
management.azure.com	HTTPS:443	Underlying Kubernetes Cluster management.
login.microsoftonline.com	HTTPS:443	Azure Active Directory authentication.
packages.microsoft.com	HTTPS:443	Microsoft packages repository.
acs-mirror.azureedge.net	HTTPS:443	Repository required to install required binaries like kubenet and Azure CNI.