South Asian Journal of Engineering and Technology Research Article

Open Access Full Text Article 102(2020)1-4 DOI: 10.26524/sajet.2020.2.2

Business continuity plan

Ashok Kumar[a]
[a]Jnana Ganga, Gulbarga, Karnataka 585106

Corresponding author.
Correspondence: Ashok Kumar
E-mail:Akchamp06@gmail.com

Article info
Received 4th May 2020
Received in revised form
11 June 2020 Accepted
14 June 2020

Keywords
Business, Continuity,Plan,Back up, Disaster plan

Abstract

The Business continuity plan and strategy provide effective solutions to Multi-cloud and Microservice approach. The business continuity plan helps to maintain backup and disaster recovery. It ensures continuous business processes during disasters and emergencies. The business continuity planning methods that include risk assessment, analyze impacts, and entire business continuity strategies.

1. Introduction

It analyzes impacts and risks in cloud computing and it provides possible solutions to mitigate the issues in the hybrid cloud. The business continuity plan facing any disasters. The business continuity plan provides data backup and disaster recovery. It operates and manages cloud solutions. It improves performance and user access to critical systems. The DSI board plan to implement a business continuity plan in the hybrid cloud. The business continuity plan provides data backup and disaster recovery strategies. It ensures continuing business services during any disasters. Application resilience, backup, and disaster recovery strategies have been discussed in this section (1).

2. Types of continuity plans

Business Continuity Plans are extremely important when you have a company that operates in many different areas, and it is important that you take the time to review your plan on a regular basis. If you are not following through with this important plan, it is possible that you could lose your business, and the people who work for you.

Some types of business continuity are not only required but they are a vital part of maintaining a company that is growing and expanding. However, before you ever start planning a plan for business continuity, you need to identify exactly what types of activities you want to include in your plan.

- When you are planning your business continuity, you need to take several things into consideration. The first thing is that you need to think about what exactly your business is about. This is extremely important, because this will help you to determine exactly what types of activities you want to incorporate in your business continuity plan. You will want to consider everything from the employees who work for you, and even the type of equipment that you have.
- The next thing that you need to consider in developing your business continuity plan is the fact that you have to think about the current and potential threats that your company might face. This will help you think about the types of security measures that you need to take. You will also want to consider the types of events that could occur, and the types of problems that could occur with the security of your business. This can be a very important aspect of your plan, because if you are not prepared for the worst, it can be devastating to your business.
- The third thing that you need to think about in developing your business continuity plan is the fact that you will want to consider the type of assets that you have at your disposal. If you have some good assets, this can be extremely important for your business, because if your assets were damaged,

then you could face serious problems. For example, if you were to lose a major computer, then you might not be able to perform as well as you would like.

All of these aspects are incredibly important for developing your business continuity plan. This is important because if you are not following through with this plan, you might have a serious problem with your business, and you might even lose your business.

3. Issues in application resilience

Application resilience is the ability to provide a reaction to the problems by applications. There are major issues in this quality. It is essential to remove that illness from the application. Losing fault tolerance is an issue in the cloud process. As the DSI process includes a huge amount of data for processing, it is important to recover this problem effectively. Although applications always react to the problem appropriately still there is some problem in predicting appropriate service in the cloud process. It often requires a massive residential place to place the data in a common repository. By implementing various approaches, the reliable scenarios become unreliable and those situations are considered as the major issue in this process. Lacking reliability is the worst case of this clouding process in the DSI model. Cloud computing needs to stay comfortable and with the large outage, the resilience of the system could be generated. This is a traditional approach to the cloud application. A single point of failure is another major issue in application resilience in this case. The challenges in workloads would be the traditional process. Balancing workloads are important in this section of the cloud process. Cloud availability is based on this issue recovery process. Data management can also be an issue in this process. Because there will be a huge amount of data need to process in this cloud migration process. Hence, data availability and data management is a major issue. For large data process, fault tolerance is another problem in this DSI cloud data process with certain constraints (2).

4. Data Backup and Disaster Recovery

Data backup plays a vital role in cloud computing. Data backup is to keep data from disasters and cyber-attacks. It manages and protects sensitive information. The cloud service provider is responsible to manage data backup to keep security and privacy. The cloud service providers should copy all files and services into backup storage. If any disasters and attacks happen, then easily restore data from data backup. The cloud service provider should take multiple copies of sensitive information and must manage multiple data backup that supports to provide an extra layer of protection. The data backup helps to reduce data loss. Data backup and disaster recovery are mainly important for security purposes in cloud computing. The availability of data backup is essential. The cloud service provider must enhance the availability of data backups. The data backup is required to keep sensitive data from cybercriminals and vulnerability attacks. Disaster recovery provides security solutions to keep data. It protecting the sensitive data and applications from any disasters and unwanted intrusions. It can protect entire servers in a cloud environment. It provides safeguard sensitive data and it easily recovers information from any kind of disaster (3).

The disaster recovery keeping data centers in the cloud environment. It can be reducing impacts and consequences in the business. The cloud service provider must take multiple copies of all information and store it into data backup. If any accidental deletion, corruption, and any kind of disasters happening, the easily recover or restore data from data backup. Disaster recovery ensures continuing business operations while disasters. The disaster recovery covers the entire strategy for reacting to a disaster event and putting the data backup process into action. It offers a high level of security of the data and other resources.

The business continuity plan offers data backup and disaster recovery strategies. It effectively protecting data and other resources from many disasters and attacks. It can reduce security risks and malicious attacks. It helps to reduce or minimize data loss and keep security in the hybrid cloud. The DSI could implement a business continuity plan in the hybrid cloud that helps to protect data from any disasters (4).

5. **Remote administration**

The remote administration can be achieved in the micro service architecture. The DSI system which uses the micro service approach to implement the efficiency of data delivery. The DSI users' needs to access the online application of spatial data with remote (4). The remote administration can be very helpful for the DSI system to share the resources from anywhere at the time. The various sensors will be used for the remote access of the micro service architecture in the DSI system. The remote procedure in micro service architecture involves the concept of RPI (remote procedure invocation). The client system which needs to access the micro service of the DSI

6. Resource management

In the micro service approach of the DSI system, different resources are there to be maintained. These services can be collaborated through the interface which is present in the DSI system. This is the challenging issue in maintaining the resources during the run time of the process in the micro service architecture (5). Hence, the gentle resource management is required. The resource management can be achieved by avoiding the resource traffic and ensures the congestion control over the network.To manage the micro service applications the management plans should be made in prior and then execute the plan in the platform. Reduce the operations involved in the micro service resources. The minimal set of operational resources will help in managing the micro service applications.The resources should be checked periodically by implementing the continuous delivery of data to the resources.The operations should be checked once again even after the finishing the reinvest of operations.Many tools are also available in the internet to manage the micro service architecture (6). These tools are available in the micro service monitoring platform. Example: Ray gun APM this tool provides the instrumentation to complete the process and contains dash board to look the data of the resources. The tool Ray gun supports the platform of .NET

7. SLA management

SLA refers to the service level agreement in the micro service approach of the DSI system. It is the process of managing the service levels and ensuring all the agreements and check the services present in the service level of the DSI system. The service level is responsible for the operational constraints and all the important aspects (7). In DSI system the important operation is to manage the large amount of operation and performs the delivery efficiently ensuring the security. Hence, the service level management is very much required to deploy the micro service architecture.The cloud SLA is an agreement between the cloud service provider and the customer where the minimum resources are shared between them (8). The cloud is a virtual environment which is adopted in the DSI system to achieve the availability and the reliability. The service level management can be of different categories that is service based SLA, customer based SLA and the hierarchical SLA (9). The defect rates, standard compliance and the technical quality are the factors needs to be calculated to determine the service level of the resources. The service level agreement works by defining the SLO (service level object). The client user should be aware of complete description about SLA and SLO and then handle the service to the application interface. The API developer should understand the concept of SLA and the SLO carefully before committing to give the required API.The structure of SLA should be satisfied by the API developer. Only then the resource can be managed successfully. The SLA can be achieved by assigning SLO to each of the controller device. The threshold value of SLO is maintained for each of the attribute (10-11).

Conclusion

Business continuity plan is essentially a detailed description of the entire plan. It will explain how and when different elements of the plan are to be put into action. It will identify what specifically is to be done in case of an emergency. It also includes the key personnel and organizational structures that must be in place at the time of the disaster. must be accurate and comprehensive. It must describe the work that must be done in terms of reducing the damage and reestablishing a functional organization. The plan must have the tools necessary to achieve that goal. That includes people, equipment, and supplies. The equipment must be properly maintained, repaired, and replaced if it is needed. People need to be trained in order to get their skills in top shape. The tools must be in working order to get them prepared for an emergency.The plan must include the steps required to get prepared. That means getting insurance, doing some minor repairs, and setting up a recovery plan. Doing these things as soon as possible will ensure that they are in place before the disaster occurs. It should contain procedures for sending out checks and notifications for relocation. In addition, the conclusion for business continuity plan should contain procedures for checking on personal survival.

References

1. Coresite. (2016). Hybrid Cloud & Business Continuity Planning. Retrieved from Coresite: https://www.coresite.com/blog/hybrid-cloud-business-continuity-planning
2. Solie, B. (2016). A Guide to Planning for Application Resiliency in Cloud Environments. Retrieved from Cloudtech: https://cloudcomputing-news.net/news/2016/jun/23/guide-planning-application-resiliency-cloud-environments/
3. V.D. Soni, Disaster Recovery Planning: Untapped Success Factor in an Organization (June 16, 2020). Available at SSRN: https://ssrn.com/abstract=3628630 or http://dx.doi.org/10.2139/ssrn.3628630
4. V.D. Soni, Importance and Strategic Planning of Team Management (June 1, 2020). INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, July 2020 , Volume: 7 , Issue: 2, PageNo: 47-50,http://ijirt.org/master/publishedpaper/IJIRT149921_PAPER.pdf.
5. O.Zimmermanne. (2017). Micro Service Tennets. Computer Science Research And Development, 1-1.
6. B.Familiar. (2015). IOT And Micro Services. Springer 2015, 1-1.
7. T.Ueda, & M.Ohara. (2016). Workload Character Of Micro Service. 2016 IEEE International, 1-1.
8. N.Dragoni, & M.Mazzara. (2017). Scaling Of Micro Service. Andrie Mershow Memorial, 1-
9. B.Butzin. (2016). Micro Service Approach For IOT. IEEE 21 st , 1-1.
10. J.Stubbs, & R.Dooley. (2017). Distributed System Of Micro Service Architecture. 7th International, 1-1.
11. V.Rangasamy, & P.Kumar. (2019). Micro Service Application Framework. Google Patents 2019, 1-1.