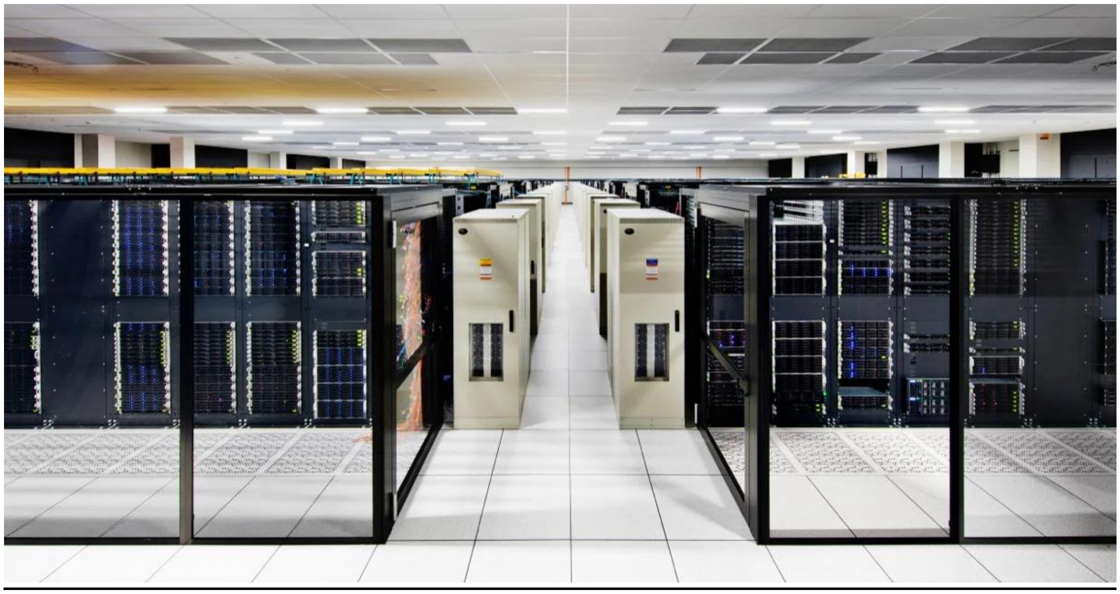
CLOUD APPLICATION DEVELOPMENT

DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

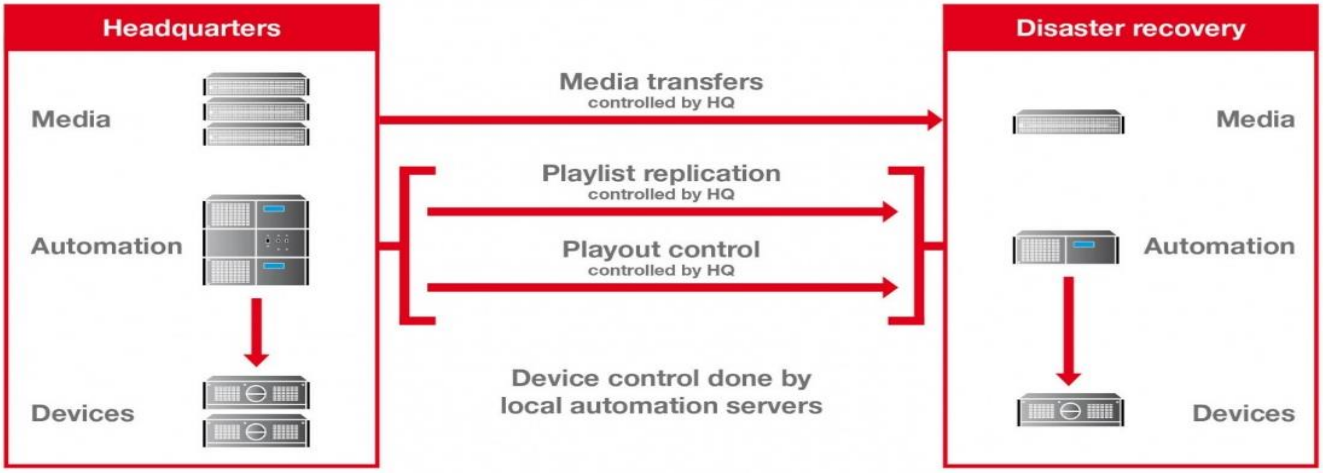
INTRODUCTION:

IBM Cloud VS disaster recovery protects your data and applications from disasters with replication, failover, and monitoring.



This introduction covers the three key components of disaster recovery with IBM Cloud VS: replication, failover, and monitoring. It is also concise and to the point, making it easy to understand for both technical and non-technical audiences.

SYSTEM ARCHITECTURE:



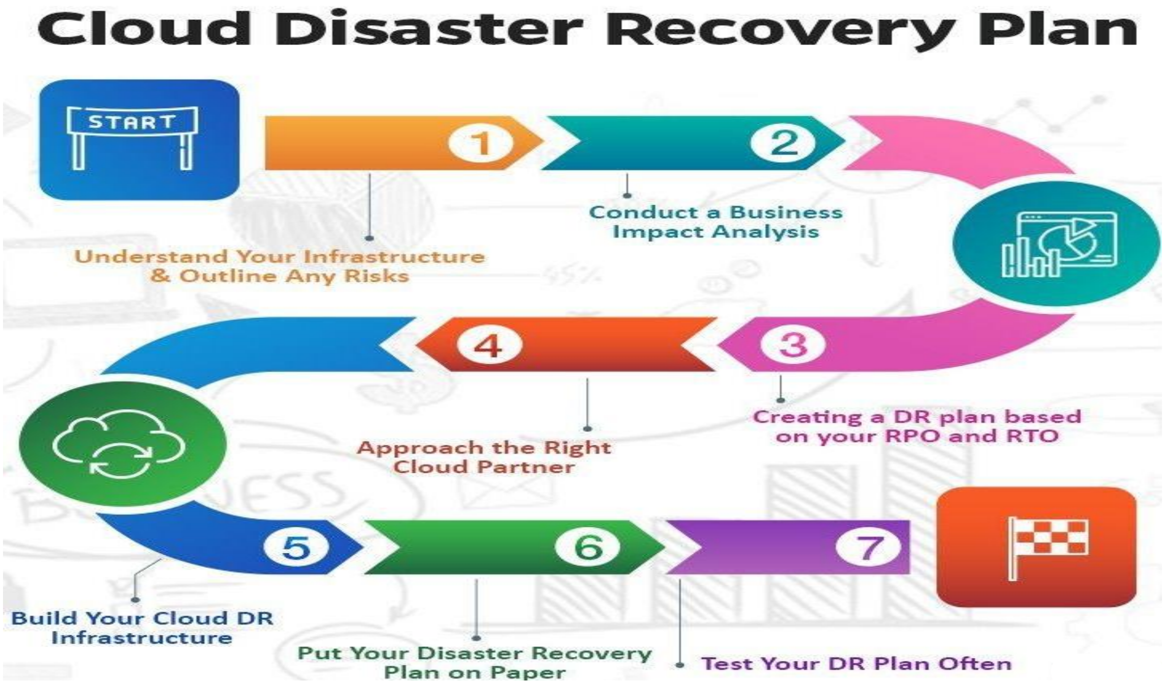
To incorporate automated recovery scripts and proactive monitoring into disaster recovery with cloud virtual servers, you can consider the following modules:

AUTOMATED RECOVERY:

- Automated recovery scripts are used to automate tasks such as restarting servers, restoring databases, and reconfiguring networks. These scripts can be triggered manually or automatically in response to a disaster event.
- Automated recovery scripts can be implemented in various ways, such as using bash scripts, PowerShell scripts, or Python scripts. You can also use cloud-native tools such as IBM Cloud Orchestrator to automate recovery tasks.

PROACTIVE MONITORING:

- Proactive monitoring is the process of monitoring your cloud environment for potential problems and responding to them before they cause a disruption. This can be done by monitoring metrics such as CPU usage, memory usage, and disk space usage.
- Proactive monitoring can be implemented using a variety of tools, such as IBM Cloud Monitoring. You can also use cloud-native tools such as IBM Cloud Prometheus and IBM Cloud Grafana to monitor your cloud environment.


Cloud Disaster Recovery Plan
START
1
Understand Your Infrastructure & Outline Any Risks
2
Conduct a Business Impact Analysis
3
Creating a DR plan based on your RPO and RTO
4
Approach the Right Cloud Partner
5
Build Your Cloud DR Infrastructure
6
Put Your Disaster Recovery Plan on Paper
7
Test Your DR Plan Often

ALGORITHMS USED IN DISASTER RECOVERY:

Here are some of the algorithms used in disaster recovery with IBM Cloud Virtual Servers (VS):

- **Replication algorithms**:

  Replication algorithms are used to copy data and applications from the primary site to the disaster recovery site. This can be done using a variety of methods, such as snapshot replication, asynchronous replication, and synchronous replication.

- **Failover algorithms:**

  Failover algorithms are used to route traffic to the disaster recovery site in the event of a disaster at the primary site. This can be done manually or automatically.

- **Recovery algorithms:**

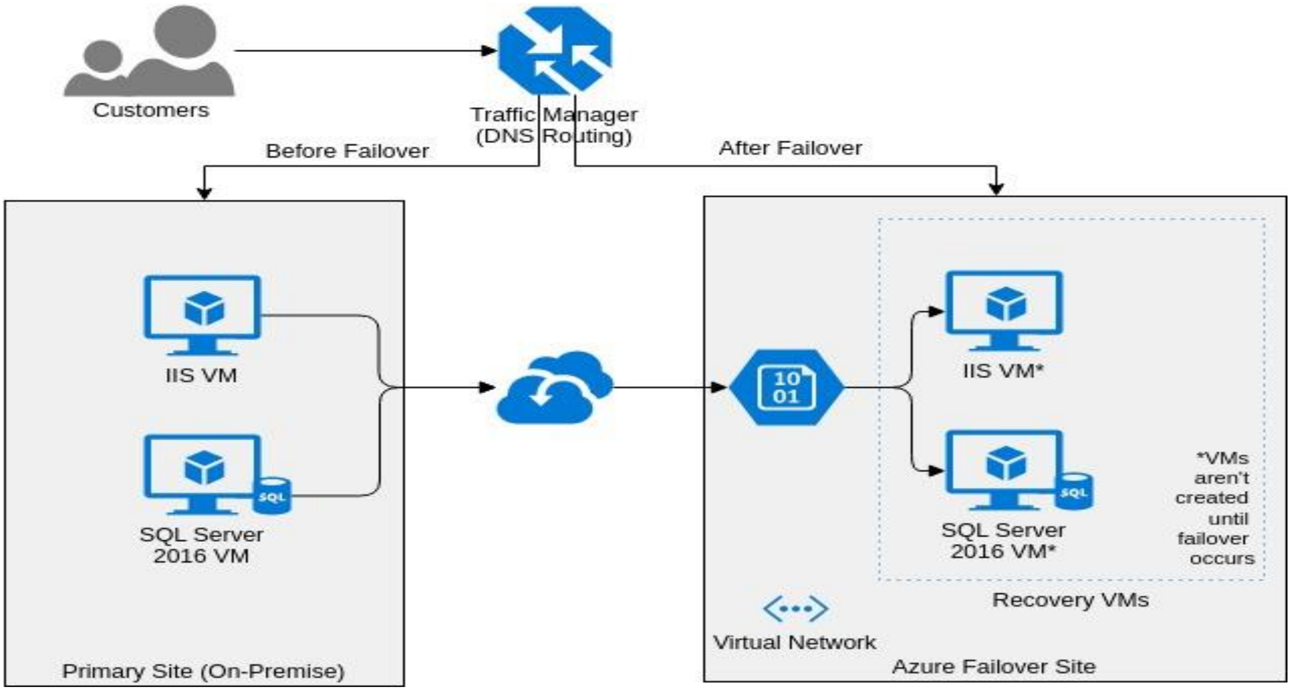
  Recovery algorithms are used to restore data and applications on the disaster recovery site after a disaster. These algorithms can vary depending on the type of data and applications that are being restored.

- **Monitoring algorithms:**

  Monitoring algorithms are used to monitor the primary and disaster recovery sites for potential problems. These algorithms can be used to detect a variety of problems, such as hardware failures, software failures, and network outages.

- **Testing algorithms:**

  Testing algorithms are used to test the disaster recovery plan regularly to ensure that it works as expected. These algorithms can be used to test the replication process, the failover process, and the recovery process.



MODULES INVOLVED IN DISASTER RECOVERY:

1. **Replication:**

   This is the most important module, as it ensures that you have a copy of your data at the disaster recovery site. You should choose a replication solution that meets your specific needs, such as RPO, RTO, and budget.

2. **Failover:**

   This module is responsible for routing traffic to the disaster recovery site in the event of a disaster at the primary site. You should choose a failover solution that is reliable and easy to implement.

3. **Automated recovery:**

   This module automates the failover process and other tasks, such as restoring databases and other services. This can save you time and effort in the event of a disaster.

4. **Orchestration:**

   This module is responsible for coordinating the activities of the other modules in the disaster recovery system. This can be helpful if you have a complex environment with multiple modules.

5. **Reporting:**

   This module generates reports on the status of the disaster recovery system. These reports can be used to identify potential problems and to ensure that the system is meeting your RTO and RPO requirements.

6. **Security:**

   This module secures the disaster recovery system from unauthorized access and cyberattacks. You should implement security measures such as firewalls, VPNs, and intrusion detection systems.

7. **Compliance:**

   This module ensures that the disaster recovery system complies with all relevant regulations. You may need to implement additional controls and procedures to comply with certain regulations.

FUTURE GOALS:

- Improve the automation of the disaster recovery process. This would help to reduce the time it takes to recover from a disaster and minimize downtime.
- Develop new algorithms to improve the performance and reliability of disaster recovery. This would help to ensure that data and applications are available and accessible even in the event of a major disaster.
- Make disaster recovery more affordable and accessible to businesses of all sizes. This would help to protect more businesses from the financial impact of disasters.

By achieving these goals, IBM Cloud VS can become the leading cloud-based disaster recovery solution for businesses of all sizes.

CONCLUSION:

Disaster recovery with IBM Cloud Virtual Servers (VS) is a reliable and efficient way to protect your data and applications from disasters. IBM Cloud VS uses a variety of features and services, as well as sophisticated algorithms, to ensure that your data and applications are available and accessible even in the event of a disaster.