Handover document (User manual)



Table of Contents

[Overview 2](#_heading=h.gjdgxs)

[Brief Company background 2](#_heading=h.30j0zll)

[Project background and goals 3](#_heading=h.1fob9te)

[Fonteyn Vakantieparken – finished moving to the cloud 3](#_heading=h.3znysh7)

[Setup and Deployment 3](#_heading=h.2s8eyo1)

[Cloud environment configuration 3](#_heading=h.17dp8vu)

[Cost-effective management setup 3](#_heading=h.3rdcrjn)

[Best practices 3](#_heading=h.4cimr9k8r3rd)

[Configuration 3](#_heading=h.1ksv4uv)

[Network Infrastructure/Architecture Diagram 3](#_heading=h.44sinio)

[Communication Definitions 4](#_heading=h.2jxsxqh)

[Proof of Concept (Working IT Infrastructure) 4](#_heading=h.z337ya)

[Automation setup 4](#_heading=h.3j2qqm3)

[Maintenance 4](#_heading=h.1y810tw)

[Security Measures and Protocols 4](#_heading=h.4i7ojhp)

[Regular Maintenance Procedures 4](#_heading=h.2xcytpi)

[Backup and Restore Guidelines 4](#_heading=h.1ci93xb)

[Innovation Implementation and Maintenance 4](#_heading=h.3whwml4)

[Monitoring and Logging 4](#_heading=h.2bn6wsx)

[Monitoring Tools and Procedures 4](#_heading=h.qsh70q)

[Logging Best practices 4](#_heading=h.3as4poj)

[Resilient and Secure Infrastructure Monitoring 5](#_heading=h.1pxezwc)

[Backup and Restore 5](#_heading=h.2p2csry)

[Backup Procedures 5](#_heading=h.147n2zr)

[Restore Procedures 5](#_heading=h.3o7alnk)

[Data Protection and Disaster Recovery 5](#_heading=h.23ckvvd)

[Backup and Restore Best Practices 5](#_heading=h.ihv636)

# Overview

## Brief Company background

Fonteyn Holiday Parks company asked for our help to organize and centralize the ICT environment. In the past the number of users working on each environment is also relatively limited. User management was a mess, because employees who have been working for the group for some time often have too many authorizations based on their previous positions. But there were also many employees in the Windows Active Directory who left the company a long time ago. There were different naming conventions for the usernames and groups and there is no password policy. There were the main problems in addition to other spillover problems.

## Project background and goals

The project involves migrating Fonteyn Vakantieparken's existing IT infrastructure to the cloud, and we're gearing up for a big move to it, called "Move2Cloud." Fonteyn already uses Azure and Office 365, which will be the foundation for the cloud migration.

## Fonteyn Vakantieparken – finished moving to the cloud

At the moment our group finished moving the infrastructure to the cloud and it was secured by pfSense firewall, monitored by Uptime Kuma, has a reliable backup configuration. We deployed website in Azure and created custom domain name.

# Setup and Deployment

## Cloud environment configuration

1. **Backup Service:**

a. **Service Name:** Azure Backup Vault

b. **Backup Policies:**

- Daily incremental backups with a retention period of 14 days.

- Weekly full backups retained for 4 weeks.

c. **Storage Configuration:**

- Utilizing Azure Blob Storage for backup storage.

- Redundancy implemented for high availability.

d. **Encryption:**

- Data in transit and at rest encrypted using AES-256.

e. **Automation:**

- Backup schedules automated using Azure Logic Apps.

- Regular verification of backup file integrity with checksums.

2. **Virtual Machine (VM):**

a. **VM Configuration:**

- Virtual Machine Name: VM-Production

- VM Size: Standard\_DS3\_v2

- Operating System: Ubuntu 20.04

b. **Applications:**

- Running critical business applications (e.g., ERP system).

c. **Data Disks:**

- OS disk and additional data disks for application data.

d. **Backup Integration:**

- Azure Backup Extension installed on the VM.

- VM included in the daily incremental and weekly full backup schedules.

e. **Monitoring:**

- Azure Monitor configured to track VM performance metrics.

- Alerts set up for CPU, memory, and disk usage thresholds.

-Kuma monitoring is also setup

3. **Container Instance:**

a. **Container Configuration:**

- Container Instance Name: kuma

- Docker Image: WebAppImage:v1.0

b. **Application Stack:**

- Hosting a web application using python, flask and sqlite.

c. **Scaling:**

- Configured for auto-scaling based on resource utilization.

d. **Data Volumes:**

- Using Azure Managed Disks for persistent data storage.

- Data volumes backed up as part of the container instance backup.

e. **Backup Service Integration:**

- Azure Backup for Containers configured to handle container backups.

- Daily snapshots of the container instance's state.

## 

## Cost-effective management setup

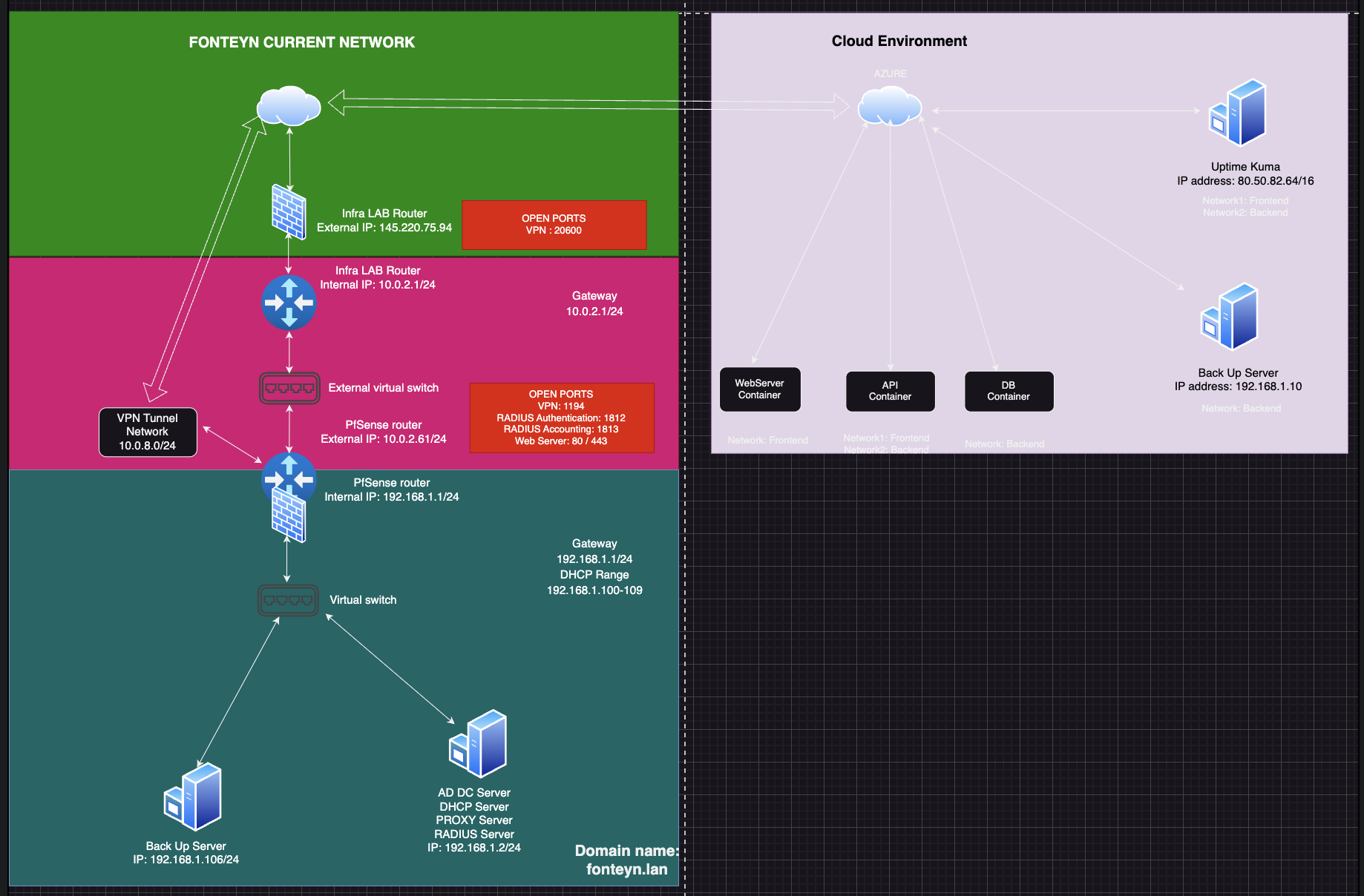
We made a cost estimation analysis and wrote down the documentation about it. We decided to use App services with Basic pricing plan, container instances and Azure functions. Totally we have 1 VM and 1 Docker container which will cost 23,94$ per month

## 

# Configuration

## Network Infrastructure/Architecture Diagram

By the finishing of the project we have following network diagram:



## 

# Maintenance

1. **Security Measures and Protocols:**

a. **Network Security:**

- Implement Network Security Groups (NSGs) to control inbound and outbound traffic to VMs and container instances.

- Utilize Azure Bastion for secure and seamless RDP/SSH access to VMs.

b. **Identity and Access Management:**

- Enforce multi-factor authentication (MFA) for all Azure accounts.

- Regularly review and update Role-Based Access Control (RBAC) policies.

c. **Data Encryption:**

- Implement Azure Disk Encryption for data at rest on VMs.

- Use Azure Key Vault for secure storage of encryption keys.

d. **Security Monitoring:**

- Set up Azure Security Center for continuous security monitoring.

- Configure alerts for suspicious activities and potential security threats.

2. **Regular Maintenance Procedures:**

a. **Operating System Updates:**

- Schedule automated OS updates for VMs during non-business hours.

- Regularly review and apply security patches.

b. **Application Maintenance:**

- Perform routine maintenance on business applications hosted on the VM.

- Implement blue-green deployments for seamless application updates.

c. **Container Updates:**

- Regularly update Docker images for container instances.

- Employ Kubernetes for orchestrating container updates without service interruption.

d. **Performance Optimization:**

- Periodically review and optimize VM and container instance configurations.

- Analyze Azure Monitor metrics for performance improvement opportunities.

3. **Backup and Restore Guidelines:**

a. **Security in Backup and Restore:**

- Ensure that backup data is encrypted during transmission and storage.

- Implement secure authentication mechanisms for backup and restore processes.

b. **Test Restorations:**

- Conduct regular tests of the restoration process for VMs and container instances.

- Validate the integrity of restored data and applications.

c. **Backup Monitoring:**

- Monitor backup job status using Azure Monitor.

- Establish alerts for backup failures and anomalies.

d. **Documentation:**

- Keep detailed documentation on backup and restore procedures up to date.

- Include contact information for key personnel involved in the process.

4. **Innovation Implementation and Maintenance:**

a. **Cloud-native Technologies:**

- Explore and implement Azure services like Azure Functions for serverless computing.

- Evaluate Azure Kubernetes Service (AKS) for container orchestration.

b. **Continuous Integration/Continuous Deployment (CI/CD):**

- Implement CI/CD pipelines for automated deployment and updates.

- Integrate Azure DevOps for end-to-end application lifecycle management.

c. **Machine Learning Integration:**

- Investigate opportunities for implementing machine learning models using Azure Machine Learning.

- Continuously update and improve models based on real-time data.

d. **Feedback Mechanism:**

- Establish a feedback loop for end-users to provide insights on application usability and performance.

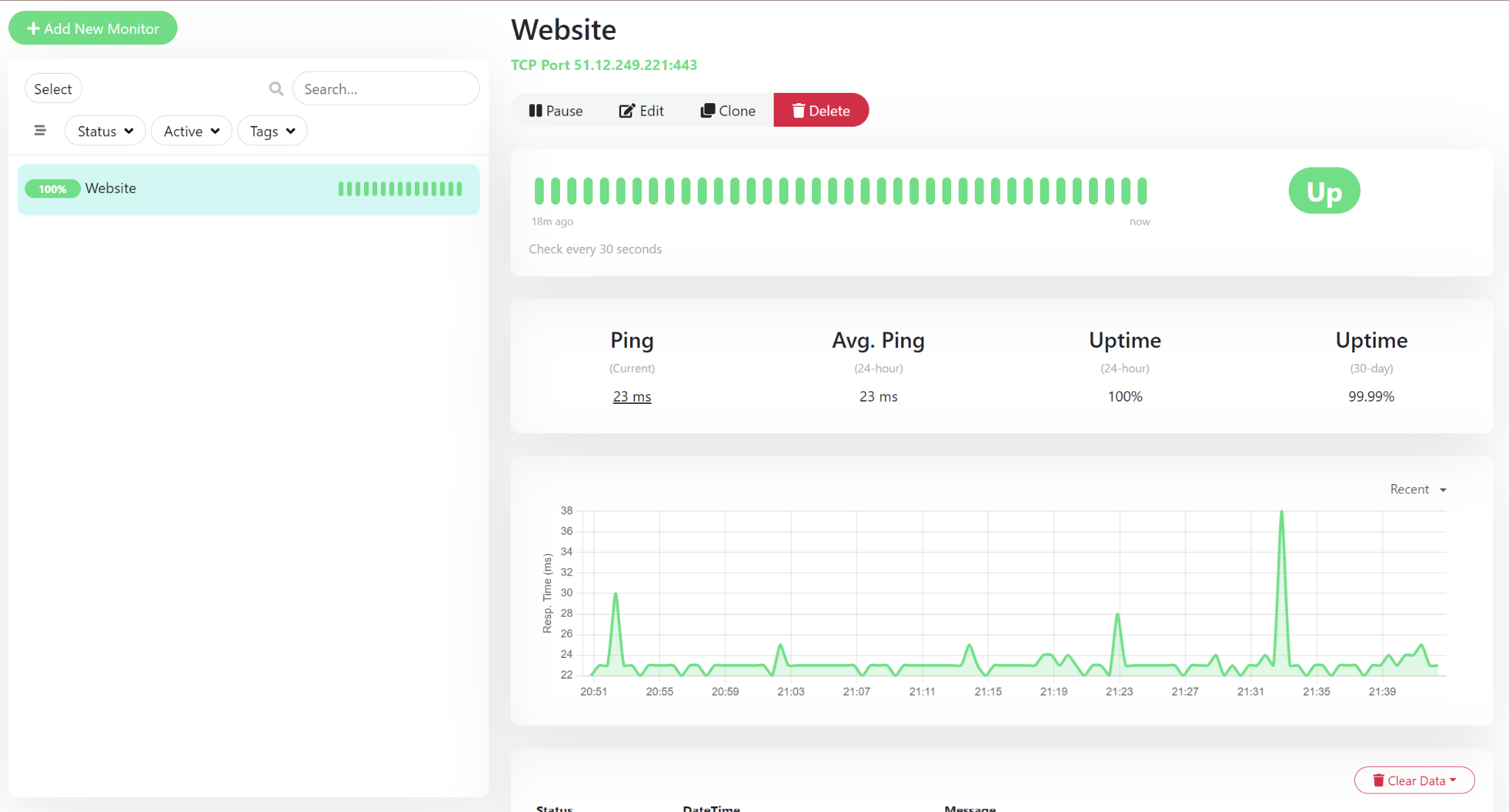
- Use feedback to drive continuous innovation and improvements.

## 

# Monitoring and Logging

## Monitoring Tools and Procedures

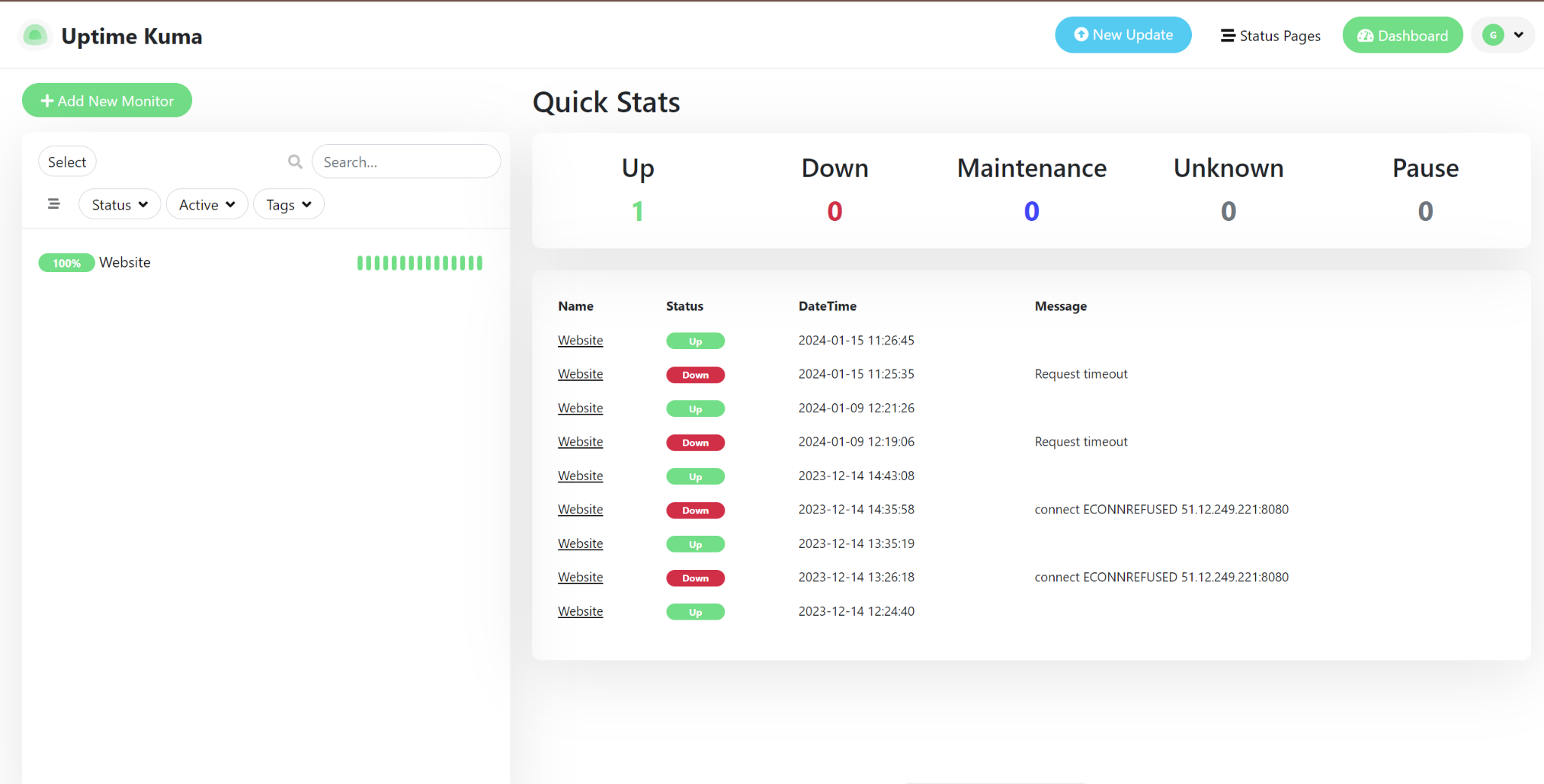
For the monitoring tool we decided to use Uptime Kuma:



This is a very effective and easy tool to use. Monitoring is performed by using TCP port of our deployed website.

## Logging Best practices

Logs of “Up” and “Down” website also displayed directly in the website:



## Resilient and Secure Infrastructure Monitoring

# Backup and Restore

Backup and Restore Operation for Azure Environment

1. **Backup Procedures:**

a. **Identify Critical Data:**

- **Critical Data:** Financial transactions, customer databases, and employee records.

b. **Define Backup Frequency:**

- **Backup Frequency:** Daily incremental backups, weekly full backups.

c. **Choose Backup Storage:**

- **Backup Storage:** Azure Backup Vault with redundant storage.

d. **Encryption:**

- **Encryption:** AES-256 encryption for data in transit and at rest.

e. **Lifecycle Management:**

- **Retention Policies:** Keep daily backups for 14 days, weekly backups for 4 weeks.

f. **Automation:**

- **Automation:** Azure Logic Apps scheduled for nightly backups.

2. **Restore Procedures:**

a. **Verify Backups:**

- **Verification:** Regularly use checksums to verify backup file integrity.

b. **Document Restoration Process:**

- **Restoration Process:** Documented steps available in the Azure wiki.

- **Dependencies:** Ensure that the target environment is available and healthy.

c. **Test Restoration:**

- **Testing:** Conduct quarterly restoration tests using a separate testing environment.

d. **Monitor and Audit:**

- **Monitoring:** Set up Azure Monitor to track restoration activities.

- **Audit:** Retain logs for audit purposes.

3. **Data Protection and Disaster Recovery:**

a. **Geo-Redundancy:**

- **Geo-Redundancy:** Azure services deployed across East US and West US regions.

b. **Replication:**

- **Azure Site Recovery:** Replicating critical VMs and applications to West Europe.

c. **Backup of Infrastructure Configuration:**

- **Backup:** Azure Policy and Azure Automation used to backup infrastructure configuration.

4. **Backup and Restore Best Practices:**

a. **Role-Based Access Control (RBAC):**

- **RBAC:** Only 'Backup Operators' have permissions to manage backup and restore operations.

b. **Monitoring and Alerts:**

- **Monitoring:** Azure Monitor set to check backup job status every hour.

- **Alerts:** Immediate alerts configured for backup failures.

c. **Regular Reviews:**

- **Reviews:** Quarterly reviews with IT and business stakeholders for adjustments.

d. **Documentation:**

- **Documentation:** Backup and restore procedures available in the Azure wiki.

e. **Version Control:**

- **Version Control:** Currently using Azure Backup v2.5.

f. **Incident Response Plan:**

- **Response Plan:** In the event of data loss, follow the incident response plan to initiate restoration.

g. **Continuous Improvement:**

- **Improvement:** Bi-annual assessments to identify areas for improvement in the backup strategy.

## 