Module – 5 (Business Continuity in the cloud)

1.How to configure, develop and maintain Security and Privacy in cloud?

Cloud Computing is no doubt the next greatest standard in the world of computing. With an unimaginable amount of data hosted online in virtual servers, the biggest concern for businesses, is maintaining considerable levels of data security and privacy. The entire realm of Information Technology considers security breaches and data vulnerability as one of the most critical issues it faces.

With Cloud Computing, businesses entrust huge volumes of sensitive, critical and confidential data that could be hosted halfway across the globe. Any unauthorized exposure to such data can be catastrophic for the companies and so data security and privacy protection has always been a major area of research for cloud technology researchers and scientists.

In order to fully secure the system, network engineers cannot overlook a single security loophole. However, when it comes to security breaches, hackers and cybercriminals only need to find a single ambiguity or loose end in the security protocols. Exposure to harmful malware and ransomware can disable the security barriers enforced and corrupt important files and databases, rendering entire systems encrypted beyond repair. The very purpose of hosting important data, applications, software, and infrastructures online becomes ineffective if it is hacked, tampered with, or even destroyed.

Cloud technologies have always been a center of attraction for cyber criminals and hackers. The fact that the end users who subscribe to cloud

technologies access virtual services over a public network that is the internet makes it even more vulnerable.

Just getting access to the user credentials can easily allow hackers to gain access to the otherwise secured servers of the cloud. Businesses and organizations need to understand and acknowledge the challenges of cloud computing before hosting critical data and deploying important software.

Ensuring Data Security and Privacy over Cloud Computing

Cloud Computing is a shared environment with no information to the end-user about who else is sharing the infrastructure. Concerns over the data and/or application hosted online can cause businesses to still be skeptical about migrating their systems online, in a publicly shared environment. How can businesses trust service providers to protect their valuable information from both external and even internal breaches? Here's an outlook of the key measures adopted by service providers into maintaining data security and privacy over the cloud:

Network Security

Applying controls to the traffic in a public network is the primary step for data protection in cloud hosting. In order to ensure that only authorized and legitimate traffic is granted access to the network is crucial. Cloud providers employ robust network architectures to monitor the access, connectivity and data transfer logs, application logs and software and hosted infrastructure logs.

Network connectivity is monitored across the hosted resources located in-house and across the internet to the end user's premises. Also, network access control is employed to screen out any unauthorized connections to the client's resources. In order to guarantee network security, service providers employ network layer control, route control, DDoS protection, traffic manager, robust firewall, and secure remote

access as well as cross-premises connectivity and monitoring and threat detection.

Encrypting Hosted Data

The very foundation of network security and data protection is encryption. Cloud service providers support encryption across all forms of storage and network elements. They can also either manage the encryption keys themselves (AWS Key Management Service) or allow users full access to their encryption keys to ensure even more privacy. Microsoft Azure provides a secure **Key Vault** that allows users to create multiple secure vaults controlling access to any data stored in their cloud. This prevents accidental loss of data since all the keys are centralized in the vault.

Authorized Access

Another aspect of data security and privacy is maintaining the authorization of access to client's data and applications hosted in cloud environments. Cloud providers establish and maintain centralized access across their services to avoid unauthorized access. There are a number of approaches that protect data integrity such as multi-factor authentication of user credentials, hardware-based authentication i.e. text and email OTP, integrating extensive APIs to support access rights for the existing customers.

Cloud providers' internal personnel are also denied access to user accounts as well as having a strict policy against having any user or administrative accounts the client's services. Finally, all access attempts are also logged for auditing and maintaining integrity and all the authorized access attempts are only granted from secure and verified workstations.

Monitoring

Encrypting data and protecting access is only a part of the story. Even the most robust and secure network architectures can still be vulnerable

to multiple cyber threats. Cloud service providers also have provisions to monitor the workload, applications and infrastructure generating alerts for any discrepancy or anomaly. They also review and update allthe baseline hardware and software configuration, upgrades and changes made.

In addition to that, service providers implement a security management process to look out for any unfortunate and unwanted incident; application failure, security threats, loss or alteration of customer's data. Finally, advanced machine learning for anomaly detection and threat recognitions are constantly employed and upgraded to monitor logs and filters out malicious and/or unauthorized actions.

Secure Workstations

The end users are the most vulnerable targets and frequently attacked points. When user credentials are compromised, hackers can gain access to entire organization since these users are administrators in their local workstations. Using secured managed workstations, eliminates the risks and ensures endpoint protection. Security tasks handled by cloud providers are just as much the user's responsibility to maintain by following network security protocols, complying to the security standards and using the access and authorization responsibly.

2.What is Portability in cloud?

Cloud portability is the ability of a cloud computing product, solution or service to be migrated to a new vendor or location without incurring substantial porting and integration issues.

Cloud portability makes it possible to switch a cloud solution between different vendors and/or migrate it across internal cloud infrastructure. Cloud portability is applicable to all service models of cloud computing - SaaS, PaaS, IaaS and hybrid - regardless of whether they are public or

private. However, most cloud portability scenarios occur in public-to-public or public-to-private cloud transfer.

Cloud portability depends on the level of interoperability a cloud service or vendor provides in their offerings. A cloud solution built on non-proprietary and open standards is most likely to be easily portable among any similar cloud vendors or architecture. OpenStack and CloudStack are among the initiatives that fosters cloud solutions, which are highly interoperable among supporting vendors.

Data portability has become commonplace -- although not universal -- among applications designed for use on many vendors' personal computers (PCs) and servers. The same cannot yet be said for CSPs. As more organizations move data and data processing to cloud services, a lack of data portability can cause problems if, for example, customers want to move data from one cloud platform to another or change their service provider.

Learn why data portability is important.

Different CSPs commonly have proprietary data formats, templates and related parameters that can lock users into specific platforms. Often,

these formats are not standardized, making data portability difficult. According to the Institute of Electrical and Electronics Engineers (IEEE), cloud interoperability and data portability are major challenges for enterprise adoption of cloud computing services.

For consumers, data portability lets people easily coordinate the personal data they keep on multiple social networking sites. On social networking sites, such as Facebook, LinkedIn and Twitter, users can share their contacts, posts, photos, videos, sound clips and personal or professional information across the various platforms. In that way, users know their data is current and consistent, without having to modify the content on each service's site. Users can, of course, opt out of this data sharing feature if they want to show different portfolios on different services.

In 2010, Facebook improved its data portability with a feature that lets users download all their network content as a single zipped file for viewing with a browser offline. This feature helps users to keep track of their data without fear that crackers might permanently alter or destroy it. The downloading feature backs up the data so it can be easily replaced in the event of a network failure causing data loss in the cloud. If the network has an outage or some other problem, users can simply upload their backed-up data to replace the damaged network data.

Data portability provides users of social networking services with added convenience when different services allow reciprocal access to first-party data. For example, a user on Facebook may import contacts from Google's Gmail email service. In a perfect world, all social networking services would allow users to freely and easily migrate data among them. Things haven't worked out that way. Instead, services sometimes take a territorial attitude toward user data.

Without data portability, a person's data is accessible only through the platform where it is stored. Such a siloed approach to data can result in vendor lock-in, inaccessible data and even data quality issues.

3.What is Reliability and high Availability in cloud?

When you access an app or service in the cloud, you can reasonably expect that:

- The app or service is up and running.
- You can access what you need from any device at any time from any location.
- There will be no interruptions or downtime.
- Your connection is secure.
- You will be able to perform the tasks you need to get your job done.

Factors like these measure the reliability of your cloud offerings. In a perfect world, your system would be 100% reliable. But that is probably not an attainable goal. In the real world, things will go wrong. You will see faults from things such as server downtime, software failure, security breaches, user errors, and other unexpected incidents.

Proper planning and cloud visualization can help you address faults quickly so that they don't become huge problems that keep people from accessing your cloud offerings. The cloud makes it easy to build fault-tolerance into your infrastructure. You can easily add extra resources and allocate them for redundancy.

Employing measures that make your cloud system more reliable ensures that:

- Redundant resources kick in automatically when the system experiences a fault.
- There is no downtime and products and services remain available.

- Employees keep doing their jobs without knowing that something went wrong.

Reliability in cloud computing is important for businesses of any size. Buggy software can cause lost productivity, lost revenue, and lost trust in your brand. Before you deploy your applications to the cloud, make sure they are thoroughly tested against a variety of real-world scenarios. This helps to ensure that they are reliable and will meet customer expectations.

High availability is the ultimate goal of moving to the cloud. The idea is to make your products, services, and tools available to your customers and employees at any time from anywhere using any device with an internet connection.

Cloud availability is related to cloud reliability.

For example, let's say you have an online store that is available 24/7. But sometimes clicking the "checkout" button kicks customers out of the system before they have completed the purchase. So, your store may be available all the time, but if the underlying software is not reliable, your cloud offerings are basically useless.

Bringing it all together

Cloud availability, cloud reliability, and cloud scalability all need to come together to achieve high availability. This means that your products and services are accessible anytime and anywhere, function reliably and as expected, and that the system can seamlessly scale up or down to accommodate customer demand without suffering a loss in performance.

Cloud service providers offer an Infrastructure as a Service (IaaS) model that gives you access to storage, servers, and other resources. IaaS provides automation and scalability on demand so that you can spend

your time managing and monitoring your applications, data, and other services.

Because IaaS provides scalability based on a pay-as-you-go model, this saves you money and frees you up to track down and address problems that may come up with the software. Having more time to monitor can help you find areas that need improvement so you can do a better job consistently deploying reliable products and services.

To survive in today's global market, it's inevitable that your company will need to move to the cloud. It won't happen overnight and will require a lot of planning. As you plan what and how you will make solutions available in the cloud, remember that it is important that your products and services and cloud infrastructure are scalable, reliable, and available when and where they are needed.

4.Describe Mobility Cloud Computing

Cloud mobility is related to balancing the resources and the costs between different cloud services which can be public or private cloud services. It is an emerging trend aimed at making workload migration across the platform easier. Mobility helps to accomplish the jobs and customer requirements in a cloud environment. It also assists cloud evolution, enhances the performance of operating applications by repositioning data to the intention host, consequently; reducing the communication consumption and solving the load balancing problems. An effective cloud mobility solution should enable the creation of policies to automatically transfer authorized data to a choice of private or public clouds. Data should remain encrypted in the cloud, and it should be easily and seamlessly recalled onsite as required or transferred to a different cloud as business demands change.

Example of Cloud Mobility :
Suppose a consumer organization has put its resources at cloud C1. As C1 is not providing good services to the organization, it decides to move to a different cloud service provider C2. Moving resources from

C1 to C2 is a complex task. It may be due to the lack of tools and support. Here's where cloud mobility comes in handy which makes it easier to move resources across different cloud services. Moreover, C1 and C2 can now work together as a distributed cloud environment which is even better.

Types of Cloud Mobility :

1. Weak Mobility –

It permits the code to migrate through the networks. In some cases, the code has initial data assigned but without execution states. In weak mobility, the codes migrate without their execution states.

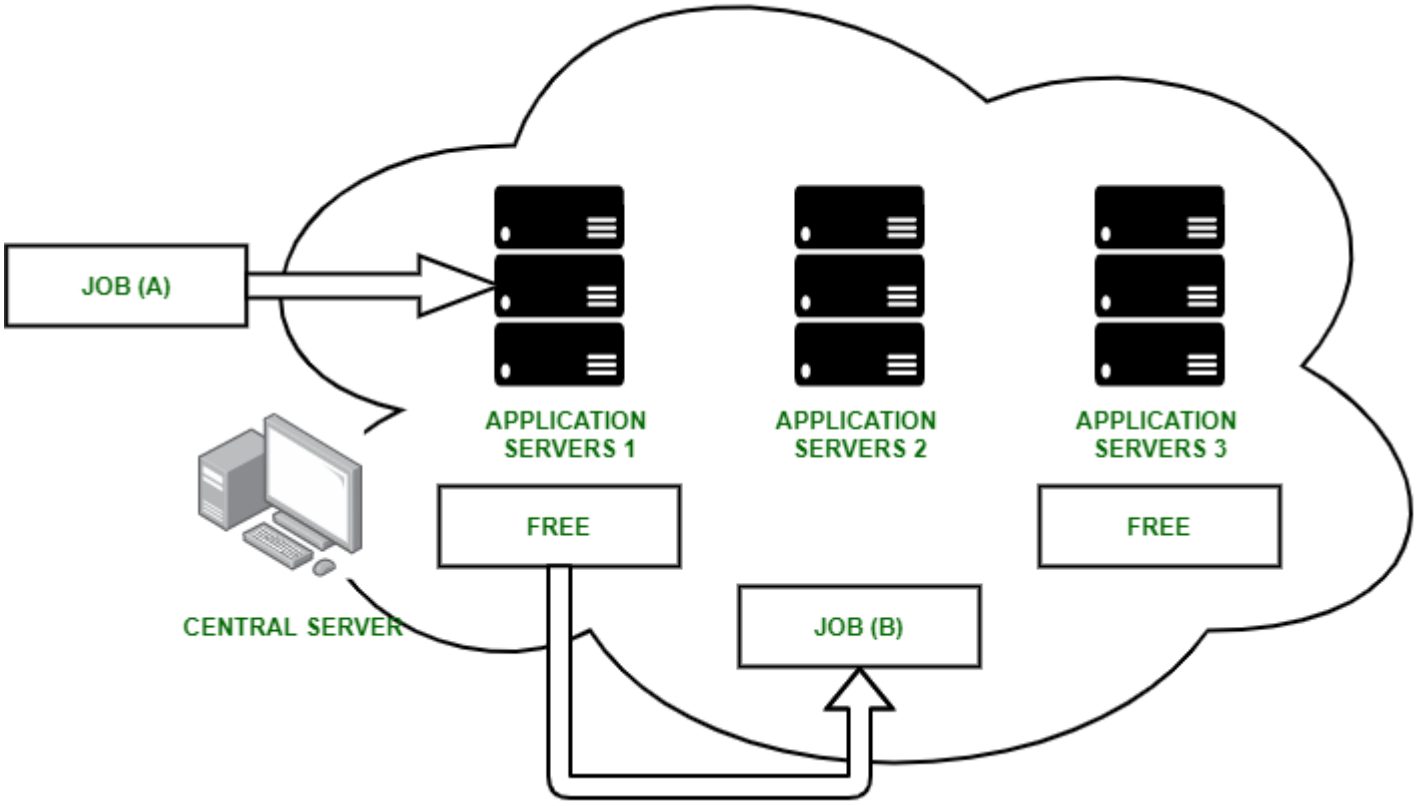
2. Strong Mobility –

It grants the code and execution state to start again at a new resource. This can save running time, processor, registers and program counters.

Mobile Cloud Framework :

The central server can relocate workloads or resources or even applications from one server to another depending on the requirements of the new job. To explain this procedure, let us assume that a new job is allocated to the cloud system and this job has certain requirements (application, data or hardware requirements) and these requirements are accessible only on some servers. In this case, the central server can transfer one or more running jobs with its execution code (strong mobility) to other available servers that can fulfill their requirements. This process of moving has created a chance for the new job to be processed in the vacated server(s).

The mobility is done when a new job comes to the cloud system. The central server inspects if this job can be operated on one of the available servers. When the central server comes to the conclusion that no available server has the essential requirements to fulfill the new job, it asks the mobility server to find the busy servers that can process the new job and the availability to transfer any of the running jobs from those servers. If the mobility server manages to relocate one of the running jobs, the new job can be processed in the vacated server.



CLOUD MOBILITY

Benefits :

1. **Increases the simplicity of business –**
   Since there is no cost involved in the movement of data from one cloud service to others, cloud mobility becomes a viable option. Moreover, not only resources can be shared, even workloads can be synced which makes it even more efficient.
2. **Increases cloud efficiency –**
   Here, we have a centralized server connected to different cloud services. This server is responsible for deciding which cloud is ideal for sharing the workload. So, the best efficient use of resources is made to improve the overall cloud efficiency.
3. **Helps in easy recovery from disasters –**
   If one of the cloud crashes in times of a failure, the data can be easily shifted to the centralized server and then to a different working cloud hence increasing the chances of data recoverability.

4. **Rapid Deployment –**
   Since it is a distributed cloud-based system, it facilitates faster deployment of the application as the resources are shared.
5. **Flexibility Management –**
   Different cloud services can be managed by different users based on our own preferences. Which makes it an ideal choice for different organizations.

5.Describe AWS, Azure, Google cloud Platforms

AWS stands for Amazon Web Services. This is a subsidiary of Amazon.com which provides on-demand cloud computing platforms to a single person, to companies, and to governments. On a paid subscription basis with a free tier option that will be available for 12 months. Amazon is completely dependent on the infrastructure of AWS. AWS has launched in 2006. It's having many services like amazon cloud, AWS lambda, Amazon S3.

Microsoft Azure

This is an ever-expanding set of cloud services to help organizations meet your business challenges. Azure has launched in 2011 with the Intend to provide a complete cloud computing platform to businesses. It has named " Microsoft Azure" in 2014, this as shown a huge process among its competitors.

Google Cloud Platform

Google cloud platform has offered by Google, which is a suite of cloud computing services that runs on this same infrastructure, that Google uses internally for its end-user products like Google search engine, YouTube, and more. But now they have introduced their enterprise services so that anyone can use Google Cloud platforms that share a similar infrastructure as that of Google search or YouTube.

Difference Between AWS, Microsoft Azure, And Google Cloud

01. Amazon Web Services is having 66 availability zones with 12 more on the way. Azure is having 54 regions worldwide and this is available in 140 countries all over the world. Google cloud platform has made available 20 regions in World, with three more on their way.

02. AWS is leading with 30% of public cloud share in its name. Microsoft Azure is in second place and it has owned around 16 % of market share

worldwide. Google cloud platform is in 3rd place and it is owned up to 10% of market share worldwide.

03. AWS is having a high profile and customers with time like Netflix, Unilever, BMW, Airbnb, Samsung, Zynga, etc. Azure is having 80% of Fortune and 500 company customers. Those are Johnson Controls, Apple, Honeywell, Fuji film, Polycom, etc. The major clients of Google Cloud platforms are PayPal, 20th-century fox, HSBC, Domino's, Bloomberg, and many more.

04. AWS is offering around 200+ services whereas azure is offering around 100+ services and google cloud platform is offering 60+ services.

05. AWS is providing instances of virtual machines and virtual servers. Azure is providing the virtual hard disc. Virtual machine instances will be provided by the Google Cloud Platform.

06. AWS applies a charge to its users per hour. Azure applies a charge to its customers as per minute. Google cloud also charges per minute.

07. Amazon cloud search is used in AWS. Azure Research is used in Microsoft azure. This is not there in Google Cloud.

08. Kinesis is used in AWS for Analytics. In the case of Azure, Azure steam analytics is used. In the google cloud platform, cloud data flow, and cloud data preparation is used for analytics.

09. AWS Cloud HSM is used for compliance. In the case of azure, azure trust center is used for compliance. Google cloud platform security for compliance.

10. For automation, AWS opsWork and config are used for automation. Azure automation is used for automation in the case of azure. Compute engine management with the puppet and chef is used for automation for Google Cloud.

11. The glacier is used for archive storage in AWS. Cold line is used for archive storage in azure and google cloud.

12. ECS is used as docker management in AWS. Container service is used for azure. In the case of Google Cloud, Google container engine is used for docker management.

13. In AWS Lambda is used for serverless computing. Azure functions are used for serverless computing in the azure. Cloud functions will be used for serverless computing in the google cloud.

14. Device farm is used in AWS for app testing. Dev test labs will be used in azure for app testing. Cloud test lab is used in GCP for app testing.

15. 128 can be the maximum processor in VM in the case of AWS. In the case of azure this can be 128. In the case of google cloud it's only 96.

These was about the difference between AWS, Microsoft Azure, and google cloud. I hope this article may you all a lot. Thank you for reading. If you have any doubts related to this article "difference between AWS, Microsoft Azure, and Google Cloud",

6.Accessing AWS, Azure and Google cloud Platforms

A cloud platform can be described as a storage place that is highly accessible, flexible, scalable and agile in all its characteristics. Users from anywhere via the internet can access their data, collaborate, share, and work together in real-time with the cloud, which means anything less than a cloud platform cannot be possible to comprehend today. The substantial dominance of cloud platforms is their authenticity and usability.

Globally, collective spending on the cloud is becoming a mainstream business proposition. Based on the latest report from Gartner, end-user spending on public cloud services is forecast to grow 23.1% in 2021 to total $332.3 billion, up from $270 billion in 2020. As the scope of business is increasingly progressing in the cloud, the investment in cloud platforms soars high.
Today, organizations are blessed with different types of cloud platforms, which varies in their capabilities and competencies. In this blog, let's explore the major players in the Cloud industry and their services in brief.

Types of Cloud Platforms
There are various types of clouds available, and they can all offer different capabilities. The three main types of cloud computing are:

- Public cloud
- Private cloud
- Hybrid cloud

The leaders or dominant names in the Cloud platforms providers are three,

Amazon Web Services – which is still growing and have a net worth of $250 Billion, and it has 33% of cloud infrastructure market share

Microsoft Azure- which has a market share of 18% of the total cloud platform and has a total worth of $5 billion

Google cloud platform- which is a latecomer and a have a market share of 4.6%

The competition for the leadership of cloud platforms is going between these three big shots. We can clearly say that these three companies hold the lead in the infrastructure as a service (Iaas) and platform as a service (PaaS) market.

7. Create compute, create network, create storage on AWS , Azure and GCP

Amazon's two main file storage offers – EFS (Elastic File Storage) and FSx (for Windows and Lustre) – are both Posix-compliant, which means they work with applications that demand, for example, file permissions, file locking capabilities, and a hierarchical directory structure via NFSv4.

Use cases targeted include big data analytics, web serving and content management, application development and testing, media workflows, database backups, and container storage.

EFS is NFS access file storage for Linux applications that can run on AWS compute instances or on-premises servers. It can scale to petabytes and comes in two service levels – standard and infrequent access (IA), with automated tiering between the two to place files in the most appropriate for their usage profile.

AWS says access to files is parallelised to achieve "high levels" of throughput (10GBps quoted) and input/output (I/O) performance (500,000 IOPS). It says the cost can be 8c per GB per month, assuming an 80/20 split between IA and Standard storage.

Amazon FSx for Windows File Server provides file storage accessible via the Windows-native SMB protocol and delivers features such as Access Control Lists (ACLs), user quotas, user file restore and Active Directory (AD) integration. Flash and spinning disk hard disk drive (HDD) media options are possible, and FSx storage is accessible from Windows, Linux, and MacOS compute instances and on-premise hardware.

Claimed performance comprises sub-millisecond latency, tens of GB per second throughput and millions of input/output operations per second (IOPS).

Data is encrypted at rest and the service claims compliance with ISO, PCI-DSS, SOC and HIPAA.

Amazon FSx for Lustre is targeted at file-based use cases such as machine learning and high-performance computing (HPC). It integrates with AWS S3 as a bulk data store at more cost-effective rates, with data presented in file format in FSx for Lustre.

Data is accessible from EC2 instances and from on-premise locations.

Microsoft Azure

Azure's cloud file storage options include native and NetApp-based performance options as well as varying levels of caching services.

Azure File provides fully managed file shares in the cloud accessible via Server Message Block (SMB) or REpresentational State Transfer (REST) that can support cloud or on-premise deployments of Windows, macOS and Linux.

Two service levels are offered in Azure File – standard and premium.

Being a Microsoft service you get the integrations you'd expect, such as Active Directory, and Azure positively encourages "lift and shift" of applications and data that can use Azure Files.

Meanwhile, Azure NetApp Files is billed as "enterprise grade" and provides file storage for Linux and Windows compute based on NetApp storage in the Azure cloud. It is aimed at performance-intensive applications such as SAP HANA, databases, HPC apps and enterprise web applications.

Access is via SMB and NFS and there are three performance/cost tiers available – standard, premium and ultra.

Microsoft Azure also offers some file storage caching services that are intended to provide speedier access to data for high performance workflows.

Azure HPC Cache is an NFS-connected service that provides single namespace storage for on-premise NAS or Azure-located application data, which can be file or Blob (object).

Meanwhile, as a result of Microsoft's acquisition of Avere in 2018, Azure offers a couple of file-based caching type services based on its technology.

Avere vFXT for Azure is billed as “a high-performance caching service” and is a software-based service iteration of the FXT Edge Filer. The idea is that vFXT is used as a cloud-based file access cache that can allow HPC applications to run without being re-factored for the cloud. It is optimised for read-heavy workloads and presents a single namespace to applications.

Azure FXT Edge Filer is a hardware product and so falls slightly out of this survey. It is something like co-located hardware, offered as a service and is presumably the underpinning for the vFXT.

FXT Edge Filer works with customer NAS and Azure Blob and Amazon S3 storage to act as a high performance cache for HPC workloads. It will scale up to 24 nodes to provide claimed millions of IOPS and hundreds of GBps throughput. FXT comes in two models that differ chiefly in the amount of RAM and storage capacity.

Google Cloud Platform

GCP’s Cloud Filestore offers two performance tiers of NFS-connected file storage with up to 64TB of capacity per share. Premium offers much higher throughput and IOPS than standard, with 1.2GBps vs 100MBps read for the former and 60,000 vs 5,000 IOPS for the latter. Stated availability is 99.9% for both tiers.

Google is a bit more modest in its proposed use cases than some of the AWS and Azure cloud file storage offers. GCP targets video rendering, application workloads, web content management and home directories.

If you want more than the basic file storage offered by GCP, NetApp Cloud Volumes are also available. This is NFS and SMB-connected for Linux and Windows application workloads.

NetApp Cloud Volumes on GCP comes in three performance/cost tiers – standard, premium and extreme at $0.10, $0.20 and $0.30 per GB per month and range from 4,000 to 32,000 IOPS and throughput of 16MB to 128MB per TB.

8.Compare Cloud pricing of resources and services on all platform

- Google Cloud and AWS pricing are almost similar in pricing for systems that operate on general-purpose and on instance types of memory-optimized cloud.
- The price difference between AWS and Azure is negligible for their respective compute-optimized cloud instances. On the other hand, Google Cloud Platform is priced the highest in this service thanks to their scalable processors and an all-core turbo performance.
- The pricing model of Google Cloud for memory-optimized and accelerated-computing instances are way higher because they do not have 4vCPUs unlike AWS or Azure. Instead, they provide 40vCPUs and 12vCPUs respectively.

All cloud service providers offer businesses discounts on on-demand instances if they commit to use for 1 or more years. For AWS, it's known as "Reserved Instances" (RI); for Azure, it's "Reserved Savings" whereas it's called "Commitment Price" in Google Cloud. These types

of discounts encourage businesses to commit themselves to a preset level of usage for a fixed period in return for a discounted hourly rate on some (but not all) instances and VMs.

To calculate discounted pricing among AWS, Azure, and Google Cloud, we've considered a **one-year commitment period with no upfront cost.**

For your information:

Currently, AWS offers three different reserved instances: Standard RIs, Convertible RIs, and Scheduled RIs. These RIs differ with each type of RI plan. There's also a three-year commitment plan offered by all three cloud technologies for businesses that are confident they will run longer. While Azure and Google Cloud provide 3-year commitment plans similar to AWS, AWS offers a fixed average discount of 40% for all 1-year commitment plans irrespective of the instance type.