Report: Moving to Azure



STEP 0: Problem Background

Contoso is an online cloth merchandise company specializing in selling activewear. They have a rented space in a local data center. They have one system administrator who makes sure all servers are working properly 24x7. Their hardware is getting old and they must decide on whether they need to spend $22,000 for new hardware or move their business to the Azure cloud services. The following list represents their current on-premises infrastructure:

| Server 1: | **Purpose:** WordPress web server  **CPU:** 8 Cores and 60% average utilization  **RAM:** 16 GB and 87% average utilization  **HDD OS:** 500 GB capacity with 57 GB used  **Web URL:** Contoso.com  **IP # Public:** 200.200.100.50  **IP #:** 10.10.1.11  **Firewall:** Inbound TCP 2222-2224, 80, 443  **Usage:** This is Contoso’s only web server. It runs WordPress and eCommerce services. Their on-line store is always open, and they receive orders 24x7  This server uses ports 80 and 443 for HTTP and HTTPS traffic |
| --- | --- |
| Server 2 & 3: | **Purpose:** Microsoft SQL 2019  **CPU:** 8 Cores and 30% average utilization x2  **RAM:** 16 GB and 87% average utilization x2  **HDD OS:** 500 GB capacity with 240 GB used x2  **HDD Data:** 2 TB SAN (Storage Area Network drive)  **IP #:** 10.10.1.12 and 10.10.1.13  **SQL Cluster:** SQLCluster.Contoso.Com  **IP #:** 10.10.1.14  **Firewall:** Inbound TCP 2222-2224, 1433  **Usage:** These two servers are running Microsoft SQL cluster services. SQL Always-On service is fully configured as Active-Passive nodes. The 2 servers use an external attached SAN drive for all data storage such as product descriptions, transaction logs, and clients lists. Annual data growth is negligible.  These servers use the standard SQL inbound TCP port 1433 |
| Server 4: | **Purpose:** ABC Backup and Restore server  **CPU:** 8 Cores and 30% average utilization  **RAM:** 16 GB and 87% average utilization  **HDD OS:** 500 GB capacity with 164 GB used  **HDD Backup:** 40 TB  **IP #:** 10.10.1.15  **Firewall:** Inbound TCP 2222  **Usage:** The ABS backup software runs daily at 8pm. It stores the last 18 months of all the SQL data drive contents onto a local D: drive (HDD Backup) with 40 TB capacity. |
| Server 5: | **Purpose:** XYZ Antivirus server  **CPU:** 8 Cores and 30% average utilization  **RAM:** 16 GB and 87% average utilization  **HDD:** 500 GB capacity with 43 GB used  **IP #:** 10.10.1.16  **Firewall:** Inbound TCP 2222-2224  This server uses ports TCP 2222-2224 for the antivirus client  **Usage:** The XYZ anti-virus services are essential for the security of Contoso’s operations security. The server is always on and constantly running. It monitors all Contoso’s servers and mitigates against viruses and hack attacks. Data grown is negligible. |

STEP 1: Assessing the On-Premises Environment

Purpose: To identify the Azure services needed to ensure Contoso’s business continuity in the cloud.

| **Current Environment**  Make a list of all current on-premises servers and services. | **1. Server 1: WordPress Web Server**  Purpose: Hosts WordPress and eCommerce services for Contoso's website.  Specifications:  CPU: 8 Cores, 60% average utilization.  RAM: 16 GB, 87% average utilization.  Storage: 500 GB HDD OS (57 GB used).  Network:  Public IP: 200.200.100.50  Private IP: 10.10.1.11  Firewall Ports: TCP 2222-2224 (management), 80 (HTTP), 443 (HTTPS).  **2. Servers 2 & 3: Microsoft SQL 2019 Servers**  Purpose: Operate as a SQL Always-On cluster for database services.  Specifications:  CPU: 8 Cores each, 30% average utilization.  RAM: 16 GB each, 87% average utilization.  Storage: 500 GB HDD OS (240 GB used each), 2 TB SAN (shared data).  Network:  Private IPs: 10.10.1.12 and 10.10.1.13  Cluster IP: 10.10.1.14 (SQL Cluster)  Firewall Ports: TCP 2222-2224 (management), 1433 (SQL traffic).  **3. Server 4: ABC Backup and Restore Server**  Purpose: Manages backup and restore operations for SQL data.  Specifications:  CPU: 8 Cores, 30% average utilization.  RAM: 16 GB, 87% average utilization.  Storage: 500 GB HDD OS (164 GB used), 40 TB HDD Backup.  Network:  Private IP: 10.10.1.15  Firewall Ports: TCP 2222 (management).  **4. Server 5: XYZ Antivirus Server**  Purpose: Provides antivirus and security monitoring for all servers.  Specifications:  CPU: 8 Cores, 30% average utilization.  RAM: 16 GB, 87% average utilization.  Storage: 500 GB HDD (43 GB used).  Network:  Private IP: 10.10.1.16  Firewall Ports: TCP 2222-2224 (antivirus client communication). |
| --- | --- |
| **Matching Azure Services** Match the list of on-premises servers and services to the corresponding Azure ones. | **1. WordPress Web Server**  Azure Equivalent: Azure Virtual Machine (VM) - B4ms  Justification:  B4ms offers 4 vCPUs and 16 GB RAM, suitable for general-purpose workloads like web hosting. The current server's CPU utilization suggests that a slightly lower core count might be efficient in Azure, leveraging cloud elasticity for scaling as needed.  Consider using Azure App Service for a fully managed platform if the primary requirement is web hosting without extensive VM management.  Additional Services:  Azure Front Door or Azure CDN for global load balancing and content delivery to enhance web performance.  Azure SQL Database for database hosting if WordPress is using an external SQL database.  **2. Microsoft SQL Servers**  Azure Equivalent: Azure Virtual Machine (VM) - D4s\_v3 or Azure SQL Managed Instance  Justification:  D4s\_v3 provides 4 vCPUs and 16 GB RAM per VM, suitable for SQL workloads with moderate CPU utilization.  Using Azure SQL Managed Instance or Azure SQL Database can reduce management overhead and offer built-in high availability.  Additional Services:  Azure Backup for database backups.  Azure Site Recovery for disaster recovery.  **3. ABC Backup and Restore Server**  Azure Equivalent: Azure Blob Storage for backups, Azure Backup Service  Justification:  Azure Blob Storage provides scalable storage options for backups, with redundancy and geo-replication options.  Azure Backup Service automates backup processes and supports long-term retention.  Additional Services:  Azure Automation for scheduling and managing backup jobs.  **4. XYZ Antivirus Server**  Azure Equivalent: Azure Security Center  Justification:  Azure Security Center provides threat protection and security management across Azure resources.  Azure Sentinel for advanced security analytics and threat intelligence.  Additional Services:  Azure Firewall or NSG to manage traffic and protect resources from threats. |
| **Discussion Question #1** A - How can you verify the running programs and services on each of your on-premises servers? List the steps taken to identify the services running for each server.  B - List your migration plans. | **Windows Servers:**  **Task Manager:**  Press Ctrl + Shift + Esc to open Task Manager.  Go to the Services tab to view running services.  Switch to the Processes tab to see active applications and their resource usage.  **PowerShell:**  Use Get-Service to list all running services: Get-Service | Where-Object {$\_.Status -eq "Running"}  Check active processes with: Get-Process  Server Manager:  Open Server Manager from the Start menu.  Navigate to Manage > Add Roles and Features to view installed roles and features.  **Linux Servers:**  **Command Line:**  Use ps -aux to list all running processes.  Check services with systemctl list-units --type=service --state=running.  Monitoring Tools:  Use tools like top or htop for a detailed view of processes and resource usage.  **B. Migration Plans**  **Assessment Phase:**  Evaluate each server's workload and performance metrics.  Identify dependencies and network configurations that need to be replicated in Azure.  **Planning Phase:**  Choose appropriate Azure services and VM sizes based on current and anticipated workloads.  Plan for high availability and disaster recovery to maintain business continuity.  **Execution Phase:**  Migrate workloads in phases, starting with non-critical systems to validate the process.  Use Azure Migrate or Azure Site Recovery to facilitate the migration.  **Validation Phase:**  Test each migrated system to ensure it meets performance and functionality requirements.  Verify security configurations and backups.  **Optimization Phase:**  Monitor resource usage and optimize costs.  Implement autoscaling and other cloud-native features to enhance efficiency. |
| **Discussion Question #2** On your on-premises servers:  A - How can you find the listing of all windows firewall port exceptions?  B - Do these firewall port exceptions have to match the NSG firewall exceptions? Please explain. | **A. Finding Windows Firewall Port Exceptions**  To find the listing of all Windows Firewall port exceptions:  **Windows Firewall with Advanced Security:**  Open the Windows Firewall application from the Control Panel or search for it in the Start menu.  Click on Inbound Rules to view all incoming port exceptions.  Click on Outbound Rules for outgoing port exceptions.  Each rule shows the allowed port and protocol.  **Command Line:**  Use netsh advfirewall firewall show rule name=all to list all firewall rules and exceptions.  Filter rules by specific ports with: netsh advfirewall firewall show rule name=all | findstr "2222".  **B. Matching Firewall Exceptions to NSG Rules**  **NSG Configuration:**  NSG rules in Azure act similarly to on-premises firewall rules, controlling inbound and outbound traffic to VMs.  Each NSG has a set of security rules that define allowed or denied traffic based on source IP, destination IP, port, and protocol.  **Comparison:**  Direct Mapping: NSG rules should directly map to necessary firewall exceptions to ensure the same level of access and security.  Network Segmentation: Azure allows more granular control and may provide additional options for network segmentation and security that were not available on-premises.  Security Best Practices: It’s essential to review and possibly tighten security during migration. Not all on-premises exceptions may be required in the cloud, and Azure offers additional security features like Azure Firewall and DDOS protection. |
| **Optional Discussion** Looking at the new Azure server farm, what will you change and why? | **Changes in Azure Server Farm:**  **Scalability and Elasticity:**  Implement auto-scaling for web and database servers to handle varying loads dynamically.  Use Azure’s elasticity to reduce costs during low-usage periods.  **Enhanced Security:**  Leverage Azure’s advanced security features, such as Azure Sentinel for threat detection and response.  Implement Azure Policy to enforce governance and compliance automatically.  **High Availability and Resilience:**  Use Azure Availability Zones for critical servers to protect against data center failures.  Consider multi-region deployments for disaster recovery and global reach. |

STEP 2: Cost Estimates

Purpose: To provide the CIO with a monthly cost estimate after the migration to Azure.

Use Azure Pricing Calculator to provide the CIO with a monthly cost estimate, including:

* The number of VMs needed
* The RAM and CPU needed for each VM
* The amount of storage needed
* Any Azure services such as anti-virus, back-up, database, etc.
* Build a list/table that includes VM type (you may use the template below or create your own)

Build / fill out the table providing your current server farm and its corresponding Azure farm. List the potential Azure replacement for each of the on-premises servers, the VM type and monthly cost. Assume your company has Hybrid benefits and are willing to commit to 3-year agreements. Use the East US Azure zone. Show the cost of all servers with a three year commitment after applying Azure Reservations cost reduction. Compare the VMs prices with and without Azure Reservations.

#### Summary Table

| **Server Name** | **CPU Cores** | **RAM (GB)** | **VM Type** | **Storage (GB)** | **Monthly Cost (No Reservation)** | **Monthly Cost (3-Year Reservation)** |
| --- | --- | --- | --- | --- | --- | --- |
| **WordPress Web Server** | 4 | 16 | B4ms | 128 SSD | $146.00 | $97.80 |
| **SQL Server 1** | 4 | 16 | D4s\_v3 | 128 SSD + 2 TB SSD | $467.66 | $416.46 |
| **SQL Server 2** | 4 | 16 | D4s\_v3 | 128 SSD + 2 TB SSD | $467.66 | $416.46 |
| **Backup Server** | 4 | 16 | D4s\_v3 | 128 SSD + 40 TB | $928.00 | $876.80 |
| **Antivirus Server** | 2 | 4 | B2s | 128 SSD | $36.43 | $24.29 |
| **Total Monthly Cost** |  |  |  |  | **$2,045.75** | **$1,831.81** |

| **Discussion Question #1** Will these 4 Azure servers provide HA/DR for Contoso? Will their site be available 24x7, 365 days? | **High Availability:**  Web Server: Utilizing Azure Availability Sets or Availability Zones ensures that the WordPress web server is resilient to data center failures. By adding an additional replica of the WordPress server, load can be balanced and availability can be enhanced.  SQL Servers: The SQL servers can be configured in an Always-On Availability Group in Azure, similar to their on-premises setup, ensuring continuous data availability and automatic failover.  **Disaster Recovery:**  Backup: Using Azure Backup and Site Recovery, we can protect data and applications. Regular snapshots and geo-redundant storage options enhance data durability and recovery capabilities.  Antivirus and Management Servers: While these do not directly contribute to HA/DR, ensuring their availability is crucial for security and operational continuity.  **Continuous Availability:**  Design Considerations: With proper configurations, the proposed Azure environment supports 24x7 operations, adhering to SLAs for uptime and performance.  Monitoring and Maintenance: Azure provides built-in tools for monitoring and maintenance, helping to proactively manage and resolve issues. |
| --- | --- |
| **Discussion Question #2** Can you change the VM type (upgrade or downgrade the configurations based on needs)? Try to downgrade one of the Azure VMs. Also, please provide a screenshot of the VM Overview settings, including VM name and size. | Can you change the VM type (upgrade or downgrade the configurations based on needs)?  **Flexibility in Azure:**  Azure VMs can be resized to different SKUs within the same series or to other compatible series based on needs. This flexibility allows for scaling up or down based on performance requirements and cost considerations.  For example, the WordPress server currently set to B4ms can be downgraded to B2ms if less performance is needed or upgraded to a higher SKU for more demanding workloads.  Screenshot Example:    **Steps to Change VM Size:**  Navigate to the VM in the Azure portal.  Select Size under the Settings menu.  Choose a new size from the list of available options and click Resize.  Screenshot Explanation:  This screenshot illustrates the VM overview settings, showing the current VM size and providing options to resize the VM. It also highlights the VM name and the resource utilization metrics. |
| **Optional Discussion** Is Contoso better off with a SQL Managed Instance? Check Azure Pricing. | Is Contoso better off with a SQL Managed Instance?  **Managed Instance Benefits:server**  Reduced Management Overhead: Azure SQL Managed Instance automates patching, backups, and maintenance, freeing up resources from manual administration.  High Availability and Performance: Built-in high availability and performance tuning features.  Seamless Integration: Supports most SQL Server features, making migration smoother and ensuring compatibility.  **Cost Considerations:**  Managed Instances can be more cost-effective when considering the total cost of ownership, including management and maintenance efforts.  Pricing Comparison: The monthly cost of SQL Managed Instances varies based on configuration and performance tiers. It's important to compare these against the combined cost of VM-based SQL Servers and associated storage.  **Conclusion:**  Considering the operational requirements and the need for high availability, SQL Managed Instances might provide a more streamlined and potentially cost-effective solution for Contoso’s SQL workloads. |

**Note:** *If you are using Udacity Cloud Labs, you will be allowed to create a few VM sizes only. Visit*[this](https://portal.azure.com/#create/Microsoft.VirtualMachine) *link to see all the possible VM sizes and go through the classroom instructions for more details.*

STEP 3 (OPTIONAL): Creating a VPN

Purpose: Build and set up a point-to-point (site to site) VPN connection between Contoso’s on-premises and Contoso’s Azure environments.

**Note:** *This step is entirely optional, and may take a considerable amount of time to implement. Therefore, it is suggested that you only attempt this step on your own after having satisfactorily completed all other project steps. You may find* [*this site*](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-classic-portal) *helpful in completing this optional step.*

STEP 4: An Additional Server

Purpose: Use Azure Resource Manager (ARM) to deploy one additional WordPress web server. This additional web server should provide web services redundancy and improve the web site’s response time.

**Create a replica of the WordPress server configuration.**

The process is summarized as:

* The current WP server settings were saved as a template during the creation process. If not, you will need to add it to your Template store.
* Deploy a new VM from a template. In the Azure portal search for TEMPLATES and run that service.
* The WP server template should be listed there. Select it.
* Make sure you load and edit the parameters file and change the values for the new VM as needed. Values such as Name, Password, etc. should be unique. Use the Azure Template Services.

Make sure you already have a resource group to place the VM in. You may need to create a Servers-RG resource group if one does not exist.

| **Configuration Process**  Provide a screenshot of the template configuration process. |  |
| --- | --- |
| **Discussion Question #1** List the benefits (at least three) of using ARM templates. Think of when, why and how you can benefit from this Azure service. | **Consistency and Repeatability:**  ARM templates allow you to define the infrastructure and configurations as code, ensuring that every deployment is consistent. This repeatability reduces human error and guarantees that each environment is set up exactly the same way.  **Automation and Efficiency:**  Using ARM templates automates the deployment process, saving time and reducing manual work. This is particularly beneficial for large-scale deployments or environments that need to be recreated frequently, such as in development and testing.  **Version Control and Collaboration:**  ARM templates can be stored in version control systems like Git, allowing teams to collaborate on infrastructure as code. Changes to infrastructure can be tracked, reviewed, and rolled back if necessary, providing greater control over the deployment process. |
| **Discussion Question #2** What is the difference between an ARM template and a server image? When will you use each and for what purpose? Make sure you consider each of the two. | **ARM Template:**  Purpose: ARM templates define a collection of resources and their configurations in a JSON format, allowing for the deployment and management of entire environments, including VMs, networks, storage, and more.  **Use Cases:**  Complex Deployments: When you need to deploy multiple resources with specific configurations and dependencies, such as a multi-tier application.  Infrastructure as Code: For maintaining infrastructure configurations in code repositories, enabling automated deployment and version control.  Consistency Across Environments: Ensuring that different environments (development, testing, production) are identical.  **Server Image:**  Purpose: A server image is a snapshot of a VM's disk that includes the operating system, installed applications, and configurations. It is used to create new VMs that are clones of the original.  **Use Cases:**  Cloning and Scaling: When you need to quickly create multiple VMs with the same setup, such as scaling out a web server farm.  Backup and Recovery: For creating a baseline image that can be used to restore a VM to a known good state.  Standardized Deployments: When deploying VMs that need to have a specific, predefined setup without the need for further configuration after deployment. |
| **Optional Discussion** Visit GitHub (<https://github.com/azure/azure-quickstart-templates>) and look at all available templates. Can you find a template that deploys 2 web servers, a load balancer, and a Resource Group? Send the link to the template or a screenshot clearly highlighting the one you will select. |  |

STEP 5: Backup and Recovery

Purpose: Use the Azure backup services to setup recurring full daily backup jobs of your products and client’s data. Test the backup process. No back is fully verified until you perform a successful restore.

**You want to ensure your VMs are all backed up. You want to ensure a working replica of each of them is saved somewhere safe.** The steps are:

1. Create a backup vault. Call it “ServersBackup”.
2. Install Azure Backup Extension on the target VM.
3. Create a backup policy in the vault. Set retention policy and daily backup points.
4. Now it is time to link the target VM to the backup policy. Click on the target VM, select Backup from the Operations tab. Then select the newly created backup policy.
5. Alternatively, you can select Recovery Services Vault from the left navigation bar. Select all the VMs you want to add to the backup.

| **Backups**  Provide screenshots of 1) the backup vault and 2) the backup policy. |  |
| --- | --- |
| **Discussion Question #1** What is the difference between Azure backup and site recovery? When would you use each service and for what reason? |  |
| **Discussion Question #2** Restore Time Objective (RTO) and  Restore Point Objective (RPO) have  similarities and differences.  A - How are they different? Make sure you consider each of the two.  B - Which backup strategy consumes more disc space? | **A - How are they different?**  **Restore Time Objective (RTO):**  Definition: The maximum acceptable amount of time that a system can be down after a failure before being restored.  Focus: Measures the time taken to recover operations and systems.  Objective: Ensures business continuity by minimizing downtime. Shorter RTOs require more resources and robust disaster recovery plans.  Example: If your RTO is 4 hours, you need to ensure that systems and applications are restored within 4 hours of a failure.  **Restore Point Objective (RPO):**  Definition: The maximum acceptable amount of data loss measured in time. It represents the age of the data that must be recovered from backup storage for normal operations to resume after a failure.  Focus: Measures the data loss tolerance.  Objective: Ensures data integrity by defining how much data can be lost during a disaster. Shorter RPOs require more frequent backups.  Example: If your RPO is 1 hour, you need to ensure that backups are taken at least every hour so that no more than 1 hour of data is lost in the event of a failure.  **B - Which backup strategy consumes more disk space?**  Backup Strategy and Disk Space Consumption:  RPO Strategy: Generally, a strategy with a shorter RPO will consume more disk space. This is because frequent backups need to be stored, leading to a higher number of backup points and more data to manage.  Example: Hourly backups will result in more stored backup copies compared to daily backups.  RTO Strategy: While RTO focuses on the time to restore, it does not directly impact disk space consumption unless specific techniques like full system snapshots are employed frequently to meet the required RTO.  **Conclusion:**  Strategies with a shorter RPO consume more disk space because they involve more frequent backups to minimize data loss. This requires storing multiple backup versions, increasing the overall storage requirement. |
| **Optional Discussion** Create more that one backup policy for each type of data. For example, you may want to create a policy that backs up certain files and folders and not the entire VM’s hard drive. Try a policy that has folder exclusion and inclusion. |  |

STEP 6: Antivirus Communication

Purpose: Enable the antivirus server to communicate with client VMs.

The XYZ antivirus server requires TCP ports 2222-2224 to communicate with the target client VMs. A firewall exception on the target VM is necessary to allow the XYZ server to scan and update the clients. Assuming Contoso will want to continue using their XYZ antivirus server, how will you alter the NSG (network security group) to allow all Contoso’s Azure servers port: TCP 2222-2224 in from the

antivirus server?

Each of the Azure servers you created have a unique internal (not public) IP address. Each one of these VMs has its own Network Security Group (nsg) associated with it as well. **Your task is to adjust the nsg of each server to allow for traffic coming from the antivirus server**. The steps are:

1. Make a list of each server and it’s internal IP.
2. For each server’s nsg, modify the settings to allow for TCP 2222-2224 from the antivirus server’s IP number.
3. Test your work by trying to deploy the antivirus agent on one of the target servers.

|  | WordPress-Server  Private IP: 10.1.0.4  NSG: Associated with its network interface  WordPress-Server-2  Private IP: 10.1.0.5  NSG: Associated with its network interface  SQL-Server-1  Private IP: 10.0.0.4  NSG: Associated with its network interface  SQL-Server-2  Private IP: 10.0.0.5  NSG: Associated with its network interface  Backup-Server  Private IP: 10.0.0.6  NSG: Associated with its network interface  Antivirus-Server  Private IP: 10.0.0.7  NSG: Associated with its network interface (though it's the source, not the target of rules)  NOTE: COULD NOT FIND ANTIVIRUS PROGRAM WITH SERVER LICENSE FOR FULL TESTING! |
| --- | --- |
| **Inbound Rules**  Provide a screenshot of the modified nsg firewall inbound rules. | Antivirus programs installed on Servers |
| **Discussion Question #1** Will you need to create an inbound port exception on your Windows OS? | Yes, you typically need to create an inbound port exception on the Windows OS firewall to allow the traffic through to the application layer. Even though the Azure NSG rules allow traffic to pass through the network layer, the operating system's firewall might still block the traffic unless explicitly allowed.  How to do this on Windows:  Open Windows Defender Firewall with Advanced Security.  Go to Inbound Rules and create a new rule.  Select Port and specify the ports (2222-2224).  Allow the connection and apply the rule to the appropriate profiles (Domain, Private, Public).  Name the rule (e.g., "Allow Antivirus Traffic on Ports 2222-2224"). |

**Note: Once you have completed your report, feel free to shut down your Azure resources to avoid charges!**