AZ-305: Case Studies for Designing Microsoft Azure Infrastructure Solutions

This document should not be shared with students, it is for instructors only. Another document, StudentCaseStudySolutionHandout.pdf, is available to provide your students with the architecture diagrams. That document is also in the MCT Download Center.

Case Study Purpose

The case studies in AZ-305 are essential to the success of the class. Being able to deliver an effective case study for your classes will provide an invaluable knowledge transfer for your learners. Feel free to use the tips, timings, and tricks in this document that best work with your style and preferences.

The main purpose of the case studies is to teach our learners how to work like an architect, taking a business problem and translating them to high-level architecture designs.

Case Study Strategies

One of the goals of this course is to have the learners be able to break down the case studies into design requirements and translate them into solutions. In a way you are teaching your learners how "think" like an architect.

Here are some strategies on how to approach the case studies.

- Be sure to read the case study all the way through highlighting the goals and requirements.
- Demonstrate how to approach a case study and give students some guidance before they begin the exercises.
- Identify some questions to help guide the learners. Starting questions are provided in the case studies.
- Highlight the business requirements and list the proposed technologies that will meet those conditions.
- For each proposed technology, list the pros and cons of the solution. The Azure technology with the most pros is the front contender in your design to answer the business need.
- Check the Azure Architecture Center to find out if a related architecture exists.
- There is no right or wrong way to complete the design. We recommend addressing this to the students up front. There is usually not a single solution just a set of resources or services that can offer the desired outcomes.
- For each proposed solution have the student explain how their design meets the business requirements presented in the original problem statement.
- Reinforce with students that if they share their designs, you will only talk about the positive things and never be critical. Encourage sharing but be careful not to set the expectation that sharing is somehow associated with completion or success.

- Decide how learners will create their solutions. There are lots of media choices (Word doc, PPT slide, Vizio, or virtual whiteboard, or diagrams.net). If needed you can download the Azure Architecture icons.
- Decide how students will share their solutions. This can include adding their screenshot to chat, verbally discussing their design, sharing a link to diagrams.net, or annotating a whiteboard.
- Use auto check-in of the learners. This will avoid managing the lobby while trying to present or work with small groups.
- Consider creating an aka.ms or bit.ly link to your team's meeting. Paste the link in the chat channel and on your screen share.
- Consider the Cloud Adoption Framework and Well Architected Framework as you design your case study solutions.
- The Fabrikam Residences case study at the end of Day 3 is a broader case study covering several modules.
- Remember the instructor's solution is only a starting point for discussion. The recommended designs are not intended to include all possible variations. Feel free to enhance and change the proposed designs to meet your audience's needs.

Case Study Delivery

You have several choices on how to present the case studies. Your delivery decision will depend on your audience, your technology, and your time constraints. Not all audiences are comfortable working collaboratively.

Generally, there are three ways to deliver the case studies:

- Have the students work individually.
- Have the students work in small groups.
- Lead the students through the case study yourself.

Work individually

Here are some things to consider.

- Students will work at their own pace. This method ensures each person takes part.
- Individuals learn and develop their skills using their own background. skillset, and experience.
- In large classes, it will be difficult to have each person share or review their designs. So, select a couple of learners to present and then ask for differences in other designs.

- Students who have limited experience may struggle without someone else to discuss design ideas.
- Individual work is good for classes that do not like to collaborate or have a culture that does not like to present or share.
- MTTs can ask the students to share the architecture diagram over the chat window and drive discussions using few images if the student strength is more.
- While MTT/learner is presenting the solution, students are encouraged to ask questions.

Work in small groups

This is another delivery style that encourages and builds a learning community. Here are some things to consider.

- This method promotes dialog and cross levels student experience.
- If working individually ask if dividing up into pairs or teams would be acceptable. It is okay if some students want to continue working independently.
- Decide which groups will present their solution. Not every group will have time to present. Rotate the discussion around the groups.
- While one group is presenting, the other groups can ask questions.
- Consider changing the groups to give students a chance to work with others in the class.
- Be sure to set some ground rules for small group work. Here are some suggestions.
  - Let everyone take part. Work as a design team.
  - Choose a way to report your results.
  - Choose a person to fill the role of the scribe.
  - Select someone to present.
  - Consider giving everyone the chance to record or present.
  - Choose the best architecture design out of the several workable options.
  - Be prepared to back up your architectural design with facts.
  - Where the case study isn’t clear, establish some assumptions.
  - Have fun and enjoy everyone’s input.
- Small groups require some way to organize your students. Consider using breakout rooms. Another choice is shared whiteboards.

Using Team Breakout Rooms

A big challenge with small groups is logistics and planning (configuration and communication). If you have Microsoft Teams, the breakout rooms are an effective way to place your students into groups. Here are some considerations.

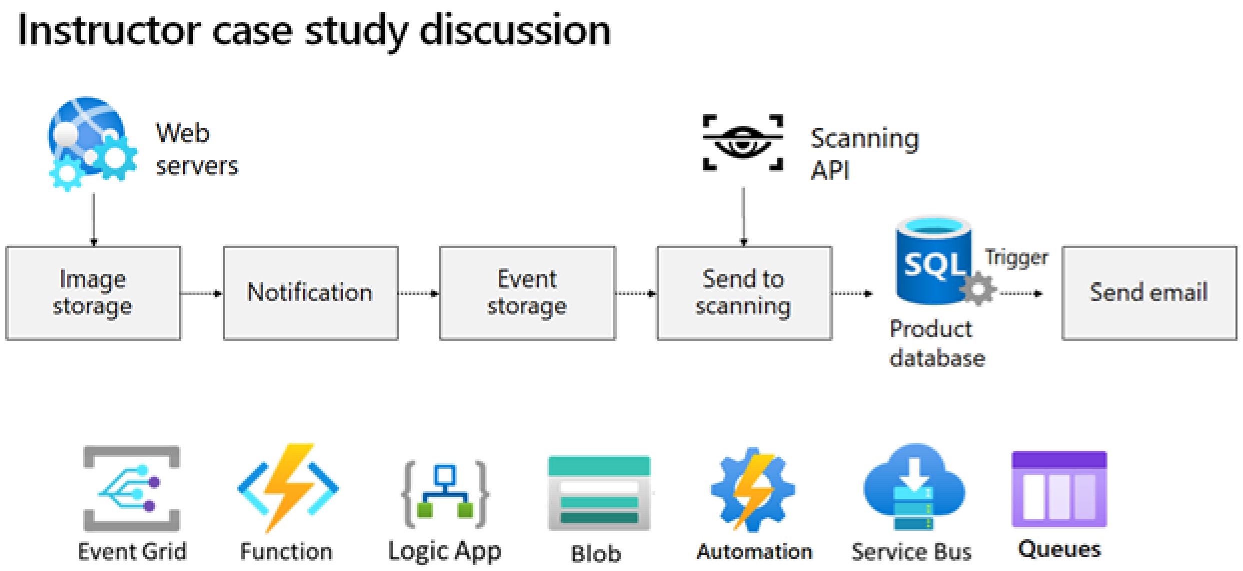
- Use auto assignments so learners will be automatically placed in the rooms.
- Use the broadcast feature to communicate announcements, such as return time.

- Practice joining each room to listen in on the conversations.
- Click close to place everyone back in the main meeting.

Instructor led walk-through

This modality presents an opportunity to help coach your learners on how to build a basic architecture. This modularity requires you to ask questions about the decisions the learners will make. Additionally, it allows the class and you to explore alternative architecture designs and technology.

Some modules have slides that give you the ability to drag and drop Azure icons onto the design as you discuss the choices.



Instructor case study discussion

This modality lets you control the timing of the case study and keep the class on track. We recommend doing the first case study as instructor lead so the students can see and understand the process and expectations. The remaining studies should use other modalities to ensure the student gets the experience necessary to build their own design skills.

Mix and match

You can choose different presentation methods for different case studies. In most deliveries combining different approaches is best. For example,

- Smaller easier case studies are best for individual work.
- Larger complex case studies are more appropriate for small group work.
- Instructor-led case studies help give insight into how you approach a design.

Presentation recommendations are provided for each case study. Feel free to change it up to keep students interested.

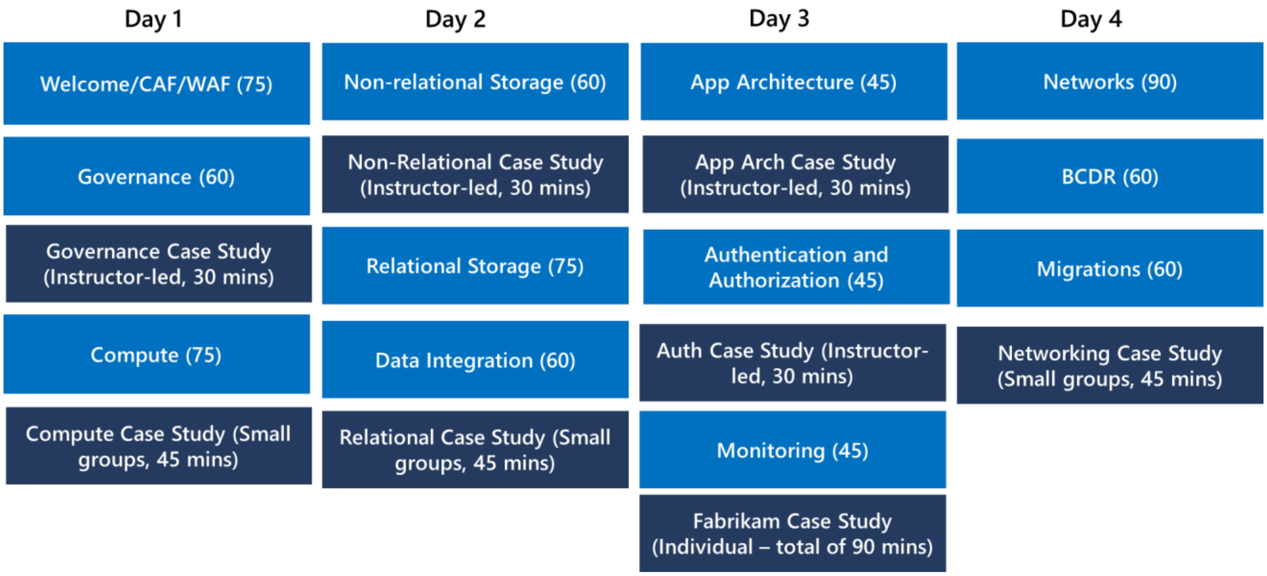
Case Study Timing

Each case study has a suggested length. Your experience may be different. Be sure to manage your time wisely. If you have a choice between extending a case study instead of lecture, try to choose the case study. Let the case studies discussions be a part of the lecture. The case studies have been the most popular part of this course, so make sure to leave time for those activities.

You will need to decide when to do the case studies. This will depend on what works best for your students and your teaching style. There are several strategies:

- Group the case studies at the end of the day.
- Cover the case study directly after the presentation.
- Start the presentation by reviewing the case study. Refer to the case study as you.

A combination of these strategies is best. We recommend creating a course schedule with your plan. Keep your plan flexible, let your students decide the direction.



Day 1	Day 2	Day 3	Day 4
Welcome/CAF/WAF (75)	Non-relational Storage (60)	App Architecture (45)	Networks (90)
Governance (60)	Non-Relational Case Study (Instructor-led, 30 mins)	App Arch Case Study (Instructor-led, 30 mins)	BCDR (60)
Governance Case Study (Instructor-led, 30 mins)	Relational Storage (75)	Authentication and Authorization (45)	Migrations (60)
Compute (75)	Data Integration (60)	Auth Case Study (Instructor-led, 30 mins)	Networking Case Study (Small groups, 45 mins)
Compute Case Study (Small groups, 45 mins)	Relational Case Study (Small groups, 45 mins)	Monitoring (45)	
		Fabrikam Case Study (Individual – total of 90 mins)	

With some case studies, you may run out of time during the delivery day to cover the case. If that happens then you have a few possibilities. You could use the case study as an instructor-led review the following morning. Alternatively, you could assign this as homework then review the following morning. A combination of both would be best - have students think through the case study as homework and then come together for a review in the morning

Design a Governance Solution Case Study

- Recommended Modality: Instructor Led (this is the first case study, and it is important to set expectations and give general guidance on using the case studies.
- Timing: 20-30 minutes

- Link: Design a governance solution

Requirements

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

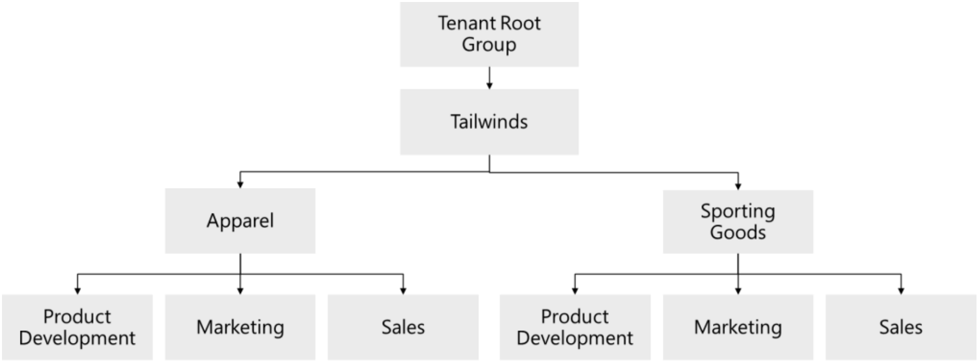
- **Cost and accounting.** Tailwind Traders has two core business units that handle Apparel and Sporting Goods. Each of the business units has three departments: Product Development, Marketing, and Sales. Each business unit and subunit will track their Azure spend. At the same time, the Enterprise IT team will handle 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 the 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 a suitable 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 include 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 is 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

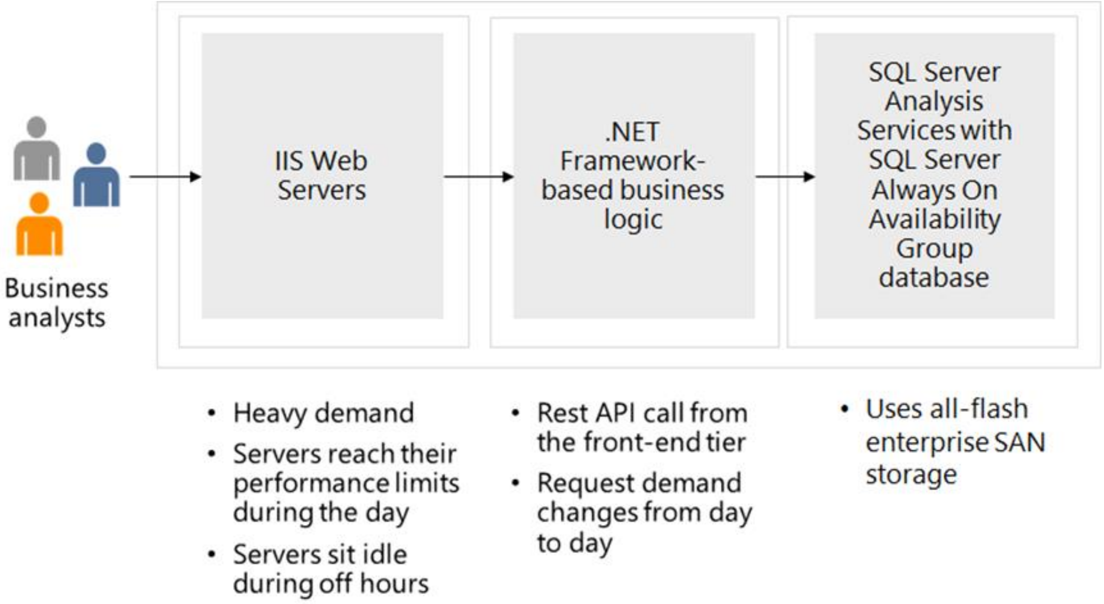
List of built-in policy definitions - Azure Policy

Design Compute Case Study

- Recommended Modality: Small Teams
- Timing: 30 minutes for teams, 15 minutes to discuss
- Link: Design a compute solution

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.


Business analysts
IIS Web Servers
.NET Framework-based business logic
SQL Server Analysis Services with SQL Server Always On Availability Group database
• Heavy demand
• Servers reach their performance limits during the day
• Servers sit idle during off hours
• Rest API call from the front-end tier
• Request demand changes from day to day
• Uses all-flash enterprise SAN storage

- The front-end 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 exceptionally long. Customers are offered email rather than waiting for a representative. But many customers seem frustrated and are disconnecting rather than waiting. 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.

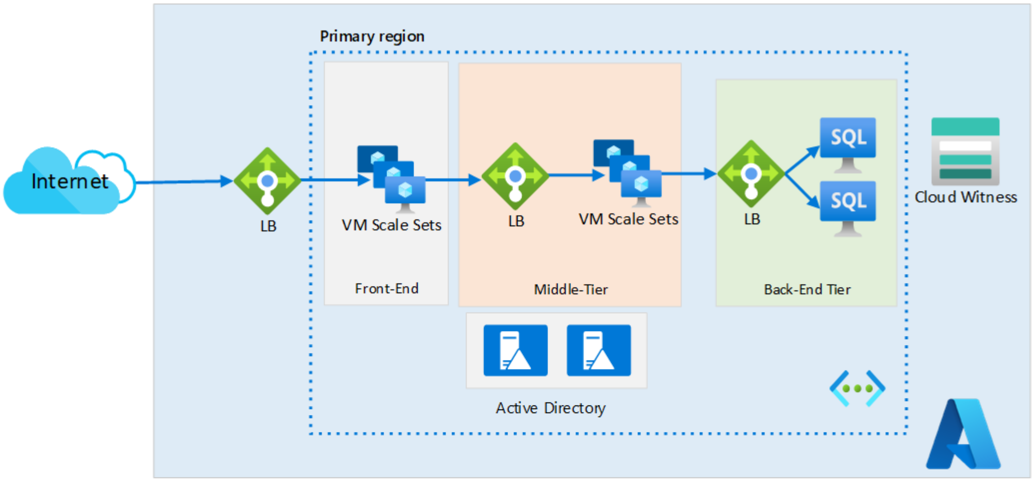
- While high availability is a concern, due to legal requirements the company must keep all the resources in a single region.

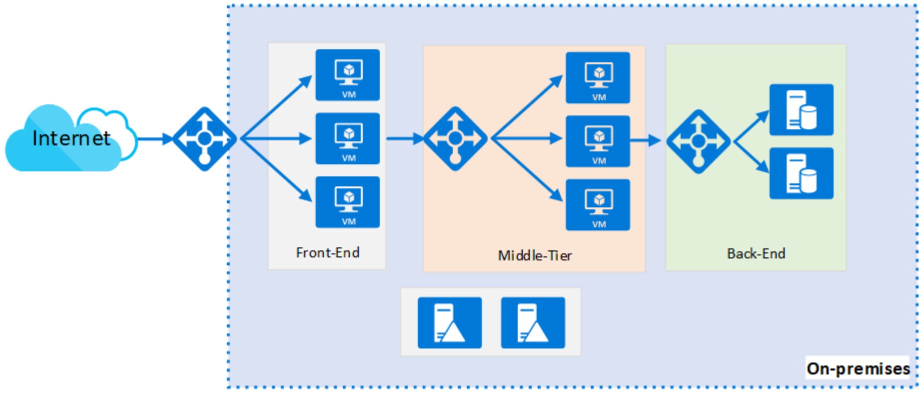
Tasks

- **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.

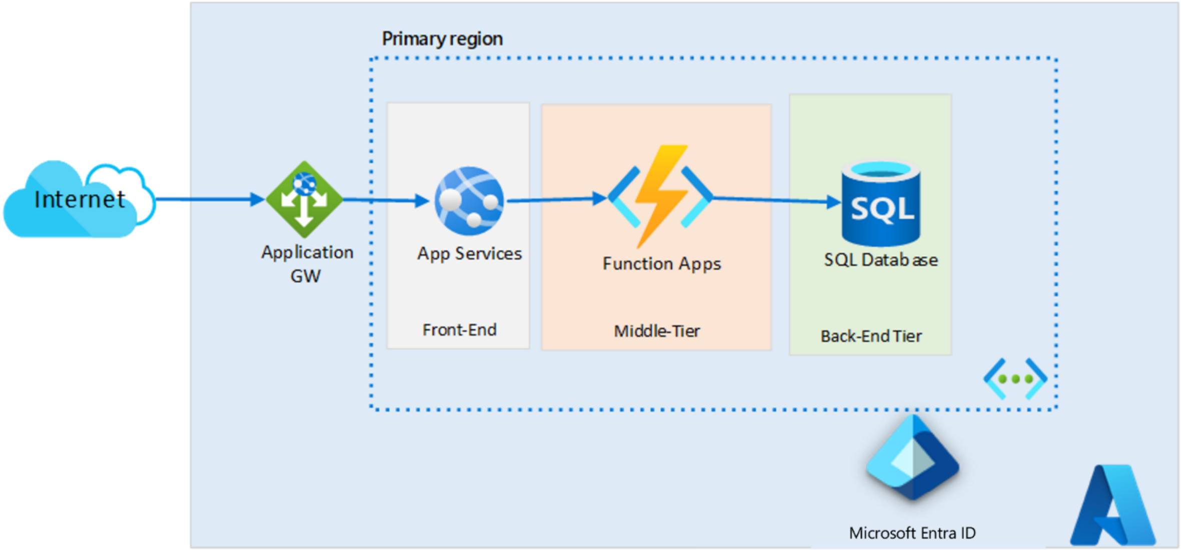
Instructor Solution

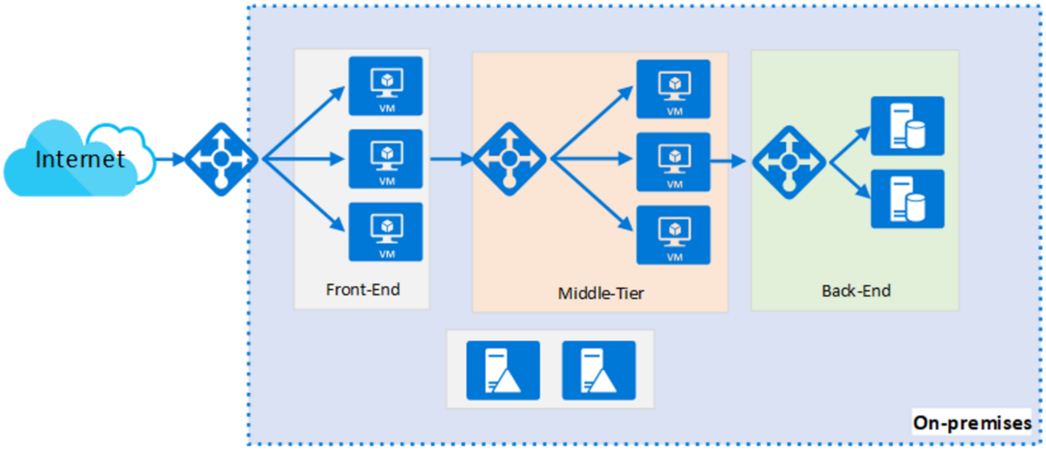
Here is an IaaS solution.





Here is PaaS 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 best 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 supply 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 supporting servers, the cloud infrastructure provides all the up-to-date resources needed
- As requests increase, Azure functions meet 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 are 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 more logging and visualizations of traffic.

Instructor references:

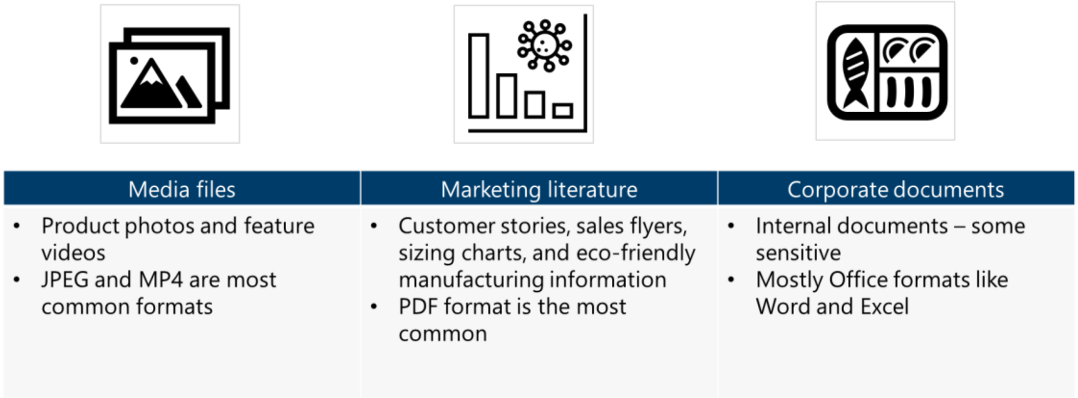
- Integration and automation platform options in Azure | Microsoft Docs
- Compare Azure messaging services - Azure Event Grid | Microsoft Docs
- Choose a compute option for microservices - Azure Architecture Center | Microsoft Docs

Design Non-relational Storage Case Study

- Recommended Modality: Instructor Led
- Timing: 20-30 minutes
- Link: Design a non-relational storage solution

Requirements

Tailwind Traders want 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 supplying 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

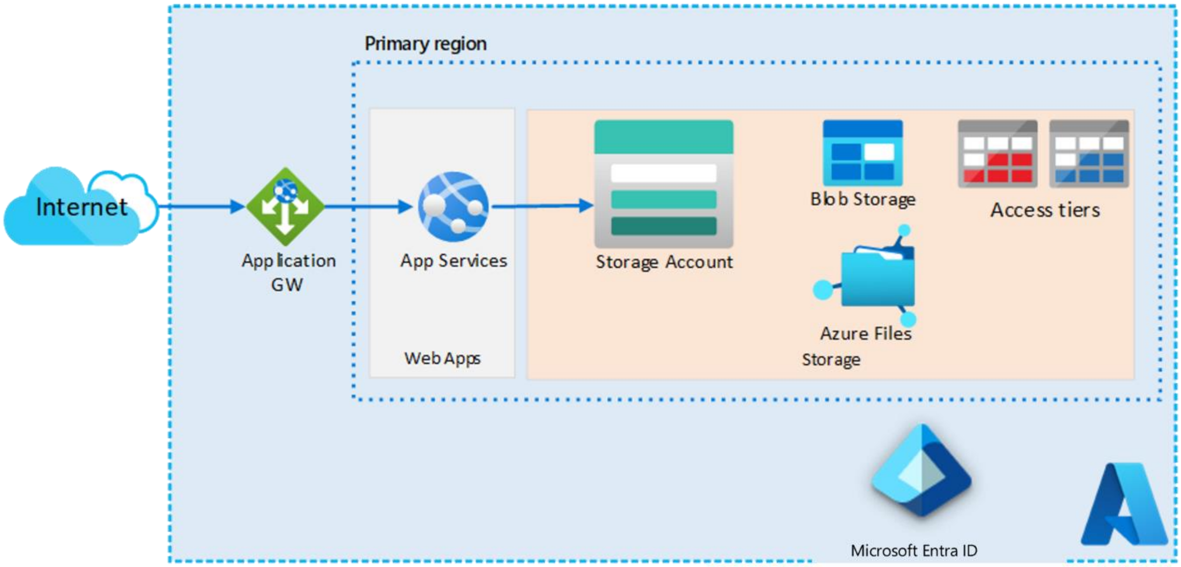
- **Media files**. Media files. Media files include product photos and feature videos that are displayed on the company's public website, which is developed and supported in-house. When a customer browses to an item, the corresponding media files are displayed. The media files are in different formats, but JPEG (Joint Photographic Experts Group) 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 kept for a specific period of time. Occasionally documents will need to be kept 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 central office datacenter. 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.

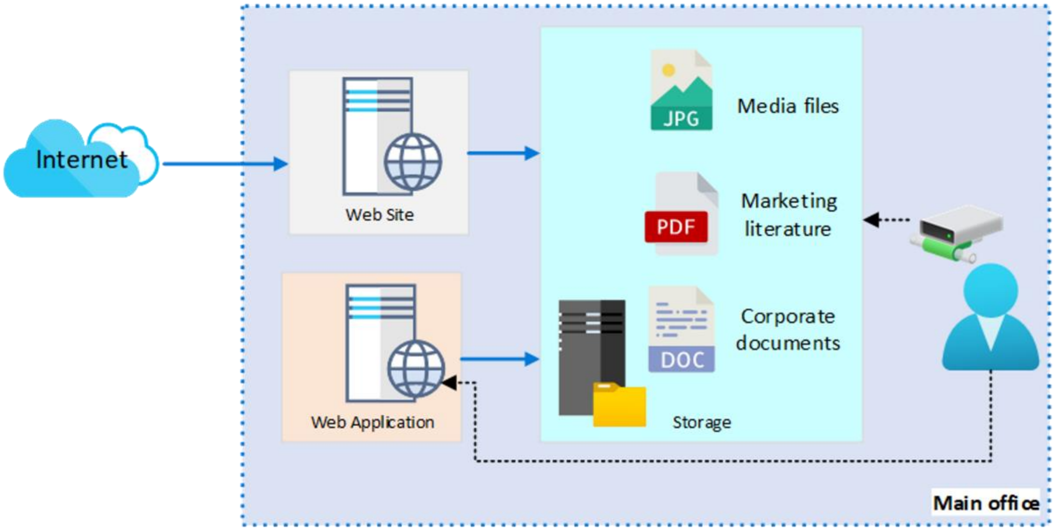
- **File access frequency.** Some products are more popular, and that data is accessed more often. However, some products, like ski gear, are only accessed during that season. Sales events also generate a lot of interest.

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 needed for marketing since the files will be 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's 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 information to decide between Cold and Archive and ask what other questions they may want to ask Tailwind Traders. 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

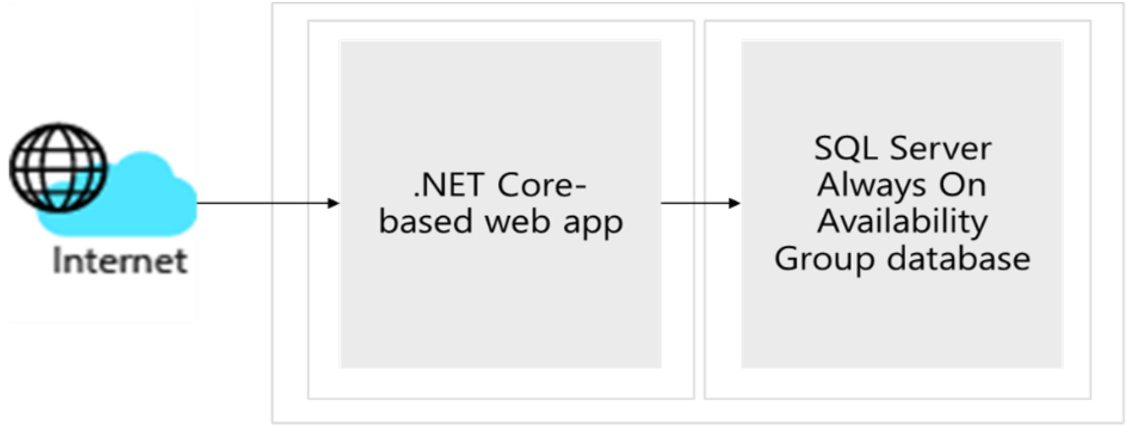
- Security recommendations for Blob storage - Azure Storage | Microsoft Docs
- Introduction to Azure Storage - Cloud storage on Azure | Microsoft Docs
- Hybrid file services - Azure Architecture Center | Microsoft Docs
- Architect storage infrastructure in Azure learning path - Learn | Microsoft Docs

Design Relational Storage Case Study

- Recommended Modality: Small Teams
- Timing: 30 minutes for teams, 15 minutes to discuss
- Link: Design a relational storage solution

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:

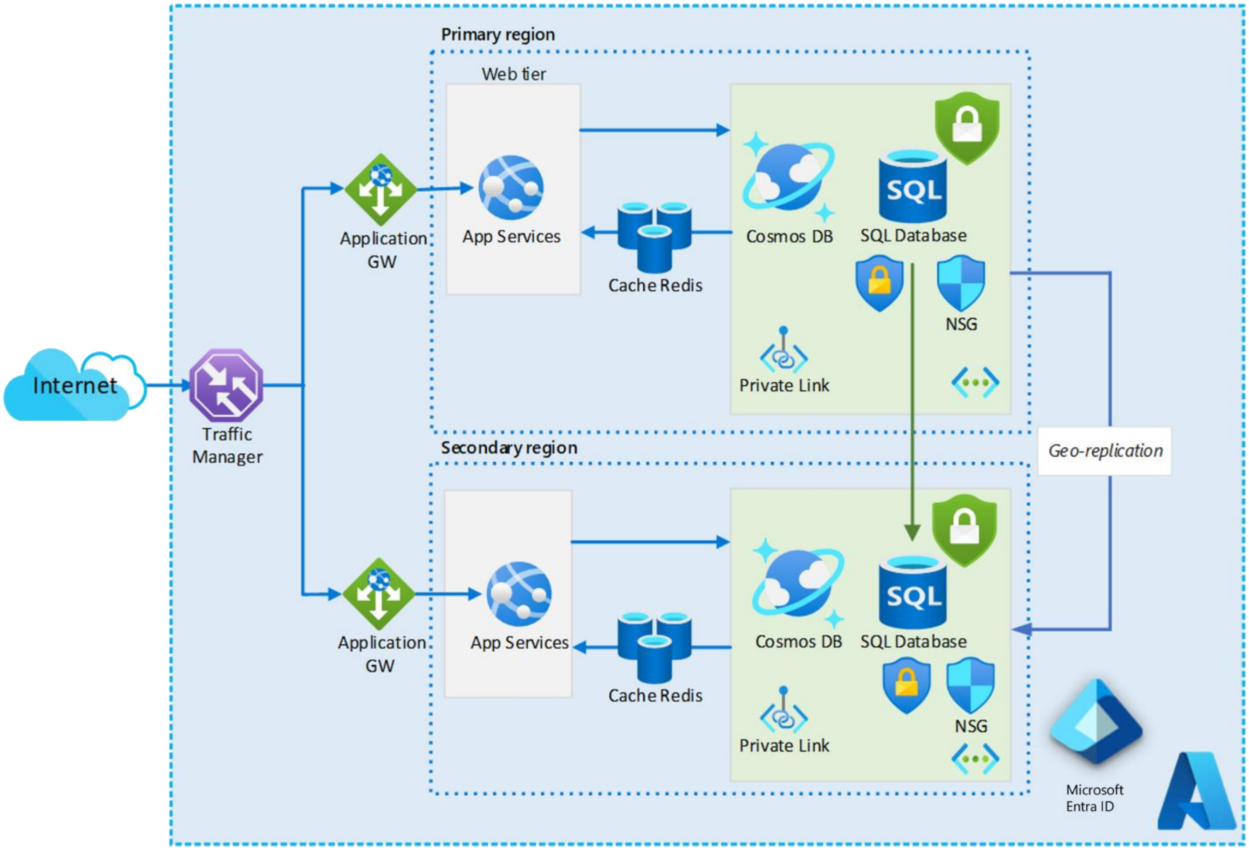
- **High availability.** A primary concern for Tailwind Traders is that this database be highly available. The database is critical to their business. Any outages may result in lost sales or customer confidence.
- **Website performance.** While the performance of placing orders is normally satisfactory, 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 using 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 to reduce the attack surface of the Azure SQL Database, and NSGs may be implemented to implement an added 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 Microsoft Entra ID, 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 needed.
- **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 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

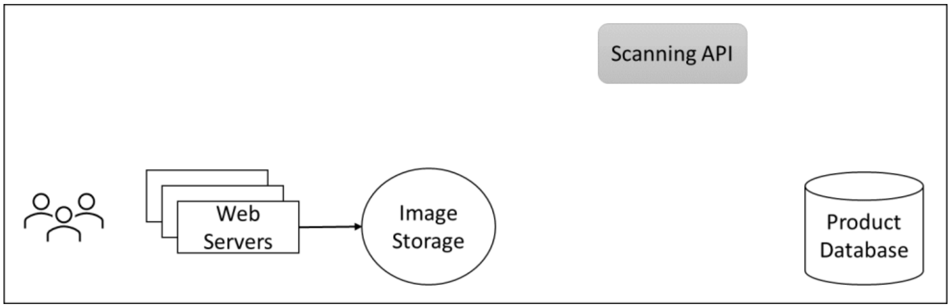
Design Application Architecture Case Study

- Recommended Modality: Instructor Led or Small teams
- Timing: 20-30 minutes (instructor led), Small teams: 30 minutes for teams, 15 minutes to discuss
- Link: Design an app architecture solution

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 buying 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 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.

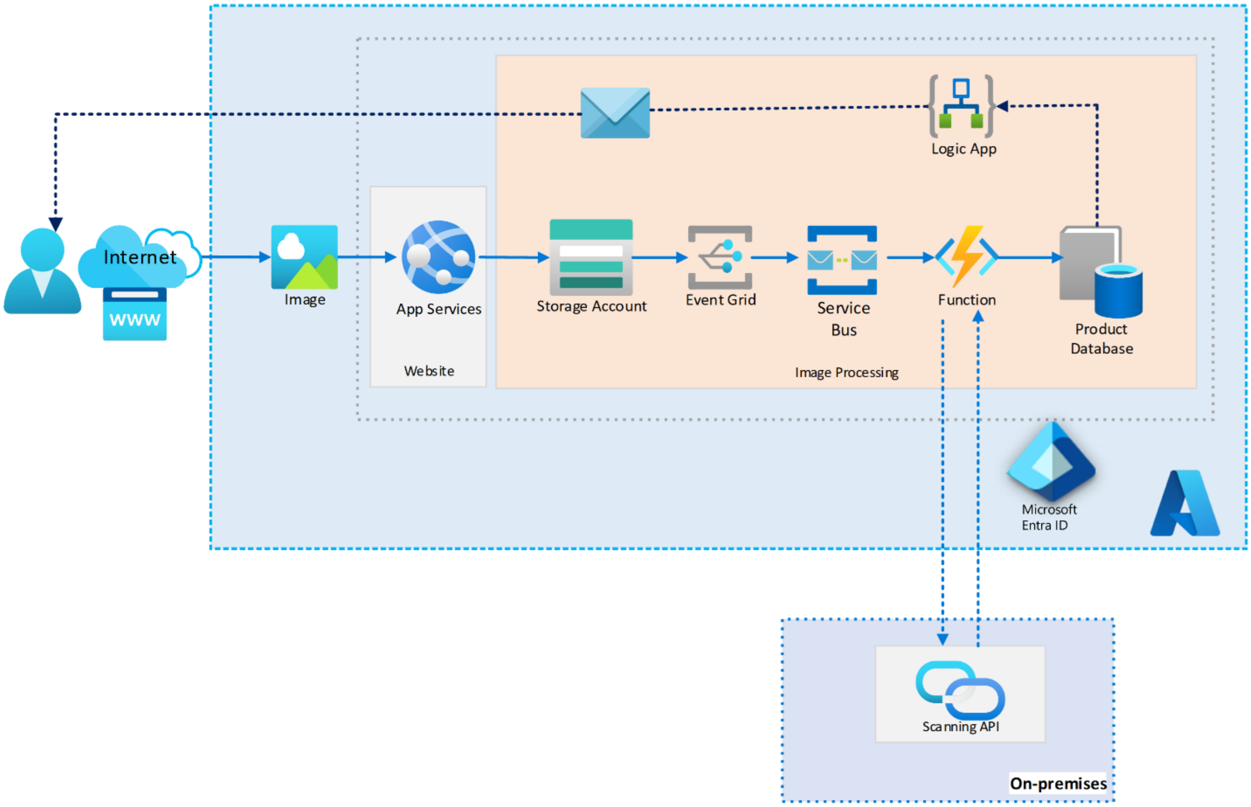


Task

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 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 supply a serverless option to get messages from the queue and send them to the Scanning API for processing.
- Logic Apps supply 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

- Recommended Modality: Instructor Led
- Timing: 20-30 minutes
- Link: Design authentication and authorization solutions

Requirements

Tailwind Traders is doing very well and is expanding their workforce. They have successfully bought an online retailer in the sports apparel space. The company has also found 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 Microsoft Entra identities in the partner's Microsoft Entra 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 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.

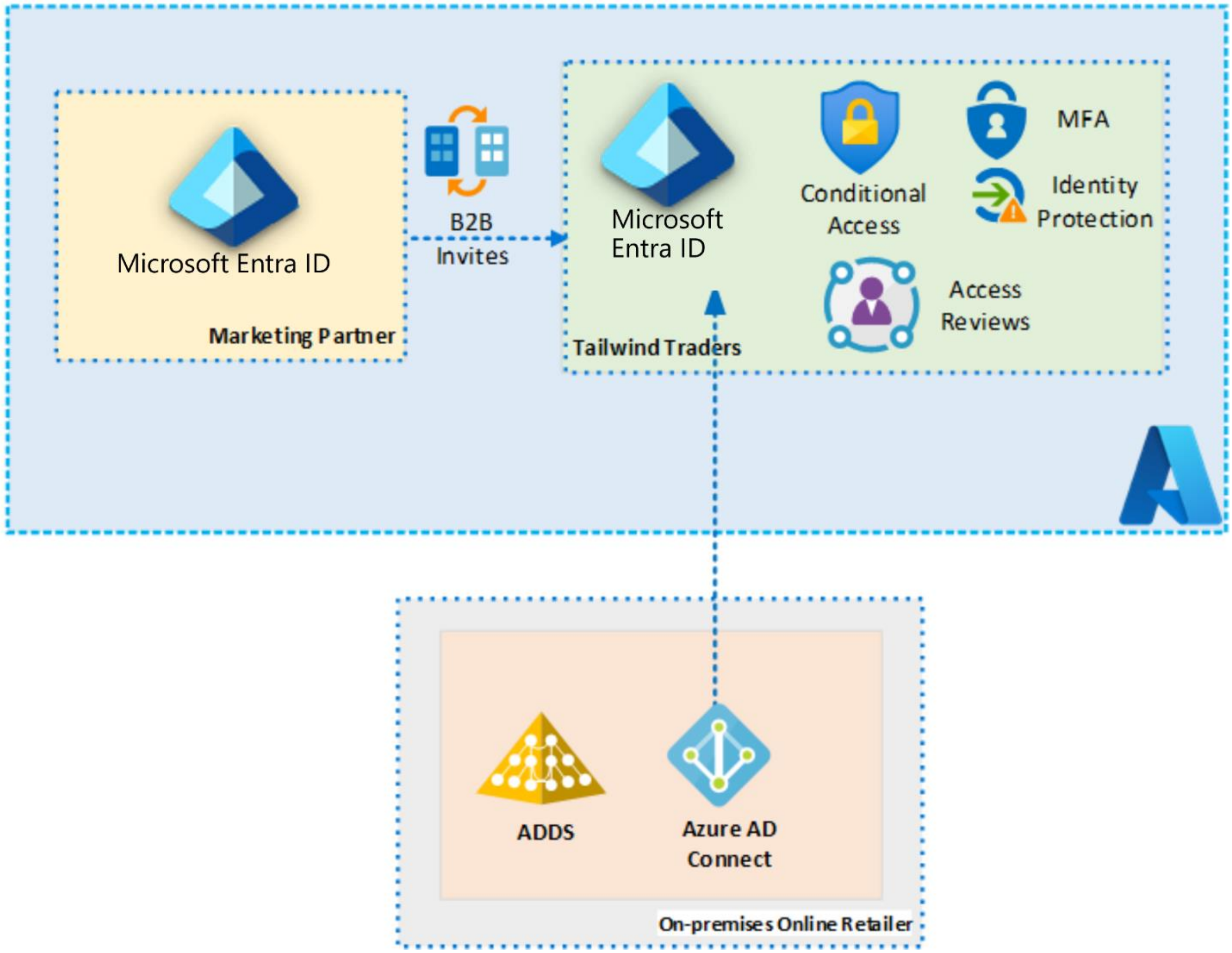
Tasks

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.

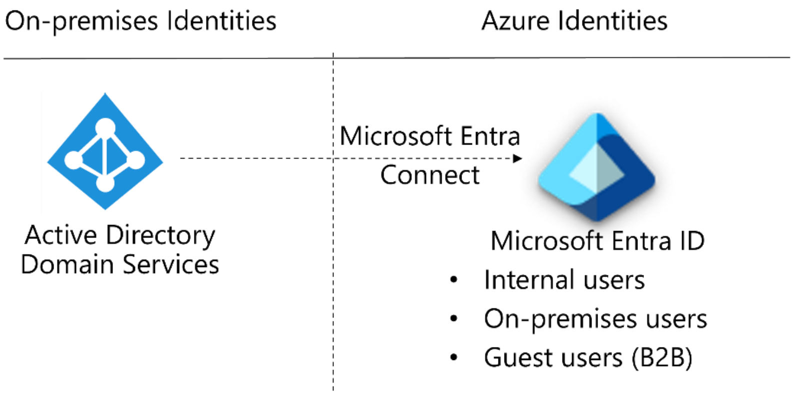
- Provide an access solution for the on-premises resources.

Instructor Solution

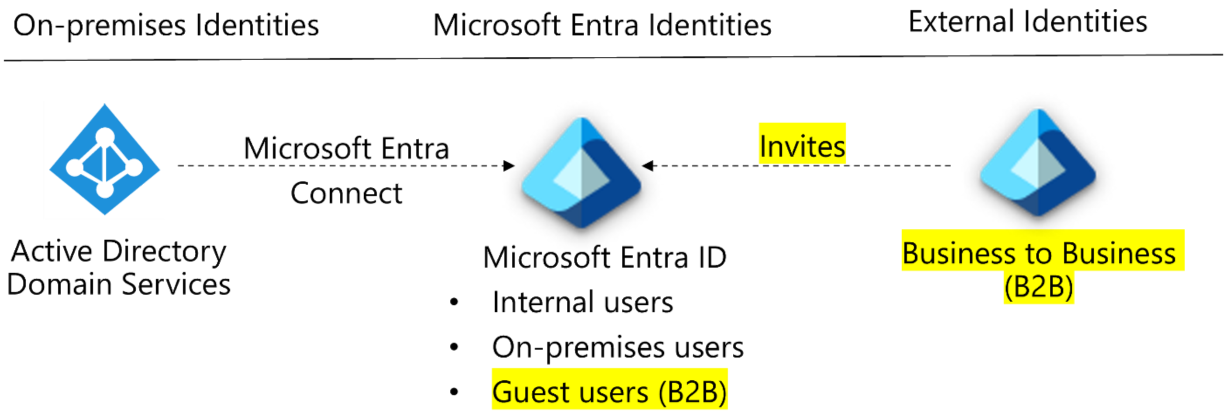
1. New employee user accounts.



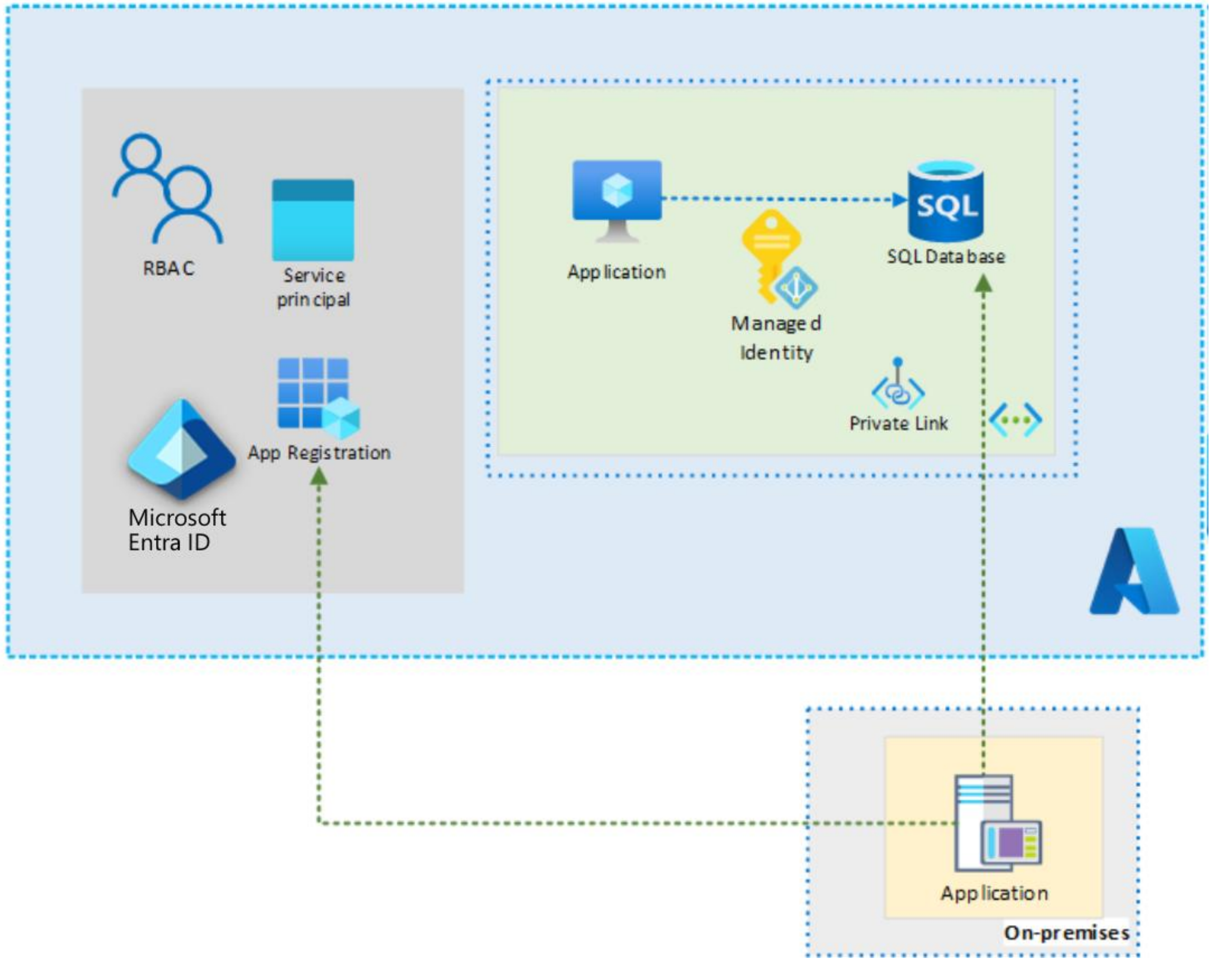
- The on-premises users can be synced using Microsoft Entra Connect. Are new groups needed in Microsoft Entra ID? How will you decide which Microsoft Entra groups to use? Are the permissions for existing groups appropriate? Use password hash for synchronization? Advantages include centralized management, synchronized changes, and ease of administration.



- The partner users can be added using Microsoft Entra B2B. These external identities will be added as guest users. What new Microsoft Entra 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 Microsoft Entra ID authentication, without needing to insert credentials into your code.

- Access solution for the on-premises resources: Register the application with Microsoft Entra ID and assign an application service principal. With Microsoft Entra ID, 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 Microsoft Entra ID 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

Fabrikam Residences Case Study (Capstone)

- Recommended Modality: Read through the case study with your learners then have them do the designs individually.
- Timing: 60 minutes then 30 minutes to discuss.
- Link: Fabrikam Residences

This case study is the only comprehensive case study in the course. This case study is not just for Log and Monitor. This case study falls at the end of Day 3 but could also be used on Day 4. You will want to give the learners about an hour to complete their designs.

This case study gives the learners a chance to put all their learning into a single design. Have your learners do their designs and then share them in the chat. You can talk through the design and focus on the things they have done well. It is a wonderful opportunity to bring all the content together in a single capstone. It is a nice proof to a learner that they can implement what they have learned.

Scenario

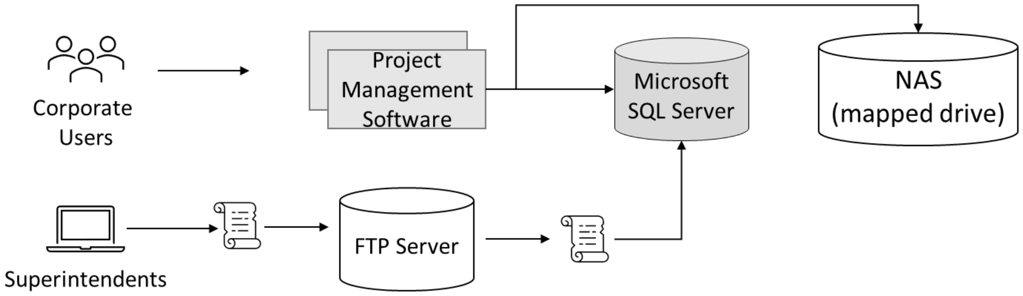
You have taken a new position with Fabrikam Residences, which is very successful and is experiencing rapid growth. Fabrikam Residences is a building contractor for new homes and major home renovations and has become successful by providing quality buildings and offering newer integrated home technologies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

Currently these technologies are provided and managed by separate subcontract 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.

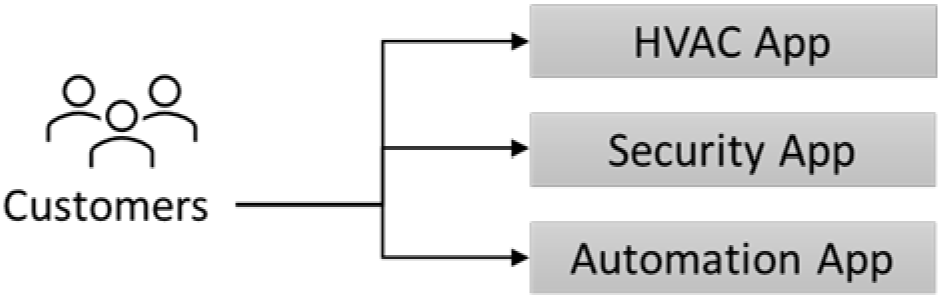
The company has seen tremendous growth over the past 2 years. The company is estimating it may double in size over the next 12-18 months. With such rapid growth in the regional market, the company has no current plans to expand outside of the regional market.

Task 1: The Fabrikam Headquarters runs 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 exists 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 process all the change files and enter their contents into the Project Management database (Microsoft SQL Server).

Task 2: The **Home Technology software** is currently provided and hosted by third parties and involves at least three different websites the customer must visit. It is proposed the software be replaced with an in-house developed and unified solution.



Requirements

Task 1: Project Management software

- Migrate as many of the systems to a public cloud provider as possible.
- Replace the existing scripts to use 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.

Task

- 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.

Task 2: New Home Technology Solution

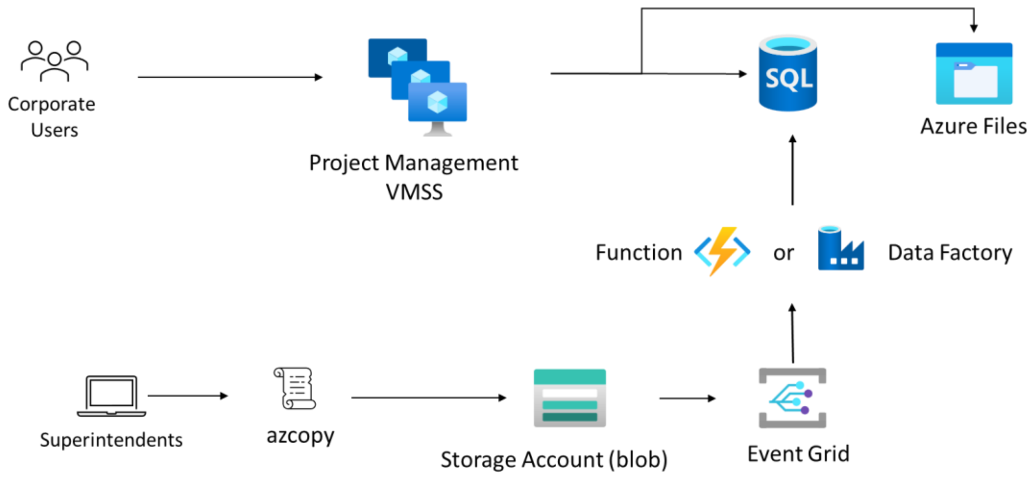
- Add a new solution to collect data continuously from the home monitoring sensors.
    - Database some sensor readings for trend analysis and reporting.
    - Provide configurable real-time alerting based on owner needs.
- Design a relational database solution to hold homeowner preferences and settings.
    - The system must be scalable.
    - Redundancy is critical.
- The new unified website will be developed in-house and hosted on Linux. This website will be used to view monitors and change preferences for items such as temperature or alert thresholds. Loads can vary widely, and the system must be able to scale quickly.
- Provide users with a way to sign into the system without creating another user account and password.
- Implement security controls and provide weekly reports outlining how the company matches up against industry best practices.

Task

- Design an architecture for the New Home Technology Solution. Be prepared to explain why you chose each component of the design and how it meets the solution requirements.

Task 1: 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 determine if that is a choice.
- An Azure SQL Database should be the first choice for the project management database. The general tier does provide some redundancies. If more redundancy is required, the database can be upgraded to the 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.

Task 2: New Home Technology Solution

- **High Availability and Redundancy**. The importance of redundancy is mentioned, but there is a suggestion to specify more details on how to achieve high availability. For instance, Azure SQL Database's built-in redundancy features could be explicitly highlighted, zone-redundancy, geo-replication, etc.
- **Scalability Considerations**. Emphasis is placed on how each component of the solution scales, especially addressing the wildly varying loads mentioned in the case. While scalability for the web application is briefly mentioned, it could be beneficial to elaborate on how AKS or App Service can handle this and provide insights into database scaling plans.
- **Data Privacy and Compliance**. Given the involvement of home monitoring and potentially sensitive user data, it is suggested to address data privacy and compliance concerns explicitly. While Azure services often comply with industry standards, explicitly mentioning this can instill confidence in stakeholders. Utilize Azure Policy to comply with privacy standards, Azure SQL audit and labeling, etc.

- **Monitoring and Logging**. Considerations for monitoring and logging are suggested. Azure Monitor and Azure Log Analytics are recommended for gaining insights into the performance and health of the solution.
- **Cost Management**. Although not explicitly mentioned in the case study, it is suggested to include a brief mention of how cost management will be handled, especially in a scalable environment. The use of Azure Cost Management tools could be considered.
- **Integration with Existing Systems**. If there are existing systems or services that need to be integrated, it is recommended to mention how this integration will be achieved. For example, integrating with existing on-premises systems or other cloud services.
- **Disaster Recovery**. A brief mention of disaster recovery planning is suggested. Azure Backup and Azure Site Recovery are noted as services that can play a role in ensuring business continuity.
- **Documentation and Training**. It is recommended to consider briefly mentioning plans for documentation and training for both the development and operational teams. This ensures that all stakeholders are well-prepared and informed.
- **Event Hubs vs. IoT Hub**. Choosing between IoT Hub and Event Hubs depends on the specific requirements of your use case. Both services offer event streaming capabilities, but they are designed for different scenarios.

  IoT Hub.

  - **Device-to-Cloud Communication.** IoT Hub is specifically designed for bidirectional communication between IoT applications and the devices it manages. It's well-suited for scenarios where you have a lot of IoT devices (sensors in this case) **that** need to send data to the cloud and receive commands or configuration updates from the cloud.
  - **Device Management**. IoT Hub provides features for managing and controlling IoT devices, including capabilities for firmware updates, device twin (to store device metadata and state), and device provisioning.
  - **Security Features.** It includes built-in security features tailored for IoT scenarios, such as device authentication and access control.

  Event Hubs.

  - **General Event Streaming**. Event Hubs is a general-purpose event streaming platform. It is designed for high-throughput, real-time event ingestion and is suitable for scenarios where you need to handle massive streams of events, such as telemetry data.
  - **Scalability**. Event Hubs can handle a lot of events per second and is optimized for scenarios where scalability and throughput are critical.
  - **Integration with Analytics Services.** Event Hubs integrates well with Azure analytics services like Azure Stream Analytics, which can process and analyze the streaming data in real-time.

- **Summary**.
    - If the primary goal is to handle telemetry data from home monitoring sensors and you require bidirectional communication and management of these devices, IoT Hub might be more appropriate.
    - If the focus is on high-throughput event streaming for telemetry data without the need for bidirectional communication and device management, Event Hubs could be a suitable choice.
    - It's worth noting that the choice between IoT Hub and Event Hubs can depend on the specific requirements and constraints of your solution, including what services it should be integrated with, and in some cases, a combination of both services may be used to meet different needs within the architecture.

Networking Case Study

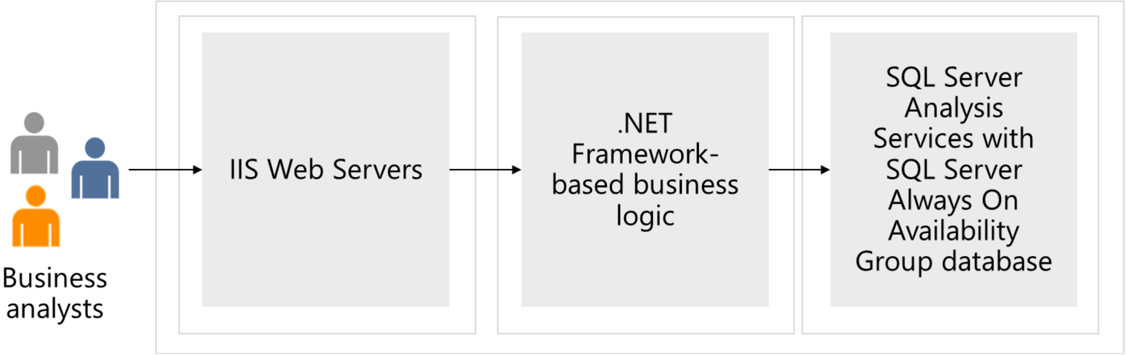
- Recommended Modality: Instructor Led or small teams
- Timing: 20-30 minutes, small teams: 30 minutes for teams, 15 minutes to discuss
- Link: Design a network solution -BI enterprise application
- **Note:** You may consider doing this as instructor lead because it is on the last day of class.

Requirements

As the Tailwind Traders Enterprise IT team prepares to define the strategy to migrate some of the company’s workloads to Azure, it must identify the required networking components and design the 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 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


Business analysts
IIS Web Servers
.NET Framework-based business logic
SQL Server Analysis Services with SQL Server Always On Availability Group database

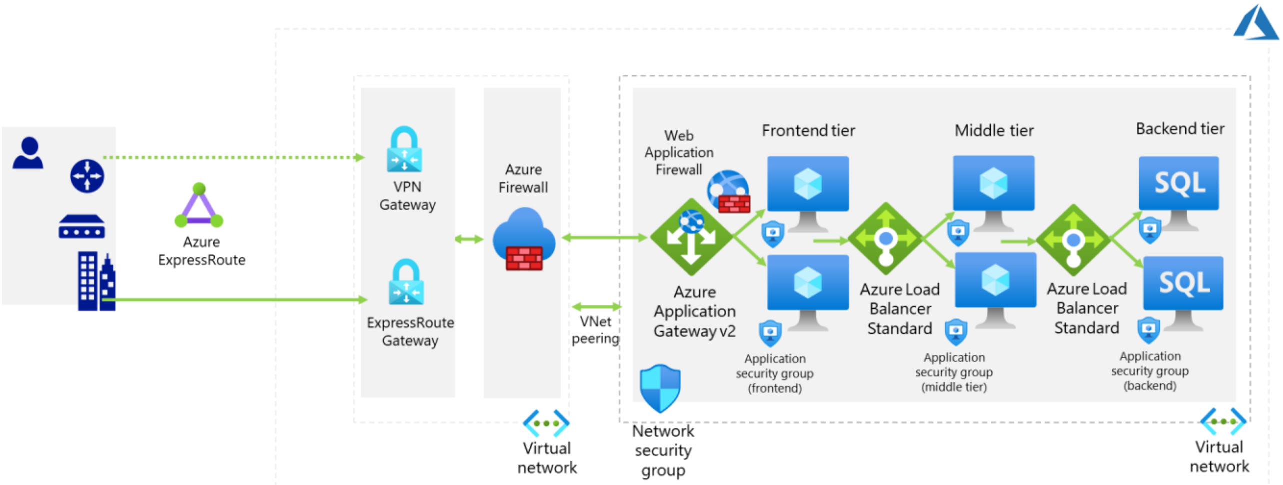
- An internal, Windows-based, three-tier business intelligence (BI) enterprise application with the front-end tier running IIS web servers, the middle tier hosting .NET Framework-based business logic, and the back-end tier implemented as a SQL Server Always On Availability Group database.
- This application 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 decided that 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 other 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 needed 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 needed 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 part of the solution.
- Based on your architect solution from the compute case study how would this affect the network design? Would you need any other 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 database 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.


Azure ExpressRoute
VPN Gateway
ExpressRoute Gateway
Azure Firewall
VNet peering
Virtual network
Web Application Firewall
Frontend tier
Middle tier
Backend tier
SQL
SQL
Azure Application Gateway v2
Azure Load Balancer Standard
Azure Load Balancer Standard
Application security group (frontend)
Application security group (middle tier)
Application security group (backend)
Network security group
Virtual network

- 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 do 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 setting up 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]