There may be more than one way to architect these solutions. These are suggested designs, feel free to enhance or modify as you deem necessary. This document should not be shared with students, it is for instructors only.

Design a Governance Solution Case Study

Estimated time: 60 minutes

Requirements

Tailwind Traders is planning on making some significant changes to their governance solution. They have asked for your assistance with recommendations and questions. Here are the specific requirements.

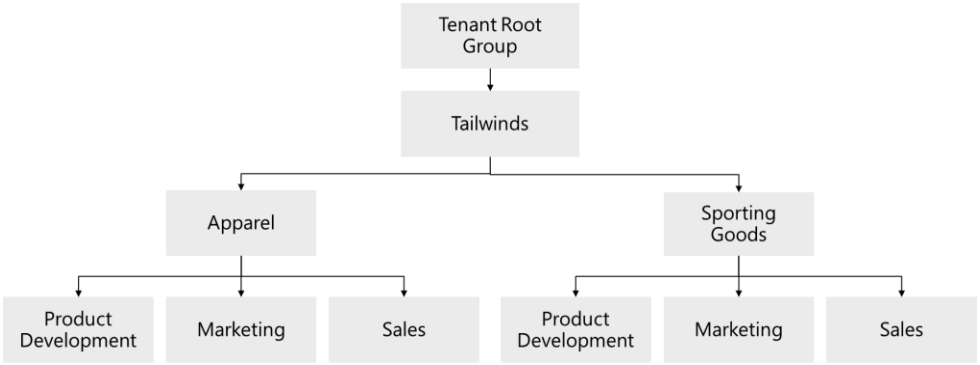
- **Cost and accounting.** Tailwind Traders has two main business units that handle Apparel and Sporting Goods. Each of the business units consist of three departments: Product Development, Marketing, and Sales. Each business unit and subunit will be responsible for tracking their Azure spend. At the same time, the Enterprise IT team will be responsible for providing company-wide Azure cost reporting.
- **New development project.** The company has a new development project for customer feedback. The CFO wants to ensure all costs associated with the project are captured. For the testing phase, workloads should be hosted on lower cost virtual machines. The virtual machines should be named to indicate they are part of the project. Any instances of non-compliance with resource consistency rules should be automatically identified.

Tasks

1. **Cost and accounting.**
    - What are different ways Tailwind Traders could organize their subscriptions and management groups. Which would be the best to meet their requirements?
    - Design two alternative hierarchies and explain your decision-making process.
2. **New development project.**
    - What are the different ways Tailwind Traders could track costs for the new development project?
    - How are you ensuring compliance with the requirements for virtual machine sizing and naming?
    - Propose at least two ways of meeting the requirements. Explain your final decision.

Instructor Solution

1. **Cost and accounting.** What would you recommend for the cost and accounting? If necessary, design a hierarchy and explain your decisions.



- Azure offers two methods to implement cost management. There is a cost management feature integrated into the Azure portal. In addition, Enterprise Agreement subscriptions also offer the ability to roll up billing at an account, department, or the Enterprise Agreement level.
- Regardless of which cost management method is used, the first step is to ensure all Azure subscriptions are organized into an appropriate hierarchy. Costs can then be aggregated at each node in this hierarchy for roll-up reporting. The cost management in the Azure portal uses the management group hierarchy. EA subscriptions are organized into a 4-level hierarchy, comprising the root (at the Enterprise Agreement level), departments, accounts, and subscriptions. Considering that Tailwind Traders has an existing Enterprise Agreement level, they might want to consider Enterprise Agreement billing and reporting mechanism. In addition, they might want to consider mirroring the Enterprise Agreement hierarchy by using management groups, to provide consistency from the billing and subscription management perspective.
- In the case of Tailwind Traders, the hierarchy will comprise the tenant root management group, a top-level management group for the company, followed by a separate management group for each business unit. Each of these management groups would, in turn, include child management groups for each department. Each of these management groups would contain subscriptions associated with their respective department.
- Each subscription constitutes a separate billing unit, so this functionality is available based on functionality inherent to subscriptions. Aggregated billing is also available

at the management group level (via Cost Management in the Azure portal) and at the department level (in the Enterprise Agreement hierarchy).

- Company-wide aggregated billing is available at the root management group level (via Cost Management in the Azure portal) and at the Enterprise Agreement level (in the Enterprise Agreement hierarchy).
- There are two ways to accomplish separate cost reporting for development, test, and production environments within each business unit.
    - If each of these environments is implemented by using a separate subscription (which would be recommended to provide sufficient level of isolation between them), then, as explained earlier, this functionality is available based on functionality inherent to subscriptions.
    - If development, test, and production resources reside in the same subscription, then each should be appropriately tagged to designate its environment. Tag information is included in the cost reporting, so it is still relatively easy to identify.

2. **New development project.** What do you recommend for the new development project? Explain how the requirements will be met.
    - There are several ways to capture costs related to the new project. Tagging could be used to identify the project resources. An Azure policy could then be used to ensure the tagging is in place. Another option is to use a subscription to report billing. If all the resources could be placed in a resource group, that could be a possible solution.
    - Azure policy can also be used to ensure that top pricing tier Azure VMs are not provisioned. The policy could be applied to a resource group or subscription. Non-compliant resources can be automatically identified.
    - Reminder - You can assign a policy definition or an initiative definition on the root management group level, which would apply to all subscriptions in the hierarchy below the root. Note that you can exclude subscriptions, resource groups, or even individual resources from such policy if you need to implement exceptions.

Instructor references:

Best practice: Name resource groups
Best practice: Implement delete locks for resource groups
Best practice: Tag resources effectively
Best practice: Manage resources with Azure management groups
Best practice: Deploy Azure Policy

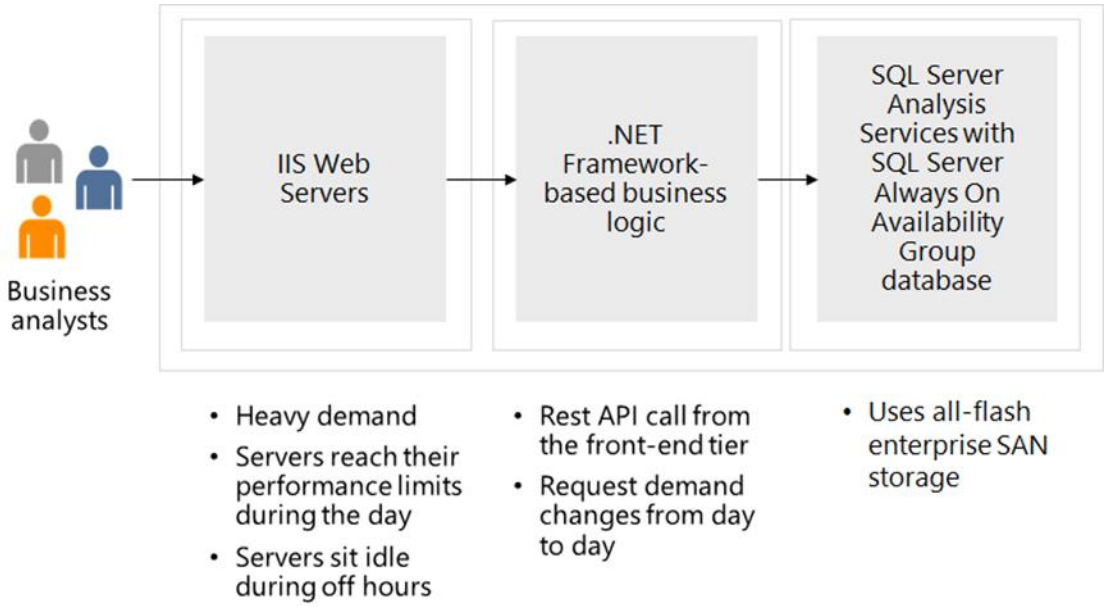
Resource naming and tagging decision guide - Cloud Adoption Framework
List of built-in policy definitions - Azure Policy

Design Compute Case Study

Estimated time: 90 minutes

Requirements

Tailwind Traders would like to migrate their product catalog application to the cloud. This application has a traditional 3-tier configuration using SQL Server as the data store. The IT team hopes you can help modernize the application. They have provided this diagram and several areas that could be improved.



- The frontend application is a .NET core-based web app. During peak periods 1750 customers visit the website each hour.
- The application runs on IIS web servers in a front-end tier. This tier handles all customer requests for purchasing products. During the latest holiday sale, the front-end servers reached their performance limits and page loads were lengthy. The IT team has considered adding more servers, but during off hours the servers are often idle.
- The middle tier hosts the business logic that processes customer requests. These requests are often for help desk support. Support requests are queued and lately the wait times have been very long. Customers are offered email rather than wait for a representative. But many customers seem frustrated and are disconnecting rather than wait. Customer requests are 75-125 per hour.
- The back-end tier uses SQL Server database to store customer orders. Currently, the back-end database servers are performing well.

- While high availability is a concern, due to legal requirements the company must keep all the resources in a single region.

Tasks

- **Front-end tier.** Which Azure compute service would you recommend for the front-end tier? Explain why you decided on your solution.
- **Middle tier.** Which Azure compute service would you recommend for the middle tier? Explain why you decided on your solution.

Instructor Solution

Front-end tier

Which Azure compute service would you recommend for the front-end tier? Discuss both the workload hosting and the web application. Explain why you decided on your solution.

- You could use an Azure VM scale set (VMSS) to satisfy the autoscaling requirement. When customer requests increase or decrease, VMSS will automatically scale. It is also recommended to create availability sets or zones.
- The optimal choice would be an Azure App Service web app. This web app supports autoscaling and can host a .NET Core-based web app. It would be recommended to use availability zones.
- To ensure you are solving the problem, Application Monitoring and Application Insights are recommended. These products provide detailed IIS web server/client performance metrics. This will help detect SLA issues and notify those users who have exceeded a threshold while holding for support representative.
- Would you need both VMSS and App Services scaling?

Middle tier

Which Azure compute service would you recommend for the middle tier application? Justify your recommendation with proper illustration.

- Azure functions provide the ability to manage message queues, like the customer help desk requests. Functions allow you to write less code, maintain less infrastructure, and save on costs. Instead of worrying about deploying and maintaining servers, the cloud infrastructure provides all the up-to-date resources needed
- As requests increase, Azure functions meets the demand with as many resources and function instances as necessary - but only while needed. As requests fall, any extra resources and application instances drop off automatically.

- Azure functions can be triggered by an event. For example, the customer selecting they would like to send email. Also, monitoring and logging is available with Azure functions.
- API Management should also be considered. APIM would allow for policies such as throttling, caching and authentication. If the middle tier were to expand or move to a microservice model later, APIM would allow for a single frontend access point with flexibility to connect or redirect to many backend API locations. In addition, APIM allows for additional logging and visualizations of traffic.

Instructor references:

- Integration and automation platform options in Azure | Microsoft Docs
- Compare Azure messaging services - Azure Event Grid | Microsoft Docs
- Choose a compute option for microservices - Azure Architecture Center | Microsoft Docs

Design Non-relational Storage Case Study

Estimated time: 60 minutes

Requirements

Tailwind Traders wants to reduce storage costs by reducing duplicate content and, whenever applicable, migrating it to the cloud. They would like a solution that centralizes maintenance while still providing world-wide access for customers who browse media files and marketing literature. Additionally, they would like to address the storage of company data files.



Media files	Marketing literature	Corporate documents
• Product photos and feature videos • JPEG and MP4 are most common formats	• Customer stories, sales flyers, sizing charts, and eco-friendly manufacturing information • PDF format is the most common	• Internal documents – some sensitive • Mostly Office formats like Word and Excel

- **Media files**. Media files include product photos and feature videos that are displayed on the company's public website, which is developed and maintained in house. When a customer browses to an item, the corresponding media files are displayed. The media files are in different formats, but JPEG and MP4 are the most common.

- **Marketing literature.** The marketing literature includes customer stories, sales flyers, sizing charts, and eco-friendly manufacturing information. Internal marketing users access the literature via a mapped drive on their Windows workstations. Customers access the literature directly from the company's public website.

- **Corporate documents.** These are internal documents for departments such as human resources and finance. These documents are accessed and managed via an internally developed web application. Legal requires that various documents be retained for a specific period of time. Occasionally documents will need to be maintained longer when legal or HR issues are being investigated. Most corporate documents older than one year are only kept for compliance reasons and are seldom accessed.

- **File location.** All the files are stored locally in the main office data center. There are numerous file shares organized by department or product line. The data servers are struggling to provide files for the website. During peak hours website pages are slow to render.

- **File access frequency.** Some products are more popular, and that data is accessed more frequently. However, some products, like ski gear, are only accessed during that season. Sales events generate a lot of interest in certain on sale items.

Tasks

1. Design a storage solution for Tailwind Traders.
    - What type of data is represented?
    - What factors will you consider in your design?
    - Will you use blob access tiers?
    - Will you use immutable storage?
    - How will the content be securely accessed?
2. Your solution should consider the media, marketing literature, and corporate documents. Your recommendations may be different depending on the data. Be prepared to discuss your decisions.

Instructor Solution

- All the content is classified as non-relational.
- The design should consider file location, compliance and regulatory requirements, performance, and storage replication. Also, the solution should be cost effective and easy to centrally manage.
- Blob storage is recommended for the media and corporate files. Blob storage is less expensive, offers the immutable storage requirements for legal, and supports API access for internal applications.
- Azure Files is recommended for the marketing literature. Azure Files is required for marketing since the files will accessed via SMB internally.
- Marketing literature access latency for internal users could be reduced by using a local Windows Server and File Sync
- Zone redundant storage is recommended. An argument could be made for Geo-redundant zone storage if the files are mission critical. Read access geo-redundant storage could be used if the front end could make use of a secondary region. This decision would depend on the customer locations and traffic.
- The hot tier should be used for all media, marketing literature and corporate documents less than one year old. The archive tier or cold tier should be used for corporate documents older than one year. This decision is based on retrieval latency, storage duration and a desire to reduce costs. Discuss that there is not enough provided

information to decide between Cold and Archive and ask what additional questions they may want to ask Tailwind Traders. A lifecycle management should be used to convert corporate documents to a cheaper storage tier after one year.

- Private endpoints and firewall policies should be applied. If private endpoints haven't been discussed yet, do not go in depth at this point. They are covered in the Networking module.

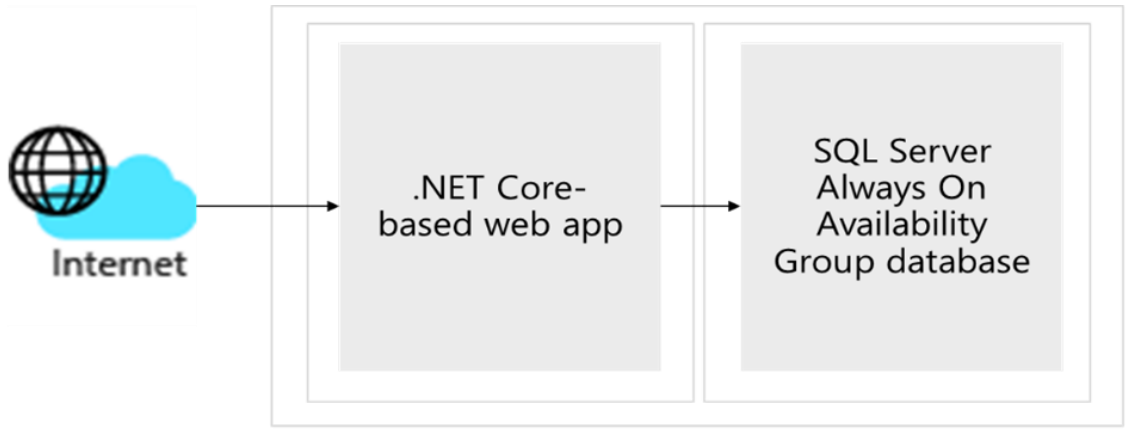
Instructor references

- Security recommendations for Blob storage - Azure Storage | Microsoft Docs
- Introduction to Azure Storage - Cloud storage on Azure | Microsoft Docs
- Hybrid file services - Azure Architecture Center | Microsoft Docs
- Architect storage infrastructure in Azure learning path - Learn | Microsoft Docs

Design Relational Storage Case Study

Requirements

Tailwind Traders is looking to move their existing public website database into Azure, as the website front end is being moved there as well. The website front end will initially only be deployed in 2 regions for redundancy. However, it is expected that as traffic increases the website will be replicated to other regions around the world. The database, which you are being asked to migrate, holds the product catalog, and all online orders. Currently the database runs on a single Microsoft SQL Server Always On availability group on premises.



- 2-tier Windows based .NET Core-based web app
- Provides access to the product catalog hosted in a SQL Server
- Categorized as mission-critical and requires high availability provisions

Primary concerns of Tailwind Traders:

- **High availability.** A primary concern for Tailwind Traders is that this database be highly available as it is critical to their business. Any outages may result in lost sales or customer confidence.
- **Website performance.** While the performance of placing orders is normally satisfactory, browsing or searching pages with many items listed is reported as being "sluggish."
- **Security.** Tailwind Traders is very concerned about personal or financial information stored in the database being exposed. In addition to implementing proper security measures, the security team needs to verify that industry standard best practices are implemented, when possible.

Tasks

1. Design the database solution. Your design should include authorization, authentication, pricing, performance, and high availability. Diagram what you decide and explain your solution.

Instructor Solution

Design the database solution. Your design should include authorization, authentication, pricing, and high availability.

- **Authorization.** You can control authorization by leveraging the Azure SQL Database and server level firewall functionality, allowing access only from the Tailwind Traders customer facing web servers. Private Endpoints may also be used reduce the attack surface of the Azure SQL Database, and NSGs may be implemented to implement an additional layer of security. To remediate potential threats and get reports against industry standard best practices, consider enabling Azure Defender for SQL. To protect data, consider implementing Transparent Data Encryption (TDE), Dynamic Data Masking, and Always Encrypted.
- **Authentication.** From the authentication standpoint, once you integrate Tailwind Traders' Active Directory environment with Azure Active Directory, your internal users will be able to authenticate to Azure SQL Database by using their Active Directory credentials. To provide access to an Azure SQL database from other Azure resources, such as Azure web apps, you can associate them with a managed identity.
- **Pricing.** We would recommend Azure SQL Database because there was no requirement that the customer remain in control of the database engine or host OS. If compatibility issues are found during the testing or pilot phase, Azure SQL Managed Instance or SQL Server on a VM may be required.
- **Performance.** Simply moving to Azure and allocating sufficient resources to the Azure SQL Database MAY resolve the noted performance issues. However, you may want to consider sharding the data and moving the product catalog to a NoSQL CosmosDB. This may provide a faster response time due to the materialized view CosmosDB would present. In addition, the database could be easily globally distributed. Note, this could require substantial effort to perform but may result in a better long-term solution.
- **High Availability.** We recommend business critical based on the high availability goals stated in the description. Specifically, it satisfies the immediate needs of not only storing relational data, but also providing low-latency, high-throughput transactions as well as the high availability of Always On and support for multiple read-only replicas. By deploying read-only replicas across different Azure regions, you could also minimize the latency of read operations from customers residing in these other regions, depending on the design of the website front end.

Instructor references

Materialized View pattern - Cloud Design Patterns | Microsoft Docs
General purpose and business critical service tiers - Azure SQL Database & SQL Managed Instance | Microsoft Docs

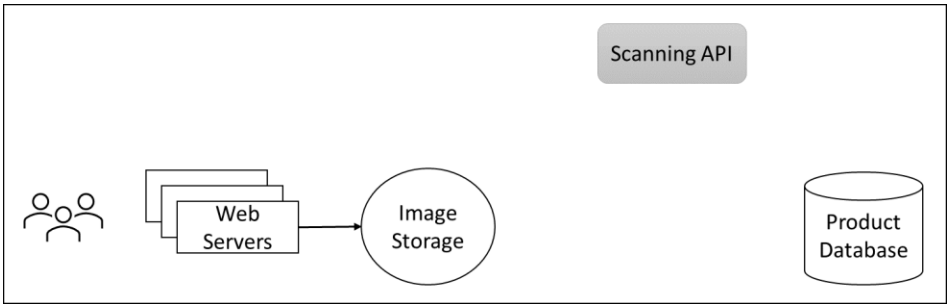
Design Application Architecture Case Study

Estimated time: 60 minutes

Requirements

Tailwind Traders is looking to update their website to include customer supplied product images in addition to the already existing photos provided by marketing. They believe that having more photos of products in use will give potential customers a better feel for how past customers loved their products after purchasing them. They do have some requirements as outlined below:

- Uploaded images will need to be scanned before getting posted on the website. Legal and Marketing are both requesting that after initial upload, the images be checked for any issues that reflect poorly upon the company or could cause legal issues. An in-house API has already been developed and deployed that can perform the necessary scanning.
- Based on existing patterns, Tailwind Traders expects the image uploads to happen very unevenly throughout the day. Certain periods may experience more uploads than the scanning software can handle, while other periods may experience very few or no uploads.
- Once an uploaded image has been scanned and approved by the system, Tailwind Traders would like for the customer to be sent an email thanking them for sharing their image.
- Cost and management of the solution is a concern, especially since Tailwind Traders isn't sure how popular this feature will be initially. Minimize costs and leverage serverless solutions where possible.



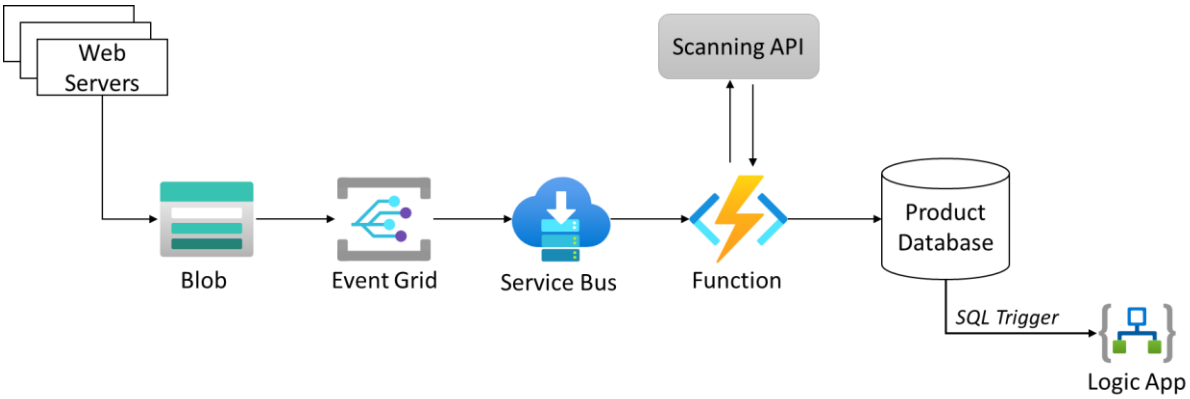
Task

Design an architecture for the customer images to be added to the company website.

- Where should the images be stored?

- How will you ensure that images being stored get scanned even when the uploads are outpacing scanning?
- Once images are approved and the catalog database is updated, how will the customer be notified?

Instructor solution



- Consider Storage Account Blobs for the image storage. Files could be used if SMB or NFS is required by the web application, but blob storage offers a lower cost and generally more features.
- Consider Event Grid to create a notification when new storage blobs are created.
- Consider Service Bus Queues to hold Event Grid notifications. The use of a queue will help balance the loads and ensure that events aren't missed through delivery guarantees.
- Functions provide a serverless option to get messages from the queue and send them to the Scanning API for processing.
- Logic Apps provide an easy, code-free option to send emails based on triggered events, such as SQL database item creation or modification.

Design Authentication and Authorization Case Study

Estimated time: 60 minutes

Requirements

Tailwind Traders is doing very well and is expanding their workforce. They have successfully acquired an online retailer in the sports apparel space. The company has also located a partner to outsource marketing literature. Tailwind Traders is using Azure Active Directory for user and groups accounts. Here are two specific initiatives the IT department would like you to help with.

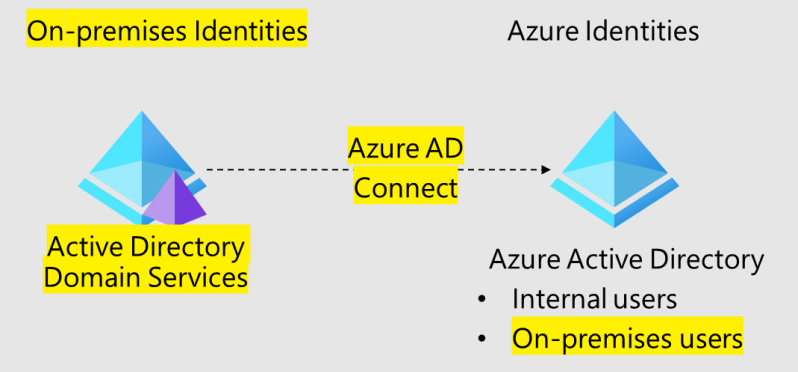
- **New user accounts**.
    - The online retailer acquisition will add 75 employees to Tailwind Traders. All the new users have on-premises Active Directory Domain Services accounts in the retailer's existing domain.
    - The new marketing partner will initially have 15 employees who will need corporate access. These employees already have Azure AD accounts in the partner's AAD tenant.
    - The new employees are located at various geographic locations and will need account privileges for their new job roles. Some changes to existing employee roles are expected.
    - The IT department wants to take this opportunity to include new identity security features.
- **New application access.** The business development team has an application running an on Azure VM and data stored in an Azure SQL database. They need to securely allow the VM to query the Azure SQL database. They also need an on-premises server to be able to securely access the SQL database without storing credentials in the application code or configuration files.

Tasks

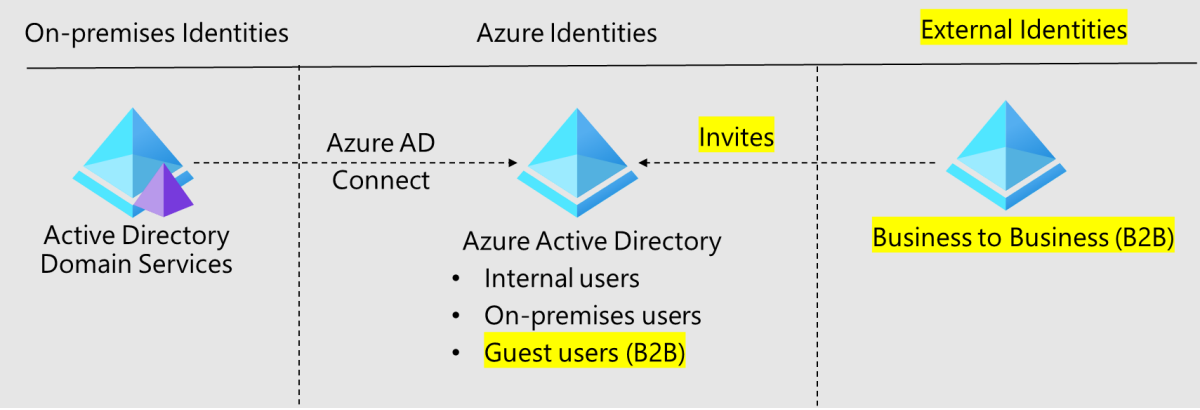
1. **New user accounts.**
    - Diagram the process for bringing in the acquired user accounts.
    - Diagram the process for adding the new partner accounts.
    - For the above 2 requirements, be sure to include any tools that will be used. List at least three benefits of your suggested solution.
    - Provide at least three recommendations for improving Tailwind Traders user identity solutions. Rank the recommendations in order of importance. Include your reasons for making these suggestions.
2. **New application access**
    - Provide an access solution for the business development application.
    - Provide an access solution for the on-premises resources.

Instructor Solution

1. **New employee user accounts.**
   - The on-premises users can be synced using Azure AD Connect. Are new groups needed in Azure AD? How will you determine which Azure AD groups to use? Are the permissions for existing groups appropriate? Use password hash for synchronization? Advantages include centralized management, synchronized changes, and ease of administration.



   - The partner users can be added using Azure B2B. These external identities will be added as guest users. What new Azure AD groups will be needed? What permissions will these users need? Who will issue the invites? Advantages include established processes, centralized management, and ease of administration.



2. **New identity solution features.** Here are some recommendations to discuss and review. Discuss the order of importance.
   - Use MFA for privileged roles like administrators. Consider MFA for the partner accounts.

- Use access reviews to ensure users changing jobs still have the correct permissions.
- Use RBAC to ensure permissions are correct. Design at the group level.
- Require users to access applications only from managed devices.
- Block access from untrusted sources, such as access from unknown or unexpected locations.
- Establish user and sign-in risk policies.

3. **New application access**
    - Access solution for the business development application: Use a Windows VM system-assigned managed identity to access Azure SQL. Managed Service Identities are automatically managed by Azure and enable you to authenticate to services that support Azure AD authentication, without needing to insert credentials into your code.
    - Access solution for the on-premises resources: Register the application with Azure AD and assign an application service principal. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.

Instructor references:

- Best practices for Azure RBAC
- Best practice: Review subscriptions and resource permissions
- Best practice: Understand resource access permissions
- Best practices for Azure RBAC
- Azure identity & access security best practices
- Best practice recommendations for managed system identities

Log and monitor Fabrikam Residences Case Study

Estimated time: 120 minutes

This case study is not just for Log and Monitor. It is more inclusive and covers compute, relational data, non-relational data, authentication, application architecture.

Summary

You have taken a new position with Fabrikam Residences, which is very successful and is experiencing rapid growth. Fabrikam Residences is a building contractor for new homes and major home renovations and have become successful by providing quality buildings and offering newer integrated home technologies than their competitors.

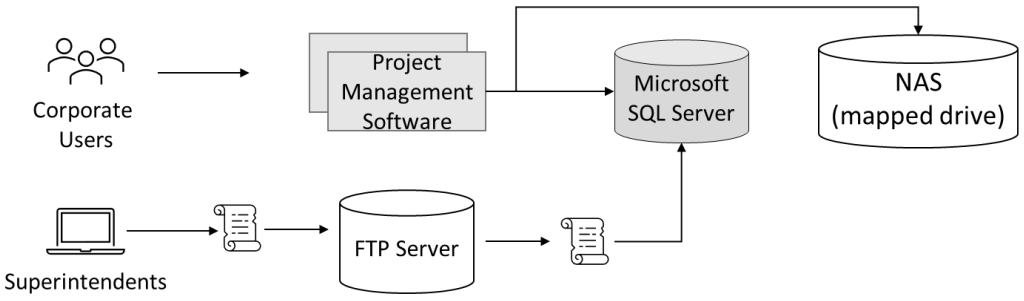
Currently these technologies are provided and managed by separate sub-contract companies. The owners of Fabrikam Residences want to begin offering these upgraded technology options in-house to provide better quality, support and data on customer patterns and needs.

Initially, the company wants to offer HVAC (heating and cooling) control and monitoring, security system monitoring and alerts, and home automation. This will require a new website, data storage solution and data ingestion solution.

The company has seen tremendous growth over the past 2 years. The company is estimating it may double in size over the next 12-18 months. With such rapid growth in the regional market, the company has no current plans to expand outside of the regional market.

Current Situation

The Fabrikam Headquarters operates a small datacenter in a single location. The datacenter hosts the company **Project Management (PM) software**.



- The PM software uses a third-party Windows application. The application runs on a 2-node Network Load Balancing (NLB) cluster with a single Microsoft SQL Server backend.
- Images and documents are stored on a mapped drive of the server, which resides on a dedicated NAS appliance.

- Corporate users, office staff, use a web front end to enter data such as supply delivery schedules and change orders.
- Field superintendents use Windows laptops and tablets offline to continuously record building progress and other details. These changes, such as new work orders, are stored in a local change file. At the end of each day, superintendents return to the office to connect to the wireless network and run a small script to upload the change file to an FTP server. A second script is scheduled to run each night to processes all the change files and enter their contents into the Project Management database (Microsoft SQL Server).

Requirements

Project Management software

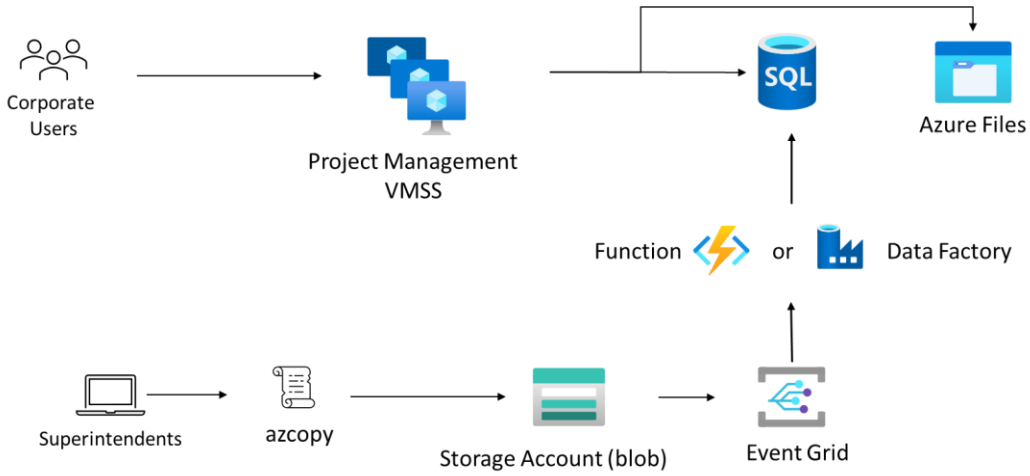
- Migrate as many of the systems to a public cloud provider as possible.
- Replace the existing scripts to leverage a system more secure than FTP, as security concerns have arisen. Also, you have been asked to make sure that change files are processed as soon as they are uploaded.
- Increase the resilience of the project management database. While performance is not an issue, the company would like to avoid losing access to the database in case of a single hardware failure.

Tasks

1. Design a solution for the Project Management software. Be prepared to explain why you chose each component of the design and how it meets the solution requirements.

Instructor solution

Project Management Software



- A VM Scale Set could be used to run the project management software. As the software already runs on an NLB cluster, it is highly likely that it would function correctly on a VMSS. VM Scale Sets would also allow for health probes and self-healing in the even one of the project management servers stopped working. Since the software is provided by a third-party vendor, it would require vendor support to run in an App Service or container. It may be worth contacting the vendor to see if that is an option.
- An Azure SQL Database should be the first choice for the project management database. The general tier does provide some redundancy. If additional redundancy is required, the database can be upgraded to Business Critical tier.
- Azure Files should be used to replace the NAS functionality as it provides SMB (mapped drive) support for the Project Management software
- Blob storage should be used to replace the FTP server. Blob storage provides the features and security necessary at the lowest price point. Azure Files may work but would come at a higher price.
- The script used by the superintendents should be upgraded to use a tool such as AZCopy. AZCopy can directly copy files to the blob storage from the local machines.
- Event Grid can be used to trigger data import immediately after superintendents' upload change files.
- Azure Data Factory or an Azure Function App could be used to import the change files into the database. Azure Data Factory would provide an easier, no-code path. If the workflow requires more flexibility, an Azure Function could be custom written.
- Consider using Private Endpoints for PaaS services to improve security.

Networking Case Study

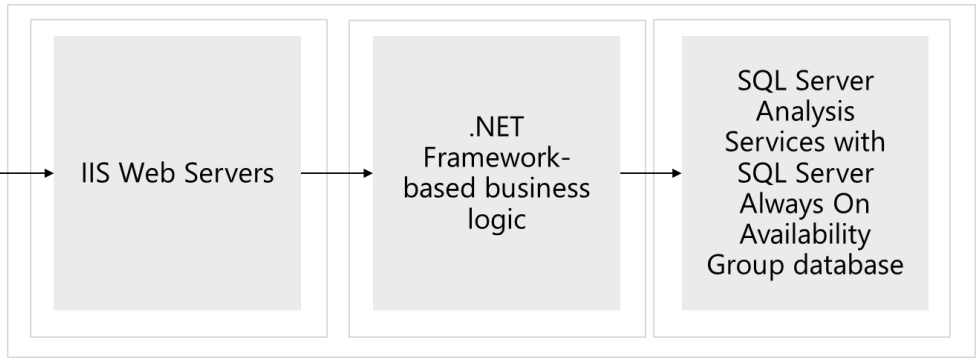
Estimated time: 120 minutes

Requirements

As the Tailwind Traders Enterprise IT team prepares to define the strategy to migrate some of company's workloads to Azure, it must identify the required networking components and design a network infrastructure necessary to support them. Considering the global scope of its operations, Tailwind Traders will be using multiple Azure regions to host its applications. Most of these applications have dependencies on infrastructure and data services, which will also reside in Azure. Internal applications migrated to Azure must remain accessible to Tailwind Traders users. Internet-facing applications migrated to Azure must remain accessible to any external customer.

To put together the initial networking design, the Tailwind Traders Enterprise IT team chose a key application, which is representative of the most common categories of workloads that are expected to be migrated to Azure:

BI enterprise application



- An internal, Windows-based, three-tier business intelligence (BI) enterprise application with the front-end tier running IIS web servers, the middle tier hosting .NET Framework-based business logic, and the back-end tier implemented as a SQL Server Always On Availability Group database.
- This application is categorized as mission-critical and requires high availability provisions with the availability SLA of 99.99% and disaster recovery provisions, with 10-minute RPO and 2-hour RTO.
- To provide connectivity to internal apps migrated to Azure, Tailwind Traders will need to establish hybrid connectivity from their on-premises datacenters. The Enterprise IT group already established that such connectivity will be implemented by using ExpressRoute circuit from its main Seattle datacenter, however, at this point it is not clear yet what would be failover solution in case that circuit becomes unavailable. The

Tailwind Traders CFO wants to avoid paying for another, redundant ExpressRoute circuit.

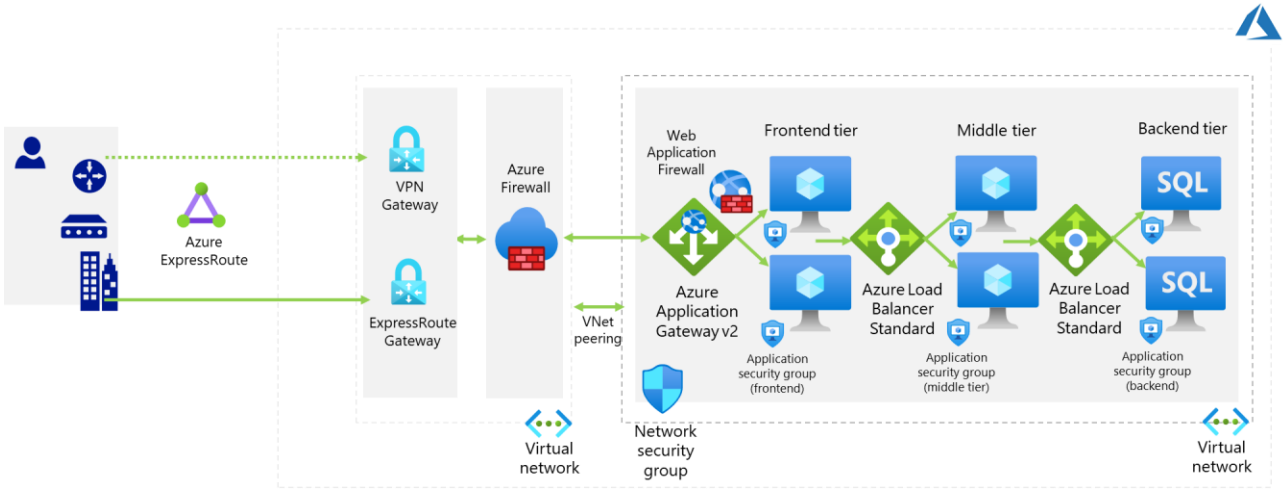
- There are additional considerations that apply to on-premises connectivity to internal apps migrated to Azure. Since the Tailwind Traders Azure environment will consist of multiple subscriptions and, effectively, multiple virtual networks, to minimize cost, it is important to minimize the number of Azure resources required to implement core networking capabilities. Such capabilities include hybrid connectivity to on-premises locations as well as traffic filtering. Incidentally, this need to minimize cost aligns with the Information Security and Risk requirements, which state that all traffic between on-premises locations and Azure virtual networks must flow via a single virtual network, which will be hosting components responsible for hybrid connectivity and traffic filtering.
- As per requirements defined by the Tailwind Traders Information Security and Risk teams, all communication between Azure VMs in different tiers that are part of the same application must allow only the ports required to run and maintain the application. However, due to IP address space limitations, it might not be possible to allocate dedicated subnets to each tier. Enterprise IT group needs to identify the optimal way to configure source and destination for traffic filtering that would not require directly referencing IP addresses or IP address ranges.

Tasks

- Design a 3-tier network solution for the BI Application. Your design could include Azure ExpressRoute, VPN Gateways, Application Gateways, Azure Firewall, and Azure Load Balancers. Your networking components should be grouped into virtual networks and network security groups should be considered. Be prepared to explain why you chose each component of the solution.
- Based on your architect solution from the compute case study how would this impact the network design? Would you need any additional networking resources to secure access to the modernized application? Would you no longer need some of the recommended solutions implemented in your original network design?
- Based on your storage (relational) case study how would you update the network design to secure access to the storage account and ensure only select users have access to the storage account?
- Based on the modernizing of the SQL backend how do you plan to enable pragmatic access to the data base so that the front end has no hard coded secrets in its code base?

Instructor Solution - BI Enterprise application

Design a 3-tier network solution for the BI Application. Your design could include Azure ExpressRoute, VPN Gateways, Application Gateways, Azure Firewall, and Azure Load Balancers. Your networking components should be grouped into virtual networks and network security groups should be considered.



- The BI application is categorized as *enterprise*, which means that it requires the availability SLA of 99.99%. To accomplish this level of availability, you need to deploy Azure VMs hosting the application into Azure availability zones, which implies that the load balancers you will be using must support zone redundancy.
- You can choose between internal (private) zone-redundant Azure Load Balancer Standard SKU and zone-redundant Azure Application Gateway v2. The latter is required for the front-tier to accommodate the Information Security and Risk team requirement that any data-driven external and internal apps that support database updates must implement traffic inspection that would identify and block exploits targeting common web and database vulnerabilities, such as SQL injection or cross-site scripting. This functionality is provided by the Web Application Firewall (WAF) component of Azure Application Gateway.
- For the middle and back-end tier load balancing, you should use zone-redundant Azure Load Balancer Standard SKU, which, unlike Application Gateway, supports non-HTTP/HTTPS traffic.
- You should use a combination of Network Security Groups and Application Security Groups. For this to work as intended, you need to assign a specific Application Security Group (such as, *SQL Servers*) to network adapters of the VMs hosting SQL Server instances. This way, within rules of a network security group assigned to the network adapters of Azure VMs in the tier that needs to connect to SQL Server

instances, you can use the *SQL Server* application security group as the rule destination.

- To implement failover, you would first need to set up a matching, three tier deployment in another Azure region, serving as a disaster recovery site. For the web and middle tier, you can accomplish this by using Azure Site Recovery. For the data tier, you can extend Always On Availability Group to include another SQL Server instance in another region, with asynchronous replication from the primary instance.
- Note that this requires establishing global peering to the virtual network hosting the secondary site. To perform a failover, you can use Azure Site Recovery. This will also require DNS changes to update IP addresses of DNS records representing the names used for communication between tiers and for connectivity to the application from internal users.
- If using Azure functions for the middle tier then private endpoint can be used to secure functions to the network.
- If using containers for the compute solution enable containers to use Azure Virtual Network capabilities
- programmatic access to SQL: managed identity

1. **Optional Review** - How would you summarize networking technologies used for the application?

Network requirement	BI application
Web tier load balancing	Azure Application Gateway v2 with Web Application Firewall (WAF)
Middle tier load balancing	Azure Load Balancer Standard
Data tier load balancing	Azure Load Balancer Standard
Traffic filtering between tiers	Network Security Groups combined with Application Security Groups
High availability networking components:	Azure Load Balancer Standard (zone-redundant) Application Gateway v2 (zone-redundant)
Disaster recovery networking components	Global virtual network peering DNS (Azure Private DNS or custom DNS, including support for AD DS-integrated DNS zones)

2. **Optional Review** - How would you summarize networking technologies used for hybrid connectivity and virtual network connectivity (including topology, primary and backup interconnectivity, and traffic filtering)?

Hybrid connectivity	Virtual network connectivity
Topology: Hub and spoke (single point of entry)	Topology: Hub and spoke
Primary interconnectivity technology: ExpressRoute (zone-redundant)	Primary interconnectivity technology: virtual network peering
Backup interconnectivity technology: VPN Gateways (zone-redundant)	Backup interconnectivity technology: N/A
Traffic filtering: Azure Firewall	Traffic filtering: Azure Firewall (across spokes) Network Security Groups and Application Security Groups within virtual networks
Traffic routing: BGP	Traffic routing: BGP + Azure User Defined Routes

Instructor references

Best practices to set up networking for workloads migrated to Azure - Cloud Adoption Framework | Microsoft Docs