**Technology: Cloud Application Development**

**Project 8:** Disaster Recovery with IBM Cloud Virtual Servers

**Problem statement:**

Safeguard business operations with IBM Cloud Virtual Servers. Create a disaster recovery plan for an on-premises virtual machine, ensuring continuity in unforeseen events. Test and validate the recovery process to guarantee minimal downtime. Become the guardian of business continuity, securing the future of your organization.

**Problem definition:**

Detailed explanation of the problem definition for our project.

**Project challenge:**

The primary site may have lost an arbitrary amount of data due to the disaster, so the replication software must be able to determine what new and old state must be resynchronized to the original site.

**Why is Disaster Recovery needed?**

Consider a scenario, a major disaster occurs at a large financial services organization, and a significant cyber-attack renders all their IT systems inoperable. This attack results in data loss, system failures, and network outages, all of which have an impact on the company's ability to conduct business and provide services to its customers. This is where a Disaster Recovery (DR) plan **comes in handy.**

**Plan Development and Documentation:**

**Step1: understand our business needs**

1.identify critical data services

2.define an acceptable RPO &RTO

3.map all of the data bricks integration points that affect your business

**Step2:** **Analysis on how to meet our DR plan**

1.assess available tools

2.additional support needed

3.network configuration modification

4.channels notify internal teams and third parties

**Step3:** **choose a recovery solution strategy**

1.active passive solution strategy

2.actie active solution strategy

3.choose our tooling (sync tool Vs CI/CD for parallel deployment)

**Step4: DR for a Data bricks workspace**

1.define all infra and data bricks objects as infra as code using data bricks terraform provider

2. data replication for batch &streams

**Step5:** **implement and test our solution**

1.plan for and test changes to configuration tooling

2.test recovery

3.test backup

**Step6:** **continuous monitoring and detection**

1.monitoring tool and metrics gathered

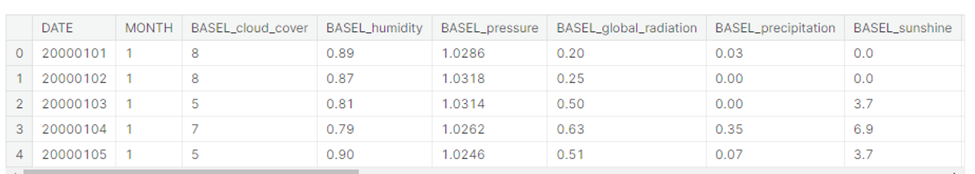
2.lerting system for notification

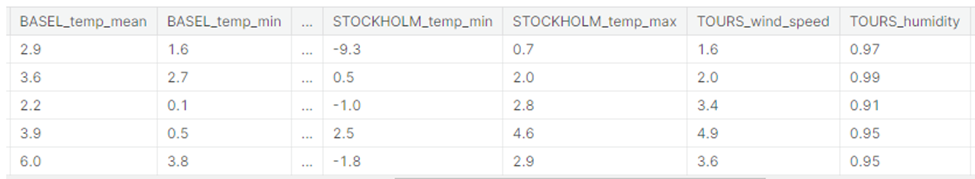
3.cluster driver logs, spark UI, stream metrics, streaming query listener

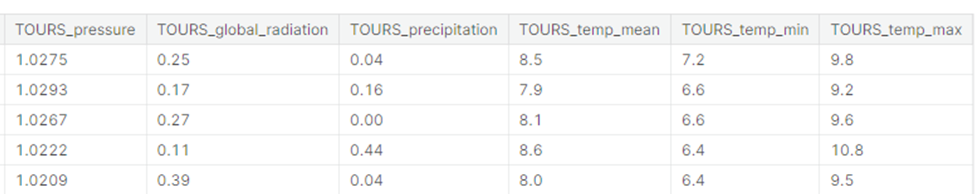
**Design loading and processing dataset**

Loading and preprocessing the dataset is an important first step in building cloud computing model. However, it is especially important for disaster recovery prediction models, as increased flexibility, scalability, and reliability.

By loading and preprocessing the dataset, we can ensure that the cloud computing algorithm is well-prepared to learn from data effectively and provide valuable insights or prediction







By using dataset loading and preprocessing……

**Design Recovery Objectives:**

Define clear **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)** for each critical system and application. **RTO** represents the maximum allowable downtime, while **RPO** determines how much data loss is acceptable.

**Disaster recovery strategy**

Develop recovery strategies and procedures that align with the RTO and RPO requirements. The choice of recovery strategy, such as backups, failover, or other mechanisms, will depend on these objectives.

if our RTO is 2 hours, you may choose to implement a hot standby server that can take over quickly in case of a failure.

**Critical Database: RTO = 4 hours, RPO = 15 minutes**

**Email System: RTO = 2 hours, RPO = 1 hours**

1.Recovery Point Objective (RPO): identifies how much data you are willing lose in the event of disaster. this value is typically specified to in a number of hours or days of data.

2. Recovery Time Objective (RTO): identifies how much downtime is acceptable in the event of a disaster.

**Design Backup configuration:**

Select and implement data backup and recovery solutions that align with your organization's needs and RPOs. This may involve regular data backups, offsite storage, and redundant systems.

Consider implementing automated backup solutions and cloud-based backup services for enhanced data protection.

**gsutil -m cp -r [SOURCE\_DIRECTORY] gs://[BUCKET\_NAME]**

**gsutil -m rsync -r [SOURCE\_DIRECTORY] gs://[BUCKET\_NAME]**

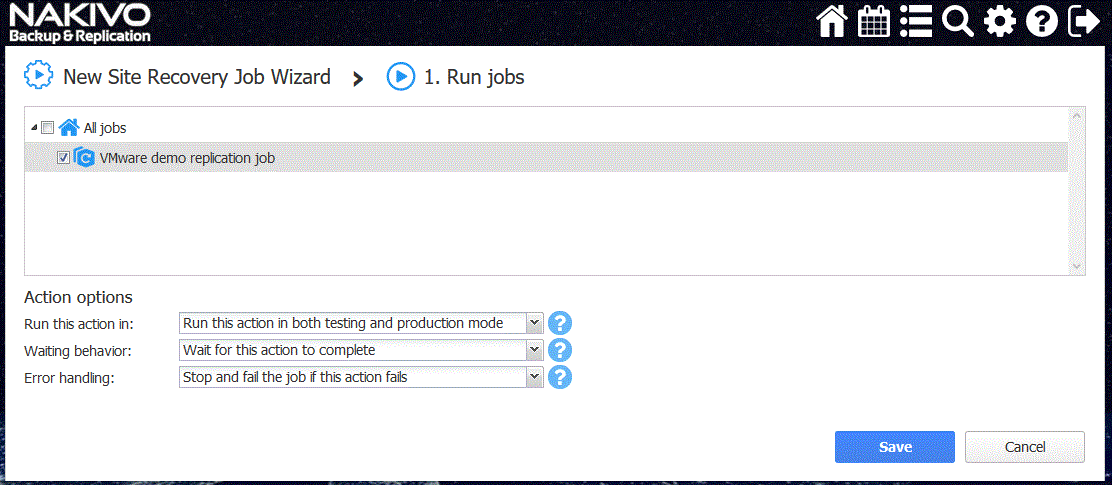
**Design replication setup:**

Choose the replication method that aligns with your disaster recovery goals:

**Synchronous Replication:** Provides real-time data consistency but may introduce latency. Data is written to both the primary and secondary locations simultaneously.

**Asynchronous Replication**: Offers lower latency but may have some data lag. Data is written to the primary location first and then asynchronously replicated to the secondary location.

crop

**Disaster Recovery testing:**

Establish a dedicated disaster recovery site or utilize a cloud-based disaster recovery solution. Ensure that this site is equipped with the necessary hardware and software to recover critical systems and data.

Regularly test your disaster recovery plan by simulating disaster scenarios. These tests help identify weaknesses, validate recovery procedures, and measure the time it takes to recover.

**Risk of business impact**

**Identifying Risks:** The first step is to identify potential risks and threats that could disrupt business operations. These can include natural disasters (e.g., earthquakes, floods), cyberattacks, hardware failures, human errors, and more.

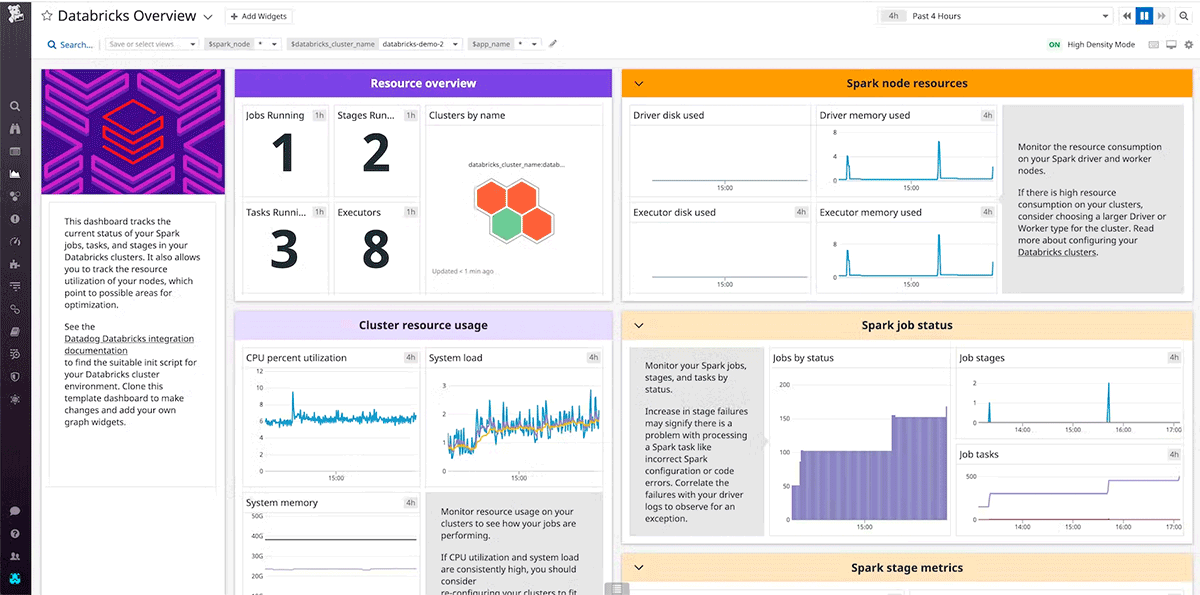
**Business Impact Analysis (BIA):** BIA assesses the criticality of various business processes and systems. It helps prioritize recovery efforts and allocate resources accordingly.

**Cloud based solution**

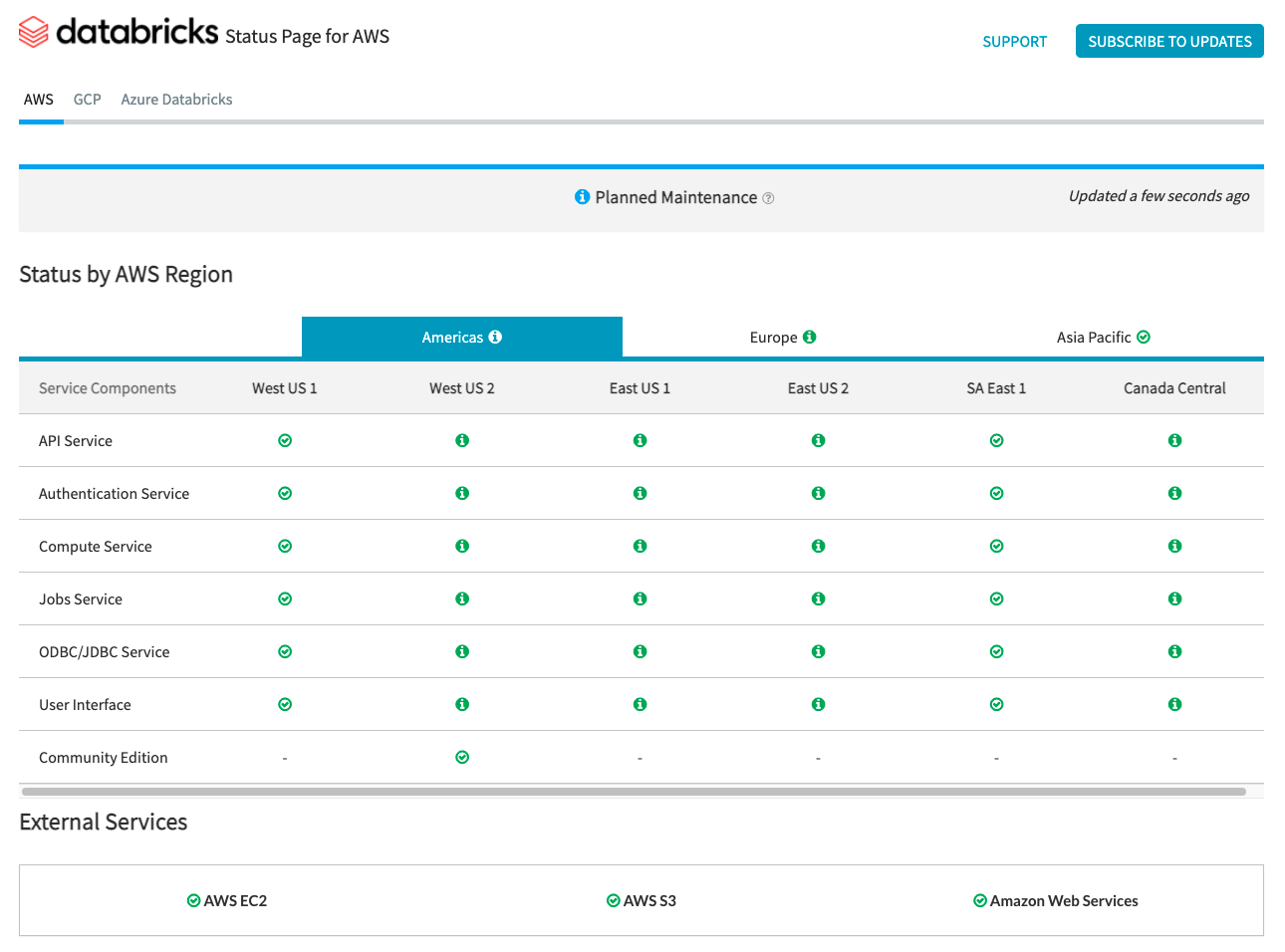
1.Consider utilizing cloud services for disaster recovery.

2.Cloud providers offer scalable and resilient infrastructure that can be quickly deployed in case of a disaster.

**Infrastructure of monitoring and overview**



**Service Status Notifications**



For status checks regarding the data plane, AWS Health Dashboard, Azure Status Page, and GCP Service Health Page should be used for monitoring.AWS and Azure offer API endpoints that tools can use to ingest and alert on status checks.

**Finalize Disaster Recovery Plan**

Ensure that disaster recovery plan is complete and well-documented. It should outline roles, responsibilities, procedures, and recovery objectives clearly.

**Conclusion**

In this phase, we have outlined the steps to take your energy consumption calculation design and transform it into an innovative solution. By following these steps, you can create a robust and accurate

system for predicting energy consumption using the provided datasets.