AZURE CLOUD ADOPTION

The solution presented by Sergey Osherov
sergey_osherov@mail.ru

Contents

Original description of the situation

Scenario

Swift Tyres Inc. is a large manufacturer of tires. They operate several production plants, have 12 office locations and about 1000 dealers across the globe. Their mission is to build the best & longest-lasting products for every market they are operating in.

While the company is still leading when it comes to product development, many of their supporting IT systems have received little attention in the past few years. They see migrating as many of their systems to the cloud as feasible as an opportunity to modernize their infrastructure and improve the quality of their internal services.

Solution Concept

Out of the assessment of existing workload, the first wave for migration has been defined which consists of 3 applications:

- Order management system
- Customer management system
- HR management system

Existing Technical Environment

All the three applications are hosted at the company HQ in Germany but accessed by employees from all office locations.

Application

1. Order management System:
    a. deployed on 4 web application servers with 4 Cores, 32 GB RAM running on MS Windows 2016
    b. off-the-shelf software
    c. integrated with Active Directory
2. Customer management System
    a. deployed on 2 web application servers with 4 Cores, 16 GB RAM running on MS Windows 2016
    b. off-the-shelf software
3. HR management system
    a. deployed on 2 web application servers with 2 Cores, 8 GB RAM running on MS Windows 2016
    b. in-house developed software
    c. integrated with Active Directory

Database

1. Order management system and Customer management system are using shared database:
    a. SQL Server 2014 R2 Enterprise.
    b. running on single server with 64 Cores, 256 GB RAM and 2x 4 TB HDD (RAID 1)

2. HR management System

a. PostgreSQL 9.5
b. single server with 8 Cores, 32 GB RAM and 1x 8 TB HDD

Cloud Environment

IT network department has used HUB and spoke network topology. In this regard, there is a hub subscription which includes:

- vNet which is connected to on-premise through ExpressRoute;
- internal facing firewall with DMZ;
- external facing firewall with DMZ.

and a spoke subscription which you're supposed to create the infrastructure for migration of applications inside it.

Technical Requirements

- Encrypt data on the wire and at rest.
- Support multiple private connections between the production data center and cloud environment.
- All migrated VMs need to remain in their original domain and keep their original on-premise name

Executive Statement

Our competitive advantage has always been our superior manufacturing process. However, our aging IT systems are becoming a hindrance for our employees and impact the quality of the service we can offer to our customers.

Our goal is to modernize all of our IT systems and transition as many as possible to the cloud before our next hardware refresh cycle. Migrating the order management system shall serve as a proof of concept for our ability to move our infrastructure to the cloud.

Questions

You are to perform the migration of the order management system to Microsoft Azure.

1. How would you design and implement resource groups for current migration and upcoming ones?
2. How would you design and implement an RBAC model on the infrastructure level?
3. Would you recommend micro-segmentation? Why would argue for or against it?
4. How would you design and implement the traffic flow for the Order Management System based on the above?
5. What kind of approaches and methodologies would you choose and implement to cover high availability for the Order Management system?
6. How would you handle logging and monitoring of migrated workload?
7. As mentioned in the technical requirements, the VMs need to keep their original on-premise name. Since you're using Azure Migrate for replication and migration of VMs, you cannot control naming of the resources. Write a PowerShell script which can be used for renaming the migrated VMs.

Solution description

Current architecture

According to the original description, the current infrastructure and applications depicted in the Figure 1

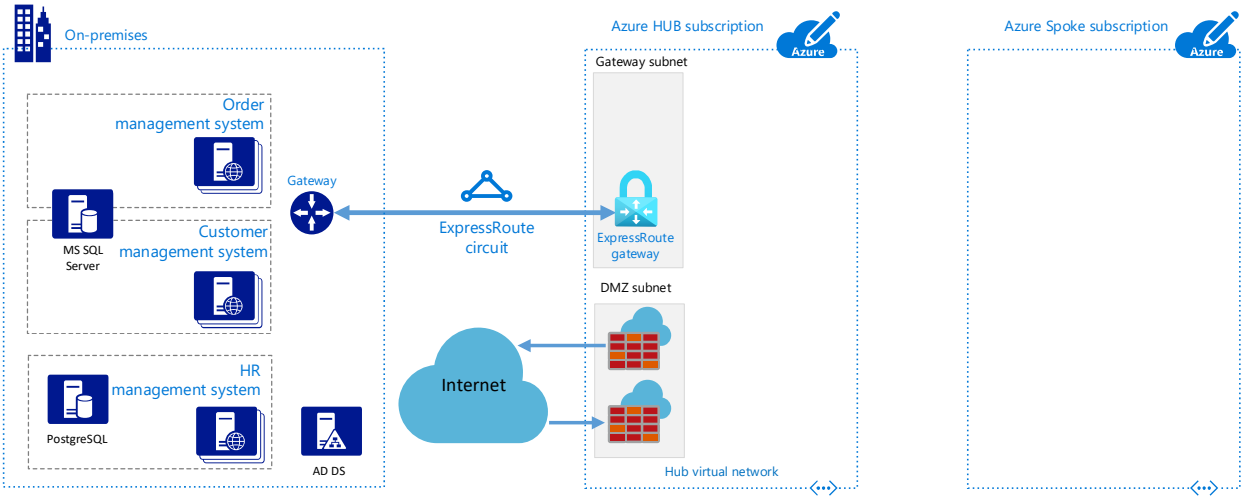

Figure 1 Current infrastructure and applications

Proposed solution

The entire solution depicted in the Figure 2

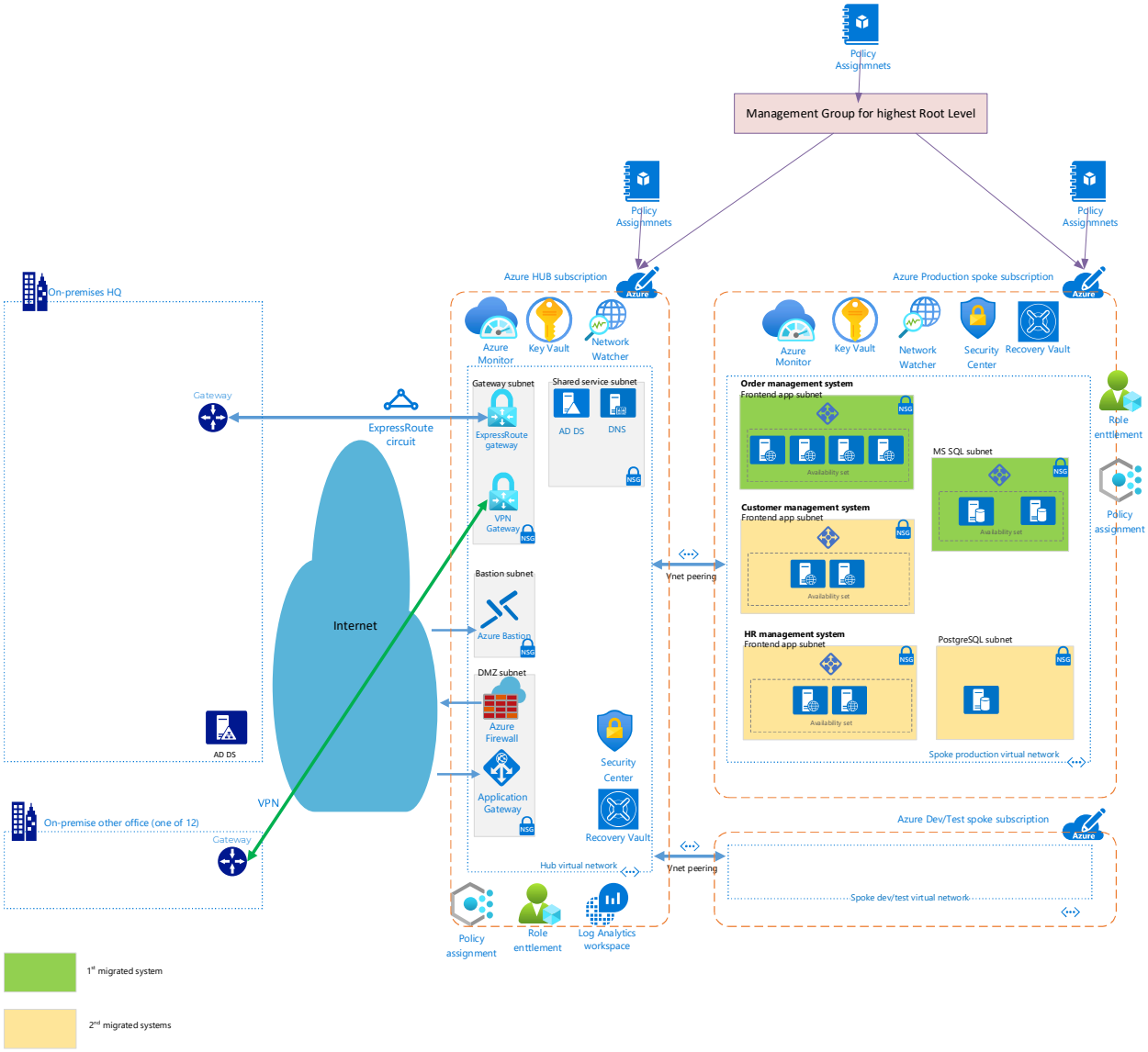

Figure 2 Proposed architecture

Satisfying the technical requirement “encrypt data on the wire and at rest”

Encrypting data on the wire

The full path of traffic consists of the following segments:

1. **On-premise source – Azure Gateway**

ExpressRoute enables private connections between cloud virtual datacenter and any on-premises networks. ExpressRoute connections don't go over the public Internet and offer higher security than typical connections over the Internet, but ExpressRoute is an extension of an on-premise wide area network, for example, using MPLS (Multi Layer Protocol Switching) which does not encrypt traffic. So, to suggest the encryption it is necessary to use additional encrypting means. There is ability to increase a security using different ways. One of them is a Site-to-Site VPN to a virtual network gateway over an ExpressRoute private peering, see Figure 3. In this case all traffic over private peering is encrypted.

For this solution we must use only zone-redundant gateways, for example, VpnGw1AZ, VpnGw2AZ, etc.

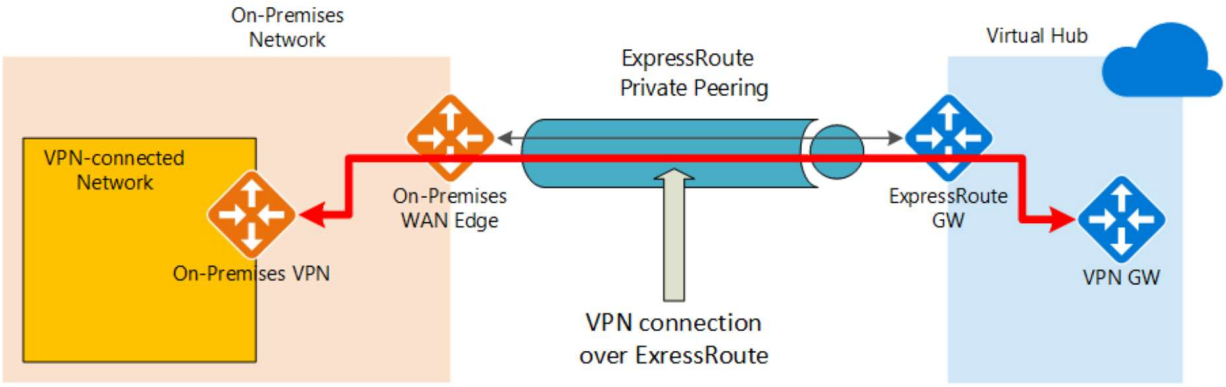

Figure 3 Site-to-Site VPN to a virtual network gateway over an ExpressRoute

2. **Virtual networks (Vnet)**

Azure virtual networks do not encrypt traffic between VMs in the same Vnet. Vnet traffic is isolated, and functions in the same way as an on-premise Vnet. For adding additional encryption, it's necessary to configure the VMs to send & receive encrypted data either based on the internal operation system means or at the applications level.

3. **Vnet – Azure services**

    a. Traffic between the Azure services and customer virtual machines

Microsoft gives customers the ability to use Transport Layer Security (TLS) protocol to protect data when it's traveling between the Azure services and customer virtual machines.

    b. Traffic to Azure Storage

Client-side encryption encrypts the data before it's sent to Azure Storage instance, so that it's encrypted as it travels across the network.

4. **Vnet peering**

Whenever Azure Customer traffic moves between datacenters-- outside physical boundaries not controlled by Microsoft (or on behalf of Microsoft)-- a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (also known as MACsec) is applied from point-to-point across the underlying network hardware. The packets are encrypted and decrypted on the devices before being sent, preventing physical "man-in-the-middle" or snooping/wiretapping attacks. Because this technology is integrated on the network hardware itself, it provides line rate encryption on the network hardware with no measurable link latency increase. This MACsec encryption is on by default for all Azure traffic traveling within a region or between regions, and no action is required on customers' part to enable.

Encrypting data at rest

Encryption at rest provides data protection for stored data (at rest).

IaaS services can enable encryption at rest in their Azure hosted virtual machines and VHDs using Azure Disk Encryption.

All managed disks, snapshots, images, and data written to existing managed disks are automatically encrypted-at-rest with platform-managed keys.

A more complete Encryption at Rest solution ensures that the data is never persisted in unencrypted form. While processing the data on a virtual machine, data can be persisted to the Windows page file or Linux swap file, a crash dump, or to an application log. To ensure this data is encrypted at rest, IaaS applications can use Azure Disk Encryption on an Azure IaaS virtual machine (Windows or Linux) and virtual disk.

Azure Disk encryption can be applied to both Linux and Windows virtual machines, as well as to virtual machine scale sets.

All Azure Storage services (Blob storage, Queue storage, Table storage, and Azure Files) support server-side encryption at rest. Some services additionally support customer-managed keys and client-side encryption.

All Azure Storage Services enable server-side encryption by default using service-managed keys, which is transparent to the application. Azure Blob storage and Azure Files also support RSA 2048-bit customer-managed keys in Azure Key Vault.
Azure Blobs, Tables, and Queues support client-side encryption. When using client-side encryption, customers encrypt the data and upload the data as an encrypted blob. Key management is done by the customer.
Data in a new storage account and managed disks is encrypted with Microsoft-managed keys by default. We can continue to rely on Microsoft-managed keys for the encryption of data, or we can manage encryption with own keys. We can specify a customer-managed key to use for encrypting and decrypting data in Blob storage and in Azure Files. Customer-managed keys must be stored in Azure Key Vault or Azure Key Vault Managed Hardware Security Model (HSM).
We can choose to manage encryption at the level of each managed disk, with own keys. Server-side encryption for managed disks with customer-managed keys offers an integrated experience with Azure Key Vault. We can either import customer RSA keys to Key Vault or generate new RSA keys in Azure Key Vault.

In our scenario, for all three systems, we consider only Windows machines.
Azure Disk Encryption for Windows virtual machines (VMs) uses the BitLocker feature of Windows to provide full disk encryption of the OS disk and data disk. Additionally, it provides encryption of the temporary disk when the VolumeType parameter is All. Azure Disk Encryption is integrated with Azure Key Vault to help control and manage the disk encryption keys and secrets.

Satisfying the technical requirement "support multiple private connections between the production data center and cloud environment"

Besides ExpressRoute gateway our solution has Azure VPN gateway that allows to connect Site-to-Site VPNs from other offices and private Point-to-Site connections from individual users.
Point-to-site users connecting to a virtual network gateway can use ExpressRoute (via the Site-to-Site tunnel) to access on-premises resources.

Satisfying the technical requirement "all migrated VMs need to remain in their original domain and keep their original on-premise name"

Previous limitations are now a thing of the past, and now we can leave all machine names in original state when using Azure Migrate. Besides, we can change the target machine name in the cloud on the step of preparation to replicate, see the in Figure 4.
Also we can use Powershell for changing properties of replicated VM based on Azure Migrate with commandlet Set-AzMigrateServerReplication. It allows to change target properties, such as name, size, resource group, NIC configuration and so on, for a replicating VM, see https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware-powershell#update-properties-of-a-replicating-vm

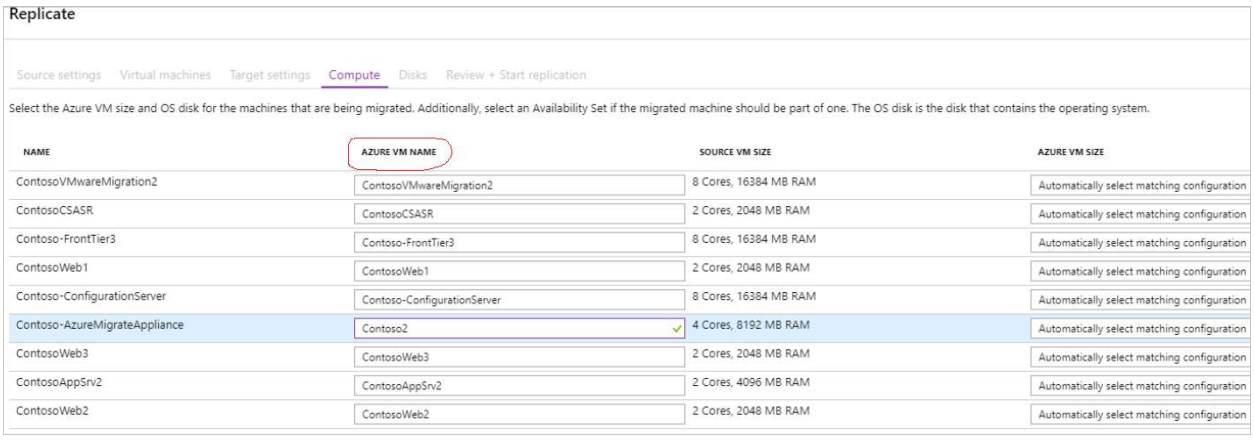

Figure 4 Checking and changing parameters of target virtual machines before replicating in Azure Migrate

Answer the questions “1” and “2” How would you design and implement resource groups for current migration and upcoming ones and how would you design and implement an RBAC model on the infrastructure level?

A resource group is simply a logical construct that groups multiple resources together so they can be managed as a single entity based on lifecycle and security. For example, resources that share a similar lifecycle, such as the resources for an application may be created or deleted as a group. In other words, everything that is born together, gets managed together, and deprecates together, goes together in a resource group.
We can use following approach for distributing resources by resources groups:

1. Are the contents of the resource group developed together?
2. Are the contents of the resource group managed, updated, and monitored together and done so by the same people or teams?
3. Are the contents of the resource group retired together?

If we answered **no** to any of the above points, the resource in question should be placed elsewhere, in another resource group.
After allocating resources to resource groups we should assign each resource group to the appropriate Azure AD user group and link it to the RBAC role.
From an identity and access perspective, we can develop own custom RBAC roles to ensure the appropriate permissions (actions/notActions) for control plane and data plane access are available for the right persona at the right scope in the Azure hierarchy, see Table 1.

Table 1 RBAC roles

Role	Usage	Actions	No actions
Azure platform owner (such as the built-in Owner role)	Management group and subscription lifecycle management	*	
Network management (NetOps)	Platform-wide global connectivity management: Virtual networks, UDRs, NSGs, NVAs, VPN, Azure ExpressRoute, and others	*/read, Microsoft.Network/vpnGateways/*, Microsoft.Network/expressRouteCircuits/*, Microsoft.Network/routeTables/write, Microsoft.Network/vpnSites/*	
Security operations (SecOps)	Security administrator role with a horizontal view across the entire Azure estate and the Azure Key Vault purge policy	*/read, */register/action, Microsoft.KeyVault/locations/deletedVaults/purge/action, Microsoft.Insights/alertRules/*, Microsoft.Authorization/policyDefinitions/*, Microsoft.Authorization/policyAssignments/*, Microsoft.Authorization/policySetDefinitions/*, Microsoft.PolicyInsights/*, Microsoft.Security/*	

Role	Usage	Actions	No actions
Subscription owner	Delegated role for subscription owner derived from subscription Owner role	*	Microsoft.Authorization/*/write, Microsoft.Network/vpnGateways/*, Microsoft.Network/expressRouteCircuits/*, Microsoft.Network/routeTables/write, Microsoft.Network/vpnSites/*
Application owners (DevOps/AppOps)	Contributor role granted for application/operations team at resource group level	*	Microsoft.Authorization/*/write, Microsoft.Network/publicIPAddresses/write, Microsoft.Network/virtualNetworks/write, Microsoft.KeyVault/locations/deletedVaults/purge/action

Including users could be done manually to the Azur AD groups that we will create for each of the roles above and make appropriate Subscription Owner/Requester an owner of the group before creating entitlements for those groups. We can facilitate and structure creating entitlements, if we use Azure AD PIM. Those who require access to Azure Resources will be able to search for the Azure AD group by name and leverage the Azure AD Self-service group management capability to join a group. Group Owners can determine whether to approve or deny a user request based on eligibility criteria. The whole mapping of Resources, Resources groups, Azure AD user groups and RBAC roles is presented in Table 2.
We can note that we link not only resource groups with Azure AD groups and roles but also Management Groups for managing appropriated Azure policies.

Table 2 Resources, Resources groups, Azure AD user groups and RBAC roles

Management Group	Subscription	Resource	Resource Group	Azure AD Group Name	Role (RBAC)
Management Group for highest Root Level				Platform Owner	Azure platform owner (such as the built-in Owner role)
Management Group for identity properties				SecOps	Security operations (SecOps)
Management Group for connectivity properties				NetOps	Network management (NetOps)
	HUB			Owner HUB	Subscription owner
	Production spoke 1			Owner Production spoke 1	Subscription owner
	HUB	Expressroute Gateway	rg-Hub-Gateway	NetOps	Network management (NetOps)
	HUB	ExpressRoute Circuit			
	HUB	VPN Gateway			
	HUB	Azure Bastion	rg-Hub-Bastion	NetOps	Network management (NetOps)
	HUB	Azure Firewall	rg-Hub-DMZ	NetOps	Network management (NetOps)
	HUB	Application Gateway			
	HUB	Azure Firewall Policy	rg-Hub-Firewall-Policies	NetOps	Network management (NetOps)

Management Group	Subscription	Resource	Resource Group	Azure AD Group Name	Role (RBAC)
	HUB	VMs (AD domain controllers)	rg-Hub-ADDC	SecOps	Security operations (SecOps)
	HUB	Network Watcher	rg-Hub-Network	NetOps	Network management (NetOps)
	HUB	NSGs			
	HUB	Vnet			
	HUB	Route-Table			
	HUB	Log Analytics workspace	rg-Hub-Management	DevOps HUB	Application operations (DevOps/AppOps)
	HUB	Scheduled Log Analytics Query			
	HUB	ActionGroup			
	HUB	Key Vault			
	HUB	Automation account			
	HUB	Azure Vault	rg-Hub-Backup	DevOps HUB	Application operations (DevOps/AppOps)
	Production spoke 1	Azure Bastion	rg-Spoke1-Bastion	NetOps	Network management (NetOps)
	Production spoke 1	Network Watcher	rg-Spoke1-Network	NetOps	Network management (NetOps)
	Production spoke 1	NSGs			
	Production spoke 1	Vnet			
	Production spoke 1	Route-Table			
	Production spoke 1	Load Balancers			
	Production spoke 1	Order Management System Frontend App VMs	rg-Spoke1-Order-Mgmt-Frontend	AppOps Order Management System	Application operations (DevOps/AppOps)
	Production spoke 1	VMs MSSQL	rg-Spoke1-MSSQL	AppOps DB	Application operations (DevOps/AppOps)
	Production spoke 1	Customer Management System Frontend App VMs	rg-Spoke1-Customer-Mgmt-Frontend	AppOps Customer Management System	Application operations (DevOps/AppOps)
	Production spoke 1	HR Management System Frontend App VMs	rg-Spoke1-HR-Mgmt-Frontend	AppOps HR Management System	Application operations (DevOps/AppOps)
	Production spoke 1	HR Management System PostgreSQL VM	rg-Spoke1-HR-Mgmt-PostgreSQL	AppOps DB	Application operations (DevOps/AppOps)
	Production spoke 1	Azure Vault	rg-Spoke1-Backup	AppOps HR Management System	Application operations (DevOps/AppOps)
				AppOps HR Management System	Application operations (DevOps/AppOps)
				AppOps HR Management System	Application operations (DevOps/AppOps)
				AppOps DB	Application operations (DevOps/AppOps)

Answer the question "3" Would you recommend micro-segmentation? Why would argue for or against it?

Segmentation is a fundamental information security principle that has been applied to data center design for a long time. Although segmentation does exist in data centers today, the network segments

are much too large to be effective and are typically created to restrict north–south traffic between the Internet and the data center or between client workstations and the data center, see Figure 5. The primary focus is on controlling north–south traffic in and out of the data center, rather than the east–west traffic within the data center upon which modern attacks are predicated. Internet edge traffic (sometimes referred to as “North-South” traffic) represents network connectivity between our assets in the cloud and the Internet.

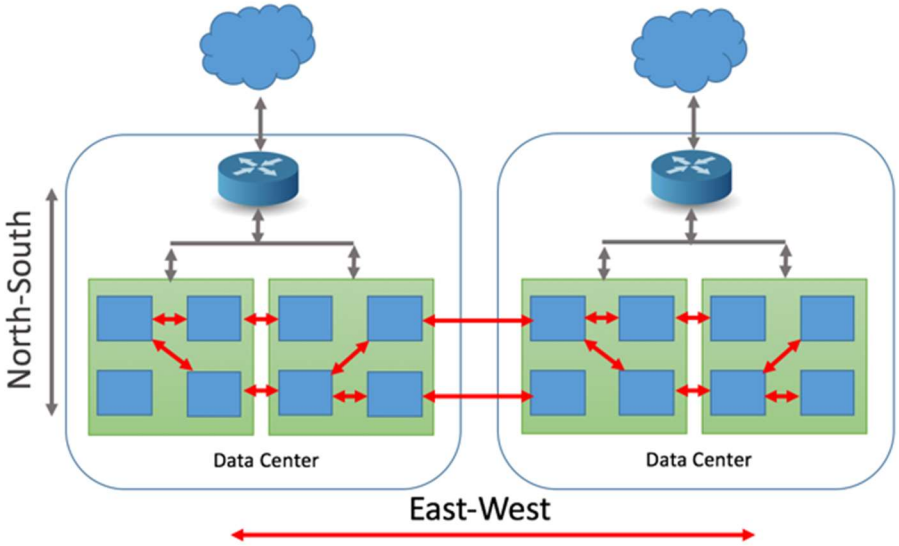

Figure 5 General representation about directions of traffic in datacenter

Legacy workloads require protection from Internet endpoints because they were built with the assumption that an internet firewall protected them against these attacks. An Internet edge strategy is intended to mitigate as many attacks from the internet as is reasonable to detect or block.
To effectively protect data centers from modern attacks, micro-segmentation down to the individual workload is needed.

Pros of Micro-Segmentation

- An advantage of this Micro-Segmentation is that if a part of application stack is compromised, we will be able to better contain the impact of this security breach and prevent it from laterally spreading through the rest of network.
- Each segment has its own ingress and egress controls to minimize the "blast radius" of unauthorized access to data. By implementing software-defined perimeters with granular controls, we increase the difficulty for unauthorized actors to propagate throughout network, and so reduce the lateral movement of threats.
- Micro-segmentation’s ability to define the scope and prevent lateral movement helps companies meets an array of compliance standards. It simplifies mandatory compliance regulations, whether it’s PCI-DSS (including the expected release of PCI-DSS 4.0 in the coming months), HIPAA, or region-specific requirements like GDPR.
- A micro-segmentation solution enables easy environment separation for modern data centers. Instead of using IP addresses and VLAN memberships, it segments the network by tagging resources hosting workloads or applications. This makes environment separation adapt to dynamic application environments, providing unparalleled operational ease and security. With micro-segmentation, we get the advantages of reusable server role, environment and application tags, reusable security policy templates, platform-agnostic separation, automatic audit trail for every action, and a zero-trust network with full visibility and control.
- Applied to Azure we can use costless Networks Security Groups between any number of subnets and network interfaces which make additional barriers between compromised segments without increasing the load in the central firewall.

- Applied to Azure we can use Application Security Groups to define fine-grained network security policies based on workloads, centralized on applications, instead of explicit IP addresses. ASGs introduce the ability to deploy multiple applications within the same subnet, and isolate traffic based on ASGs. With ASGs we can reduce the number of NSGs in a subscription.

Cons of Micro-Segmentation

- Deploying hundreds (or even thousands) of appliance-based firewalls inside the data center to protect each individual workload is financially and operationally infeasible.
- If instead of micro-segmentation create macro-segmentation, the attack surface increases. In practical terms, deployment of network-based micro-segmentation is not very granular because it is extremely difficult to map business segmentation needs to networking constructs.
- At scale, network-based micro-segmentation is very expensive and disruptive. It requires teams to upgrade all of their infrastructure and reconfigure their networking. The project could take months and even years, and companies will typically need a dedicated staff for maintenance.

Answer the question "4" How would you design and implement the traffic flow for the Order Management System based on the above?

The traffic flow for the Order Management System of different kind of users is depicted in the Figure 6. We can see that for internal users traffic goes through an encrypted channel IPSec over ExpressRoute. Then it gets into the "Gateway subnet" of "Hub virtual network" where it has to go through this subnet network security group. Next, it goes to the peered "spoke production virtual network" and gets into the "Fronted app subnet" of Order Management System. Here, it has to go through assigned subnet network security group. Going through local load balancer traffic gets into the one of the frontend application servers. Then the server initiates a new connection to the MS SQL server, that is located in the "MS SQL subnet", again going through the network security group that restricts connection only from the "Fronted app subnet" sources. Thus, we can see that micro-segmentation approach allows to define several restrictions for lateral traffic using a lot of network security groups.
Similar traffic is from the external users that are located somewhere in the Internet. The path of traffic does not match at the initial stage when gets in to the point of distribution based on the Azure Application Gateway.

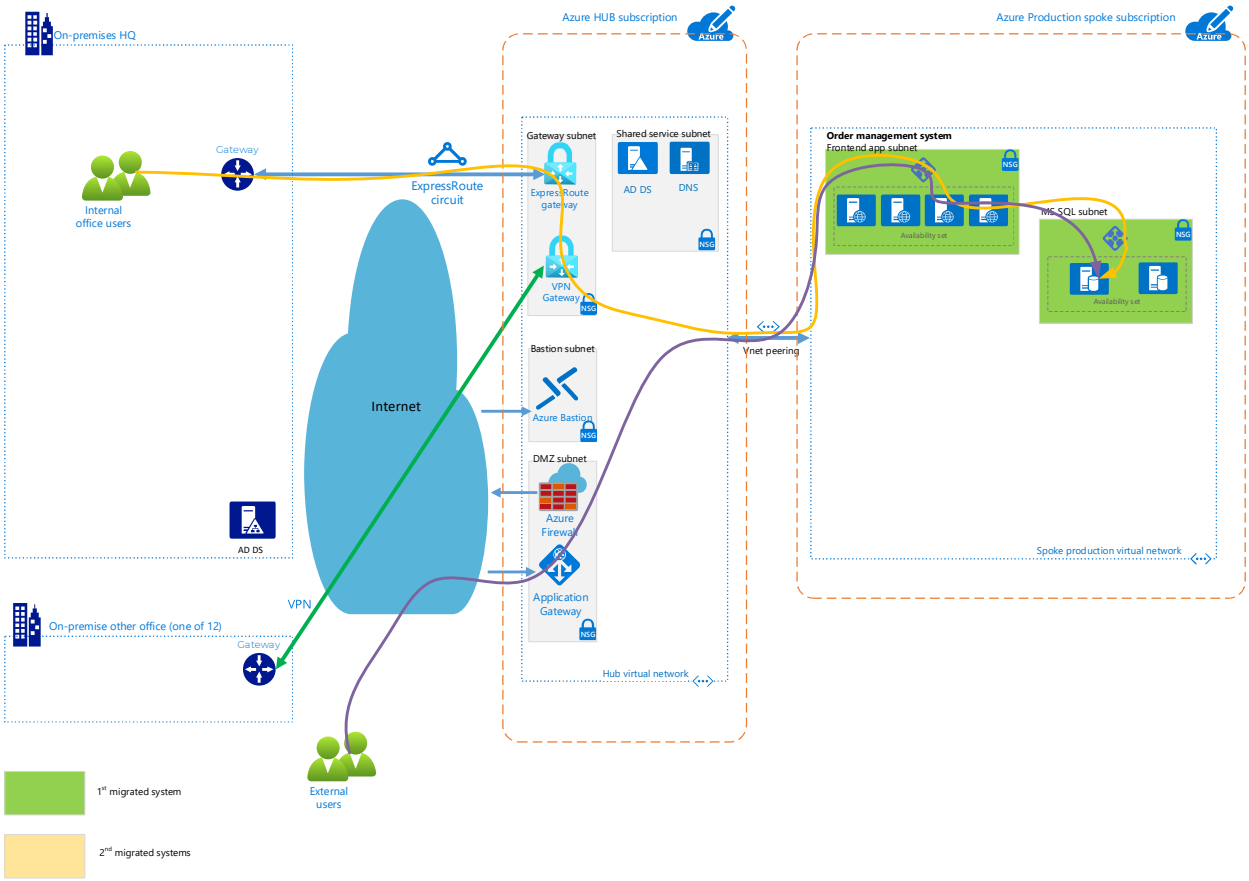

Figure 6 The traffic flow for the Order Management System

Answer the question "5" What kind of approaches and methodologies would you choose and implement to cover high availability for the Order Management system?

We don't consider the network connections between internal users and components of the Order Management system, because all networks connections are duplicated, and focus should be on the application tiers. The fronted tier has already included high availability solution with distributed fronted servers and balancer on the front of them. The main question is suggesting high availability for database.

For high availability of MS SQL database, we can use different approaches:

- The first kind of them based on the features of MS SQL Server;
- Another way is using Azure SQL DB.

On the first way the application database will be migrated to an Azure SQL Server VM. It will be placed in a Windows Server failover cluster with two nodes that uses SQL Server Always On availability groups. VMs will run Windows Server 2016 with SQL Server 2014R2 Enterprise edition. If customer doesn't have licenses for this operating system, it can use an image in Azure Marketplace that provides the license as a charge to the company's Azure Enterprise Agreement commitment.

For this way the customer has to deploy an internal load balancer that listens for traffic on the cluster and directs it to the appropriate cluster node.

Another way based on using Azure SQL DB, allows to use internal high availability of Azure PaaS. In this case the main step is to do right assessment before the migration. We must assess the compatibility of current database on-premise solution with Azure SQL DB. This assessment can be done using Azure Database Migration Assistant. After the assessment we can migrate databases using the Azure Database Migration Service.

Answer the question "6" How would you handle logging and monitoring of migrated workload?

We can implement platform logging, security and networking using Azure native services such as Log Analytics, Monitor, Security Center, Sentinel, and Network Watcher. All core management infrastructure will exist inside the "Hub Subscription" and will be deployed and governed by Azure Policy; the requisite configuration for workloads and Subscriptions will be driven through Azure policy as new Subscriptions and Resources are being created.

We can use a single Log Analytics workspace within one region for centralized platform management which will also act as the hub for all security and networking data across our Azure platform. With this design and implementation, we will achieve:

- A single, central, and horizontal view of the platform across security, auditing, and networking, all enforced by Azure Policy;
    - Consume security data centrally from all Subscriptions;
    - Consume networking data centrally from all regions and Subscriptions where networks are deployed;
- Granular data retention per data table in Log Analytics;
- Resource centric and granular RBAC for application teams to access their monitoring data;
- At scale emergency VM patching as well as granular VM patching for application teams per RBAC;
- Centralized alerting from a platform perspective;
- Centralized, interactive Azure dashboards through the lenses of networking, security, and overall platform health.

The following policies related to management and monitoring will be assigned:

Policy	Intent	Assignment scope	Result
Enforce Log Analytics for platform logging	Ensure infrastructure for logging and security is in place for the Azure platform	HUB Subscription	Deploys and configures Log Analytics
Enforce Activity Logs	Enable and configure activity logs on every Subscription	Management Group for highest Root Level	Ensures Activity Log from all Subscriptions are collected centrally
Enforce VM logging	Ensure all virtual machines are connected to Log Analytics	Management Group for highest Root Level	Every virtual machine deployed will have the Log Analytics VM extension installed and be connected to a Log Analytics workspace
Enforce Network Watcher	Deploy Network Watcher on all Subscriptions with virtual network	Management Group for highest Root Level	Every Subscription with virtual networks will have associated network watchers deployed per region
Enforce diagnostics/metrics to platform workspace	Ensure supported Resources will ingest telemetry to Log Analytics	Management Group for highest Root Level	All platform related telemetry is routed to central Log Analytics workspace
• NSG			
• Public IP			
• NIC			
• Recovery Vaults			
• KeyVault			
• Azure Firewall			
• Express Route			
• DNS			
• App Gateway			

Answer the question "7" As mentioned in the technical requirements, the VMs need to keep their original on-premise name. Since you're using Azure Migrate for replication and migration of VMs, you cannot control naming of the resources. Write a PowerShell script which can be used for renaming the migrated VMs.

You can see the script on my GitHub repository https://github.com/stenastena/AzureOps2

Also, the script and table of source virtual machines for renaming can be viewed in the Code 1 and Code 2.

Code 1 The PowerShell script for VMs renaming

```
Connect-AzAccount
Select-AzSubscription -SubscriptionID YYYYYYYYYYYYYYYYYYYYYYYYYYYY
$rgName = 'rgVmMigrated' # Resource Group Name

#Import VMs for renaming
$VMList = Import-Csv -Path .\VMs.csv

#There is no way to directly rename a VM in Azure.
#We have to split the current VM into its components.
#After that, we create a new VM and connect the old parts to it.
function Set-VmNewName ($rgName, $vmOldName,$newVMName, $KindOfOS)
{
    # $KindOfOS have to be Windows or Linux
    try
    {
    # Save VM properties

    $oldVM = Get-AzVM -ResourceGroupName $rgName -Name $vmOldName -
ErrorAction Stop

    # Delete the Old VM
    Remove-AzVM -ResourceGroupName $oldVM.ResourceGroupName -Name $oldVM.Name -
Force -ErrorAction Stop

    # Initiate a new virtual machine configuration
    $newVM = New-AzVMConfig -VMName $newVMName -
VMSize $oldVM.HardwareProfile.VmSize -Tags $oldVM.Tags -ErrorAction Stop

    # Attach the OS Disk of the old VM to the new VM
    if ($KindOfOS -eq 'Windows') {
        Set-AzVMOSDisk -VM $newVM -CreateOption Attach -
ManagedDiskId $oldVM.StorageProfile.OsDisk.ManagedDisk.Id -
Name $oldVM.StorageProfile.OsDisk.Name -Windows -ErrorAction Stop
    }
    else {
        Set-AzVMOSDisk -VM $newVM -CreateOption Attach -
ManagedDiskId $oldVM.StorageProfile.OsDisk.ManagedDisk.Id -
Name $oldVM.StorageProfile.OsDisk.Name -Linux -ErrorAction Stop
    }

    # Attach all NICs of the old VM to the new VM
```

```
    $oldVM.NetworkProfile.NetworkInterfaces | ForEach-Object {Add-
AzVMNetworkInterface -VM $newVM -Id $_.Id} -ErrorAction Stop

    # Attach all Data Disks (if any) of the old VM to the new VM
    $oldVM.StorageProfile.DataDisks | ForEach-Object {Add-AzVMDataDisk -
VM $newVM -Name $_.Name -ManagedDiskId $_.ManagedDisk.Id -Caching $_.Caching -
Lun $_.Lun -DiskSizeInGB $_.DiskSizeGB -CreateOption Attach} -ErrorAction Stop

    # Create the new virtual machine
    New-AzVM -ResourceGroupName $rgName -Location $oldVM.Location -VM $newVM -
ErrorAction Stop
    }

    catch
    {
        Write-Host "Something wrong." -ForegroundColor Blue
        Write-
Host "Probably the source VM '$vmOldName' doesn't exist or connection between you
r PC and Azure was lost." -ForegroundColor Blue
        Write-Host "The process of renaming continues to work..." -
ForegroundColor Blue
    }

    #Check the existence and parameters of the new VM
    #Get-AzVM -ResourceGroupName $rgName -VMName $newVMName
}

foreach ($VM in $VMList)
{
    try
    {
        Set-VmNewName -rgName $rgName -vmOldName $VM.OldName -
newVMName $VM.NewName -KindOfOS $VM.OS -ErrorAction Stop
    }
    catch
    {

    }
}

Write-Output "There are next VMs:"
Get-AzVM -ResourceGroupName $rgName | Format-Table -AutoSize
```

Code 2 The virtual machines for renaming

```
"OldName",          "NewName",          "OS"
"VmWin1",           "VmNewWin1",        "Windows"
"VmLin0",           "VmNewLin0",        "Linux"
"VmLin1",           "VmNewLin1",        "Linux"
"VmWin1",           "VmNewWin2",        "Windows"
```