



Good Health Is The Root
Of All Heppiness

123

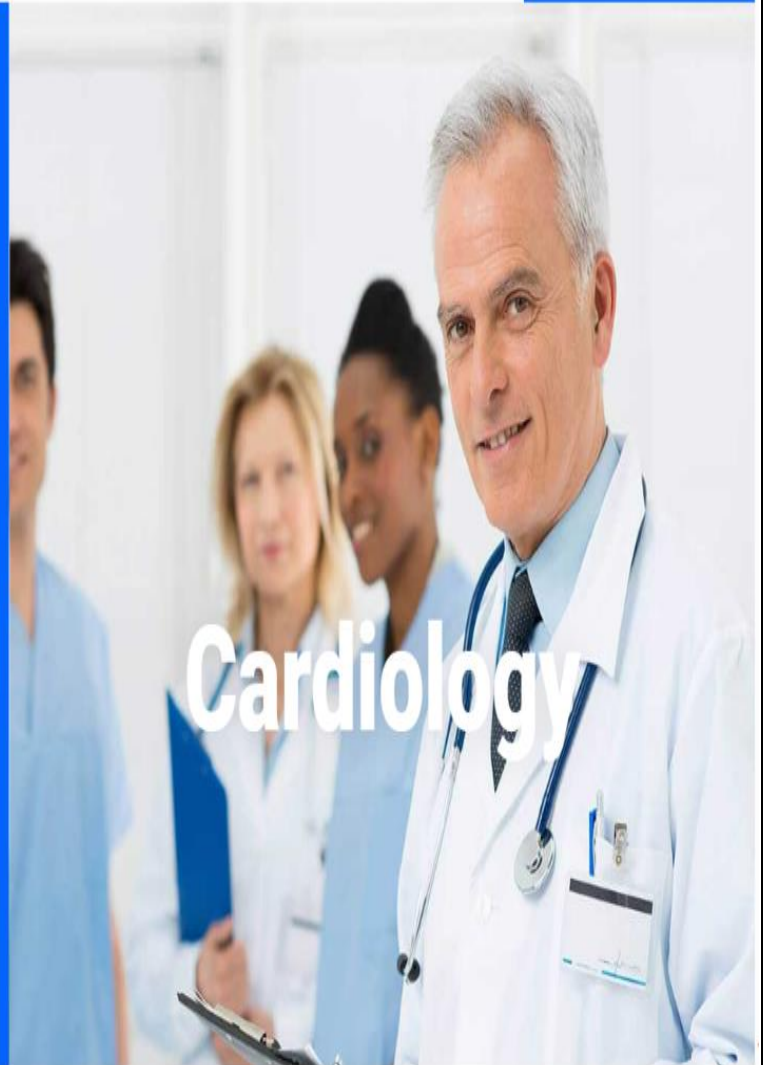
Expert Doctors

1234

Medical Stuff

12345

Total Patients



Dr's Klinik Using Azure Services

Azure Documentation

Created By: Sanjana Pal

22 october,2023

project Guide: John Devassy

Vikram Patil ,Suraj Waghmare

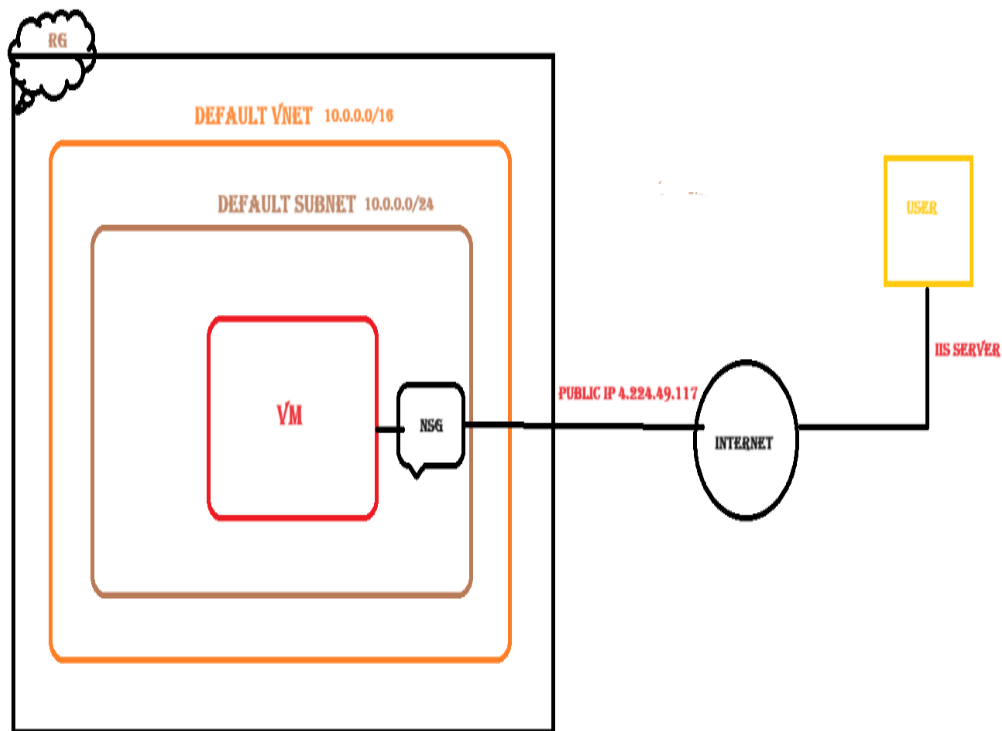
ABSTRACT

This project report presents the design and implementation of Dr's Klinik an Dr's Klinik that offers subscription-based access to various appointment using various Azure services. D's Klinik is hosted on two separate Azure VMs and then load-balanced using Traffic Manager and backed up using Recovery Service Vault, it also uses Azure DNS Zone. The Dr's Klinik website project represents a transformative approach to healthcare services by leveraging Microsoft Azure's robust cloud infrastructure. This web-based platform is designed to streamline patient interactions, enhance medical record management, and provide valuable healthcare information. The project's primary objective is to offer an efficient and secure healthcare solution that ensures high availability, scalability, and data protection.

Table of Content

| | |
|----------------------------------------------|----|
| 1. Chapter 1: Introduction..... | 5 |
| I. Project Overview..... | 5 |
| II. Project Objective..... | 5 |
| 2. Chapter 2: Prerequisites..... | 6 |
| I. Azure Subscription..... | 6 |
| II. Admission Access to azure portal..... | 6 |
| III. Knowledge of IIS Web Server..... | 6 |
| IV. A copy of Dr's Klinik Website..... | 6 |
| 3. Chapter 3: Azure Resources Setup..... | 7 |
| I. Steps to Create Virtual Machine..... | 8 |
| II. IIS Server Development..... | 10 |
| III. Configuration of Traffic Manager..... | 13 |
| IV. Recovery Service Vault..... | 15 |
| 4. Chapter 3: Testing..... | 16 |
| 5. Chapter 4: Website Overview..... | 17 |
| 6. Chapter 5: Maintenances..... | 19 |
| 7. Chapter 6: Troubleshooting | 21 |
| 8. Chapter 7: Conclusion..... | 23 |

TOPOLOGY



- Here both VM and Vm2 are created in same region central india , both have same v-net and subnet . First VM is connect with RDP in VM using IIS server I am deploying my dummy website and check in browser.
- After deploying website in VM, I am using two services traffic manager and Recovery service vault , traffic manager is the part of load balancer which is used to manage the traffic. Recovery service vault used to recover both the Virtual machine.

INTRODUCTION

Project Overview

The Dr's Klinik website is a modern and dynamic web application designed to cater to the needs of healthcare providers, patients, and clinic administrators. This website serves as a central platform for healthcare services, offering features and functionalities such as appointment scheduling, patient records management, medical billing, and information dissemination. Azure, Microsoft's cloud computing platform, is chosen for this project to leverage its robust capabilities, scalability, and various services tailored to web application hosting and management.

Objective of Project:

1. **Appointment Booking:** Allow patients to schedule appointments with healthcare professionals online. Patients can choose their preferred date, time, and healthcare provider, making the booking process efficient and convenient.
2. **Patient Records Management:** Provide healthcare providers with a secure and organized system for managing patient records, including medical histories, treatment plans, and test results.
3. **Accessibility:** Ensure the website is accessible on various devices, making it easy for users to interact with it from desktops, laptops, tablets, and mobile phones.
4. **Medical Billing:** Streamline the billing process for healthcare services. The website integrates with billing systems to facilitate secure and efficient financial transactions between healthcare providers and patients..

Prerequisites:

1. **Azure Subscription:** You need an active Azure subscription to access Azure's cloud services, including virtual machines, traffic manager, and recovery services. If you don't have one, you can sign up for an Azure subscription on the Azure website
2. **Administrator Access to Azure Portal:** As the administrator of the Azure resources, you'll need administrative access to the Azure portal. This access allows you to create, configure, and manage the resources required for your project.
3. **Knowledge of IIS Web Server:** Understanding the Internet Information Services (IIS) web server is crucial for deploying web applications on Windows-based virtual machines. You should be familiar with configuring IIS, creating websites, setting up bindings, and managing application pools.
4. **A Copy of the Dr's Klinik Website:** You'll need the Dr's Klinik website's source code and content. This includes HTML, CSS, JavaScript files, and any backend components. Make sure you have a complete copy of the website that you intend to deploy on Azure.

With these prerequisites in place, you can proceed with setting up the virtual machines, configuring IIS, deploying the Dr's Klinik website, and implementing the Traffic Manager and Recovery Service Vault as mentioned in your project plan.

Azure Resources Setup:

A . Steps to create Virtual Machine:

Step 1: Sign in to the Azure portal:

- Open your web browser and navigate to the Azure Portal.
- Sign in with your Azure account, ensuring you have the necessary permissions to create virtual machines

Step 2: Create a Virtual Machine:

1. Once you're in the Azure Portal, click the "+ Create a resource" button.
2. In the "Search the Marketplace" field, type "Windows Server" or "Linux," depending on your choice of operating system.
3. Select the desired operating system image, such as "Windows Server 2019"

Step 3: Virtual Machine Configuration:

1. Click the "Create" button to begin the VM creation process
2. In the "Basics" tab, provide the following information:
 - **Project Details:** Choose your subscription, resource group (or create a new one), and region.
 - **Instance Details:** Enter a unique VM name and choose a suitable size for your VM. VM sizes vary in terms of CPU, memory, and disk space. Select the one that meets your requirements
 - **Administrator Account:** Set a username and password for the VM's administrator account
 - **Inbound Port Rules:** Configure the necessary inbound port rules to allow traffic to your VM. For a web server, you should open port 80 for HTTP or port 443 for HTTPS.
 - **Public Inbound Ports:** Choose "Allow selected ports" and select HTTP (80) and HTTPS (443). Select rdp also to connect with vm and run website using IIS server.

Step 4 : Set the Mangement and networking default one and click on review and create

Step 5: Wait For Deployment

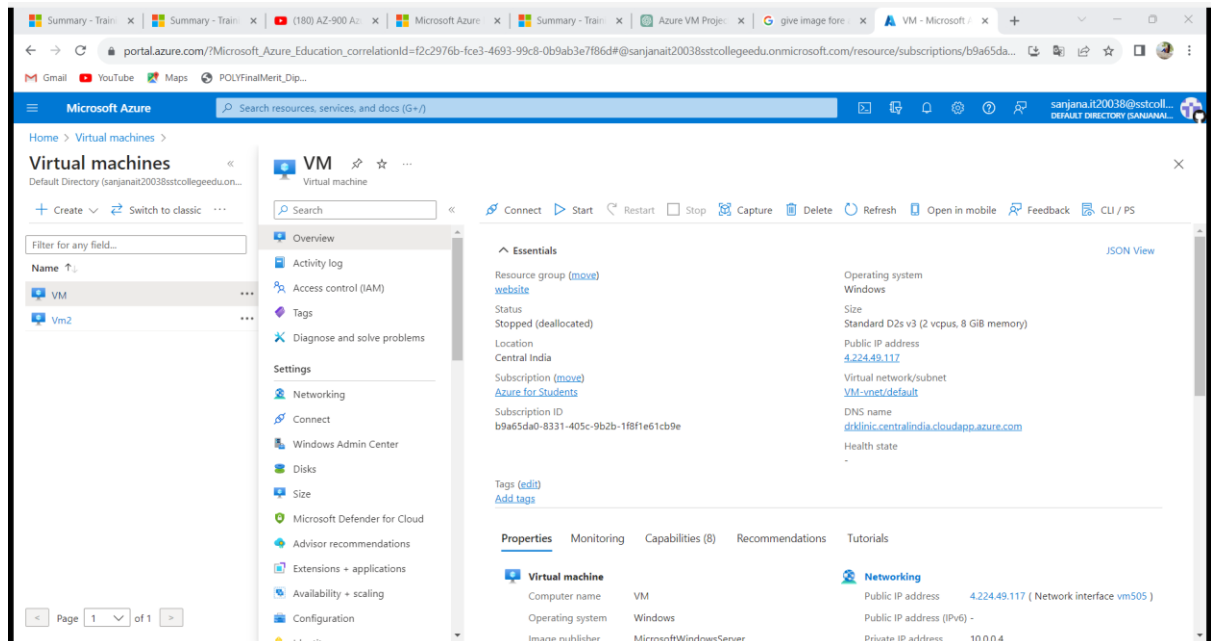
Azure will start deploying your virtual machine. You can monitor the progress on the Azure Portal dashboard.

Step 6: Repeat for Second Virtual Machine

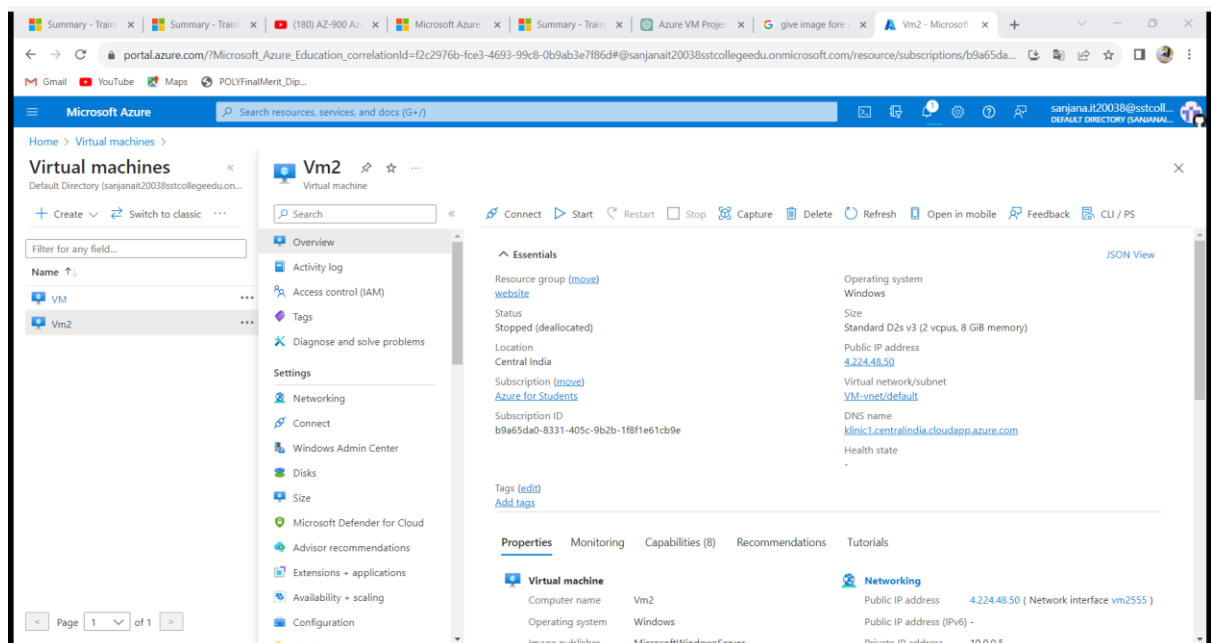
1. Once the first VM is deployed successfully, repeat the same process to create the second virtual machine. Ensure you choose the same region, virtual network, and subnet to keep them within the same network

By following these steps, you will create two virtual machines in Azure with the specified VM specifications, chosen operating system, and networking configurations. These VMs can now be used to host your Dr's Clinic website using IIS.

VM



VM2



B. IIS Server Deployment

Deploying the Dr's Clinic website on each virtual machine using Internet Information Services (IIS) involves several steps, including copying website files, creating virtual directories, and configuring application pools. Here's a detailed guide on how to do this:

Step 1: Copy Website Files

1. Ensure you have the website files for Dr's Klinik available, including HTML, CSS, JavaScript, and any other necessary assets.
2. RDP (Remote Desktop Protocol) into the virtual machine to which you want to deploy the website. You can do this via the Azure Portal or using a tool like Remote Desktop Connection.
3. Once connected to the VM, create a folder for your website files. You can create it in the default web root directory (usually **C:\inetpub\wwwroot**) or any other location of your choice.
4. Copy the website files into the folder you created on the virtual machine

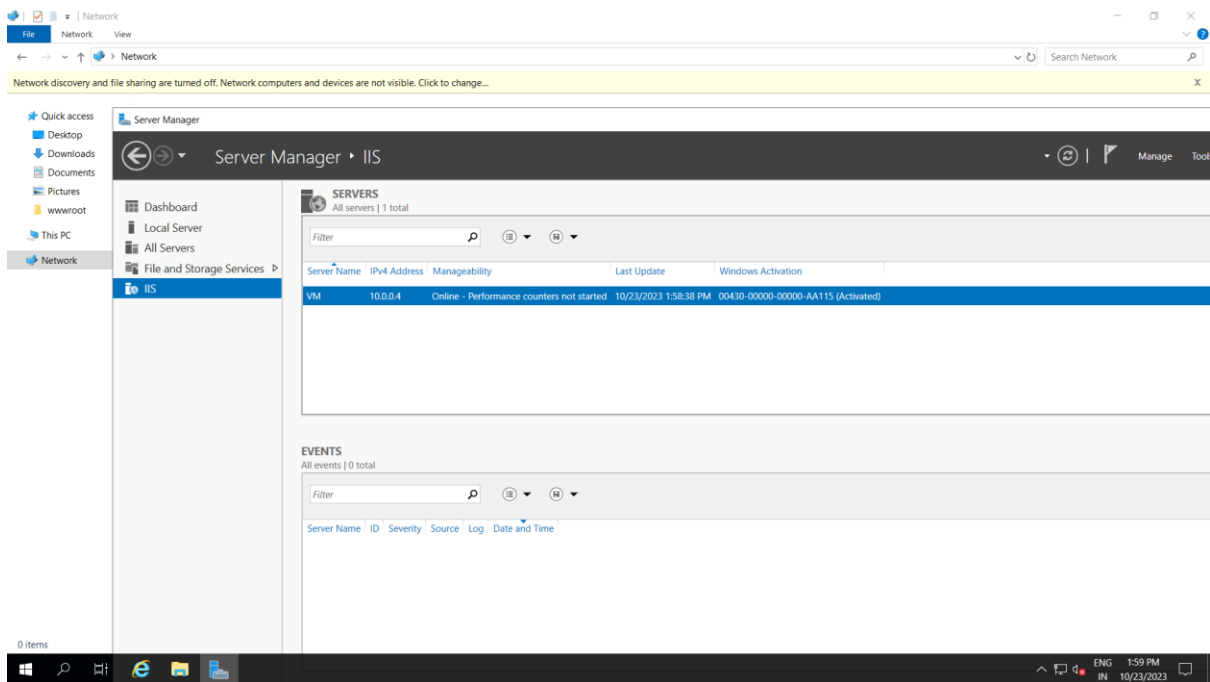
Step 2: Create Virtual Directory

1. Open IIS Manager on the virtual machine by searching for "IIS Manager" in the Start menu
2. In the Connections pane on the left, expand the server node, and then expand "Sites."
3. Select the default website (or the website where you want to host Dr's Klinik)
4. In the Actions pane on the right, click on "Add Virtual Directory."
5. In the Add Virtual Directory dialog, you'll need to specify an alias (a friendly name) for the virtual directory, and the physical path to the folder where you copied the website files in Step 1. Click "OK" to create the virtual directory.

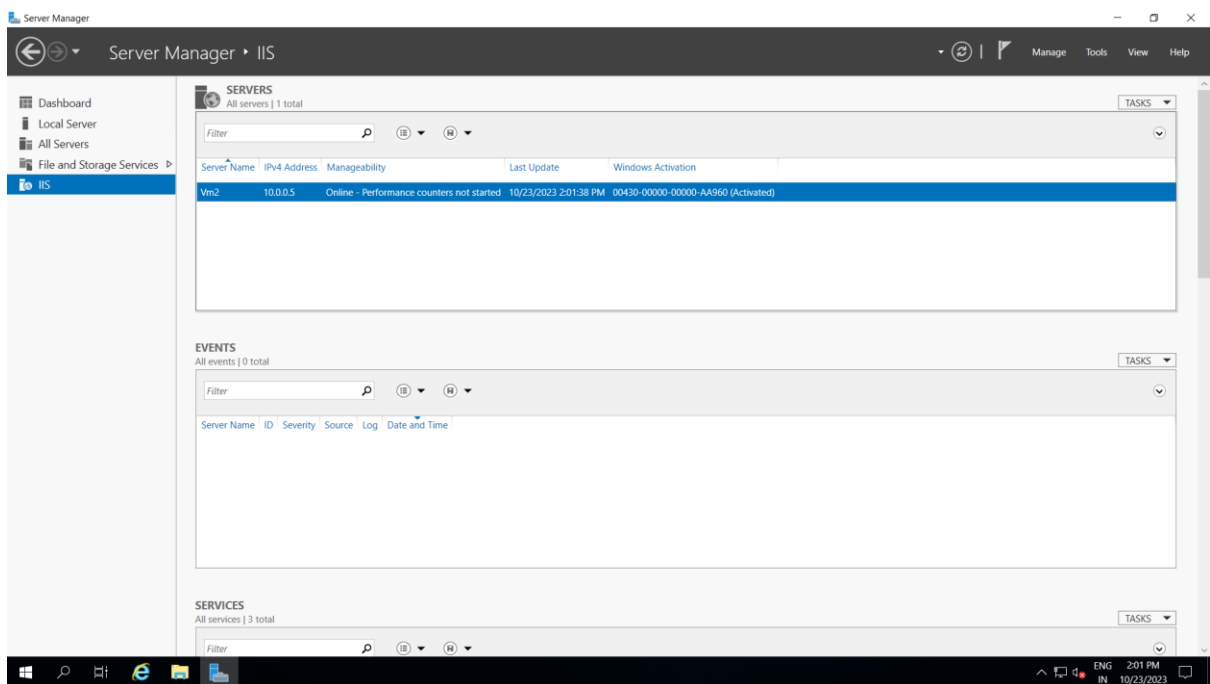
Step 3: Test Websites Deployment

1. Open a web browser and navigate to the public IP address or domain name associated with your virtual machine.
2. You should now see the Dr's Klinik website live and accessible to users. Make sure that all the web pages, scripts, and features function correctly.

By following these steps, you've successfully deployed the Dr's Klinik website on the virtual machine using IIS. Repeat these steps for the second virtual machine to ensure both instances are hosting the website. Additionally, you should consider load balancing and configuring a Traffic Manager to distribute traffic between these virtual machines for high availability and performance.



For Vm2



C . Configuration of Traffic Manager:

Step 1: Sign in to the Azure Portal

1. Open your web browser and navigate to the Azure Portal.
2. Sign in with your Azure account.

Step 2: Create a Traffic Manager Profile

1. Click the "+ Create a resource" button.
2. In the "Search the Marketplace" field, type "Traffic Manager".
3. Select "Traffic Manager profile" from the results.

Step 3: Traffic Manager Profile Setting

1. In the "Create Traffic Manager profile" page, fill out the details:
 - **Subscription:** Choose your subscription
 - Resource Group: Select an existing resource group or create a new one
 - **Name:** Enter a unique name for your Traffic Manager profile.
 - **Routing Method:** Choose one of the following routing methods based on your needs:
 - I. **Priority:** Use this method if one virtual machine should be the primary and the other is a backup.
 - II. **Weighted:** Assign different weights to your virtual machines to distribute traffic based on the configured weights.
 - III. **Performance:** Route traffic to the virtual machine with the lowest latency based on Azure's monitoring.
 - IV. **Geographic:** Direct users to specific virtual machines based on their geographic location.
 - V. **DNS TTL(Time To Live):** Set the DNS Time to Live value, which determines how long DNS resolvers should cache the DNS records. This affects the frequency of DNS record updates.
2. Click "Review + create" and then "Create" to create the Traffic Manager profile.

Step 4: Configure Endpoints

1. After the Traffic Manager profile is created, go to the profile's settings.
2. In the left menu, select "Endpoints."
3. Click "+ Add" to add a new endpoint for each virtual machine.
4. Configure the endpoint details for each virtual machine:
 - I. Type: Select "Azure Endpoint."
 - II. Name: Enter a unique name for the endpoint.
 - III. Target resource type: Choose "Public IP address."
 - IV. Target Resource: Select the public IP address associated with the respective virtual machine.

Set the priority or weight based on the routing method chosen.

Step 5: DNS Configuration

1. Go back to the Traffic Manager profile settings.
2. Under "Settings," click "Configuration."
3. Under "DNS," you can choose the "Create new DNS name" or "Use an existing DNS name."
4. Select the routing method and click "Save."

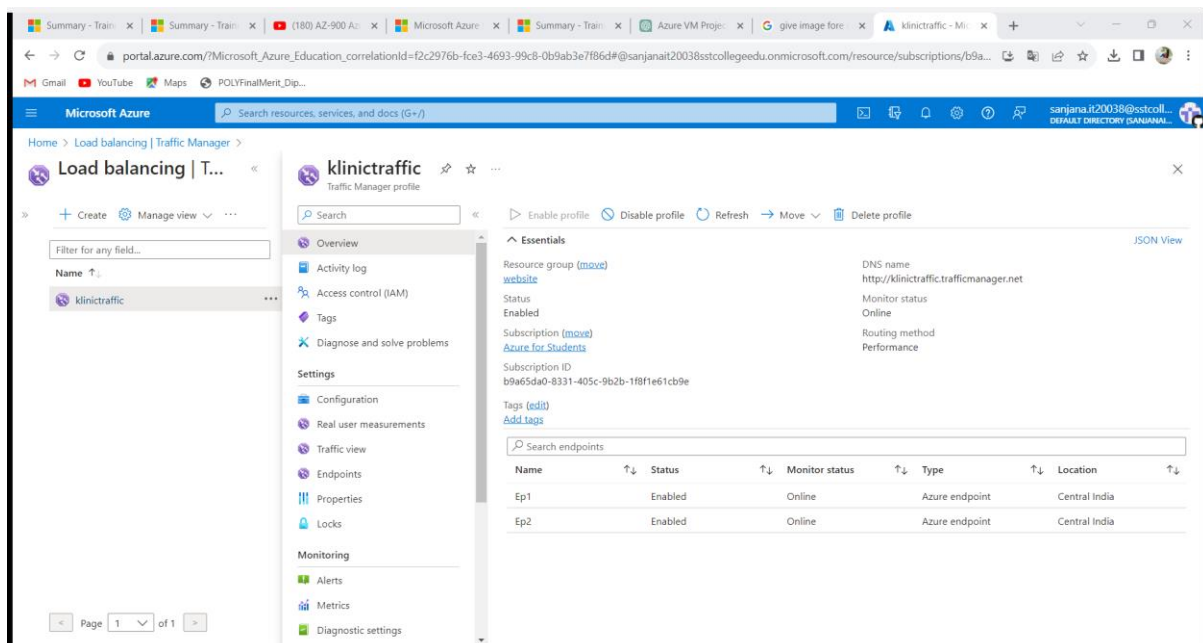
Step 6: Update DNS Records

1. After creating the Traffic Manager profile, you'll receive a DNS name associated with it.
2. Update your domain's DNS records to point to the Traffic Manager's DNS name.

Testing:

1. Wait for DNS changes to propagate. It may take some time depending on your DNS TTL settings.
2. Wait for DNS changes to propagate. It may take some time depending on your DNS TTL settings.

By following these steps, you've configured the Azure Traffic Manager to load balance traffic between the two virtual machines using DNS and public IP addresses. The choice of routing method (e.g., priority, weighted, geographic) depends on your specific requirements for high availability, performance, or geographic distribution of users.



D. Recovery Service Vault:

Setting up a Recovery Service Vault in Azure for the backup and recovery of virtual machines involves several steps, including defining backup policies, schedules, and retention settings. Here's a detailed guide on how to configure the Recovery Service Vault for this purpose:

Step 1: Create a Recovery Service Vault

1. Sign in to the Azure Portal.
2. Click the "+ Create a resource" button.
3. In the "Search the Marketplace" field, type "Recovery Services vault."
4. Select "Recovery Services vault" from the results.

5. In the "Create Recovery Services vault" page, fill out the details:
 - **Subscription:** Choose your subscription.
 - **Resources Group:** Select an existing resource group or create a new one.
 - **Name:** Enter a unique name for your Recovery Service Vault.
 - **Region:** Choose the region for your vault.
6. Click "Review + create" and then "Create" to create the Recovery Service Vault.

Step 2: Register Resource Providers

To perform backup and recovery, you may need to register resource providers if they're not already registered. Resource providers can include the following:

- Microsoft Compute (for VMs)
- Microsoft Network (for virtual networks)
- Microsoft Storage (for storage accounts)

You can register these resource providers by navigating to "Subscriptions" in the Azure Portal, selecting your subscription, and then clicking "Resource providers."

Step 3: Define Backup Policy

1. In the Azure Portal, go to your newly created Recovery Service Vault.
2. In the left menu, select "Backup."
3. Click on "Backup policies."
4. Click "+ Add" to create a new backup policy.
5. In the "Create policy" page, configure the backup policy details:
 - **Policy name:** Give your policy a meaningful name.
 - **Backup Schedule:** Define the frequency and time of backups. You can choose daily or custom schedules.
 - **Retention Settings:** Set the retention duration for daily, weekly, and monthly backups.
6. Click "Create" to save the backup policy.

Step 4: Enable Backup For Virtual Machine:

1. In the Recovery Service Vault, navigate to "Protected items."
2. Click "+ Add" to configure the items to protect.
3. Select "Virtual Machine" as the workload type.
4. Choose the virtual machines you want to back up. You can select VMs from the list.
5. Click "OK" to add the selected VMs.
6. In the "Backup policy" section, choose the backup policy you created in Step 3.
7. Click "Enable Backup" to initiate the backup process.

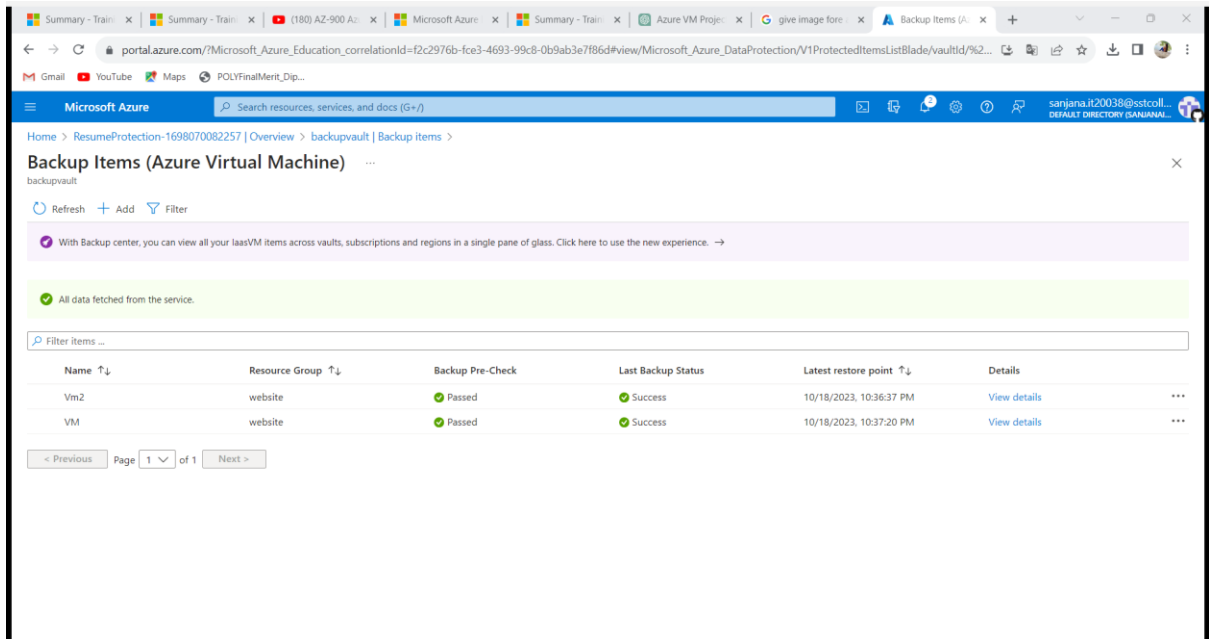
Step 5: Monitor and Test Backups:

1. Once backups are configured, you can monitor the status, backup jobs, and retention settings in the Recovery Service Vault.
2. Test the recovery process to ensure that you can successfully restore virtual machines and data if needed.

Step 6: Set up Alerts and Notification

You can configure alerts and notifications to be informed about the status of backup jobs, any issues, or if the backup vault is nearing its storage limits.

By following these steps, you've set up a Recovery Service Vault for the backup and recovery of virtual machines in Azure. Regularly monitor the status of backups, test the recovery process, and ensure that your retention settings align with your data retention policies and compliance requirements



The screenshot shows the Microsoft Azure portal interface for managing backup items. The breadcrumb navigation indicates the path: Home > ResumeProtection-1698070082257 | Overview > backupvault | Backup items >. The page title is "Backup Items (Azure Virtual Machine)". Below the title, there are options to Refresh, Add, and Filter items. A message states: "With Backup center, you can view all your IaaS VM items across vaults, subscriptions and regions in a single pane of glass. Click here to use the new experience. →". A green status bar indicates "All data fetched from the service." Below this is a filter bar and a table of backup items.

| Name ↑↓ | Resource Group ↑↓ | Backup Pre-Check | Last Backup Status | Latest restore point ↑↓ | Details |
|---------|-------------------|------------------|--------------------|-------------------------|------------------------------|
| Vm2 | website | Passed | Success | 10/18/2023, 10:36:37 PM | View details |
| VM | website | Passed | Success | 10/18/2023, 10:37:20 PM | View details |

At the bottom, there is a pagination control showing "Page 1 of 1" with "Previous" and "Next" buttons.

Testing

Testing the setup of the Dr's Klinik website on Azure to ensure that it functions correctly and that traffic is being balanced evenly between the two virtual machines involves several steps. Here's a guide on how to perform these tests:

Testing Website Functionality:

1. Individual VM Testing:
 - Access each virtual machine's public IP address or DNS name directly in a web browser.
 - This allows you to check if the website functions on each VM individually.
2. Content Validation:
 - Ensure that all web pages, scripts, and functionalities of the website work as expected.
 - Test features like appointment booking, patient record management, and billing.

Load Balancing Testing:

1. Traffic Manager DNS Testing:
 - Access the Traffic Manager DNS name in a web browser. Ensure that it directs traffic to one of the two virtual machines according to the configured routing method (e.g., priority, weighted, geographic).
2. Failure Testing:
 - Simulate failures by temporarily stopping one of the virtual machines. Confirm that the Traffic Manager automatically directs traffic to the healthy VM.
 - After the test, bring the stopped VM back online and verify that traffic is balanced again.

User Testing:

1. User Acceptance Testing(UAT):
 - Conduct UAT with actual users to gather feedback on the website's performance, user-friendliness, and any issues they encounter.
2. Performance Testing:
 - Perform load testing using tools like Apache JMeter or Azure's Load Testing Service to ensure the website can handle expected traffic loads.

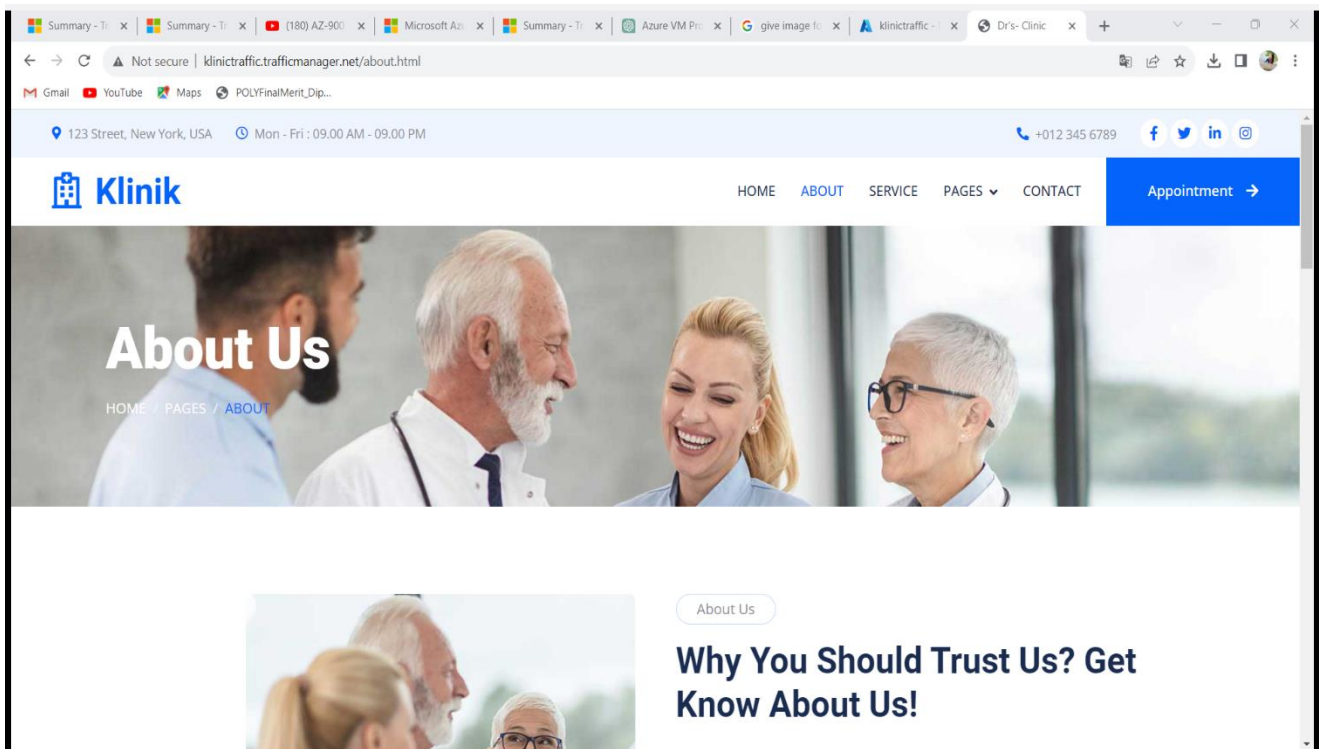
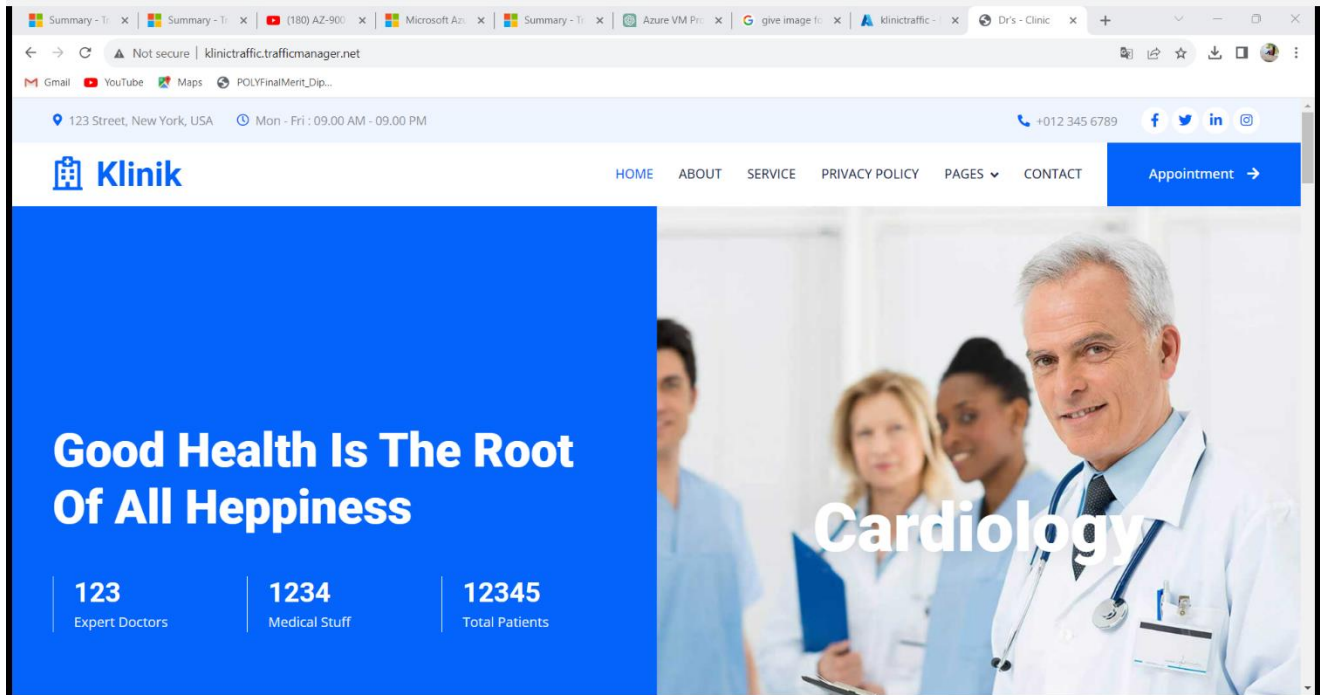
Monitoring and Logging:

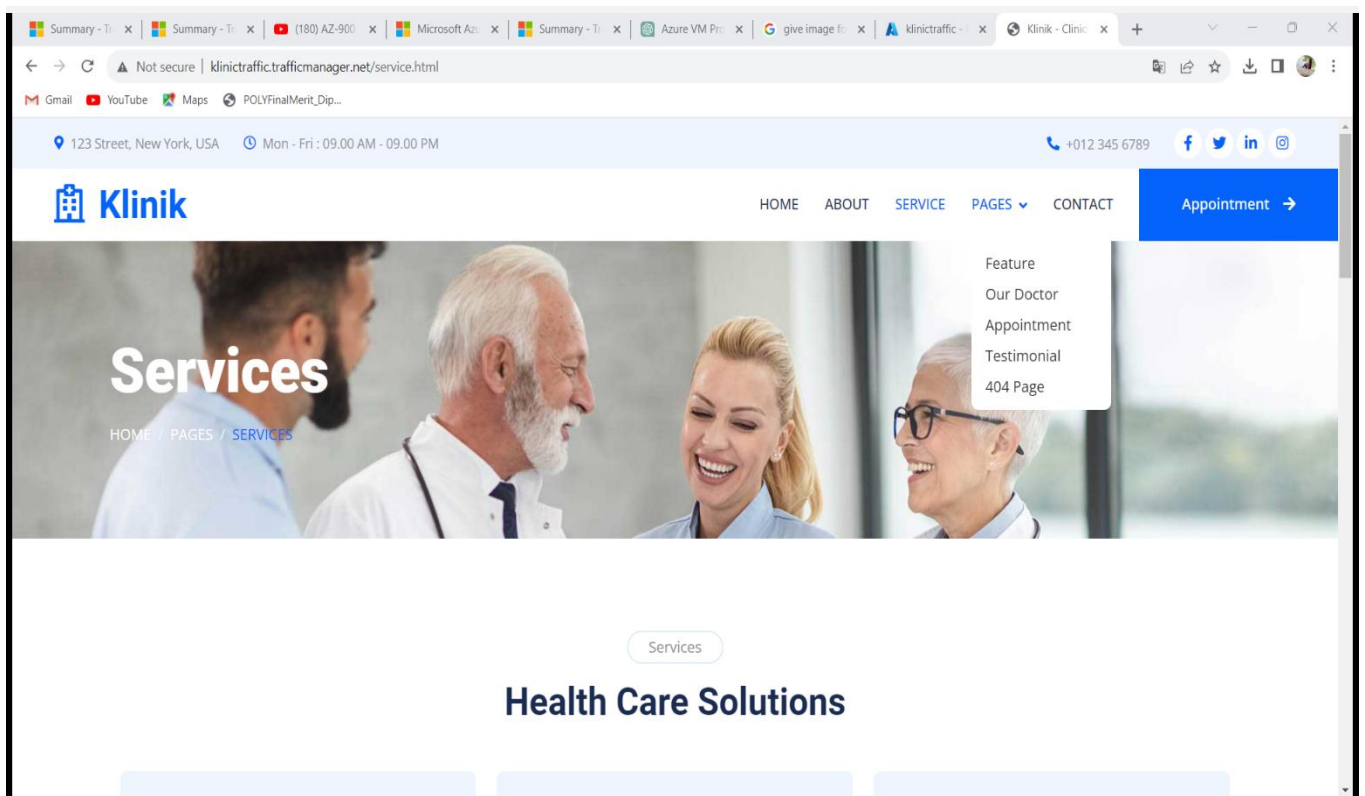
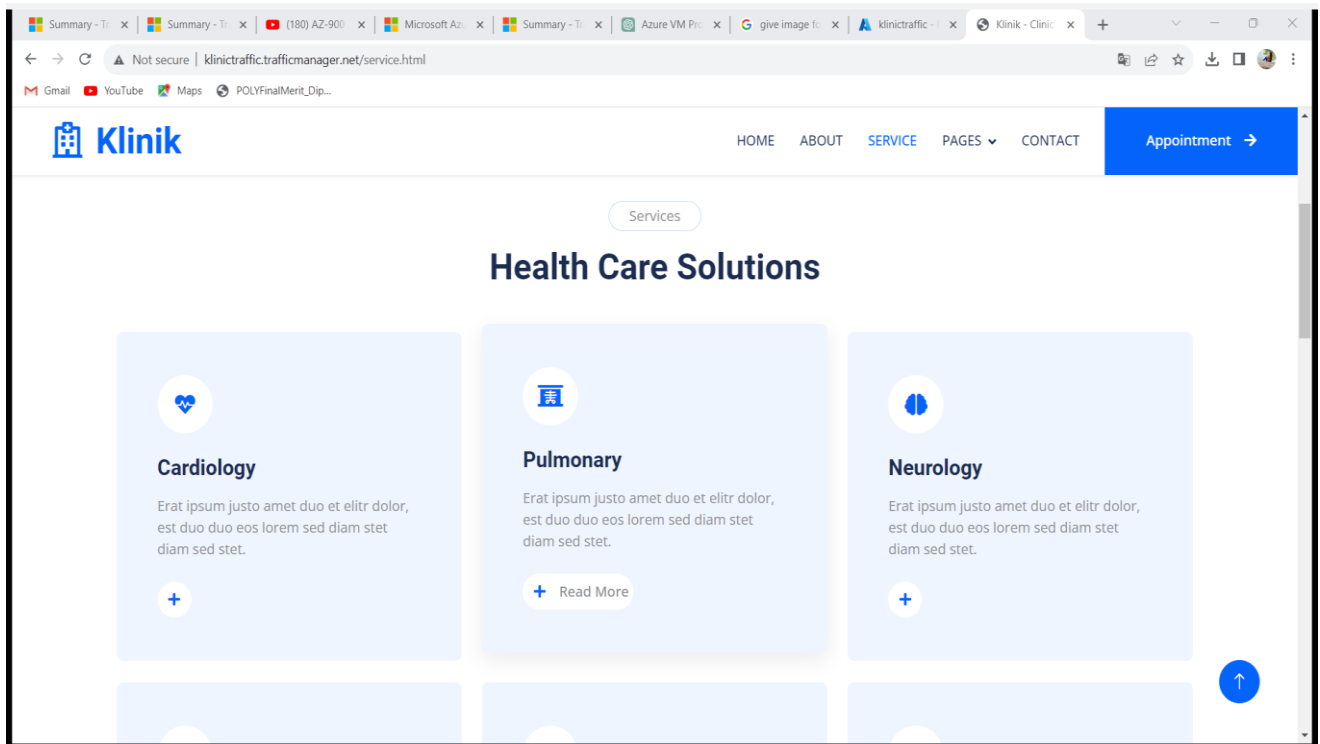
1. Set up monitoring and logging for your virtual machines, website, and Traffic Manager using Azure Monitor and other monitoring tools. Regularly check logs and metrics for any anomalies.
2. Set up alerts and notifications to be informed of any issues or service disruptions.

3. Regularly review performance data to optimize and fine-tune your website and load balancing configuration.

By performing these tests, you can ensure that the Dr's Klinik website functions correctly, and traffic is balanced evenly between the two virtual machines. Regular monitoring and testing are essential to maintain the reliability and performance of the website and the load balancing solution.

Website Overview





Maintenance

Routine maintenance is critical to keep your Azure-based Dr's Klinik website and infrastructure running smoothly, secure, and performant. Here's an overview of routine maintenance tasks, including best practices:

1. **Security Updates And Patching:**
 - **OS Update:** Regularly apply operating system updates and patches to the virtual machines to address security vulnerabilities and improve stability.
 - **Application Updates:** Keep the web application, including the CMS, server-side scripts, and third-party software, up to date.
2. **Monitoring and Alerting:**
 - Implement Azure Monitor and other monitoring tools to track the health and performance of your website and infrastructure.
 - Set up alerts for metrics related to CPU usage, memory, disk space, and website availability. Define thresholds for when alerts should trigger.
3. **Backup And Disaster Recovery:**
 - Continuously monitor the backup status and retention policies for your Recovery Service Vault. Ensure backups are running as scheduled.
 - Periodically test the restoration process to verify that backups can be successfully restored.
4. **Cost Management:**
 - Use Azure Cost Management tools to track and optimize your cloud spending. Set budgets and alerts to avoid unexpected cost overruns.
 - Identify underutilized resources and consider decommissioning them to reduce costs.
5. **Documentation:**
 - Maintain up-to-date documentation that includes configurations, settings, network diagrams, access credentials, and contact information for the team responsible for maintenance.
6. **Testing:**
 - Regularly conduct testing and quality assurance checks for website functionality, ensuring that features are working as intended.
 - Implement automated testing and continuous integration/continuous deployment (CI/CD) pipelines for code changes.
7. **Disaster Recovery Drills:**
 - Conduct periodic disaster recovery drills to ensure that in the event of a failure or disaster, you can quickly recover data and services.
8. **Documentation and Training:**
 - Document any changes to configurations, security settings, or deployment processes. Train the team on these changes.
9. **Optimization:**

- Regularly review and optimize your website and infrastructure for cost-efficiency, performance, and security.

10. Communication and Incident Response:

- Establish communication and incident response protocols to ensure timely response to outages or security incidents.

11. Regular Audits:

- Conduct regular security and compliance audits to ensure adherence to regulations and best practices.

By consistently performing these maintenance tasks and adhering to best practices, you can help keep your Dr's Klinik website and Azure infrastructure healthy, secure, and responsive to user needs. This not only improves the overall user experience but also mitigates potential risks and reduces operational costs.

Troubleshooting

Certainly, troubleshooting common issues that may arise in your Azure-based Dr's Klinik website, Traffic Manager, and Recovery Service Vault is crucial to maintaining a reliable service. Here's a section on common issues and how to troubleshoot them:

Common Issues and Troubleshooting

IIS Server Issues:

1.Website Not Accessible:

Issues: The website is not accessible, showing server errors or a blank page.

Troubleshooting:

- Check the virtual machine's status. Ensure it's running without errors.
- Review IIS logs and event logs on the VM for specific error messages.
- Verify that the website application pool is running.
- Test the website internally by accessing it directly through the VM's local IP address to isolate external network issues.

2.Slow Website Performance:

Issues: Traffic is not evenly distributed among the virtual machines as expected.

Troubleshooting:

- Check the Traffic Manager's routing method. Ensure it aligns with your intended load balancing strategy (e.g., priority, weighted, geographic).
- Verify that both VMs are healthy and responsive. The Traffic Manager won't send traffic to unhealthy endpoints.
- Check if there are latency or health probe issues impacting routing.

3.Traffic Manager Failover Issues:

Issues: The Traffic Manager doesn't fail over to the secondary VM when the primary VM is unavailable.

Troubleshooting:

- Review the health probe settings. Ensure that the probes accurately detect the VM's status.
- Check the configuration of the primary and secondary endpoints. The primary should be set to the healthy VM, and the secondary should be set to the backup VM.

Recovery Service Vault Recovery Procedures:

1. VM Data Loss:

Issues: Data on one of the VMs is lost or corrupted, and you need to recover it from the backups.

Troubleshooting:

- Access the Recovery Service Vault.
- Go to "Protected items" and select the VM you want to restore.
- Choose a recovery point and initiate a restore operation.
- Follow the wizard to restore the VM data.

2. Backup Failures:

Issues: Backup jobs are consistently failing.

Troubleshooting:

- Check the VM's connectivity to the Recovery Service Vault. Ensure it can reach the Azure Backup service endpoints.
- Review the backup policies and ensure they're correctly configured.
- Verify that there's enough storage in the Recovery Service Vault for backups.
- Check if the Azure Backup agent is updated to the latest version.

For any of these common issues, consider referring to Azure's documentation, support forums, and Microsoft's support channels for specific troubleshooting steps or guidance tailored to your environment. Regularly monitoring your systems and maintaining accurate documentation can help identify and address issues proactively.

CONCLUSION

Summarize the project and its successful implementation. Mention any lessons learned or future improvements that could be made.

Project Summary:

The Dr's Klinik website project successfully deployed a healthcare web application using Azure cloud services. The project encompassed the creation of two virtual machines to host the website, the configuration of load balancing with Azure Traffic Manager, and the implementation of backup and recovery procedures through the Recovery Service Vault. The website offers features such as appointment scheduling, patient record management, medical billing, and information dissemination.

Successful Implementation:

- The website is live, accessible to users, and functional, meeting the objectives of providing healthcare services efficiently.
- Azure's scalability and high availability features ensure that the website can handle fluctuations in traffic while maintaining uptime.
- The backup and recovery procedures in place provide data protection and disaster recovery capabilities.
- The use of Azure's security features helps maintain data security and compliance with healthcare regulations.
- Regular monitoring, testing, and maintenance ensure the system's health and performance.

Lesson Learned and Future Improvements:

- **Performance Optimization:** Regular performance tuning and optimization can enhance website responsiveness.
- **Security Enhancement:** Continuous security monitoring, threat detection, and adherence to evolving security best practices are essential.
- **Disaster Recovery Drills:** Periodic disaster recovery drills can enhance confidence in the recovery process.
- **Automation:** Further automation of deployment, monitoring, and scaling processes can streamline operations.
- **Documentation and Training:** Ensure that documentation is up-to-date, and team members are trained in Azure and website management.
- **Compliance:** Stay updated with changes in healthcare regulations and adapt the system to remain compliant.

Overall, the successful implementation of the Dr's Klinik website project demonstrates the advantages of using Azure's cloud services for hosting a healthcare application. Lessons learned and future improvements will help the project evolve, ensuring it continues to provide efficient healthcare services and maintain data security and compliance.