Solution Proposal

Azure Foundation Design for Cloud Adoption

**Group A**

Kanan Garach, Nitika Gupta, Anjali Kumari, Mark Nguyen

SYST8200 – Capstone Implementation

Ronak Patwa

# Table of Contents

[Table of Contents 2](#_Toc95591211)

[Introduction / Overview 2](#_Toc95591212)

[Scope 3](#_Toc95591213)

[Assumptions 3](#_Toc95591214)

[Dependencies 3](#_Toc95591215)

[Design Decisions 3](#_Toc95591216)

[Solution Description 4](#_Toc95591217)

[Single subscription architecture 6](#_Toc95591218)

[Hub Spoke model 7](#_Toc95591219)

[Multiple vNets 8](#_Toc95591220)

[Naming standards 9](#_Toc95591221)

[Deployment 9](#_Toc95591222)

[Technologies 9](#_Toc95591223)

[Use Cases 11](#_Toc95591224)

[Infrastructure and Networking Details 12](#_Toc95591225)

[Server Sizing Table 12](#_Toc95591226)

[Infrastructure Components / Subnet Details 12](#_Toc95591227)

[Network topology Diagram (end state) 13](#_Toc95591228)

[Security Considerations 13](#_Toc95591229)

[General Security Considerations 13](#_Toc95591230)

[Solution Specific Security Considerations 14](#_Toc95591231)

[Pricing / Run Cost – Azure Pricing Calculator 15](#_Toc95591232)

[Risk Assessment 16](#_Toc95591233)

[Future scope of current project 16](#_Toc95591234)

[Appendices 16](#_Toc95591235)

[Licensing 16](#_Toc95591236)

[Approval – sign off 16](#_Toc95591237)

[References 17](#_Toc95591238)

# Introduction / Overview

Cloud technologies and services today are beginning to redefine the way businesses utilize their IT infrastructure. Many organizations have begun to transition many of their digital assets to the cloud for various different reasons. As a result of the COVID 19 pandemic, a large amount of the existing IT infrastructure for many had to be transitioned to a cloud-based solution in order to support remote accessibility. For an organization to successfully implement a cloud solution, it requires a large amount of development and planning surrounding it.

Our solution is based on providing a framework for cloud adoption and future migrations.

Company NAIKA is currently running all of their IT infrastructure from their on-premises data center. The future strategy is to migrate all IT services to cloud and follow **“Cloud Only”** principles. To achieve this, Microsoft Azure is the strategic cloud platform that has been selected for now. Our solution provides core foundation technologies, architecture, and design guidelines that will enable business functions in NAIKA to build and operate in cloud with adequate guardrails around security, access, network, and governance.

## Scope

The scope of this document is to cover foundational design and technologies that will provide a standard platform in which early cloud adopters can consume cloud resources in a secure and supportable manner in a Microsoft Azure public cloud environment. The subsequent sections cover the following: foundation design core components, Azure resources, description related to different technologies used in the deployment of the solution. The scope also includes:

* Integration with NAIKA’s partner company KAN, over a private network to access the services across two domains.
* Secure Outbound internet connectivity via HA Proxy

## Assumptions

1. Network topology and Azure resources can be deployed using the Microsoft Azure Free Tier subscription
2. The end state deployment would match the solution topology
3. All chosen services are available with the Free/Trial licenses (OS + Application)
4. The pricing provided in the solution can serve as the starting point of budget approvals for similar deployment methods

## Dependencies

1. Successful deployment and integration of virtual networks using vNet peering and Private Link connection methods
2. Microsoft Azure Free Tier subscription comes with limitations respective to Azure resources, therefore this solution is dependent on what can be achieved solely through the Free Tier

# Design Decisions

In the table below, key design decisions have been taken into consideration while solutioning the Cloud Foundation Design for NAIKA to enable it to deploy and run services in Azure Cloud.

|  |  |  |
| --- | --- | --- |
| Decision ID | Design Decision | Justification |
| DD01 | Single account, Single subscription | Azure Free tier allows single subscription |
| DD02 | One vNet per Business function | Network level isolation for resources specific to a business function |
| DD03 | Hub vNet peered with another tenant vNet | KAN subscription will be peered with NAIKA via Hub vNet |
| DD04 | Each Business Function will be vNet peered to Hub vNet | Centralized management |
| DD05 | One NSG per application will be created | NSGs will be created at instance level for traffic filtering |
| DD06 | No open outbound connectivity to Internet | HAProxy Forward proxy will be used for outbound connectivity to Internet. This reduces risk of virus /malware attacks |
| DD07 | Different Azure Regions for NAIKA and KAN | NAIKA and KAN have global presence |
| DD08 | Single instance deployment | Since this is a lab environment, single instance will be deployed for each resource / service |

In an industry scenario, a Hub network will run all tooling for management and support of the infrastructure services. This would include patch management, vulnerability assessment tools, backup tooling, monitoring, cost management etc.

In our scope we are only demonstrating secure outbound internet connectivity using HAProxy forward proxy solution as one of the shared core services.

# Solution Description

This solution is being referred to as “**Azure Cloud Foundation Design (ACF)”** for adopting Microsoft Azure services. In an industry scenario, the customer would work with Microsoft to design a foundation framework that meets the strategic vision of the organization. The ACF establishes the governance around infrastructure workload utilization and consumption within the cloud, ensuring that the right security controls have been met. This Foundation Design must meet requirements for all business functions; hence this is an exhaustive exercise done through multiple workshops in collaboration with business heads.

Azure Cloud Foundation Design covers a portion of some key aspects that organizations must consider when they adopt cloud and make it available within the organization. This architecture serves as the **landing zone** and comprises of services and standards required for running future apps in Cloud. Application specific components are built on top of landing zone services.

The below diagram represents high level architecture for the Foundation design:

**Diagram

Description automatically generated**

Figure 1 High Level Topology

The solution comprises of a Hub vNet and multiple vNets (one for each business function) in a single subscription for NAIKA domain.

The Hub vNet serves as the shared services and perimeter vNet within the architecture. This will be used for running shared services and network components to enable connectivity across multiple vNets within the NAIKA network and connectivity to its partner product company KAN. KAN has few services running in the cloud on Azure and they will be integrated with NAIKA over private network to ensure the security of product data owned by these two companies.

Business function vNets will be used to run respective services in private network. Different vNets allow logical network level segregation so that secure point to point connectivity can be established between applications.

The core components and technologies in the solution are explained in subsequent sections.

Core components of this design are:

## Single subscription architecture

Our solution is based on single subscription model as Azure Free Trial account permits Single subscription.

It is important to organize the cloud resources to manage, secure and track costs of them.

**Account –** Signing up for Azure account allows customers to access and manage Subscriptions, and to use Azure cloud services.

Azure offers four levels of management:

**Management Groups** – They provide a level of governance by helping mange policies, access, and compliance above Subscriptions. *All subscriptions in a management group automatically inherit the conditions applied to the management group.*

**Subscriptions** – They are logical grouping of services and administration. Subscriptions are limited by the quotas and limits; hence they provide a boundary for resources, growth, administration, and billing. These quotas help to define the subscription model in large organizations where multi-Subscription model is more suitable.

**Resource Groups** – They are logical containers to deploy and manage Azure cloud resources like databases, webapps, load balancers, virtual machines etc. These are created under Subscriptions.

**Resources** – These are instances of resources created in a Resource Group. These would include instance of Blob, SQL database instance, Virtual machine instance etc.

The below image has been taken from Microsoft to represent the hierarchy; the blue highlighted section is what will be deployed as part of this solution.

Shape

Description automatically generatedGraphical user interface

Description automatically generated with medium confidence

Figure 2 Azure Management Levels and Hierarchy

(Organize your Azure resources effectively, 2021)

## Hub Spoke model

Our solution is based on Hub Spoke Topology with Shared Services. This is one of the recommended networking models from MS for managing connectivity across different internal and external networks, better security and providing shared services like Proxy, Firewall through Hub. This model addresses following concerns:

1. Isolation - way workloads can be isolated while sharing and centralizing core services.
2. Cost Effectiveness – Avoids creation of redundant core services as they are shared. It further reduces the monthly billing and management overheads to manage them
3. Subscription limitation – In an industry scenario, multiple subscriptions will be created basis the business requirements. Large workloads will consume more resources and Azure subscriptions have limits and quotas. Peering virtual networks help to overcome this limit.
4. Perimeter Security – Since, all connections whether internal or external are routed via Hub vNet, it provides perimeter security.

In our solution, single subscription is created, multiple vNets represent different business functions which would be independent subscriptions otherwise.

Below diagram is an example of Microsoft Hub-Spoke topology. The Hub network shows connectivity to different Hubs and subscriptions / Spokes.

Diagram

Description automatically generated

Figure 3 Example of Hub-Spoke Topology from Microsoft

(Hub-and-spoke network topology, 2021)

## Multiple vNets

For small sized organization, multiple vNet in single subscription model may be created to run prod and non-Prod workloads for different platforms.

Integrating azure services to an azure virtual network enables private access to the service from virtual machines or compute resources in the virtual network.

Azure routes traffic between subnets, connected virtual networks. However, additional security rules may be created to filter traffic and overrise default routes.

In this solution, each virtual network is allocated a non-overlapping /24 network address space. Traffic between business vNets will be allowed through Hub vNet, there is no direct connectivity between Business vNets.

(Virtual Network - Azure, n.d.)

## Naming standards

Naming standards ensure that all resources follow standard naming convention and can be easily identified in portal, reporting and billing. There is guidance available from Microsoft for naming standards to be followed in Azure. Our solution naming convention is as below:

|  |  |  |
| --- | --- | --- |
| Azure Resource | Naming Convention | Example |
| Load Balancer | <domain>-<LB>-NN | NAIKA-LB-01 |
| Virtual Machine | <domain>-<OSROLE>-NN, L=Linux, W=Windows | NAIKA-LWEB-01 |
| Resource Group | <domain>-<RG>-NN | NAIKA-RG-01 |
| Database PaaS | <domain>-<PDBTYPE>-NN | NAIKA-PMySQL-01 |
| Azure Firewall | <domain>->AZFW>-NN | NAIKA-AZFW-01 |
| Client machines | <domain>-<DEVTEST>-NN | KAN-DEVTEST-01 |

# Solution Deployment

In this solution we are deploying single instance of each Azure resource type as this is a Lab environment. In an industry scenario, all these services will be built with high availability and disaster recovery considerations. Further sub-sections include the Azure technologies that will be deployed in this design and the use cases for each one of them.

## Technologies

**vNet** – Azure virtual network allows segmented networks to be created to deploy Azure services in private network for secure communication between them, to the internet or even to On-Premises network. vNet is similar to traditional VLANs, relies on Azure backbone network.

**Subnet** – Subnets are created using vNet CIDR and help with further segmentation of network. vNets and subnets span across all Availability Zones (AZ) in a region. There is no division required at AZ level.

**NSG** – Network Security Group (NSG) allows filtering of inbound and outbound traffic to and from resources by source and destination IP address, port, and protocol. These are security rules to allow or deny traffic from Azure resources.

**vNet Peering** – Virtual network peering allows seamless connectivity direct connectivity between two or more virtual networks. The traffic between peered networks uses Microsoft backbone infrastructure.

This solution uses both virtual network peering and global virtual network peering. vNet peering will provide low latency, high throughput network with no requirement of any internet or VPN gateways. It’s a direct secure private connectivity.

**Private Link** – Azure private link allows PaaS services and partner hosted serv ices to be accessed over a private endpoint in virtual network. this traffics traverses over Microsoft backbone network and does not require to be exposed to Internet.

In this solution, private link will be used to connect services from KAN network to NAIKA network over private endpoint. This will prevent any data leakage scenario as the connection is only to specific resource instance. Access to any other service is blocked.

**Azure Firewall** – Azure firewall is a cloud native, fully stateful, firewall as a service that provides protection against threat for cloud workloads running in Azure. The firewall has inbuilt high availability and unlimited scalability features.

This solution is using Azure firewall – Standard tier for routing traffic across vNets and from KAN partner network. Standard firewall provides L3-L7 filtering, NAT traffic, and allows traffic based on filtering rules. The outbound traffic is controlled by the firewall that blocks any outside components automatically. Firewall with web categories policy allows administrators to proceed or deny user access to the internet based on the categories. This reduces the time admins have to spend on managing URLs. This can be considered as the application rule destination type in standard version.

The below figure is taken from Microsoft website to show supported features of azure Firewall. We will be implementing only filtering rules in the lab environment of this solution.

Diagram

Description automatically generated

Figure Standard Azure Firewall features - MS

(What is Azure Private Link?, 2021), (Virtual network peering, 2022), (What is Azure Firewall?, n.d.)

## Solution Use Cases

Following use cases have been finalized to demonstrate the interconnectivity and functionality of different azure resources.

Use case 1 – Build XAMPP app with MySQL DB. Access the database using MySQL Workbench tool running on one of the client machines

Use case 2 - Access Blob over Private Network using vNet Service Endpoint

Use case 3 – Cross tenant vNet peering via Azure Firewall

Use case 4 - Access an Internal LB from Client workstation using Private Link

Use case 5 – Test connectivity across subnets over ICMP

Use case 6 – Connect to public URL from App server via HAProxy in Hub subnet where internet access is not allowed on the server

# Infrastructure and Networking Details

## Server Sizing Table

The table below contains the information highlighting the servers that will be used and their associated resources sizing allocation within Microsoft Azure Cloud.

|  |  |  |  |
| --- | --- | --- | --- |
| Server Name | Server Role | Server Sizing | Service Tier |
| NAIKA-WFTPS-01 | FTPS Server | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| NAIKA-LWEB-01 | XAMPP Web/App Server | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| NAIKA-WWEB-01 | Windows Web server | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| NAIKA-PMYSQL-01 | MySQL PaaS Database | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| KAN-DEVTEST1-01 | Windows Client / User machine | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| KAN-DEVTEST1-02 | Windows Client / User machine | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| NAIKA-LPROXY-01 | Forward Proxy | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |
| NAIKA-AZFW-01 | Cloud Service Firewall | B1s (1 vCPU, 1GB, 4GB) | Free Service Tier |

## Infrastructure Components / Subnet Details

The table below displays the information relating to the resource components that have been selected within Azure cloud to build the proposed solution design.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Infrastructure components | Server Name | IP Address Space | Operating System | Application Software | App licensing |
| FTPS Server | NAIKA-WFTPS-01 | 10.8.1.0/24 | Windows server 2019 Std. Edition | File + FTP | N/A |
| XAMPP WEB/APP Server | NAIKA-LWEB-01 | 10.6.1.0/24 | Windows server 2019 Std. Edition | XAMPP Stack | Marketplace Image |
| Windows Web server | NAIKA-WWEB-01 | 10.8.1.0/24 | Windows server 2016 Std. Edition | IIS ( ver - TBC) |  |
| MySQL Server | NAIKA-PMYSQL-01 | NA | Windows server 2019 Std. Edition | MySQL Server 8 | Community |
| Windows Client / User machine | KAN-DEVTEST-01 | 10.6.1.0/24 | Windows Based | DevTest Tools | Marketplace Image |
| Windows Client / User machine | KAN-DEVTEST-02 | 10.9.1.0/24 | Windows Based | DevTest Tools | Marketplace Image |
| HAProxy Server | NAIKA-LPROXY-01 | 10.7.1.32/27 | RHEL 7.x | HAProxy |  |
| Azure Firewall | NAIKA-AZFW-01 | 10.7.1.0/27 | NA | NA |  |

## Network topology Diagram (end state)

This network topology is created using Packet Tracer, the successful end state deployment would match this topology.

Diagram

Description automatically generated

# Security Considerations

There are key security considerations that any organization must follow when deploying services in cloud. We have covered some of them as generic considerations and called out a few which are design specific.

## General Security Considerations

**User Access** - Microsoft Azure offers for the Azure Identity protection from the Directory service for authentication requirements. The Azure Directory will control the information of the devices that connect during transmission by monitor for locations and device details and require for verifications. The multifactor authentication helps our system detect if there is an authorized access.

**Data** - All data in the Storage Account is encrypted by default at the service level using industry-standard AES 256-bit encryption. The layered security approach always includes data encryption measures. All requests over HTTP alone will fail when this option is enabled, and only HTTPS-based requests are allowed. Microsoft-managed encryption keys, or for added security, you can use a customer-managed key with Azure Key Vault or Azure Key Vault Managed HSM, currently in public preview.

**Network traffic** - Azure offers the DDoS protection for the control of public IP access in the virtual network. Inside virtual network service, we can enable the DDoS Protection to avoid DDoS attacks by providing the always-on monitoring for cyber threats. These attacks can effect on the total cost scale when the systems go for deployment.

## Solution Specific Security Considerations

1. Our solution comes up with the concern about the leak of network resources while transferring messages from NAIKA company and the partner company KAN.
2. The solution goes with the Hub subscription, all vNets acquire perimeter security with Azure Firewall to protect against cyber threats. Azure provides Firewall services for the Virtual Network resources. The picture below shows an example of the hub virtual network that the spoke machines and the on-premises are controlled by the Azure Firewall and the way it works.
3. For servers and databases, solution will, have Azure native encryption enabled. However, for data in transit we are not installing any SSL certificates

“Graphical user interface, diagram, application

Description automatically generated

Figure Azure Firewall Security

(Microsoft, 2021)

# Pricing / Run Cost – Azure Pricing Calculator

The below pricing has been created to provide a rough estimate for budget approvals in case this needs to be deployed in other regions.

There will be egress cost associated with data which cannot be gauzed at this time as it will be based on real time traffic.

There is no cost for vNet and subnet, they are free of charge.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Virtual Machine | Roles | Size | Region | Price (per month) |
| NAIKA-FILE | File server + FTPS Server | B1s (1 vCPU, 1GB, 4GB) | East US | 48.03 US$ |
| NAIKA-LWEB | XAMPP Web/App Server | B1s (1 vCPU, 1GB, 4GB) | East US | 48.03 US$ |
| NAIKA-WWEB-01 | Windows Web server | B1s (1 vCPU, 1GB, 4GB) | East US | 48.03 US$ |
| NAIKA-PMYSQL-01 | MySQL PaaS Database | Gen 5 (2v Core, 5GB storage) | East US | 128.47 US$ |
| KAN-DEVTEST1-01 | Windows Client / User machine | B1s (1 vCPU, 1GB, 4GB) | Canada East | 49.02 US$ |
| KAN-DEVTEST1-02 | Windows Client / User machine | B1s (1 vCPU, 1GB, 4GB) | Canada East | 49.02 US$ |
| NAIKA-LPROXY-01 | Forward Proxy | B1s (1 vCPU, 1GB, 4GB) | East US | 48.03 US$ |
| NAIKA-AZFW-01 (standard) | Cloud Service Firewall | B1s (1 vCPU, 1GB, 4GB) | East US | 912.5 US$ |

(Pricing calculator, n.d.)

# Risk Assessment

1. The applications may face interoperability issues with other systems in foundation in the future scope, so there’s a risk associated with computability.
2. This is first time deployment in lab, most the services have not been built as part of our course. There’s a risk that some services may not be fully functional.
3. Public Cloud in general poses a risk w.r.t data security, so any organization that uses this or similar foundation designs for cloud deployment must enable adequate security controls deemed suitable for the industry, region and province.

# Future scope of current project

1. The Azure Cloud Foundation Design (ACF) can be used as a blueprint for multiple landing zones creation in an organization using template deployment methodologies. This can also be used in multi-region deployment scenarios.
2. Establishing connectivity with On-Premises in a hybrid deployment model would be achievable via this foundation design. The Hub network is the central point of connectivity across multiple networks. This will allow the company to keep the critical workloads on the premises and migrate the non-critical workloads to be moved to the cloud.
3. For future migrations to cloud, this foundation design will be baseline for architecture principles, guidelines, and governance.

# Appendices

## Licensing

All the application software used in this solution deployment are either free or trail versions. Windows OS and marketplace images licensing is already covered under subscription model in azure.

## Approval – sign off

# References

(n.d.). Retrieved from https://www.google.com/url?sa=i&url=https%3A%2F%2Frahulsahay19.medium.com%2Fazure-subscriptions-and-resources-fff5e634deef&psig=AOvVaw1o9GIuwkvYd\_1kVMXLYpY0&ust=1644773204570000&source=images&cd=vfe&ved=0CAgQjRxqFwoTCJDyherX-vUCFQAAAAAdAAAAABBe

*Hub-and-spoke network topology*. (2021, August). Retrieved from Micrsoft Docs: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/hub-spoke-network-topology

Microsoft. (2021). Hub-spoke network topology in Azure. https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli.

*Organize your Azure resources effectively*. (2021, Decemeber 23). Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

*Virtual Network - Azure*. (n.d.). Retrieved from Microsoft docs: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

*Virtual network peering*. (2022, January). Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

*What is Azure Firewall?* (n.d.). Retrieved from Microsoft docs - Azure: https://docs.microsoft.com/en-us/azure/firewall/overview

*What is Azure Private Link?* (2021, August). Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/private-link/private-link-overview