Business Continuity Plan for Individual project

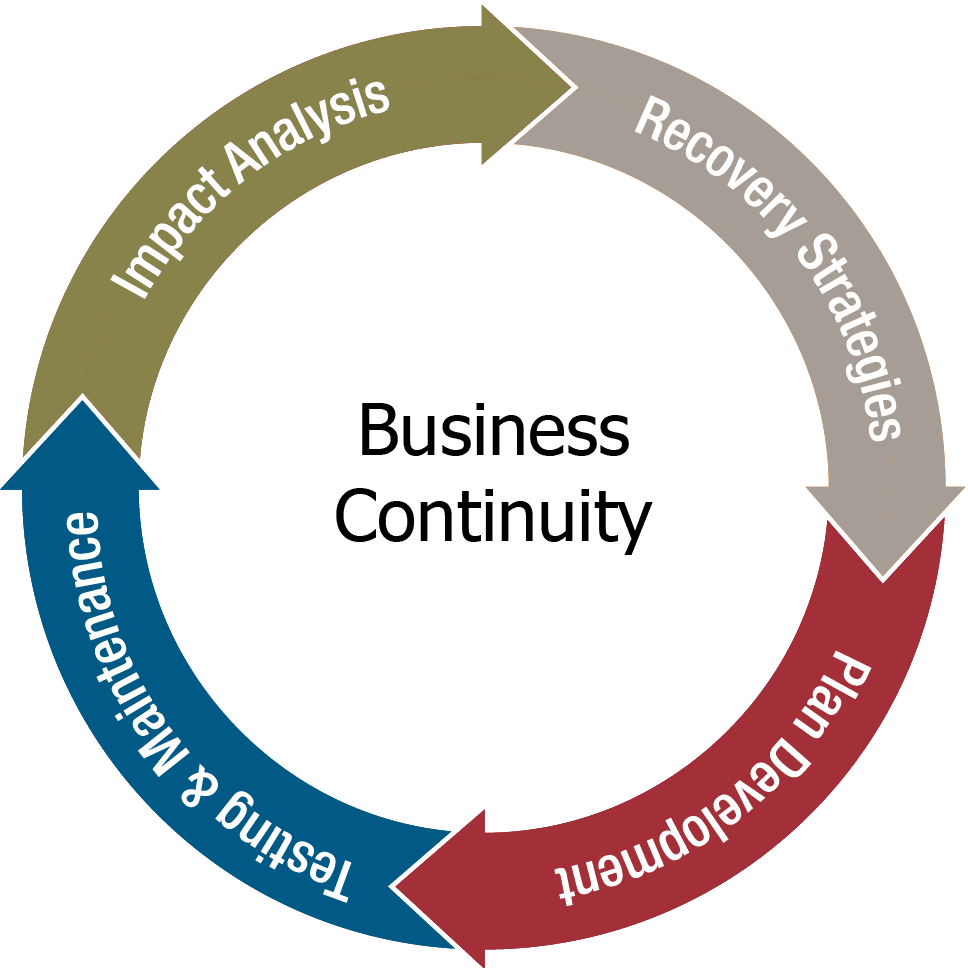


Table of Contents

[1. INTRODUCTION: 4](#_Toc156156895)

[2. ACTIVATION OF THE PLAN AND EMERGENCY DECISION-MAKING: 4](#_Toc156156896)

[Activation of the BCP: 4](#_Toc156156897)

[Triggers for Activation: 4](#_Toc156156898)

[Communication Protocols: 4](#_Toc156156899)

[Incident Response Team: 4](#_Toc156156900)

[Emergency Decision-Making Protocols: 5](#_Toc156156901)

[Decision Criteria: 5](#_Toc156156902)

[Escalation Procedures: 5](#_Toc156156903)

[3. CHECKLIST - IMMEDIATE ACTIONS FOLLOWING INCIDENT OR EMERGENCY: 5](#_Toc156156904)

[Stopping the Cluster by Mistake: 5](#_Toc156156905)

[Through Command Line: 5](#_Toc156156906)

[Through Azure: 5](#_Toc156156907)

[Deleting the Cluster by Mistake: 6](#_Toc156156908)

[Through Azure: 6](#_Toc156156909)

[Not being able to access Azure or GitHub accounts: 6](#_Toc156156910)

[Losing Access to GitHub Account: 6](#_Toc156156911)

[Losing Access to Azure Account: 6](#_Toc156156912)

[If you lose access to the Kubernetes cluster due to credential issues: 6](#_Toc156156913)

[Other Potential Issues: 6](#_Toc156156914)

[Network Failures: 6](#_Toc156156915)

[Data Loss: 7](#_Toc156156916)

[Security Breaches: 7](#_Toc156156917)

[Resource Exhaustion: 7](#_Toc156156918)

[Application Failures: 7](#_Toc156156919)

[Lack of Documentation: 7](#_Toc156156920)

[4. CRITICAL BUSINESS FUNCTIONS AND RESOURCES: 7](#_Toc156156921)

[Application Deployments: 7](#_Toc156156922)

[Persistent Volumes (PVs) and Persistent Volume Claims (PVCs): 7](#_Toc156156923)

[Configuration Data: 7](#_Toc156156924)

[Service Discovery and Load Balancing: 8](#_Toc156156925)

[Network Policies: 8](#_Toc156156926)

[Monitoring and Logging Systems: 8](#_Toc156156927)

[Identity and Access Management (IAM): 8](#_Toc156156928)

[Cluster Configuration: 8](#_Toc156156929)

[Ingress and API Gateways: 8](#_Toc156156930)

[Third-Party Integrations: 8](#_Toc156156931)

[Resource Quotas and Limits: 8](#_Toc156156932)

[5. RECOVERY PLANS: 8](#_Toc156156933)

[6. COMMUNICATIONS: 8](#_Toc156156934)

[7. EMERGENCY PACK LOCATION AND CONTENTS: 8](#_Toc156156935)

[8. ACTION AND EXPENSES LOG: 8](#_Toc156156936)

[9. KEY CONTACTS: 9](#_Toc156156937)

# 1. INTRODUCTION:

The comprehensive Business Continuity Plan (BCP) is designed to safeguard the availability and reliability of services within the Kubernetes cluster on Azure. It is extremely important for the whole project that it stays up and running as if it goes down and cannot be fixed fast it might have a grave effect on the business-have it lose a large amount of revenue or directly be critical for the company. That is why it is very important for this document to be updated and reviewed every 2 months at the least.

# 2. ACTIVATION OF THE PLAN AND EMERGENCY DECISION-MAKING:

## Activation of the BCP:

### Triggers for Activation:

The BCP should be activated under the following conditions:

Severe service disruption affecting critical business functions.

Major security breach or unauthorized access.

Unavailability of key personnel required for normal operations.

Any other event deemed by the incident response team to require BCP activation.

### Communication Protocols:

Notification Channels:

The incident response team will be notified through work app including email, messaging apps, and phone calls.

Contact List:

Terry Brown-CTO-tbrown@fontayne.co.nl-0612345678(Weekdays from 09:00 till 17:00)

Nikola Cherkov-Cloud engineer-ncherkov@fontayne.co.nl-0612345678(Weekdays from 09:00 till 17:00)

Jorn van Haimer-DevOps-jhaimer@fontayne.co.nl-0612345678(Weekdays from 09:00 till 17:00)

Alternative Communication Channels:

Main branch number:

-0612345678

### Incident Response Team:

Mentioned above in the contact list.

### Emergency Decision-Making Protocols:

Chain of Command:

It goes depending on the the people present from top to bottom:

Terry Brown-CTO-tbrown@fontayne.co.nl-0612345678(Weekdays from 09:00 till 17:00)

Nikola Cherkov-Cloud engineer-ncherkov@fontayne.co.nl-0612345678(Weekdays from 09:00 till 17:00)

Jorn van Haimer-DevOps-jhaimer@fontayne.co.nl-0612345678(Weekdays from 09:00 till 17:00)

### Decision Criteria:

Whatever the highest on the chain of command orders is what is to be done during an emergency.

### Escalation Procedures:

If the problem has not been resolved for 30 minutes, the priority of the problem becomes higher and the person who is working on it should look for help from the CTO.

# 3. CHECKLIST - IMMEDIATE ACTIONS FOLLOWING INCIDENT OR EMERGENCY:

## Stopping the Cluster by Mistake:

### Through Command Line:

Identify the cluster name and node details using kubectl get nodes.

Execute the kubectl drain command on each node to safely evict pods.

To restart, execute kubectl uncordon on each node.

### Through Azure:

Access the Azure Portal.

Navigate to the Kubernetes service.

Identify the cluster, and under the "Settings" section, find the "Scale" option.

Adjust the node count to the desired level and apply the changes.

## Deleting the Cluster by Mistake:

### Through Azure:

Refer to the installation guide or GitHub repository for the project.

Follow the documented steps to recreate the Kubernetes cluster.

Ensure data recovery mechanisms, like backups, can still be used from the persistent storage. Check on them and update them every week.

## Not being able to access Azure or GitHub accounts:

### Losing Access to GitHub Account:

Attempt to reset your GitHub account password using the account recovery options provided by GitHub.

Follow the password recovery process, typically involving email verification.

If you are unable to recover your GitHub account through the automated process, contact GitHub Support for assistance.

Provide as much information as possible to verify your identity.

### Losing Access to Azure Account:

Attempt to reset your Azure account password using the account recovery options provided by Azure.

Follow the password recovery process, which may include verification through email or phone.

If account recovery is not possible through automated means, contact Azure Support for assistance.

Be prepared to provide detailed information to verify your identity.

## If you lose access to the Kubernetes cluster due to credential issues:

Retrieve the Kubernetes configuration file (kubeconfig).

Update or replace credentials in the configuration file.

Use the updated configuration file to regain access to the Kubernetes cluster.

Regularly rotate and securely manage access credentials to avoid unauthorized access.

## Other Potential Issues:

### Network Failures:

Should not destroy the cloud as it is cloud, but backup everything either with a cloud provider or in you personal machine as a local file, preferably both.

### Data Loss:

Regularly backup important data stored in Persistent Volumes.

Integrate Azure Backup services for data backups.

### Security Breaches:

Regularly update and patch the cluster components.

Implement Azure Active Directory integration for enhanced security.

Monitor and audit cluster activities for security anomalies.

### Resource Exhaustion:

Implement resource quotas and limits for pods.

Monitor cluster resource usage regularly.

### Application Failures:

Implement health checks for applications(although Kubernetes also has in built check to see the health it is mainly for the pod and container, not for the application itself).

Use Helm charts or other package managers to version control and rollback applications.

### Lack of Documentation:

Regularly update and review project documentation.

Include troubleshooting guides in the documentation.

# 4. CRITICAL BUSINESS FUNCTIONS AND RESOURCES:

## Application Deployments:

Identify the core applications and services running on the Kubernetes cluster. Prioritize those applications that are critical for business operations and revenue generation.

## Persistent Volumes (PVs) and Persistent Volume Claims (PVCs):

Data storage is often critical for applications. Identify and prioritize Persistent Volumes and Claims associated with databases, file storage, or any other critical data.

## Configuration Data:

Configuration data, stored in ConfigMaps or Secrets, is crucial for the proper configuration of applications. Prioritize the recovery of configuration data required for critical services.

## Service Discovery and Load Balancing:

Services in a Kubernetes environment often rely on service discovery and load balancing. Identify and prioritize components like Ingress controllers, LoadBalancer services, or any other mechanism used for traffic routing and distribution.

## Network Policies:

If network policies are in use to control communication between pods, identify and prioritize these policies to ensure proper network segmentation and security.

## Monitoring and Logging Systems:

Systems responsible for monitoring, logging, and alerting play a critical role in maintaining visibility into the health and performance of the cluster. Prioritize the recovery of monitoring and logging components.

## Identity and Access Management (IAM):

If Kubernetes clusters integrate with identity and access management systems, prioritize the recovery of configurations and access controls to ensure proper security measures are in place.

## Cluster Configuration:

Refer to the deployment design document.

## Ingress and API Gateways:

Components responsible for managing external access to services, such as Ingress controllers or API gateways, should be prioritized to ensure external connectivity is restored efficiently.

## Third-Party Integrations:

There are no third party integrations for this project.

## Resource Quotas and Limits:

If resource quotas and limits are in place for pods, namespaces, or other resources, prioritize their recovery to ensure resource management is maintained.

5. RECOVERY PLANS:

Refer to Backup Solution Document.

# 6. COMMUNICATIONS:

Refer to 2: Communication protocols.

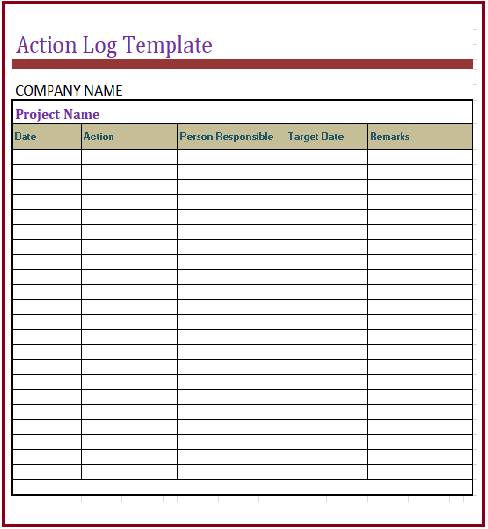
# 7. EMERGENCY PACK LOCATION AND CONTENTS:

The emergency pack is locatedin two places: one is the GitHub repository with all of the necessary documents and the other is a backup created on Azure.

Contents include documentation, configuration files, and contact information.

# 8. ACTION AND EXPENSES LOG:

This is a template to write down the expenses and actions during an emergency:



# 9. KEY CONTACTS:

Refer to 2: Communication protocols.