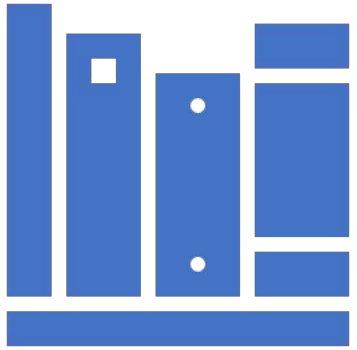


Cloud Infrastructure Architecture for MultiSoftware Enterprise

Transitioning On-Premises Infrastructure to Microsoft Azure

Team Members: Gialama Alexandra, Papadopoulou Eleni, Valsami Anna F. , Veskou Maria

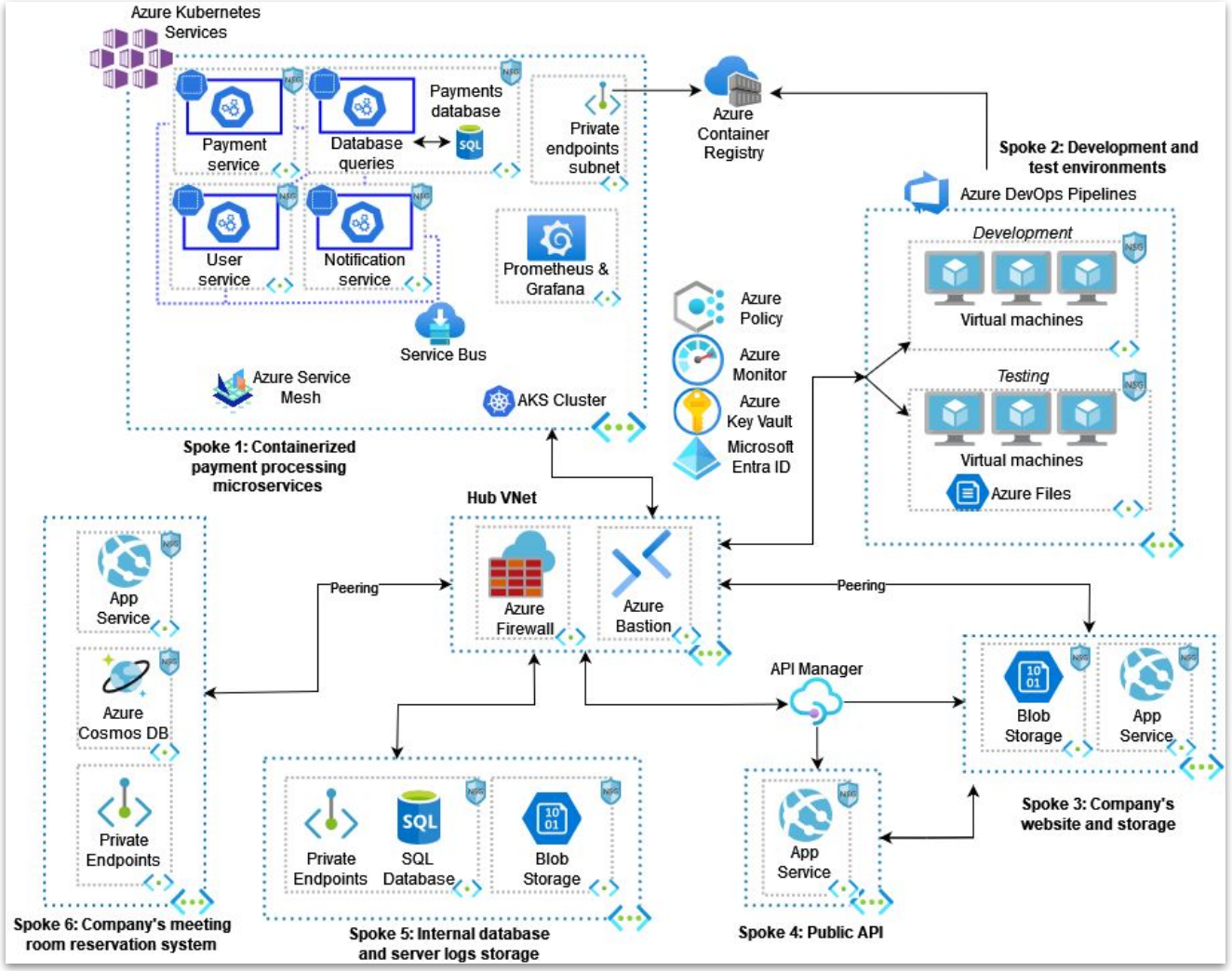
July 26, 2024

Architecture Diagram

1 Hub Virtual Network

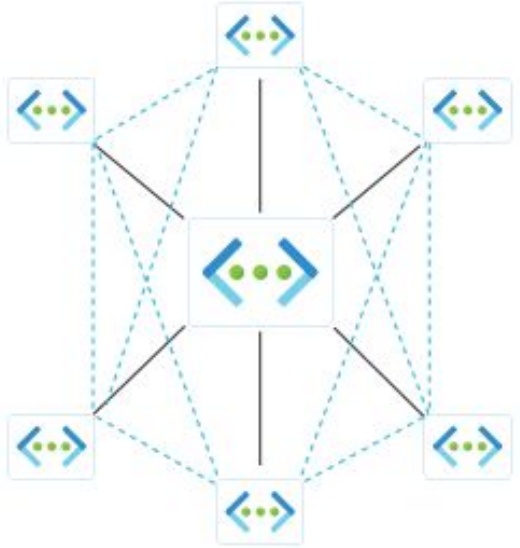
6 Spoke Virtual Networks

All services and resources were deployed in the North Europe region due to the stability and the variety of supported features.



Hub-and-Spoke Topology

- Offers centralized control over connectivity: selective connectivity between spokes and isolation of certain environments.
- Access to shared services placed in the hub virtual network.
- Cost efficiency: Centralized services in the hub can be shared across multiple spokes, reducing duplication and overall costs.
- Fault isolation: Failures in one spoke do not necessarily affect other spokes or the hub, enhancing the overall resilience of the system.



- The creation of a Hub and Spoke topology in Azure Portal requires a Network Manager instance and the definition of network group members to create the corresponding connectivity configuration.

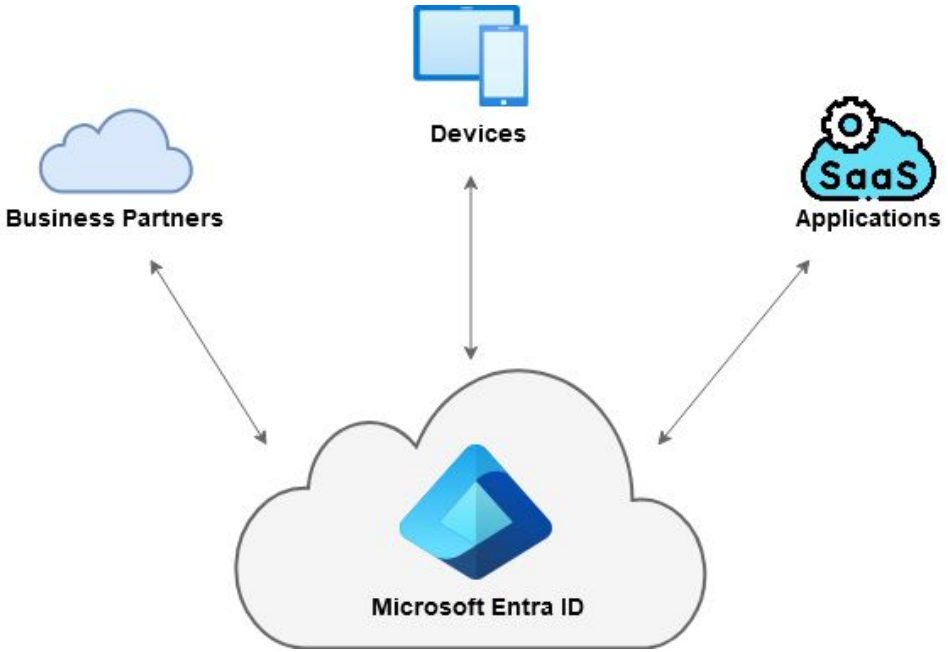
Network Security & Traffic Management

1. Virtual Network Peering: Create peering connections between
   - The hub and the spokes
   - “Spoke 3: Company’s Website and Storage” and “Spoke 4: Public API”.

2. Azure Firewall Policy Rules:
   - **DNAT Rules:** Forward traffic from a public IP address (assigned to Azure Firewall in the hub) to the private IP addresses of the website in the spoke 3 and API in the spoke 4.
   - **Network Rules:** Allow traffic from hub to spokes, from spokes to hub, from the public website to the public API and from the public API to the public website, deny traffic from the internet to the internal database etc.
   - **Application Rules:** Allow DevOps resources in “Spoke 2: Development and test environment” to access GitHub and Azure DevOps.

3. Network Security Groups (NSGs): Create inbound security rules in the NSGs associated with the subnets in the spoke VNets.

Authentication & Authorization



- Premium P1 tier was used for all Microsoft Entra ID settings.
- Set up an Microsoft Entra tenant and bulk import all company employees using a CSV file to create user accounts efficiently.
- Configure Single Sign-On (SSO) for Office 365 and other applications to streamline user access. Assign licenses to users to enable service access.
- Set up Self-Service Password Reset (SSPR) to allow users to manage their own passwords securely.

Authentication & Authorization

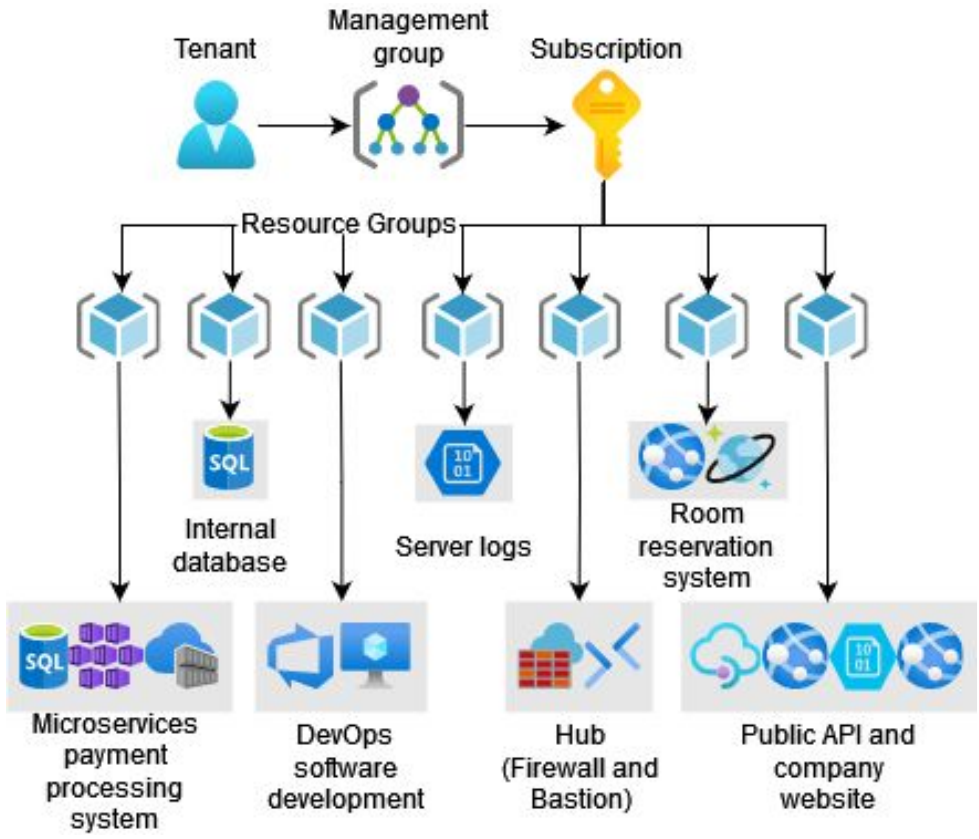
- For the users, the company’s office IP ranges will be added as trusted locations, and a Conditional Access policy will be created. The policy will be applied to all users and all cloud apps, configuring to include all locations and exclude the trusted locations. Multi-factor authentication will be required for access (Password & SMS).

- A Conditional Access policy should be created and applied to a group based on directory roles with administrative privileges for all cloud apps. In addition, access control should be set to require multi-factor authentication (Password & Windows Hello).

- Ensure that the laptops are running either Windows 10 or 11 Pro, Enterprise, or Education. Once this has been done, the devices must be joined to Entra ID by entering the users' Office 365 credentials.

Resource Groups

- One tenant, management group and subscription for the organization
- Resource groups isolate the hub and spokes further



User Role Permissions

- We defined roles for developers and administrators through the Role-based Access Permission (RBAC) Azure service.

- Developers can:
  - Read all resources → */read action
  - Edit resources → Relevant DataActions enabled

- Administrators can:
  - Read and create all resources
    → */read and */write actions
  - Edit them → Relevant DataActions enabled

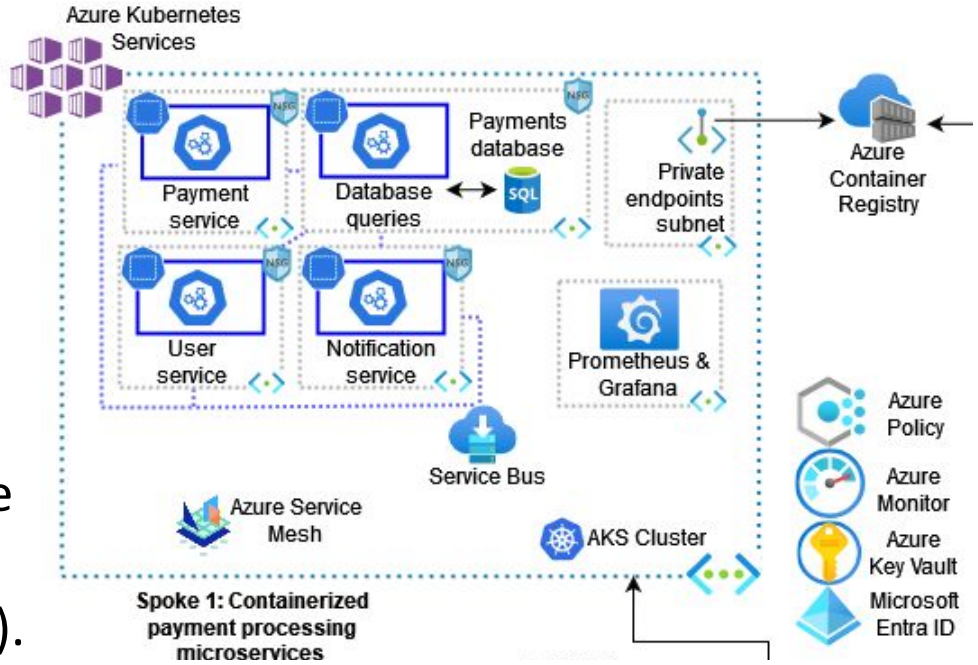
- Assign the roles to users or groups.

```
"permissions": [
  {
    "actions": [
      '*/read',
      '*/write'
    ],
    "notActions": [],
    "dataActions": [
      'Microsoft.Compute/*',
      'Microsoft.Cdn/*',
      'Microsoft.Network/*',
      'Microsoft.Storage/*',
      'Microsoft.DomainRegistration/*',
      'Microsoft.CertificateRegistration/*',
      'Microsoft.ContainerRegistry/*',
      'Microsoft.ContainerService/*',
      'Microsoft.Cache/*',
      'Microsoft.DocumentDB/*',
      'Microsoft.Sql/*',
      'Microsoft.Purview/*',
      'Microsoft.ApiManagement/*'
    ],
    "notDataActions": []
  }
],
```

Microservices Payment Processing System

We chose to use Azure Kubernetes Services (AKS) for this application.
We separated the microservices payment processing into 4 assumed service modules:

- Payments service
  - Payment processing functions
- User service
  - User login, authentication, registration
- Notification service
  - Alerts and messages sent to the users
- Database service
  - Communication with the transactions database



Networking:

- Use of Azure CNI Node Subnet (Azure network policy).
- The AKS cluster is set as private, in an isolated spoke.
- The microservices are in separate subnets and namespaces.
- There is a subnet for Private Endpoints and another for Prometheus/Grafana.
- The payments SQL database is placed in the database service subnet.

Microservices Payment Processing System

Communication between the microservices:

- Azure Service Bus
  - Handles asynchronous calls to the services and ensures reliable delivery
  - Decoupling of services and scalability
  - Encryption of messages on transit and at rest
  - Advanced messaging features

- Azure Open Service Mesh
  - Automation of service communication management, traffic control
  - Built-in mTLS (mutual Transport Layer Security) → security, control
  - Metrics for service interactions
  - Seamless integration with AKS

Microservices Payment Processing System

- We selected the Premium pricing tier as it offers 2 years of support.
- Availability: North Europe location, 3 availability zones
- Authentication/authorization
  - Microsoft Entra ID (system-assigned managed identity), RBAC
- Separate node pools
  - Database service node pool: memory-optimized VMs (Standard_E4s_v5)
  - Payment service node pool: high-performance VMs (Standard_D4ps_v5), 3-20 nodes, 30 pods per node max
  - Other services: Standard_D4ps_v5, 1-10 nodes, 20 pods per node max
- Monitoring Services: Container Insights, Managed Prometheus, Managed Grafana
  - They give us the ability to monitor the AKS cluster performance and resource demand, in order to make adjustments and up/down-scaling as needed.
- Alerts are activated, to prevent system failure and payment function halt
- Node images are stored in an Azure Container Registry instance

Development & Testing Environments

- We created a separate Spoke for this application.
  - There is one subnet for the development environment and one for testing.
  - Users are redirected to their appropriate VM initially through the Azure Bastion in the hub and then via subnet NSGs.
- Users connect via their Microsoft Entra ID identity and according to their role permissions.
- The testing environment includes a shared file system, supported via an Azure Files instance.
- The development and testing environment can be integrated with Azure DevOps Pipelines, to ensure automated deployments, scalability, efficiency and enhanced security.
- The DevOps environments are connected to Azure Container Registry, to ensure CI/CD workflows with service images used in the microservices payment processing system hosted in the AKS cluster.

Data Regulation Compliance

As the company is located in Greece and has customers and website viewers in Europe, the data processing in our system must be GDPR-compliant. We achieve this as follows:

- Resources are created in North Europe, with availability options set to West Europe.
- Data stored in the architecture is encrypted on transit and at rest, when possible.
- Microsoft Entra ID and Role-based Access Control are used to ensure appropriate user permissions.
- Use of Azure Monitor to track and log data access.
- Assignment of Azure Policies to ensure continued data regulation, for example:
  - Allowed locations (new resources are created within Europe)
  - Transparent Data Encryption on SQL databases should be enabled (data encryption)
  - API Management secret named values should be stored in Azure Key Vault (control access)
  - Key Vault secrets should have an expiration date (security)
  - Azure SQL Database should have Microsoft Entra-only authentication (control access)
  - Configure Container registries to use private DNS zones (security)
  - Azure Managed Grafana workspaces should disable public network access (control access).

Company’s Internal Database

- Azure SQL Database was chosen for the company's internal database for its performance, scalability, and managed services.
- A private endpoint was used to ensure secure access within the internal network
- Geo-redundancy was implemented with the primary region in North Europe and redundancy in West Europe to guarantee data availability and durability across multiple regions.

  This setup offers a secure, reliable, and efficient solution for managing critical data.

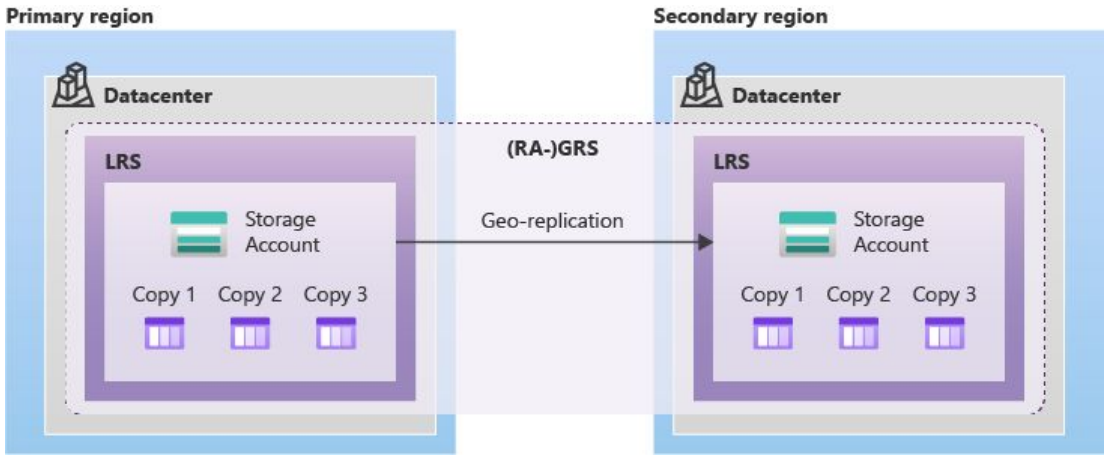


Image credit: Microsoft Corporation

Meeting Room Reservation System

- Azure Cosmos DB is chosen for the meeting room reservation system due to its:
  - Global distribution
  - Low latency
  - Scalability

- Azure Cosmos DB provides global distribution, ensuring low-latency data access and high availability. This makes it ideal for a meeting room reservation system used by employees in different locations.

- Cosmos DB is highly scalable. This ensures that the database can handle increasing amounts of data and higher request volumes seamlessly.

- Hosting the API with Azure App Service
  Azure App Services was chosen because it provides a managed, scalable, and secure environment for hosting the API, along with integrated monitoring

Server Logs - Lifecycle Management Policy

- To efficiently manage and store detailed server logs, Azure Blob Storage has been configured with geo-redundant storage (GRS) to ensure high availability and durability.
  - Network Security: Public access is disabled to ensure data is only reachable via private network connections.
  - Data Protection: Soft delete is enabled to recover accidentally or maliciously deleted blobs.
  - Encryption: Data is encrypted using Microsoft-managed keys, with support for customer-managed keys if needed

It uses a lifecycle management policy that automatically moves data from the Cool tier to the Archive tier 30 days after modification. This policy helps optimize storage costs by keeping frequently accessed data in the Cool tier and transitioning older, infrequently accessed data to the more cost-effective Archive tier for long-term storage.

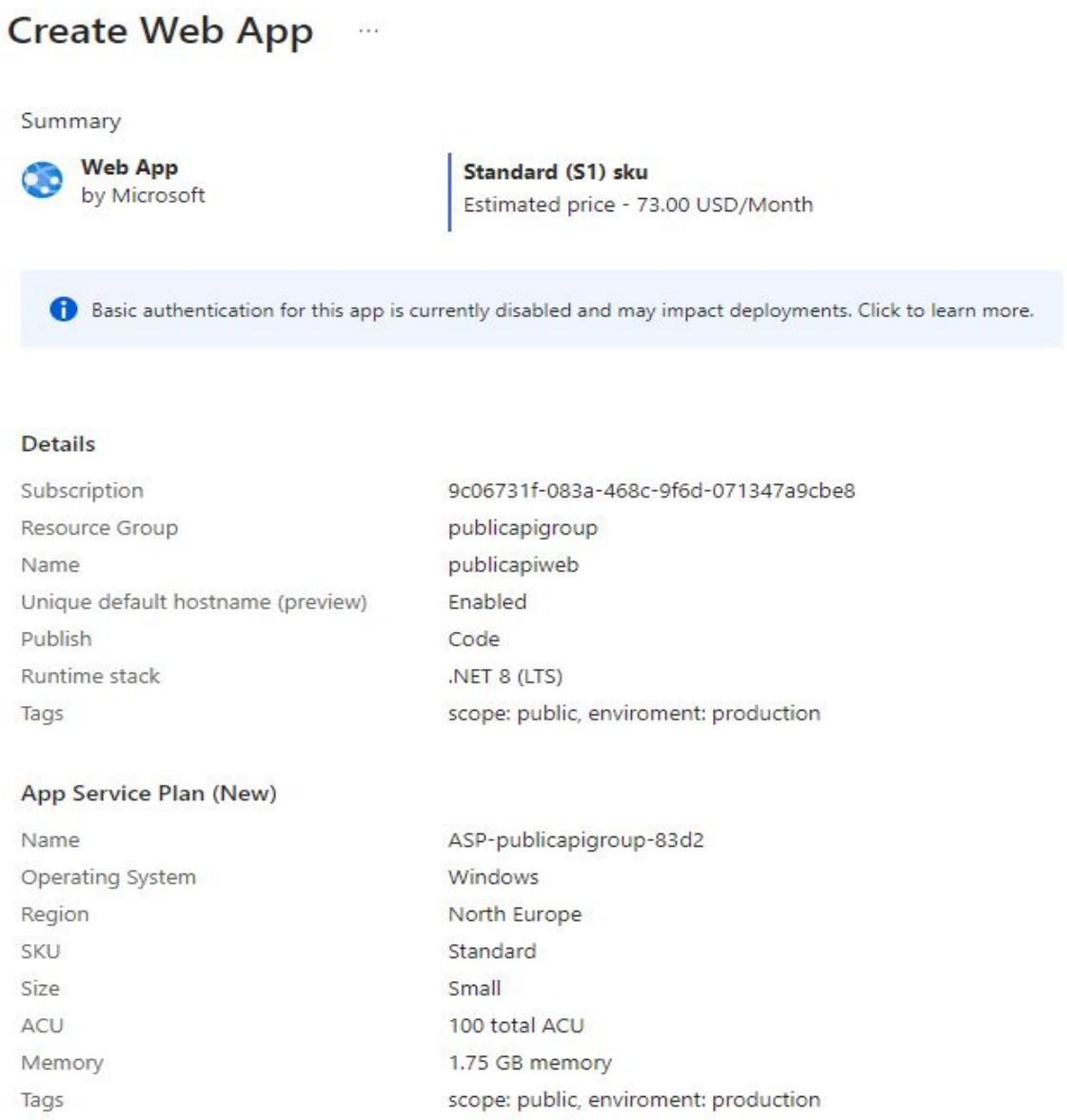
Company’s Website & Storage

- Azure App Services → Web App (Hosting)
  - Dedicated Hosting: Stable and Reliable Performance, Exclusively Available for Customer Use
  - Runtime Stack .NET 8.0: The most up-to-date performance improvements, security enhancements, and new features, that make developing and running applications more efficient and flexible.
  - Pricing Plan Premium V3 P1MV3: Serve the needs comfortably while providing reliability and scalability.

- Azure Storage Account → Blob Storage
  - Performance Standard general-purpose v2: Adequate for the given requirements.
  - Azure Blob Storage: Hot Tier
  - Block Blobs: Suitable for unstructured data, providing high scalability

Company’s Public API

- Azure App Services ⟶ Web App
  - Additional Functionality: The reliability, efficiency and robustness are ensured.
- API Management
  - The traffic is routed, depending on the type of requests, regarding the Company’s Website or the Public API.
  - Tier: Standard v2 (SLA) 99.95% - Unit: 1



Key Vault

- Unique entity in our topology (centralized encryption).
- Secure storage and access to secrets of Kubernetes and Databases (API keys, passwords, certificates, or cryptographic keys).
- Connection via Managed Identities and RBAC.

Image Reference

Billing

- Estimated total monthly cost: €15,489.09
  - Cost analysis through Pricing Calculator
  - Minimize the cost by choosing the Azure Hybrid Benefit

- Monthly cost with additional services: €20,822.65
  - VMs (developing): D4s 8 vCPUs, 26 RAM
  - Microsoft Defender
  - SQL Database for company's website (metadata for files)

Image Reference

Further Work Ideas

- Adopt a Content Delivery Network to significantly improve website performance and the experience of users around the world.
- Deploy the Hub Network across multiple regions to ensure that if one region fails, others can continue to function. Additional we could enrich the Hub with other safety nets (VPN Gateway).
- Use of Microsoft Defender, for company’s internal DB, as an extra layer of security (threat detection).
- Further measures for data regulation via Microsoft Compliance/Purview.
- Use of Service Health alerts for maintenance awareness and incident management.

Project Management

Image Reference

Communication Tools:

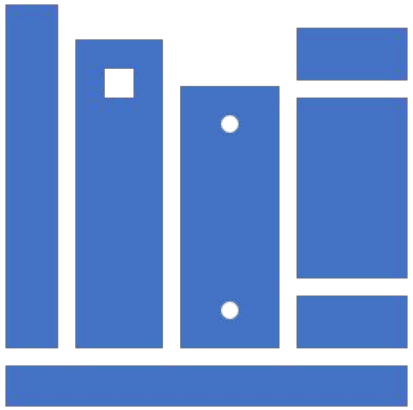
- Microsoft Teams: Announcements, scheduled meetings and video conferencing
- Trello Workspace: Project organization and knowledge sharing
- Monday Project Management: Task and time management
- GitHub: Version control

Bibliography

1. Connectivity configuration in Azure Virtual Network Manager | Microsoft Learn
2. Hub-spoke network topology in Azure - Azure Architecture Center | Microsoft Learn
3. Create a hub and spoke topology in Azure - Portal | Microsoft Learn
4. Data redundancy - Azure Storage | Microsoft Learn
5. Deploy Start/Stop VMs v2 to an Azure subscription | Microsoft Learn
6. Understand Azure role definitions - Azure RBAC | Microsoft Learn
7. Create or update Azure custom roles using Bicep - Azure RBAC | Microsoft Learn
8. Azure Firewall policy rule sets | Microsoft Learn
9. Azure network security groups overview | Microsoft Learn
10. Azure virtual network traffic routing | Microsoft Learn
11. Create or update Azure custom roles using the Azure portal - Azure RBAC | Microsoft Learn
12. API change log for Microsoft.Authorization deployment resource types - Bicep, ARM template & Terraform AzAPI reference
13. API versions of Azure RBAC REST APIs | Microsoft Learn
14. Implement multifactor authentication (MFA) Training | Microsoft Learn
15. Microsoft Purview compliance portal
16. Add or edit Azure role assignment conditions using the Az
17. Create node pools in Azure Kubernetes Service (AKS)
18. Open Service Mesh (OSM) add-on in Azure Kubernetes Service (AKS)
19. Azure Container Registry service tiers
20. Azure API Management - Overview and key concepts | Microsoft Learn

Bibliography

21. Upgrade and scale an Azure API Management instance | Microsoft Learn
22. .NET and .NET Core official support policy
23. Auto-upgrade Node OS Images - Azure Kubernetes Service | Microsoft Learn
24. Kubernetes cluster architecture
25. Advanced Azure Kubernetes Service (AKS) microservices architecture
26. Microservices architecture on Azure Kubernetes Service
27. Configure Azure CNI networking in Azure Kubernetes Service (AKS)
28. Concepts - IP address planning in Azure Kubernetes Service (AKS)
29. Protecting privacy in Microsoft Azure: GDPR, Azure Policy Updates
30. Configuring Azure non-regional services for the EU Data Boundary - Microsoft Privacy
31. Services that will temporarily transfer a subset of Customer Data or pseudonymized personal data out of the EU Data Boundary - Microsoft Privacy
32. Services that transfer a subset of Customer Data or pseudonymized personal data out of the EU Data Boundary on an ongoing basis - Microsoft Privacy
33. List of built-in policy definitions - Azure Policy | Microsoft Learn
34. Automate Azure VM Start-Stop with Azure Automation and Tags | AzureIs.Fun
35. Virtual Machines - Power Off (REST API) (Azure Compute) | Microsoft Learn
36. Microsoft Defender portal - Microsoft Defender XDR | Microsoft Learn
37. Best practices for using Azure Key Vault | Microsoft Learn
38. Managed identities for Azure resources | Microsoft Learn




Thank you for your attention!

Any Questions ?