Microsoft

Design considerations & Best Practices for commonly used Microsoft Azure Workloads

Vikram Pendse – Enterprise Architect at e-Zest & Microsoft MVP

@VikramPendse | @ezest

vikram.pendse@e-zest.in

Microsoft

Agenda

Design considerations in cloud application development

- Availability
- Multisite Deployment and Traffic Manager
- Database and Storage
- Monitoring and Management
- Security
- Cost

What is “your” definition of “availability”

What is acceptable downtime ?

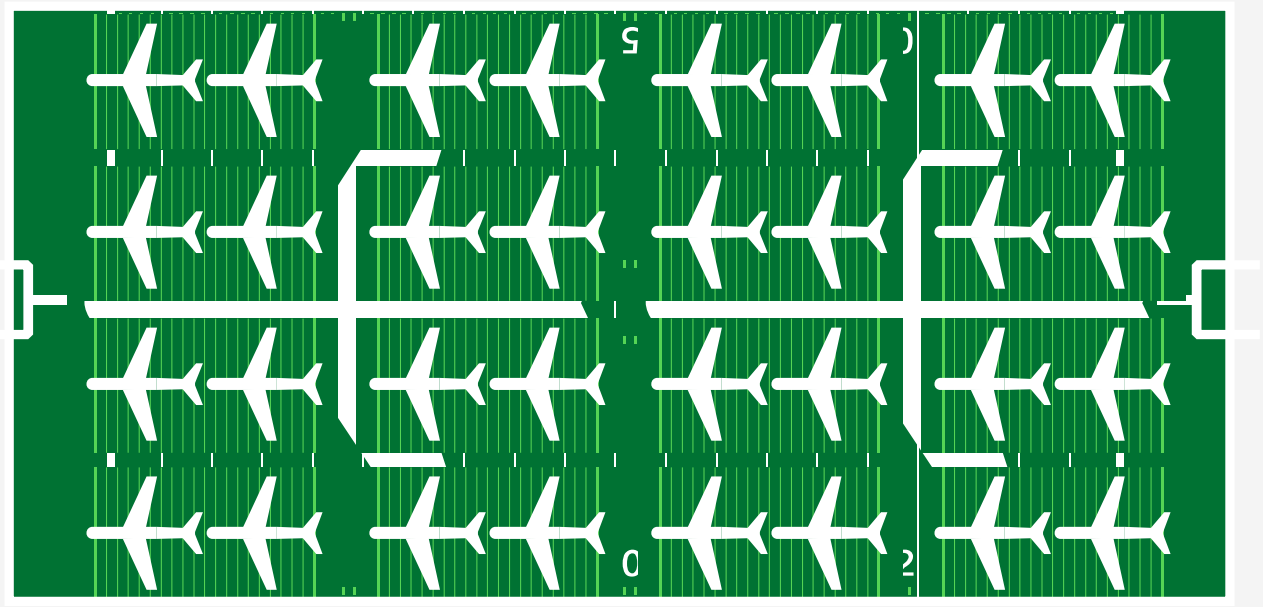
What happens in case of failure ?

Acceptable Performance

Microsoft

High Availability design for IaaS on Azure

We understand but we don't do it !



- Cost
- Lack of SLA knowledge
- Which VMs should be in HA?

- Impact
  - Downtime
  - Loss of Data
  - Loss to Business (in some cases)

Microsoft

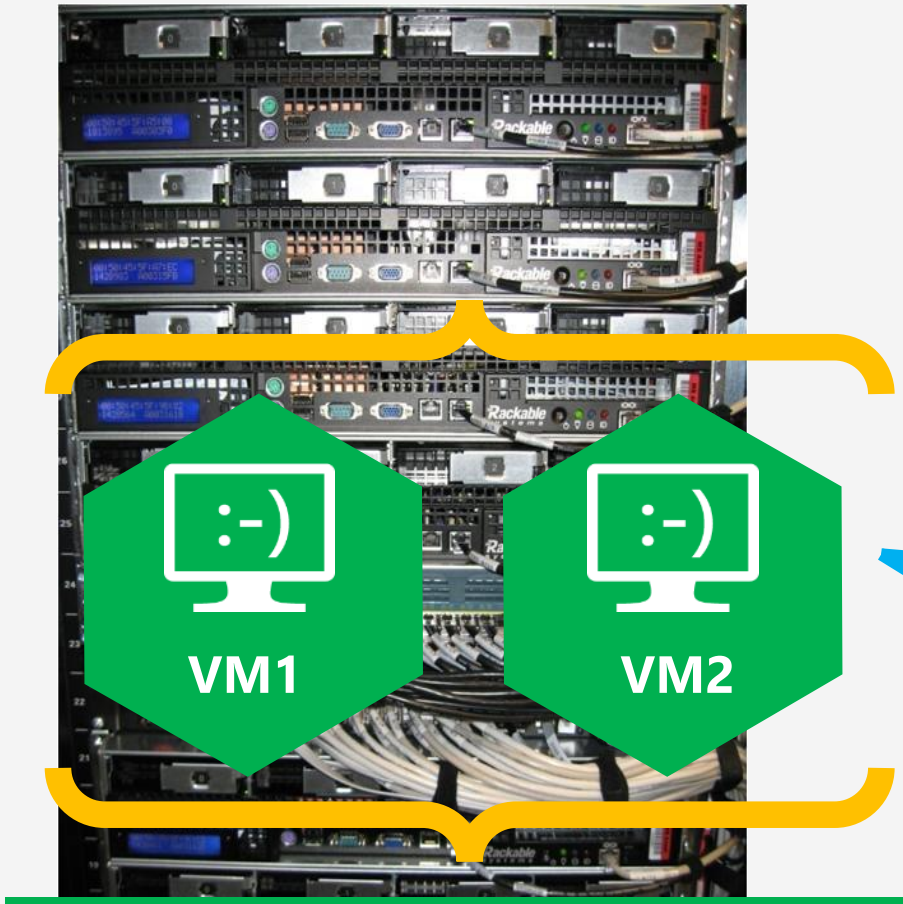
Availability Sets

Physical Machines

Power Unit
Rack Switch

Microsoft

Availability Sets



Availability Set

Physical Machines

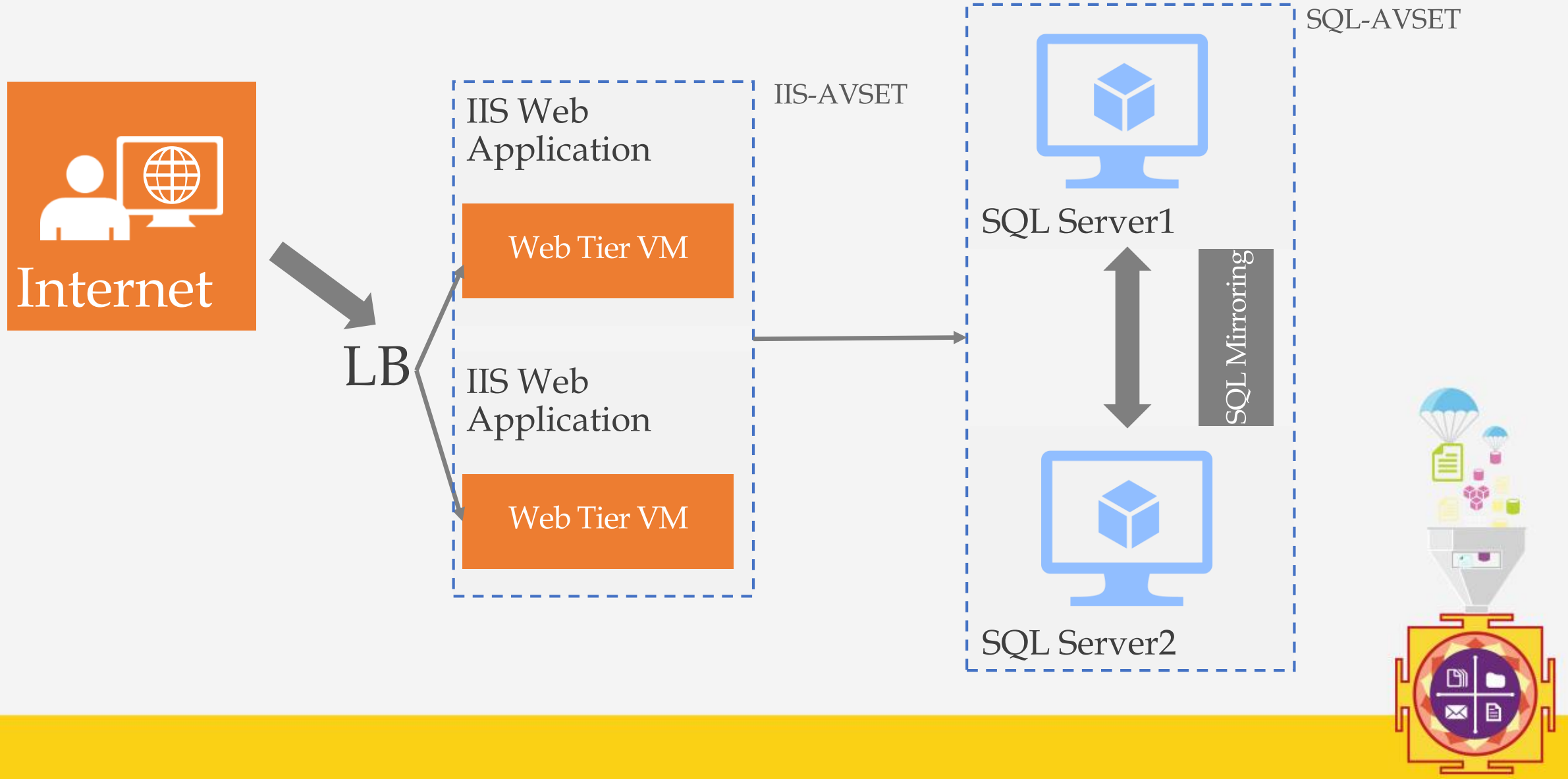
Power Unit
Rack Switch

VM1

VM2

VM2

End to End Highly Available Solution



Microsoft

Availability Set Guidance

- VMs in Availability Set Must Be in Same Resource Group
- Availability Set: 5 Update Domains, 3 Fault Domains
  - Update Domain – Host Maintenance
  - Fault Domain – Isolation from component failure in rack unit
- Maximum of 100 VMs in a Availability Set
- Avoid Availability Sets with Single VM
  - This eliminates notification for host maintenance operations

Microsoft

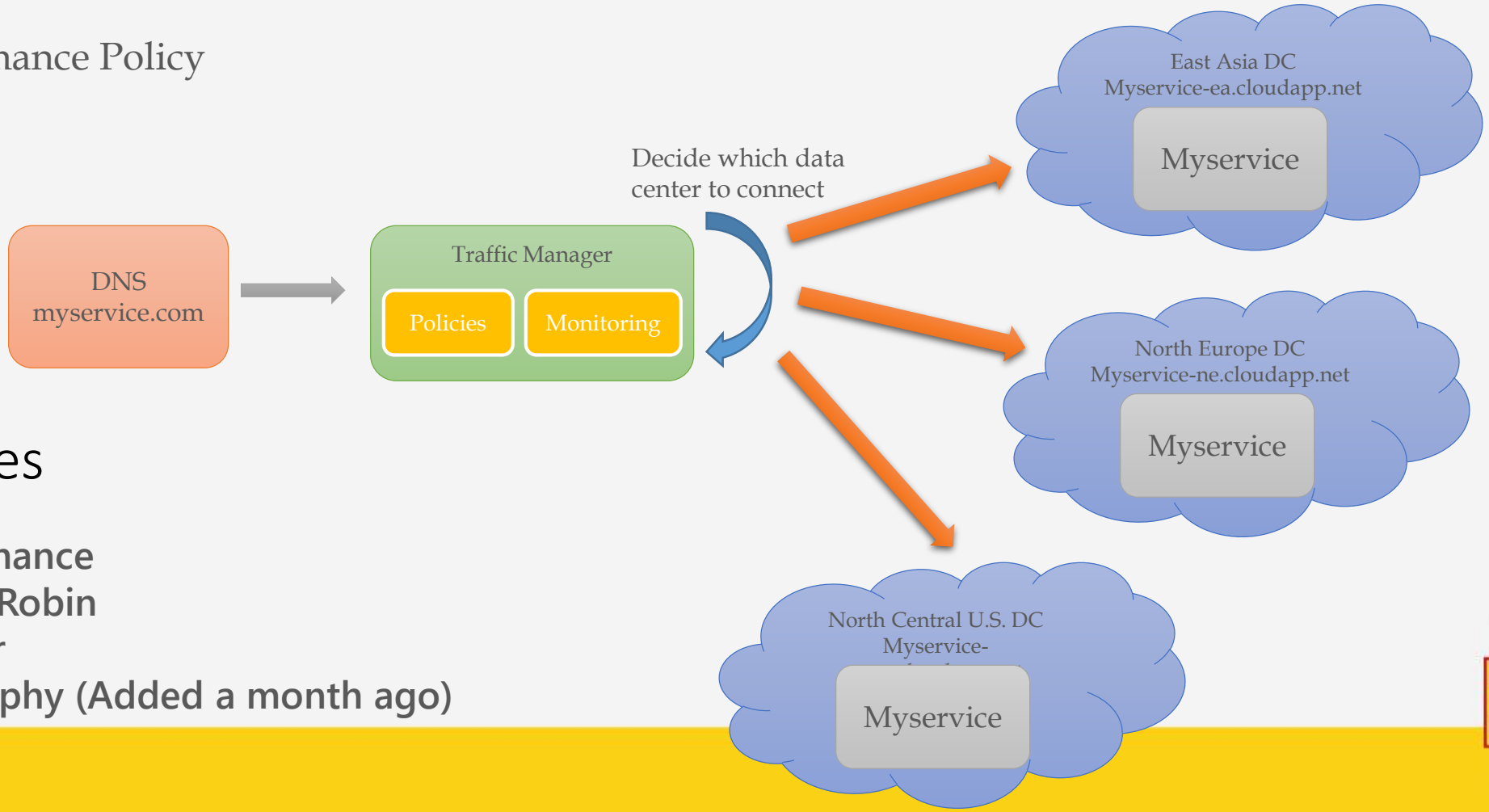
Microsoft Commitment – Single Instance SLA!!

- Microsoft now provides Single Instance SLA*, no competitor provides. (Since November 2016)
- SLA – 99.9%

*VM with all **premium storage disks** will have single instance SLA applicable.

How does “Traffic Manager” work ?

e.g. Performance Policy



Policies

Performance
Round Robin
Failover
Geography (Added a month ago)

Microsoft

Databases and Storage

- Azure Storage
  - Blob
  - Table
  - Queue
  - File
- NoSQL/Open Source – DocumentDB, Mongo etc.
- SQL
  - SQL PaaS
  - SQL IaaS

File Share on Azure

- Azure Files
  - SMB Protocol
  - Upto 5 TB
  - APIs
  - Managed by Platform
- VM
  - Configuration
  - Security
  - Manage VM

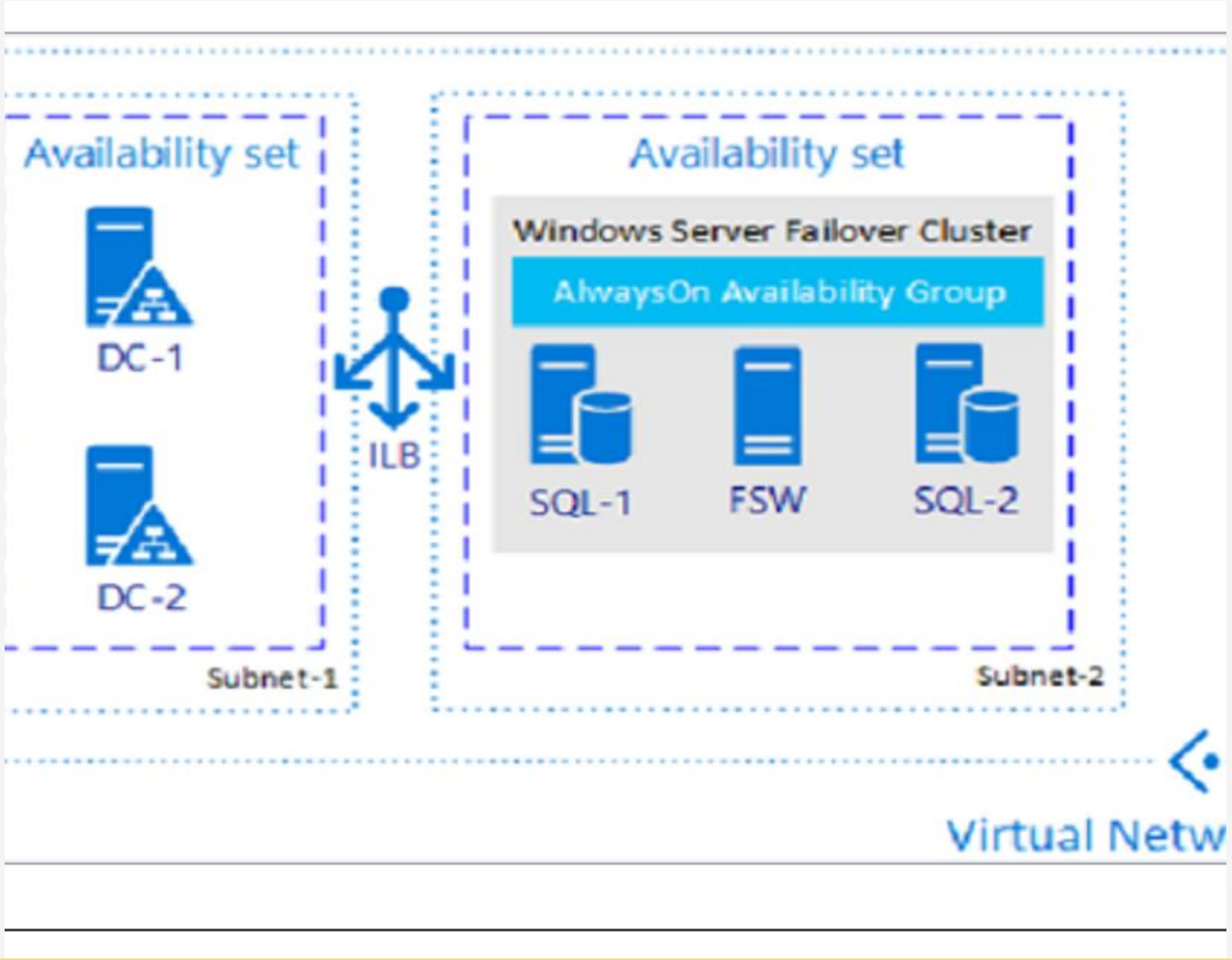
Microsoft

SQL PaaS Vs SQL IaaS

#	SQL SERVER ON VM	SQL AZURE DATABASE
1	This is IaaS offering on Azure	This is PaaS offering on Azure. It is also termed as "Database as a service (DBaaS)".
2	Access to underlying VM is available.	Access to underlying VM is not available and everything to be accessed over TDS (Tabular Data stream) based endpoint.
3	Automated backups, DR and high availability is not available and one needs to configure it.	DR, Backup and High availability is available default.
4	Eliminates Hardware cost	Eliminates hardware and administration cost as well.
5	Distributed transaction or all SQL server capabilities are supported.	- Distributed transaction is not supported. - Additionally there are restrictions on the usage of some reserved keywords also. - Use command not supported.
6	DB mirroring, Log shipping, transaction replication supported.	DB mirroring, Log shipping, transaction replication not supported.
7	SSIS, SSRS, SQL agent is available.	SSIS, SSRS, SQL agent is not available.

Database HA for IaaS

- SQL Always On configuration
- Provisioning from Portal



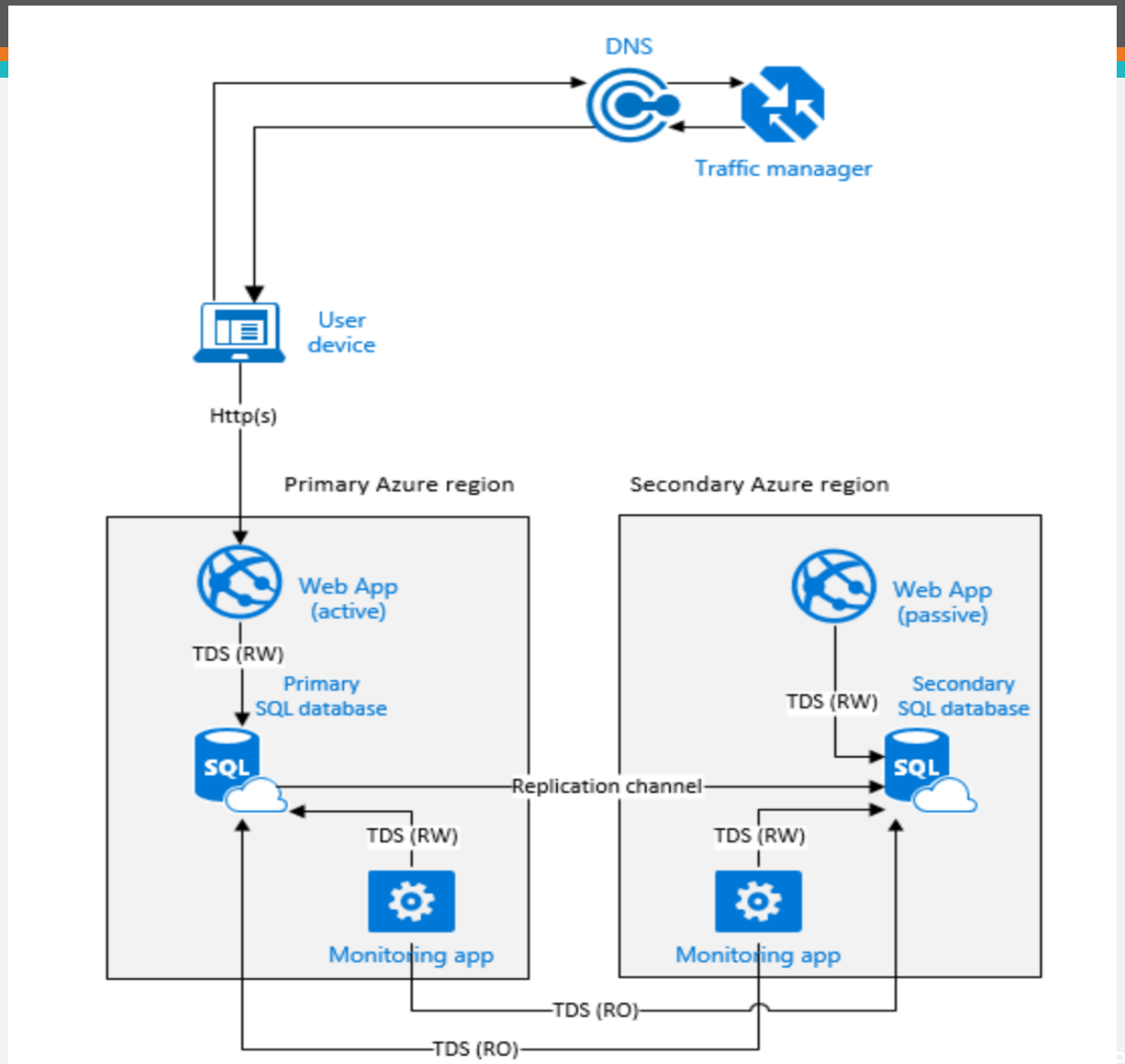
Microsoft

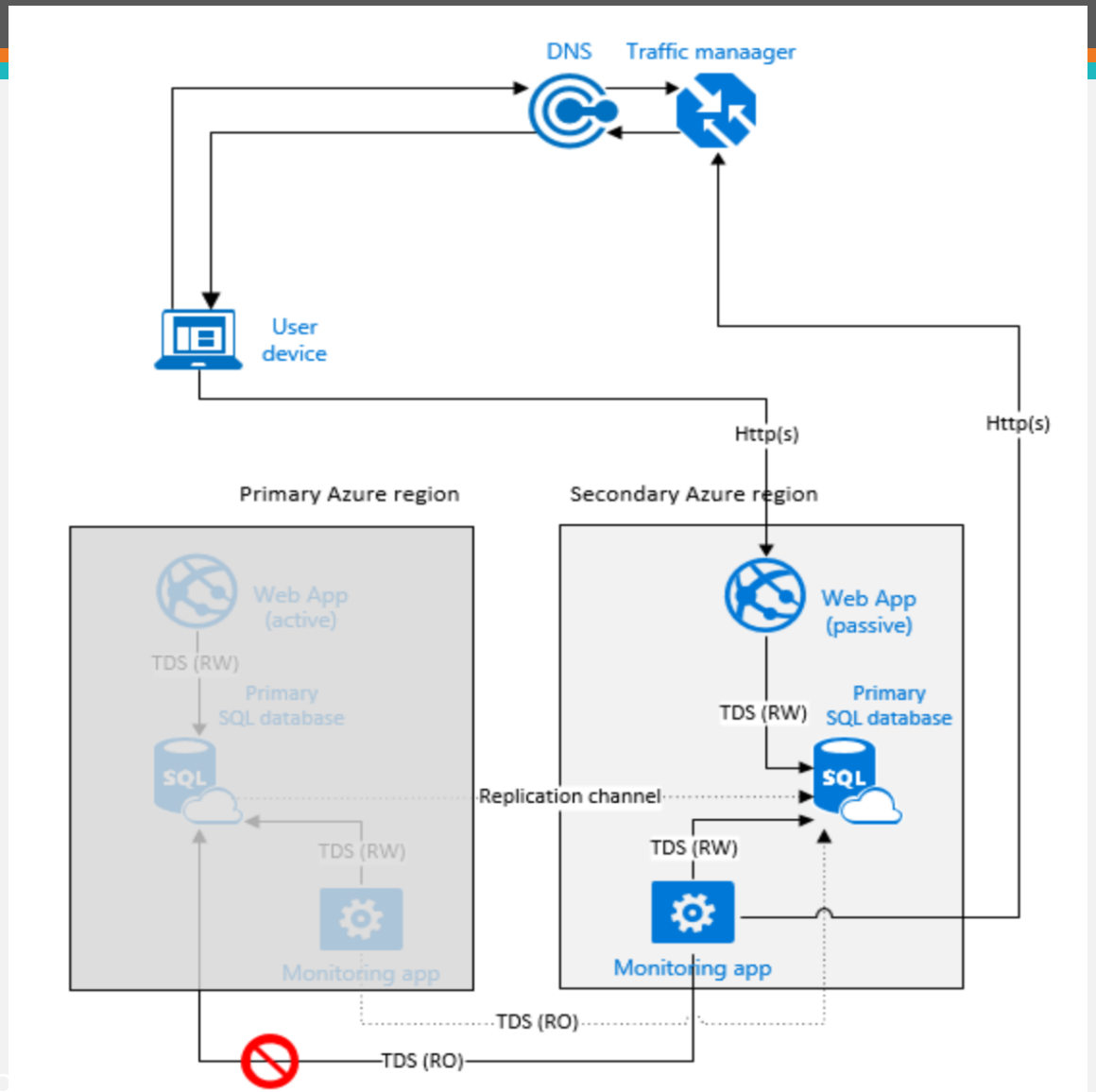
Database HA for PaaS

- SQL Azure DB being PaaS, High Availability is inbuilt.
- Backup is inbuilt and automatically taken care for you.

Microsoft

Pattern 1 - Active-Passive Disaster Recovery with Co-located DB

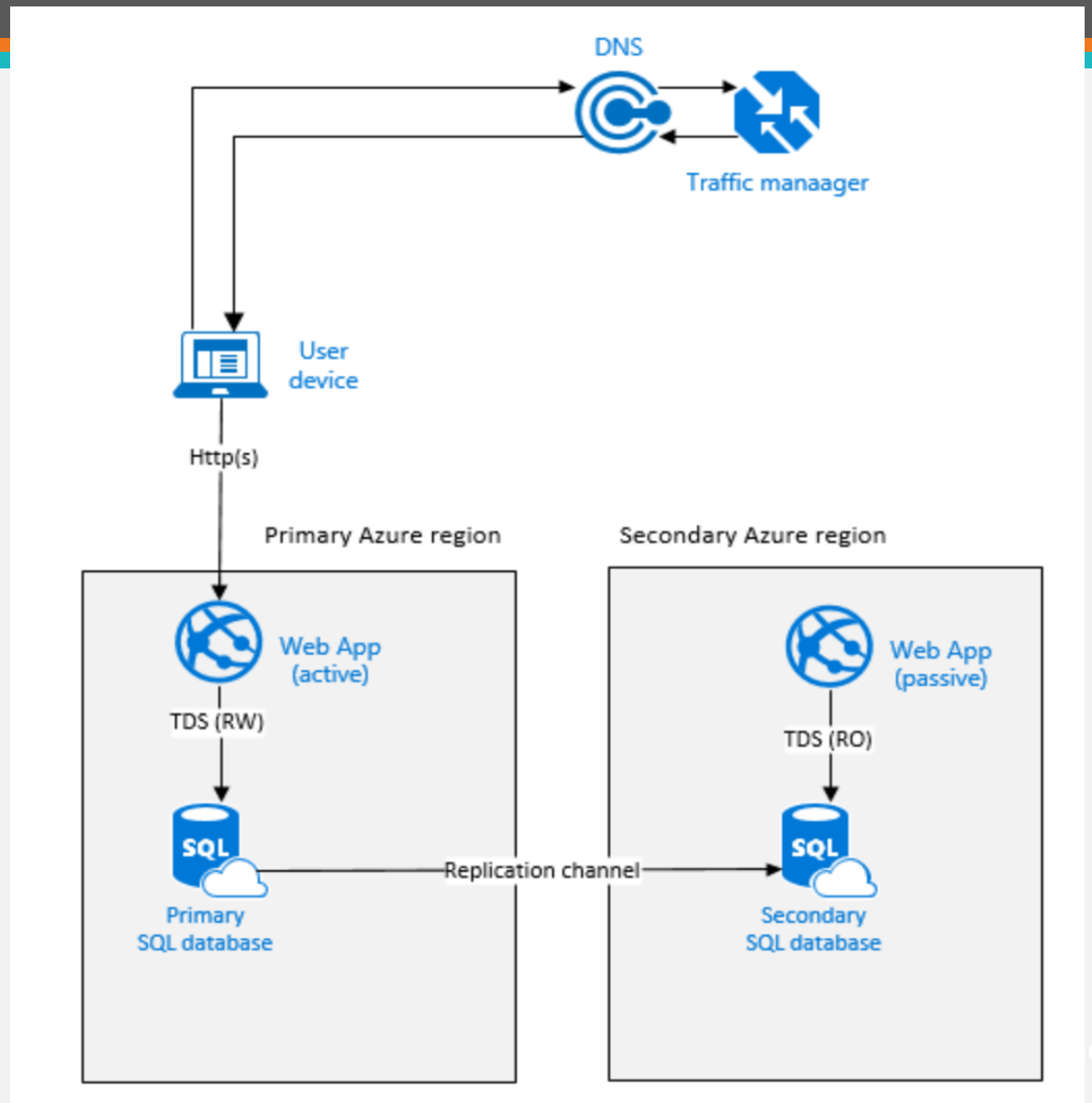


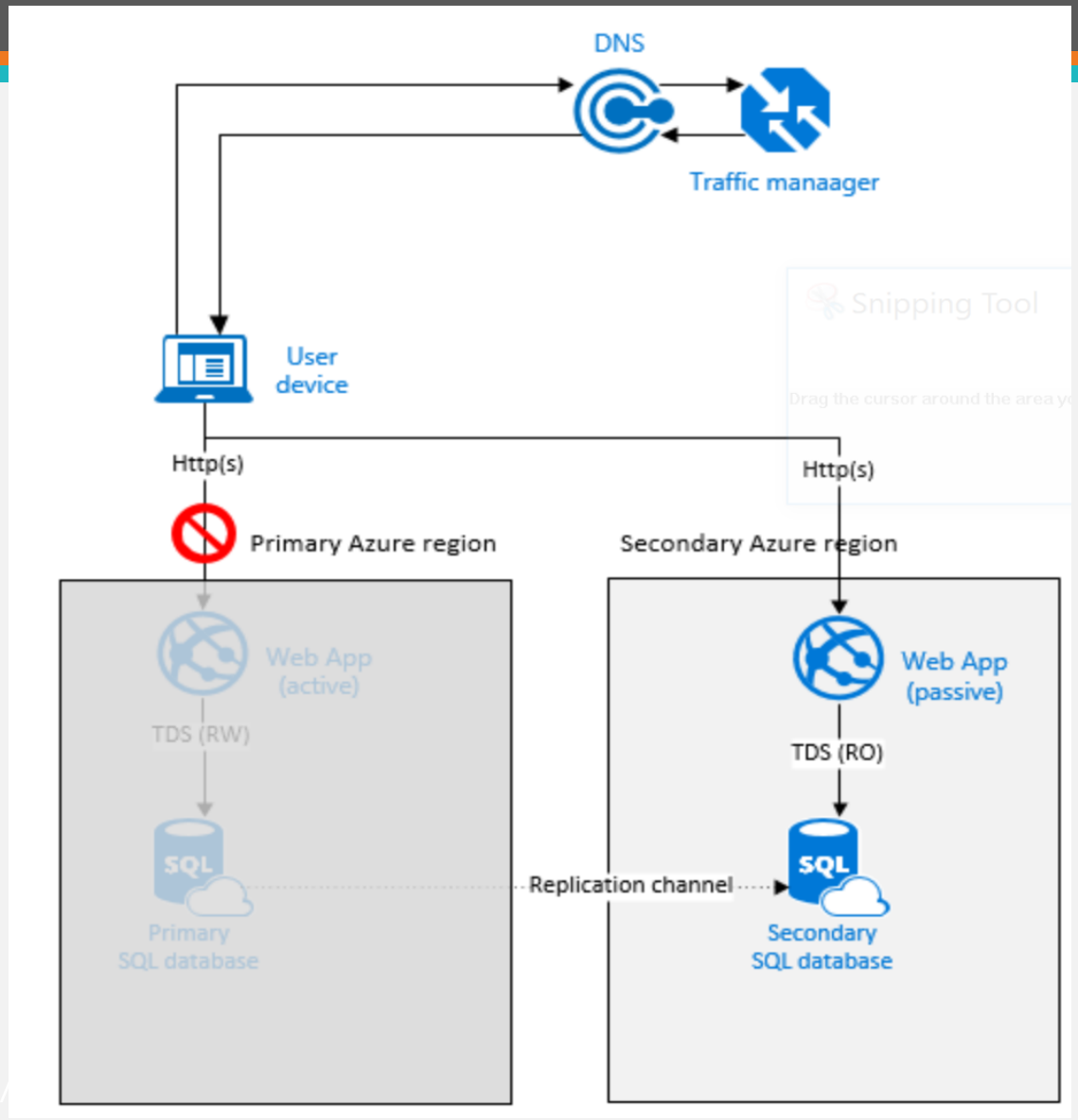


Microsoft

Pattern 2 - Active-Passive Disaster Recovery with Data Preservation

Microsoft Azure





Microsoft

Monitoring and Management

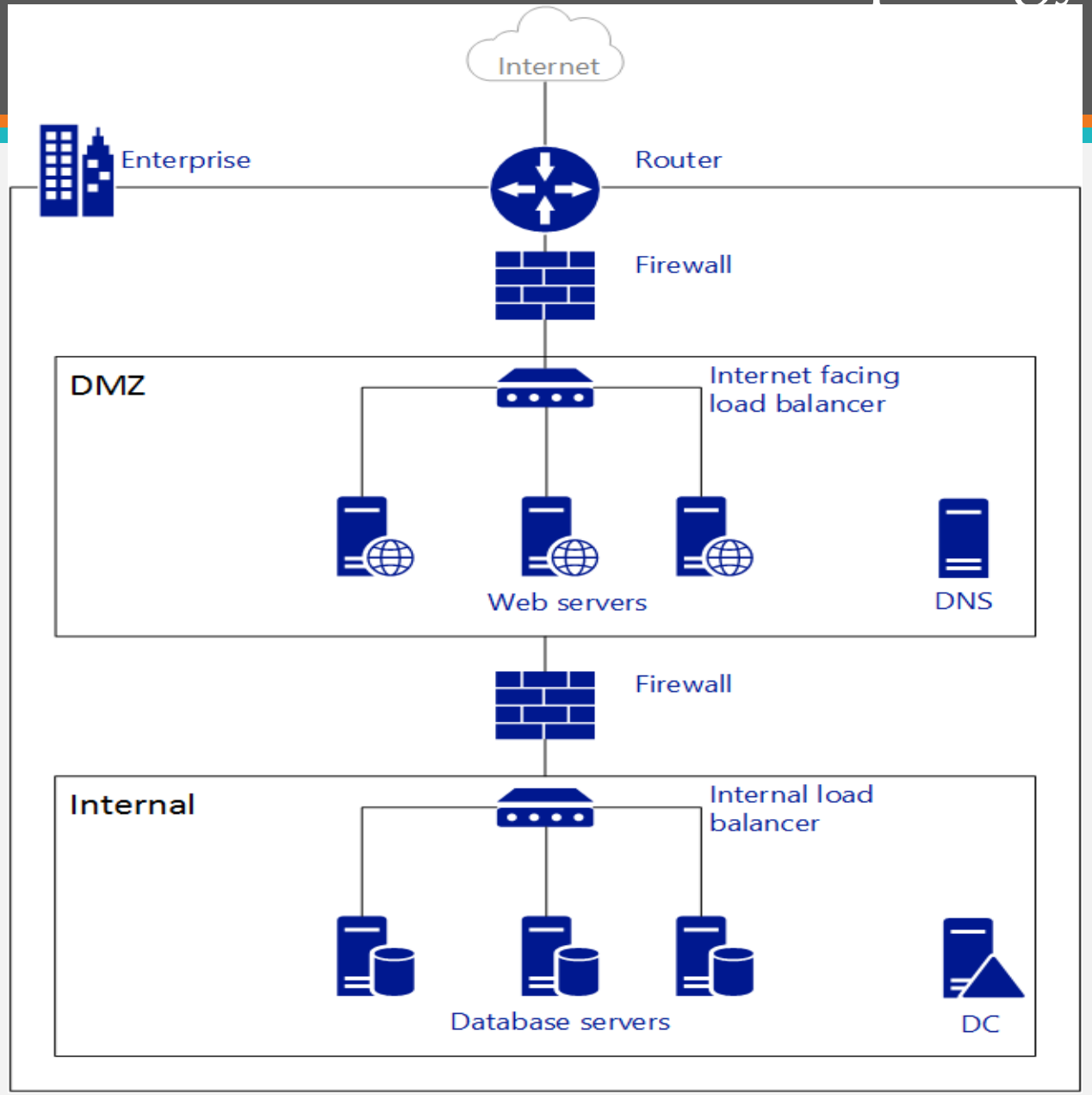
- Use Operational Management Suite to monitor the infrastructure hosted on Azure.
- Use Application insights to monitor custom developed applications hosted on Azure.
- Use Azure Resource Manager patterns to design your application management topologies.
- Use Azure resource locks to avoid accidental deletions.
- Use Automation to automate repetitive and boring tasks

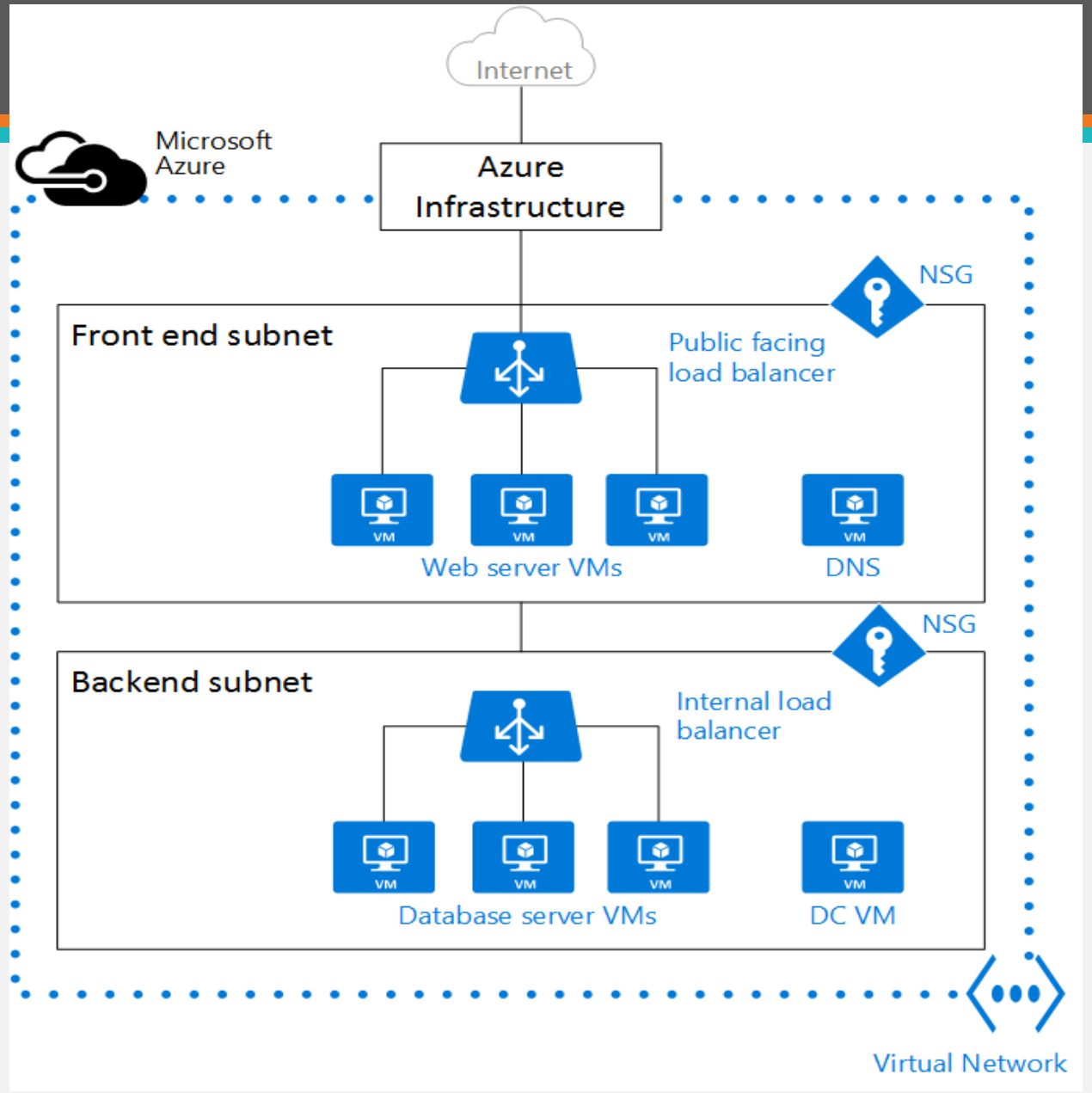
Microsoft

Scaling guidance

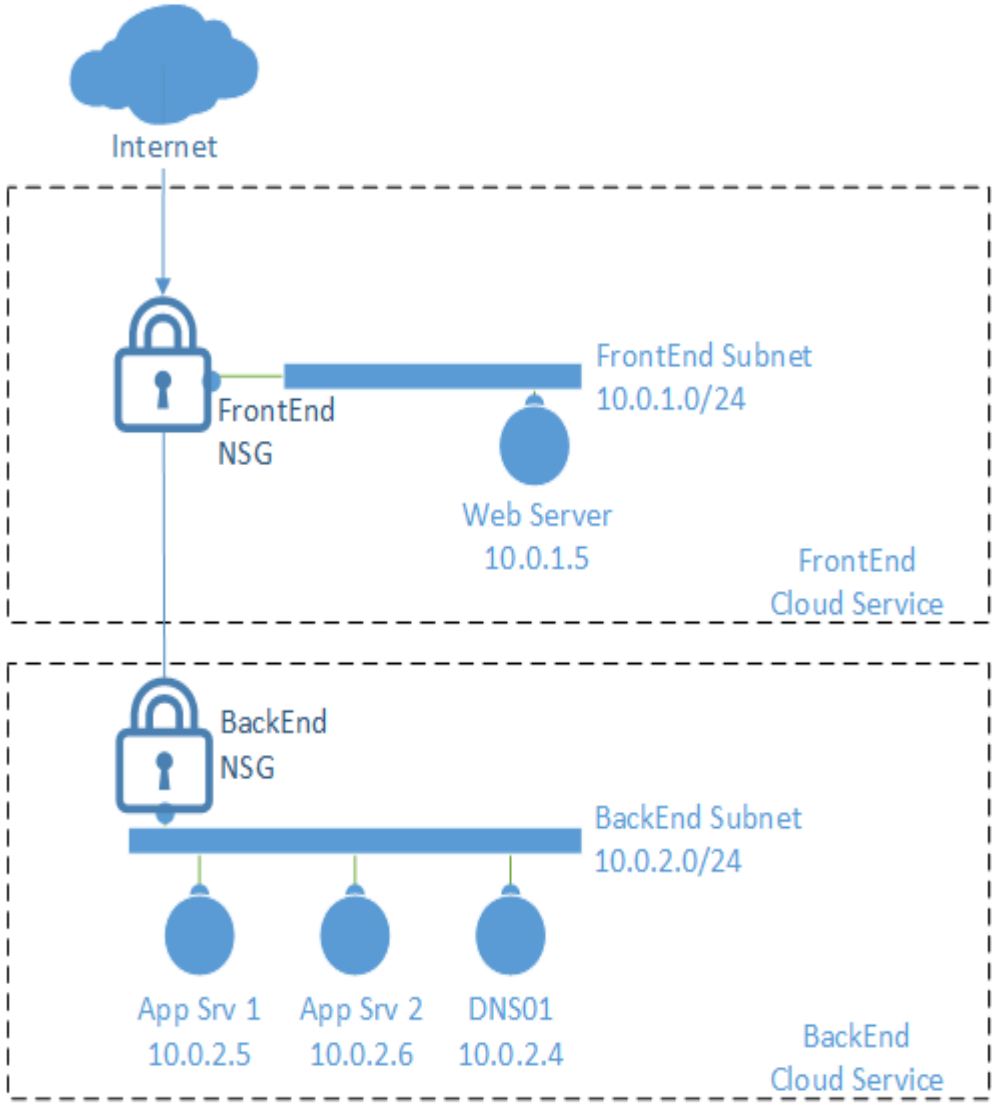
- Configure scaling based on CPU % for PaaS deployments
- Use VM Scale Sets for auto scaling IaaS deployments

On Premises vs Azure topology





DMZ with only NSG



1.Internal DNS traffic (port 53) is allowed
2.RDP traffic (port 3389) from the Internet to any VM is allowed
3.HTTP traffic (port 80) from the Internet to web server (IIS01) is allowed
4.Any traffic (all ports) from IIS01 to AppVM1 is allowed
5.Any traffic (all ports) from the Internet to the entire VNet (both subnets) is Denied
6.Any traffic (all ports) from the Frontend subnet to the Backend subnet is Denied

```
Get-AzureNetworkSecurityGroup -Name $NSGName | ` Set-
AzureNetworkSecurityRule -Name "Enable Internal DNS" ` -Type
Inbound -Priority 100 -Action Allow ` -SourceAddressPrefix
VIRTUAL_NETWORK -SourcePortRange '*' ` -
DestinationAddressPrefix $VMIP[4] ` -DestinationPortRange '53' `
-Protocol *
```

Scenarios –

1. Internet to Web server?
2. RDP to backend?
3. Internet to backend?

Microsoft

Scaling guidance

- Always design Azure VNET address range with growth perspective.
- Logically segment the subnets with access control using NSGs.
- Control routing behavior. In most cases default routes should suffice but if you are using NVA then use UDRs.
- It is good idea to enable force tunneling if cross premises connectivity exists – choose forced tunneling over split tunneling.
- Avoid exposure to internet by using Express route dedicated WAN links.
- To create sticky sessions (ex. Shopping cart), SSL offloading, content based routing use application gateway.
- Use external load balancer (SLB) whenever we have stateless applications accepting traffic from internet.
- To implement HA at DB layer use Internal load balancer.
- When an application is distributed across multiple Geo region then use Azure traffic manager load balancing technique for uptime and HA and DR.

Microsoft

Cost optimization guidance

- Use Auto shut down for Azure VM in Dev/ Test/ UAT
- Use Azure Dev Test Labs to implement capping on resource provisioning
- Use Azure Resource Groups and Role Based Access Controls to control the access to Azure resources
- For HA implementation use lower sizing/ pricing tier than expected.
- Use Azure Automation to lower the tier of PaaS services during off period.
- Enable and Use Azure Advisory tool to receive security and cost optimization tips.

Microsoft

Resources :

http://blog.e-zest.net/author/vikram-pendse

http://www.dotnetcurry.com/author/vikram-pendse

Microsoft

Thanks