MISK FOUNDATION CLOUD MIGRATION TO ALIBABA CLOUD

By :
Lama Ayash
Rawan Alshehri
Noura Alsmari
Jaza Alqhtani

Alibaba Cloud

Misk مسك
مؤسسة محمد بن سلمان
Mohammed Bin Salman Foundation

Table of Contents

Table of Figures and Tables

Nowadays, people are spending much time on the internet and this habit plays a role in improving IT which makes us leverage the existing infrastructure of different cloud servers, intranets, etc. which in turn avails much flexibility for users to work anytime, anywhere.

In the time of the rapid development of technology. It became necessary to keep pace with this development. The cloud environment is the landscape that will develop business increasing capacity and adding capabilities on the fly without investing in new infrastructure with higher performance and minimal utilization of computing power.

We aim in Saudi Arabia to be a hub for cloud computing technologies across the region. Provide support for economic diversification and digital transformation, in line with Vision 2030.

We encourage Misk to join Alibaba Cloud, the technology arm of Chinese e-commerce to boost the website to be able to host anywhere from 10-10,000 visitors at a time to enable customers to register for programs and internships to reach the ultimate objective of building a society based on knowledge. risk by building a digital infrastructure that can provide the website with a competitive edge and visitors with the best possible experience.

With many of the services available through Alibaba Cloud. It's worth noting that the company has jumped on some recent trends like containers, big data analytics, microservices, machine learning, and AI. It also offers extensive high-performance computing capabilities and bare-metal servers Elastic Computing Storage & CDN, Networking, Database, Security, Monitoring & Management, Domains & Website, Analytics & Big Data, Application Service, Media Services, Middleware, and Hybrid Cloud

The tie-up aims to create a break new ground in the technology sector and position Saudi at the forefront of efforts to modernize the wider global technology.

While cloud computing has gotten a lot of attention, regarding being one of the most influential technology in the new era .there is still a lot of room for the technology to grow. As a result, many businesses have yet to figure out how to shift and migrate to the cloud.

Our cloud solution for MISK is to upgrade their current business to the next level. We noticed that the company servers are all in-house which might be dangerous to our infrastructure since we don't have disaster recovery, Due to the current situation as a medium-sized Internet enterprise, we offer a helping hand with our Alibaba solution. We will need to have to use the hybrid migration solution to migrate cloud resources from a classic network to a virtual private cloud (VPC). And deploy several ECS instances, Alibaba Cloud ApsaraDB for RDS across-region in the closest regions to Saudi Arabia for low latency and high availability. We will configure VPCs, Security Groups, and RAM users. We will explain our plan for Disaster Recovery and Failover.

HIGH-LEVEL OVERVIEW OF MISK FOUNDATION CLOUD MIGRATION TO ALIBABA CLOUD

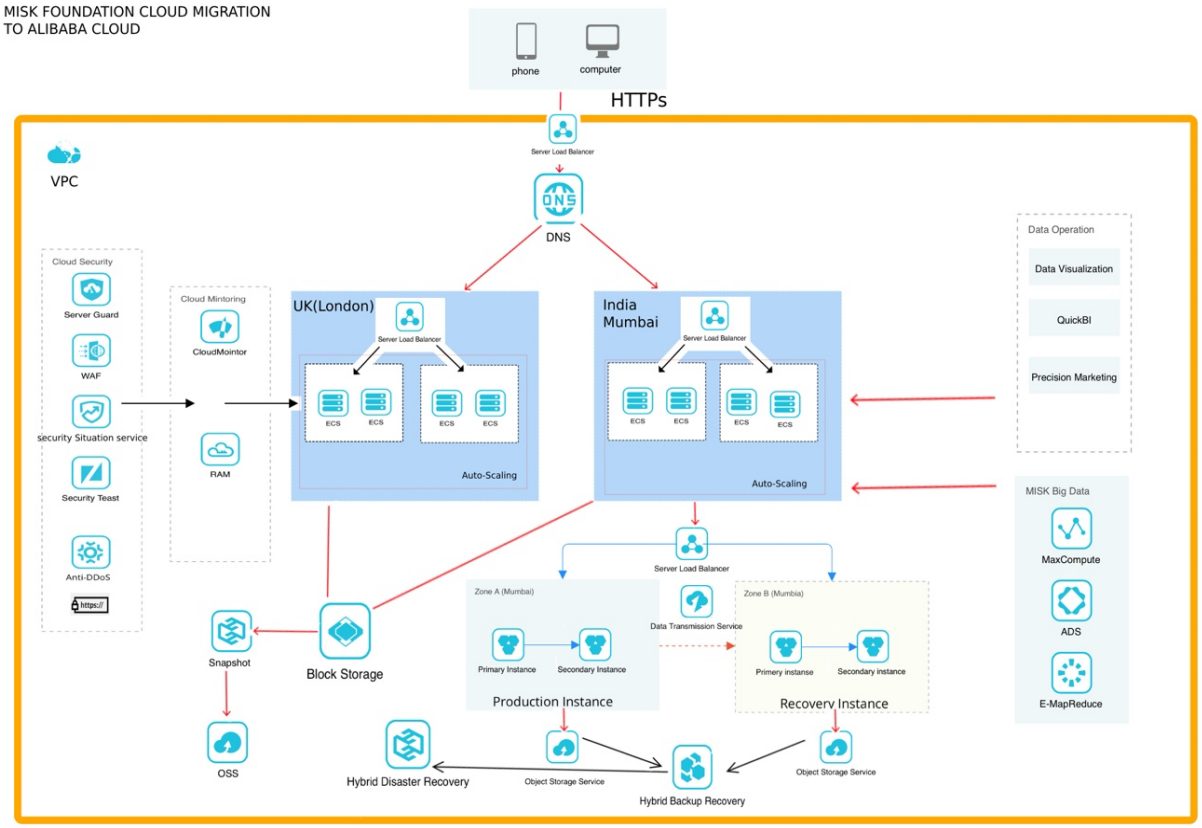

Figure 1:MISK Cloud Computing Overview

First of all, we have security services that would help MISK to secure their data and tier resources starting with Server Guard. Traditional enterprise-level anti-virus software often lacks effective methods of defending against attacks on administrator permissions, including database hits, brute-force cracking, and weak passwords. We will ensure the security of our cloud. Alibaba Cloud has developed a cloud host security product specifically to address this problem.

In addition, we will deploy Alibaba Cloud WAF that combines the smart protection engine, expert protection rules, proactive defense, detection engine, and cloud threat intelligence capability to identify web attacks and malicious web requests in real-time.

Next, Security Situation Awareness, Security Test, and anti-Dodos which is proxy-based mitigation services provided by Alibaba Cloud to mitigate DDoS attacks. These services can be used to protect network servers against volumetric DDoS attacks.

To protect servers against volumetric and resource exhaustion DDoS attacks, Anti-DDoS Pro and Anti-DDoS Premium forward traffic to the Alibaba Cloud anti-DDoS network by using DNS resolution.

CloudMonitor monitors the resources of all cloud services within our Alibaba Cloud account. We can view the status of the specified resources and the usage of metrics in the cloud service. We can also configure alert rules for the metrics. If an alert is triggered based on the alert rules, CloudMonitor also sends an alert notification.

We will create RAM users and authorize the RAM users to access different resources. If multiple users in MISK need to simultaneously access resources, we can use RAM to assign the least permissions to the users. This prevents the users from sharing the username and password or AccessKey pair of an Alibaba Cloud account and reduces the security risks.

Security services and RAM are connected to the ECS instance through a VPC. We will deploy our ECS instance in two different regions India and UK each region has multiple zones. Each zone connects the other via Server Load Balancer to distribute network traffic across these groups of backend servers to improve the service capability and application availability.

Each region connects the other via DNS that helps MISK convert human-readable domain names into machine-readable IP addresses and then routes user requests to required website or application servers. and for

high-performance and low-latency, the ECSs instances connected to block storage EBS that supports random read and write to meet the data storage requirements of our business.

To create a snapshot to all disks categories to back up or restore the entire disk. Crash-consistent snapshots are an effective solution to disaster recovery and can be used to back up data, create images, and implement disaster recovery for applications.

Then, to store this data we will deploy an Object Storage Service (OSS) that enables MISK to store a large amount of data in the cloud. OSS provides scalable capacity and processing capability and multiple storage classes to cover a variety of data storage scenarios from hot data storage to cold data storage, which helps MISK minimize your storage costs.

All ECS in auto-scaling group computing resources based on our volume of user requests. When the demand for computing resources increase, Auto Scaling automatically adds ECS instances to serve additional user requests or removes instances in the case of decreased user requests.

For the database, we will deploy Relational database MySQL in one region for low latency which is the India region, and with two zones A and B. It connects the ECS instance with a services account that intends to represent a non-human user that needs to authenticate and be authorized to access data in the database, and a server load balancer to distribute the traffic.

Zones connect each other through a data transmission service that helps us to migrate data between data stores, we can use DTS to migrate MISK data to Alibaba Cloud. DTS supports several data replication modes, including data migration, data integration, data synchronization. Each zone is connected to OSS to store a large volume of data at a low cost. OSS connects to Hypered backup recovery which is an easy-to-use and cost-effective online backup service.

This service would help MISK to back up data from desktops, servers, and virtual machines to a backup repository on Alibaba Cloud, which ensures secure and efficient cloud storage, backup, and management for customer data.HBR connect to HDR demonstration presented the end-to-end process of MISK application disaster recovery with Alibaba Cloud's second-level recovery point objective (RPO) and minute-level recovery time objective (RTO).

Data operations like data virtualization and Alibaba Cloud Quick BI connect to the ECSs. Alibaba Cloud Quick BI is a next-generation intelligent business intelligence (BI) service platform. It is designed for users on the cloud. Quick BI allows MISK to analyze large amounts of data online in real-time. It also supports drag-and-drop operations and rich visualization features to help us analyze data, explore business data, and generate reports. Quick BI is a tool that allows MISK to view data. It can also be used to accelerate digital operations.

In addition, MISK Big data use ADS, MaxCompute which is a fully managed online data warehousing service in a serverless architecture. MaxCompute eliminates the limits of traditional data platforms in terms of resource extensibility and elasticity, minimizes operations and maintenance (O&M) costs, and allows enterprises to efficiently analyze and process large amounts of data at low costs, and Alibaba Cloud Elastic MapReduce (EMR) which is a big data processing solution that runs on the Alibaba Cloud platform.

EMR is built on Alibaba Cloud ECS instances and is based on open-source Apache Hadoop and Apache Spark. Alibaba Cloud E-MapReduce (EMR) is a big data platform based on open-source engines such as Hadoop, Spark, HBase, Hive, and Flink. EMR is built on Alibaba Cloud ECS instances that provide a variety of big data solutions. It allows MISK to use open source technologies on the cloud to process big data in scenarios such as data warehouse creation, batch processing, streaming processing, and ad hoc queries.

All components in our cloud migration connect via VPC. Alibaba virtual private cloud (VPC) we can control over our VPC. we will specify the CIDR block and configure route tables and gateways. In our VPC, we will deploy Alibaba Cloud resources, including Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, and Server Load Balancer (SLB) instances.

Furthermore, we will connect our VPC to other VPCs and on-premises networks through Express Connect circuits to create a custom network environment. This way, we can migrate applications to the cloud and extend data centers.

MISK'S DATABASE ON ALIBABA CLOUD

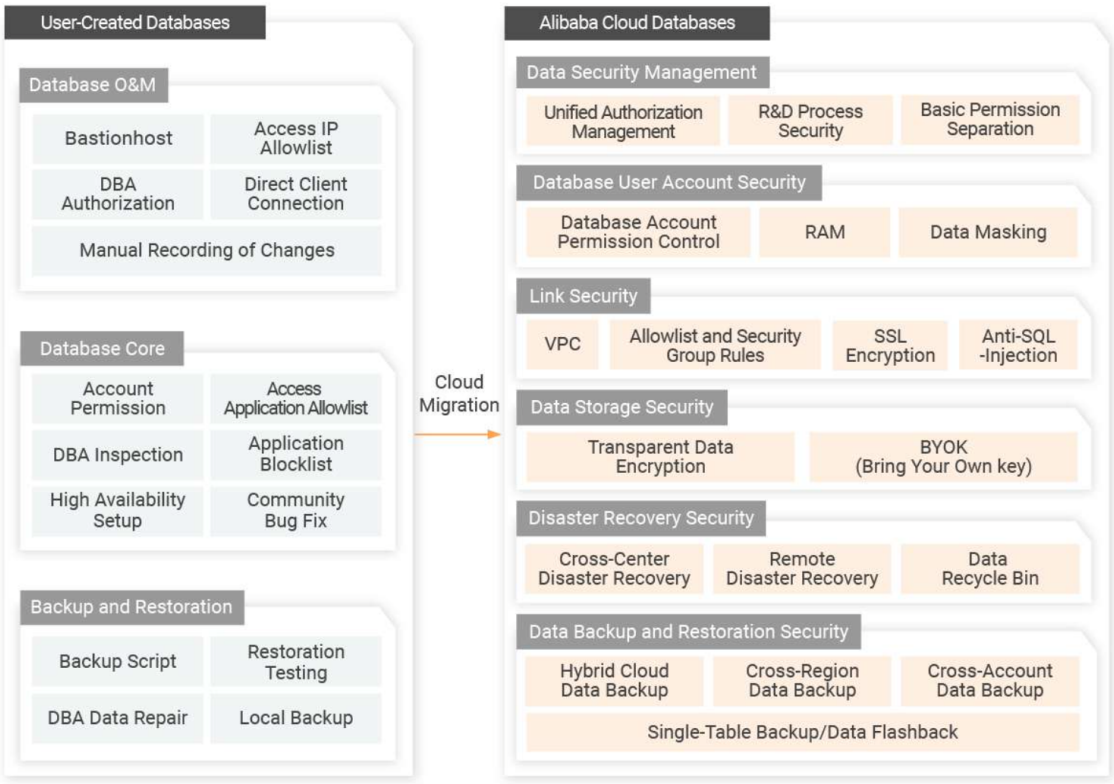

Figure 2: Alibaba Database

Alibaba Cloud ApsaraDB for RDS is an on-demand database service that handles some of the administrative tasks associated with managing a database, thus leaving us with more time to focus on our core business in MISK. ApsaraDB for RDS is offered with many popular RDBMS engines, including MySQL, SQL Server, and PostgreSQL. RDS handles routine database tasks such as provisioning, patch up, backup, recovery, failure detection, and repair. ApsaraDB for RDS can also protect against network attacks and intercept SQL injections, brute force attacks, and other types of database threats.

Moreover, we will choose MySQL since MySQL is an easy interface to other software. It is easy to use MySQL as part of a larger software system. For example, we can write programs that can interact directly with a MySQL database. Most major programming languages have libraries of functions for use with MySQL; these include C, PHP, Perl, Python, Ruby, and the Microsoft .NET languages. MySQL also supports the Open

Database Connectivity (ODBC) standard, making it accessible even when MySQL-specific functionality isn't available.

We will create the database in the following steps:

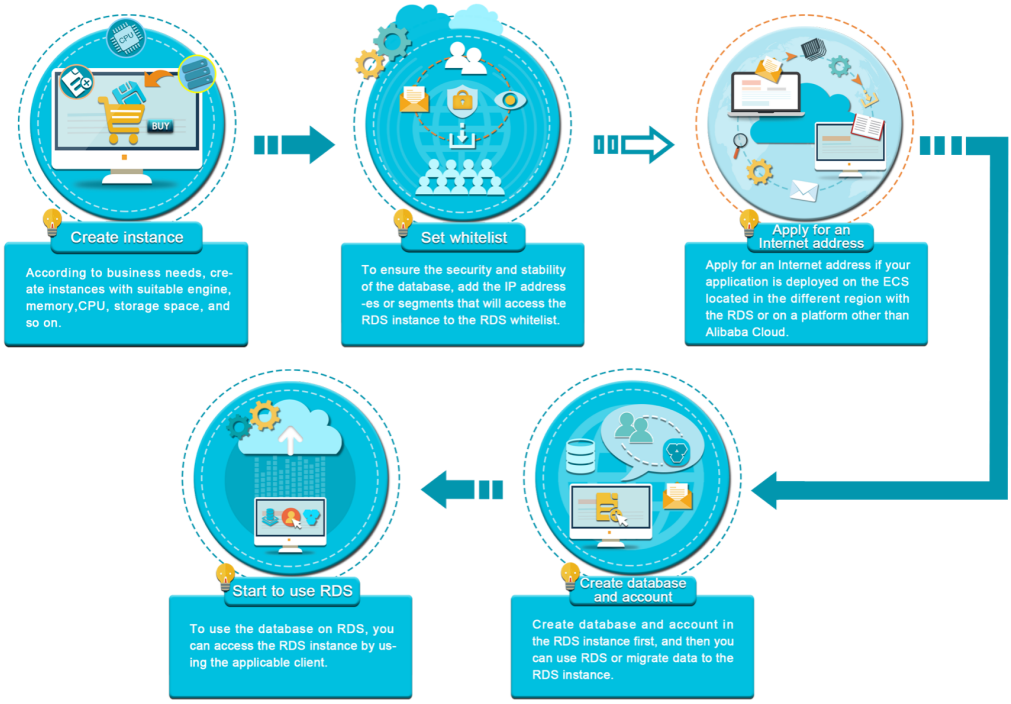

Figure 3:Alibaba Cloud ApsaraDB for RDS Creation

We will connect our database to webservers with service accounts. Service accounts are needed for the persistent applications so that we can perform actions on behalf of the users of the application. In other words, service accounts are proxies for performing limited actions for users that have no access to sensitive data and systems. In addition, we will deploy a server Load balancer to distribute network traffic across database instances to increase the throughput of our applications. We will use SLB to prevent service disruptions caused by single points of failure (SPOFs) and improve the availability of applications. We will configure an RDS in one region for low latency in India zone A and zone B.

MISK's main job is to provide courses for graduates and internships. Thus, we will mention the most important data to store in our database.

Application Technology Meta-Data: MISK automatically collects information when users visit and engage with the learning platform, through the collection of IP addresses and Cookies. MISK uses the information collected by these technologies as described in their Privacy Policy and Cookie FAQ including to better help

us identify the origin of technical issues, and support user login and security. For example, browser settings enable students and teachers to stay logged in while they go to different areas of the Platform.

Application Use Statistics: MISK also automatically collects information about how users and visitors engage with the various features of the learning platform. MISK uses this "Engagement Data" information as described in their Privacy Policy and Cookie FAQ to identify resources and features in the platform that users find useful. For example, if there are resources that teachers access repeatedly, that may be a sign that they see value in those resources. Conversely, if there are resources that teachers don't use often, that could be a sign that there is room for improvement. The same applies to student interactions with resources.

Observation data: Teachers in MISK use observations as another way of determining the progress students are making. For example, they may observe student peer interactions through project work. Student performance on some projects is assessed by oral presentation, and the teacher can input feedback and grades for those presentations.

Attendance: Courses and internship attendance teachers use this information to help them monitor for chronic absence, which can have an adverse impact on student achievement.

Demographics: MISK may choose to provide demographic data to better understand how the MISK learning platform is meeting the needs of their diverse student populations. This includes these types of information. Date or year of birth, gender, ethnicity or race, language information (native, preferred, or primary language spoken by the student), and other demographic information.

Student scheduled courses and Teacher names: schedule which details the students in specific courses as well as who the teachers are. MISK needs to connect students to courses and the teachers teaching them.

Student Contact Information: Email addresses are needed to set up a student's account on the MISK website and phone numbers are needed to set up a student's account on the MISK website

Student Survey Responses: Student responses to surveys or questionnaires: These optional student surveys are carried out in order to better understand a student's experience with MISK.

Additional data element used, stored, or collected by our application includes Teacher feedback on coursework Teacher curricula and notes and feedback about students' teacher to surveys about the services or curriculum and feedback.

To secure MISK's database the database is only accessible by service account only. MISK needs to provide persistent protection to a variety of data, and current data volume is huge. To back up and archive the data completely on-premises, it would be time-consumed to construct, the scalability is poor, the maintenance workload is heavy, especially the high cost, which is a heavy burden for MISK. Luckily, Alibaba Cloud will back up MISK's offline databases, files, emails, and other types of data for disaster recovery to Hybrid Cloud Storage Array (HCSA) hybrid cloud disaster recovery all-in-one cluster. The data that needs to be persistently protected and stored are migrated automatically to Alibaba Cloud Object Storage Service (OSS) with the automatic data migration function. With data lifecycle management, the infrequently used data is moved to Archive Storage of OSS to optimize TCO. The data is secured end-to-end during the transporting.

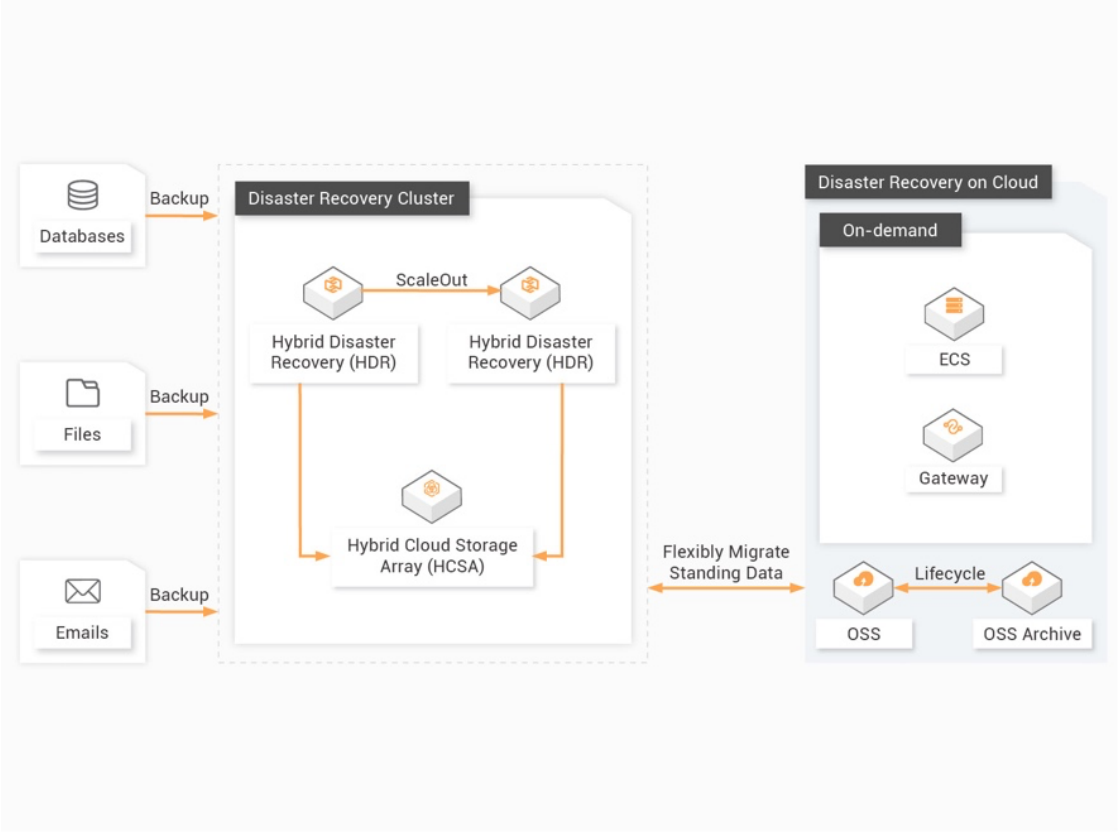

Figure 4: Database Disaster Recovery Plan

The data will be backed up every day at 2:00 am the Saudi time zone. When a system failure occurs, the database can automatically switch services from the primary node to a read-only mode. We will specify a read-only node as the new primary node to switch services from the primary node to the read-only mode. We will set automatic failover active-active architecture that ensures high availability. If the primary node that supports reads and writes is faulty, services are automatically switched to the read-only mode that is elected by the system as the new primary node.

A failover priority is assigned by the system to each node in a cluster. During a failover, a node is elected as the primary node based on the probability that is determined by this priority. The probability of being elected as the primary node is the same for the nodes that are assigned the same failover priority.

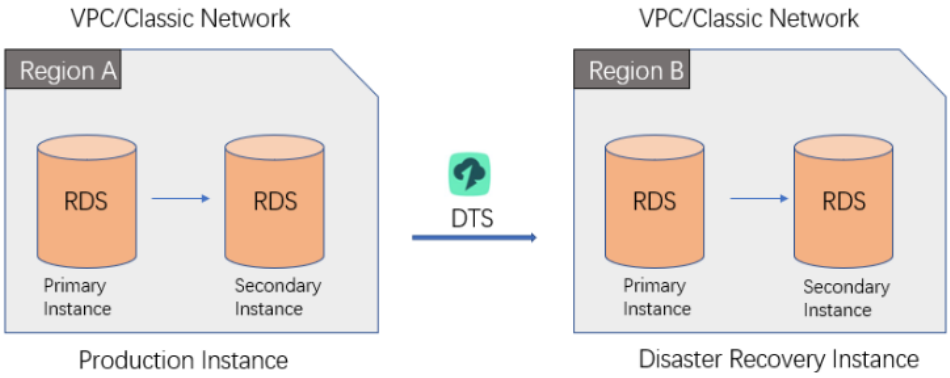

Figure 5: Database Automatic Failover

MISK'S DATABASE OVERVIEW:

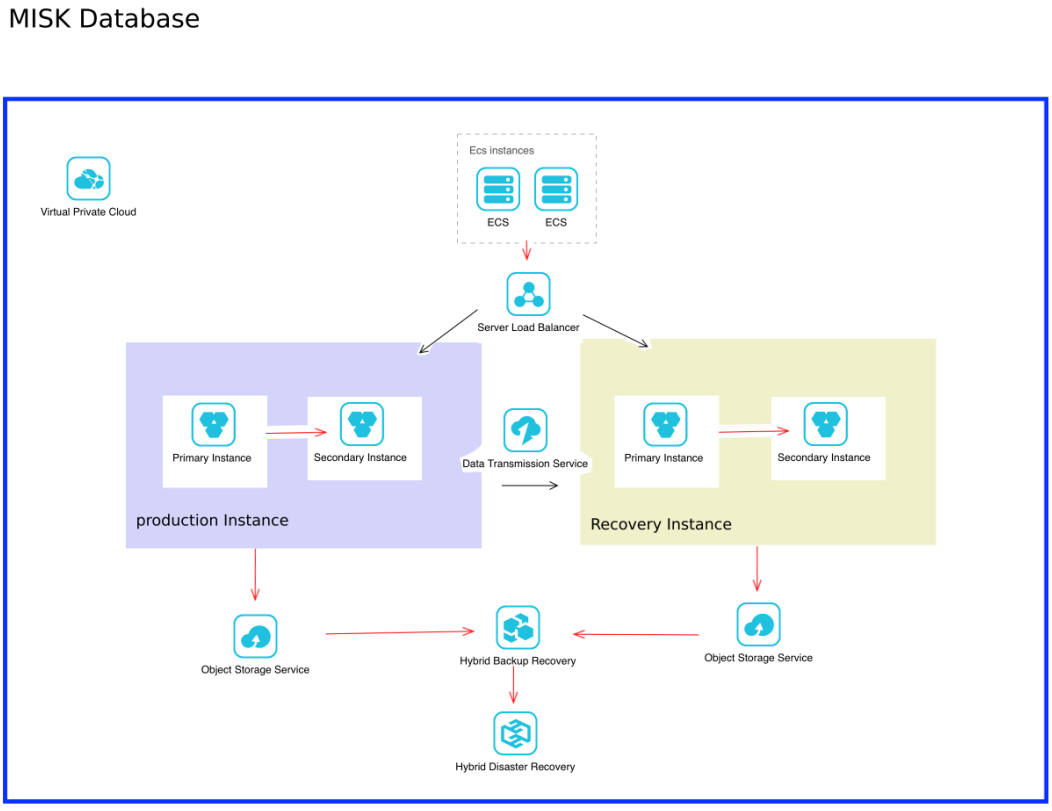

Figure 6:MISK'S DATABASE OVERVIEW.

MISK'S ECS INSTANCES ON ALIBABA CLOUD

We will configure 20 ECS instances across-region in the closest regions to Saudi Arabia for low latency and high availability. Each region has multiple zones India (Mumbai) as Zone A and Zone B also UK (London) Zone A and Zone B. For high availability, security, and elasticity. Elasticity is a key benefit of cloud computing. Alibaba Cloud is capable of providing IT resources required by a medium-sized Internet enterprise within a few minutes.

We will deploy our ECS instance according to the table below:

Number Of ECS	Instance	Region	Network Type	Instance Type	Image	Storage
5	ECS	India Zone A	VPC	ecs.g6.4xlarge （16 vCPU 64 GiB,General Purpose Type g）	Windows Server	ESSD-50GiB
5	ECS	India Zone B	VPC	ecs.c5.2xlarge （8 vCPU 16 GiB,Compute Type c5）	Windows Server	ESSD-50GiB
5	ECS	UK Zone A	VPC	ecs.r5.6xlarge （24 vCPU 192 GiB,Memory Type r5）	Windows Server	ESSD-100GiB
5	ECS	UK Zone B	VPC	ecs.d1ne.2xlarge （8 vCPU 32 GiB,Big Data Type with Enhanced Network Performance d1ne）	Alibaba Cloud linux	ESSD-100GiB

To prevent data loss because of disasters or any other reason. We will deploy a snapshot which is a point-in-time backup of our disks. The first snapshot of a disk is a full snapshot that does not contain copies of empty data blocks. Subsequent snapshots are incremental snapshots that store only changed data blocks.

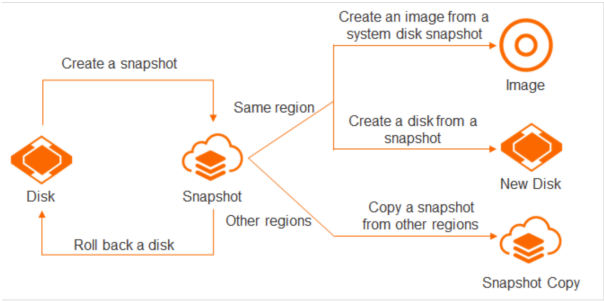

Figure 7: ECS Snapshot

As long as this snapshot needs storage, we will deploy block storage that creates a file system in a disk partition. The file system manages disk space. These management tasks the form of I/O requests in the disk. The disk records the status of data blocks and copies data to OSS. Snapshots are created in this process. The following figure shows the relationship between a file system and a snapshot.

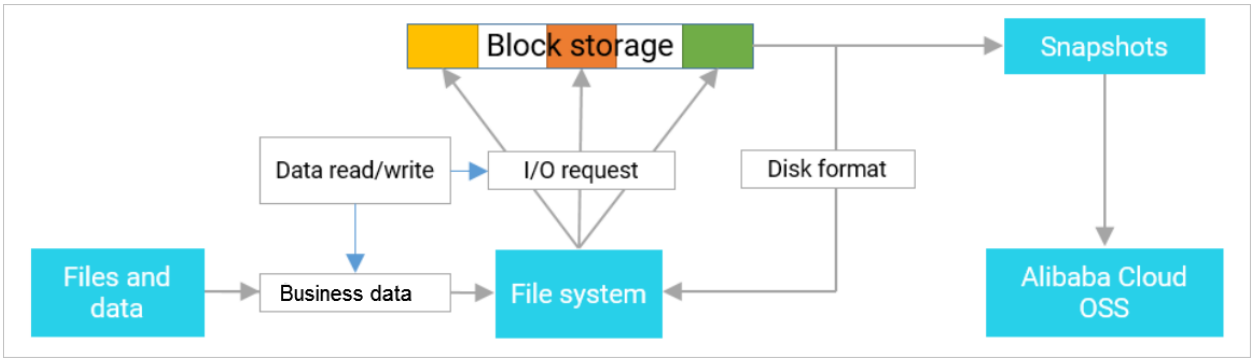

Figure 8:Relationship Between A File System And A Snapshot

To improve resource utilization and significantly reduce costs. We will deploy Auto Scaling which is a management service that automatically adjusts the number of elastic computing resources based on MISK business demands and policies. When business loads increase, Auto Scaling automatically adds ECS instances to ensure sufficient computing capabilities. When business loads decrease, Auto Scaling automatically removes ECS instances to save costs. It is suitable for applications with fluctuating or stable business loads.

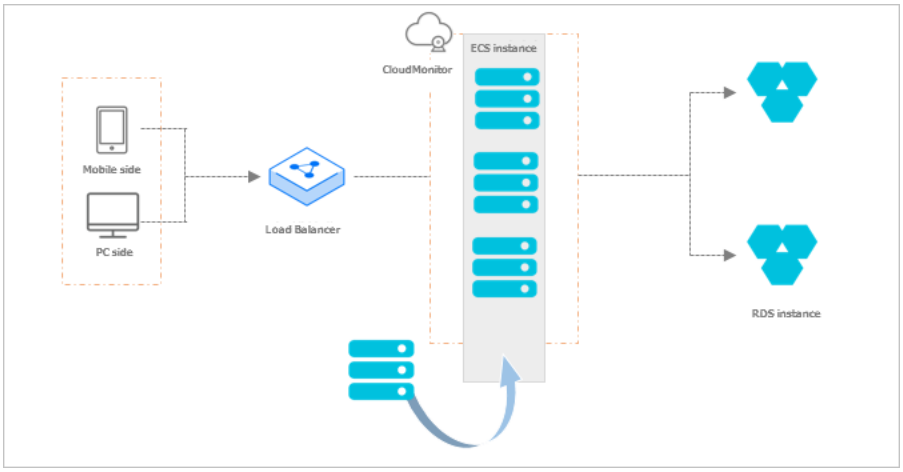

Figure 9:Alibaba Auto-Scaling

These ECS instances will host the Official websites and the learning platform of MISK. MISK used to face High traffic problems so we can upgrade the ECS instance configurations or add ECS instances at any time to provide sufficient resources for handling traffic spikes.

These servers will run the web application Apache and host databases, and store files. In addition, we will use our ECS with Object Storage Service (OSS) to store static images, videos, or downloaded packages to reduce storage costs. In addition, ECS can work with Alibaba Cloud Server Load Balancer (SLB) to shorten waiting time, reduce public bandwidth costs, and improve service availability. ECS will support MISK MySQL databases with high I/O requirements. A high-configuration I/O optimized ECS instance can be used with ESSDs to achieve high I/O concurrency and higher data reliability.
Applications and websites with sharp traffic fluctuations

MISK will utilize big data instance families that support Hadoop distributed computing, log processing, and large data warehouses. Big data instance families adopt a local storage architecture, which helps deliver better network performance for Hadoop and Spark clusters while providing abundant storage space and higher storage performance

We will configure a virtual private cloud (VPC). To have full control over our VPC, we can define and customize by specifying the Classless Inter-domain Routing (CIDR) block, configuring route tables, and creating gateways. We can connect it with Elastic Compute Service (ECS) instances, ApsaraDB for RDS (RDS) instances, and Server Load Balancer (SLB) instances in our VPC.

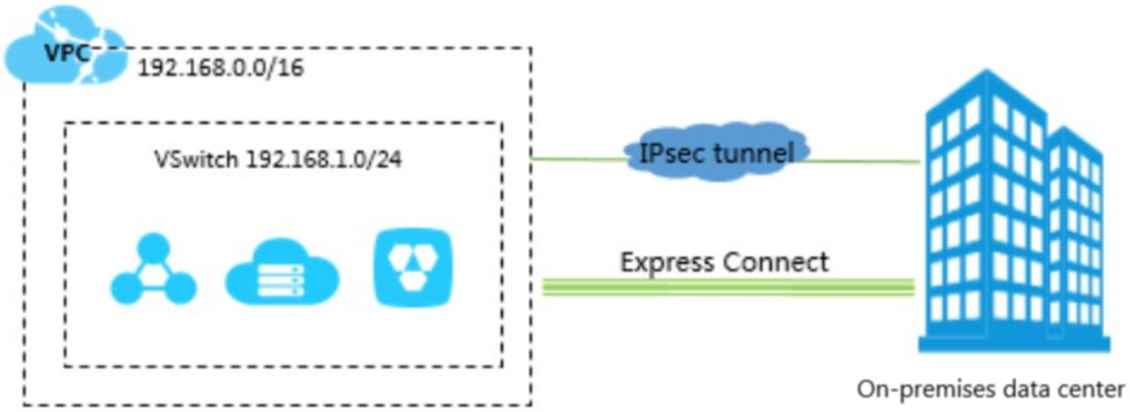

Figure 10:Alibaba VPC

After we deploy our ECS instances we will connect them to a Server Load Balancer instance, that uses virtual IP addresses (VIPs) to virtualize these ECS instances into backend servers in a high-performance server pool that ensures high availability. Client requests are distributed to the ECS instances based on forwarding rules.

Server Load Balancer checks the health status of the ECS instances and automatically removes unhealthy ones from the server pool to eliminate single points of failure (SPOFs). This enhances the resilience of our applications. We will also use Server Load Balancer to defend our applications against distributed denial of service (DDoS).

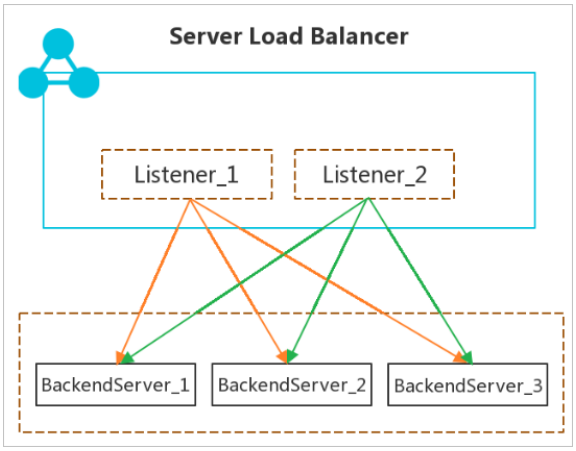

Figure 11:Alibaba SLB

MISK'S ECSs INSTANCES OVERVIEW:

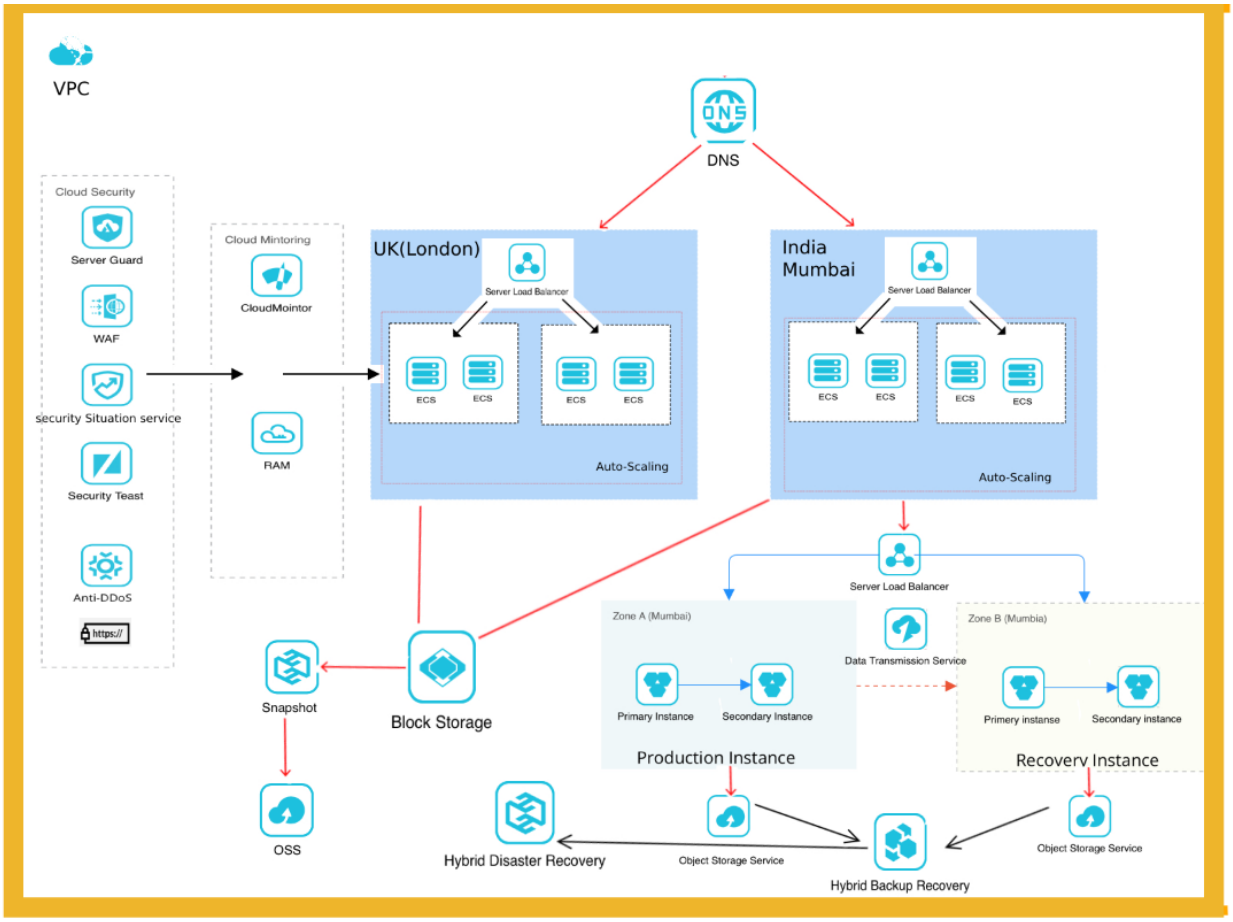

Figure 12:MISK'S ECSs INSTANCES OVERVIEW

MISK'S NETWORKING VPN/VPC

Alibaba Cloud provides a range of connectivity options to allow Internet and intranet access. MISK Applications deployed in a VPC which will provide services to the outside. To control access to the applications over the Internet, we will create a security group of rules and configure whitelists. We will also isolate application servers from databases to implement access control. We will deploy web servers in the UK region that can access the Internet, and deploy databases in the other webserver India region that cannot access the Internet. Then, we will create different subnets in a VPC to deploy different services. Additionally, we can connect a VPC to an on-premises data center or another VPC to extend the network architecture.

The webservers in the UK region connect the internet via Server Load Balancer (SLB). Provides layer-4 and layer-7 server load balancing, which makes ECS instances accessible from the public network.
The DNAT function of SLBs allows them to forward an Internet request to multiple ECS instances. SLB expands the external service capabilities by distributing traffic to multiple ECSs and improves the availability of application systems by eliminating single points of failure.

VPN Gateway is an Internet-based service that securely and reliably connects enterprise data centers, office networks, and Internet terminals to virtual private clouds (VPCs) of Alibaba Cloud through encrypted channels. We will deploy a VPN That connects our VPC to the clients and the data center in UK and India. For high security: we will use the IPsec protocols to encrypt data for secure and reliable data transmission. And for high availability VPN Gateway adopts the hot-standby architecture to achieve failover within a few seconds, session persistence, and zero service downtime.

The encrypted Internet-based connections provided by VPN Gateway are more cost-effective than Express Connect circuits. VPN gateways are easy to use, it can start to work immediately after we deploy them.

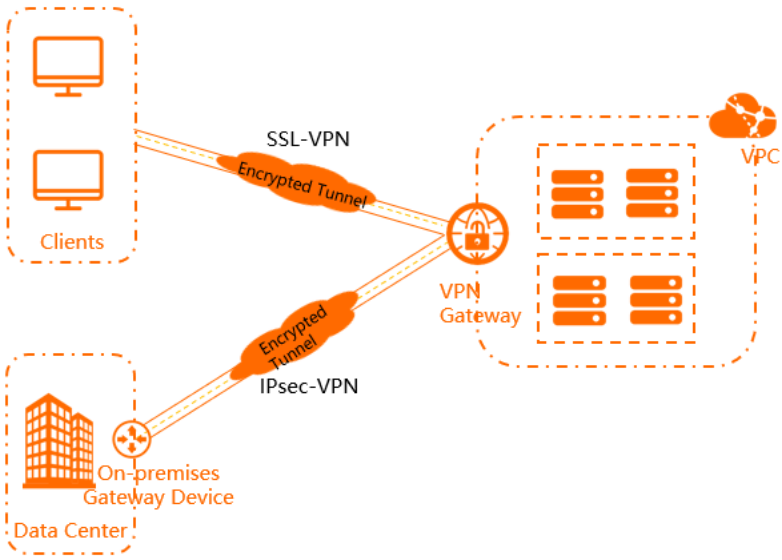

Figure 13:Alibaba Cloud VPN

We will deploy SSL-VPN that allows clients to connect to a virtual private cloud (VPC) and access applications and services that are securely deployed in the VPC.

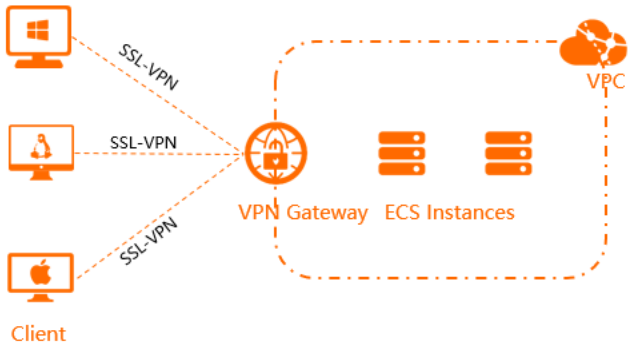

Figure 14: Alibaba SSL-VPN

We will use a vSwitchs in our VPC to connect cloud resources. will deploy a VPC in each region. However, a VPC covers all zones of the region to which the VPC belongs. We will create one or more vSwitches in a zone

to create one or more subnets for the VPC. The system automatically creates a system route table and adds system route entries to control the traffic of the VPC.

When multiple route entries match the destination IP address, the route entry with the longest subnet mask prevails and is used to determine the next hop. This ensures that the traffic is routed to the most precise destination.

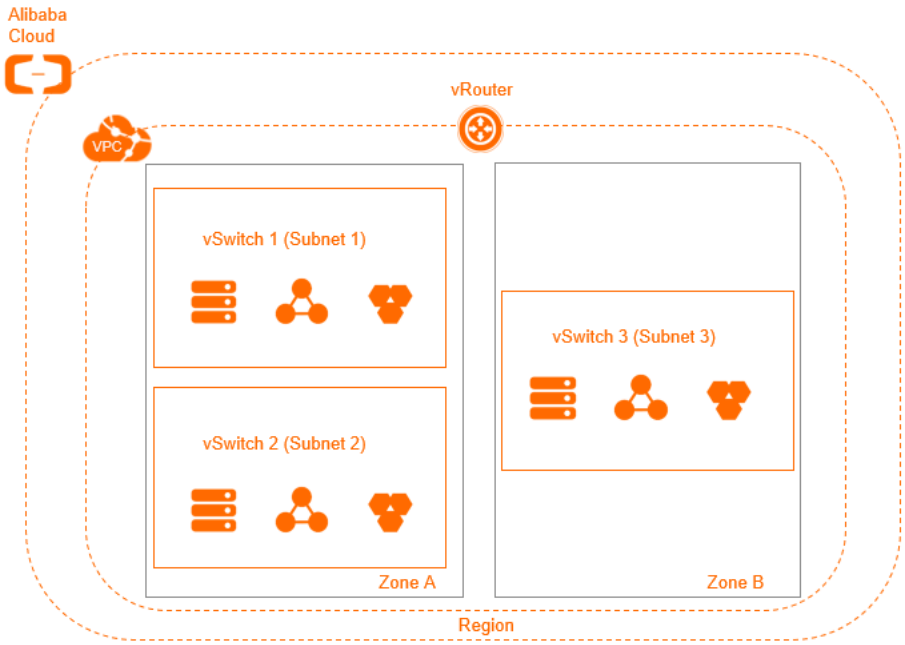

Figure 15:Alibaba vRouter

We will deploy a security group in our VPC to control inbound and outbound traffic and improve security. Security groups provide Stateful Packet Inspection (SPI) and packet filtering capabilities.

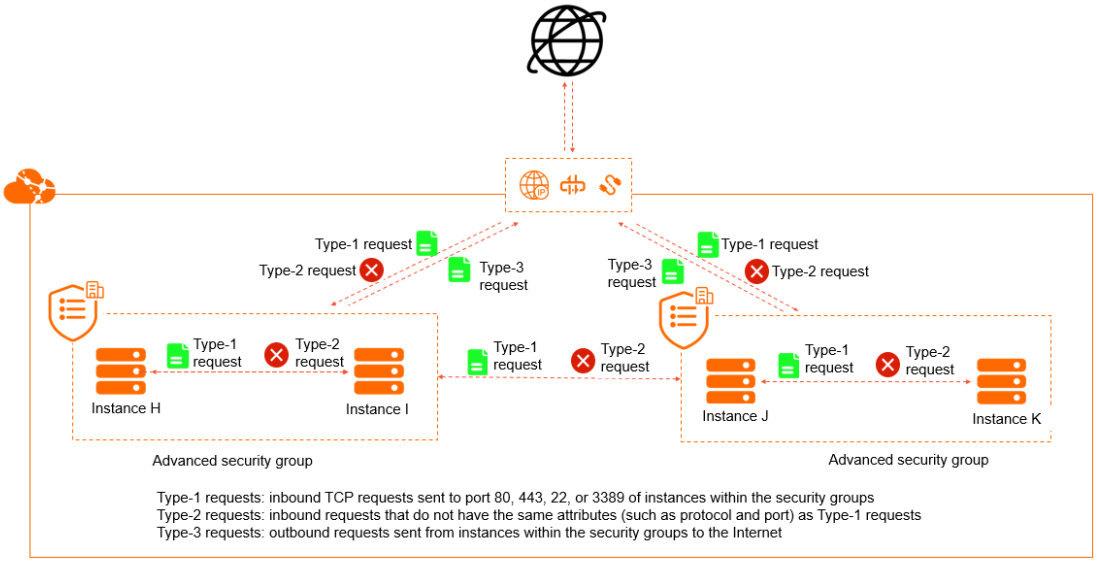

Figure 16:VPC Security Groups.

To accelerate failovers, we will create a failover group that consists of two virtual border routers (VBRs). After the system detects failures of the active VBR by using Bidirectional Forwarding Detection (BDF), the system can seamlessly switch workloads to the standby VBR in the failover group within less than one second.

Virtual border routers (VBRs) are an abstraction of Express Connect circuits that are isolated and virtualized by using the Layer 3 overlay and vSwitch technologies in the Software-Defined Network (SDN) architecture. A VBR is deployed between customer-premises equipment (CPE) and a virtual private cloud (VPC) to exchange data between the VPC and the data center.

After we connect our data center to an access point of Alibaba Cloud through an Express Connect circuit, we will attach the associated virtual border router (VBR) to a Cloud Enterprise Network (CEN) instance. The CEN instance must be connected to the virtual private cloud (VPC) to access. data centers can communicate with the VPC through private connections.

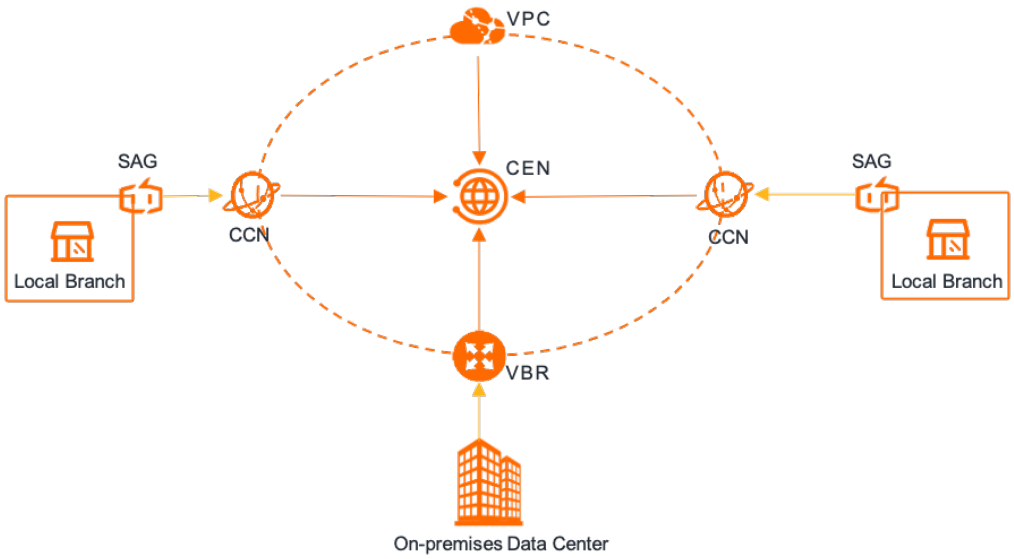

Figure 17:Alibaba VBR

In addition to this, multiple-connection redundancy is required for the MISK cloud to be stable, and the redundancy switching function is performed in the VPC. We will configure health checks for redundancies and manage the network through the VPC console.

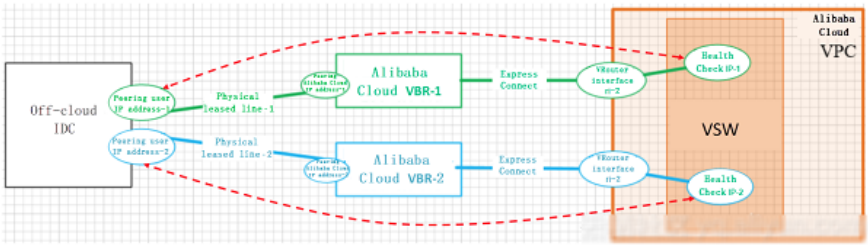

Figure 18:multiple-connection redundancy

In MISK we will use a network access control list (NACL) that tells a server the access rights of a network. It is the first line of defense to block the traffic at a subnet level and it is stateless. We will open both inbound and outbound ports explicitly to allow traffic based on MISKs needs. Clients use different ports to initiate requests. We will select different port ranges for network ACL rules based on the client type. The following table lists ephemeral port ranges for common clients.

Client	Port range
Linux	32768/61000
Windows Server 2003	1025/5000
Windows Server 2008 and later	49152/65535
NAT gateway	1024/65535

Table 2:Ports Range

MISK'S NETWORKING OVERVIEW:

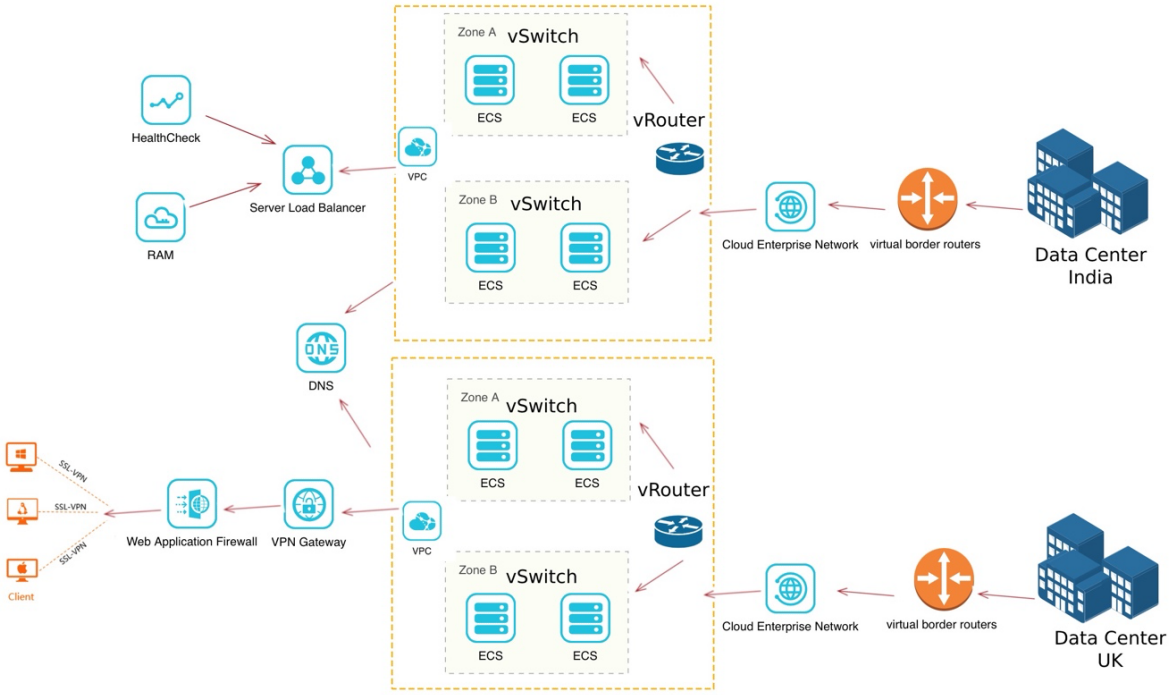

Figure 19:MISK'S NETWORKING OVERVIEW

MISK'S RAM USERS

Cloud computing has made way for multi-tier processing and access systems. Different environments allow for different models of SDLC, and the information delivery mechanism has also evolved to support wider system implementation. Deployments want to keep a close eye on security compliance, and access authorization.

Alibaba Cloud Resources and Access Management (RAM) allows MISK system administrators to create and manage RAM users for employees, systems, applications, students, and any other required identities. These identities can be easily managed with Alibaba Cloud RAM to assign permissions to different users to access Alibaba Cloud Resources. In MISK where multiple users collaborate and manage cloud resources within an organization, Alibaba Cloud RAM allows the administrator to keep the Alibaba Cloud account and password confidential. Alibaba Cloud RAM also allows the administrator to grant users the minimum required permissions to ensure high security.

MISK regular student has access to their accounts as a student to utilize the courses material and edit their profiles information. all their information about their regular account will be saved securely in MISK databases and only accessible by their teachers' regular account and the administration that already has their passwords and regular accounts.

MISK decided to migrate from on-premises to a cloud computing system while deploying using Alibaba Cloud products and services, such as the ECS, OSS with SLB, and a choice of database. The administrator needs to assign different tasks to different teams and individual users.

These users will be assigned different tasks and will need various permissions to complete the tasks. Alibaba Cloud RAM will facilitate every need related to authorization and permission management in MISK.

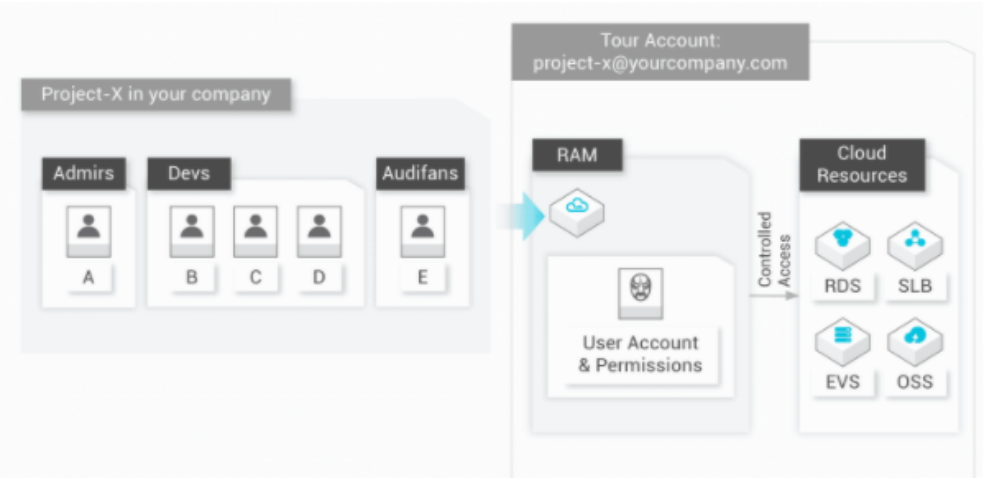

Figure 20:Alibaba RAM

MISK Administrator accounts multiple users/teams are assigned for a particular account. is a gateway for them to access any cloud resource that the enterprise has deployed. This controlled access offers a lot of features and benefits, including resource management and moderated access depending on the requirement. The exact task requirements and resource usage reports can be compared to analyze employee and team performance. This could lead to a better-managed system with optimal usage and team collaboration exercises.
MISK we will create custom policies, grant permissions by binding more policies to a user and user group, create access keys and credentials, provide access to one or multiple cloud resources, provide time-based or location-based access rules, Bind the primary account to an MFA device and configure the MFA independently.

MISK will enable multi-factor authentication (MFA) device for a Resource Access Management (RAM) user. Virtual MFA devices and Universal 2nd Factor (U2F) security keys are two types of MFA devices. After we enable an MFA device, it provides higher security protection for our RAM users. Before we enable a virtual MFA device, we will download and install the Google Authenticator app on our mobile device. We will select required for enabling MFA when we create a RAM user, we will require to bind an MFA device upon the logon of the RAM user. We will select Virtual MFA Device in the Enable MFA Device dialog box. If a RAM user of our Alibaba Cloud account is allowed to manage its MFA device, the RAM user can enable the MFA device in the RAM console. To enable an MFA device, we will Move the pointer over the profile picture in the upper-right corner of the console and click Security Information Management. On the Virtual MFA Device tab and Enable Virtual MFA Device.

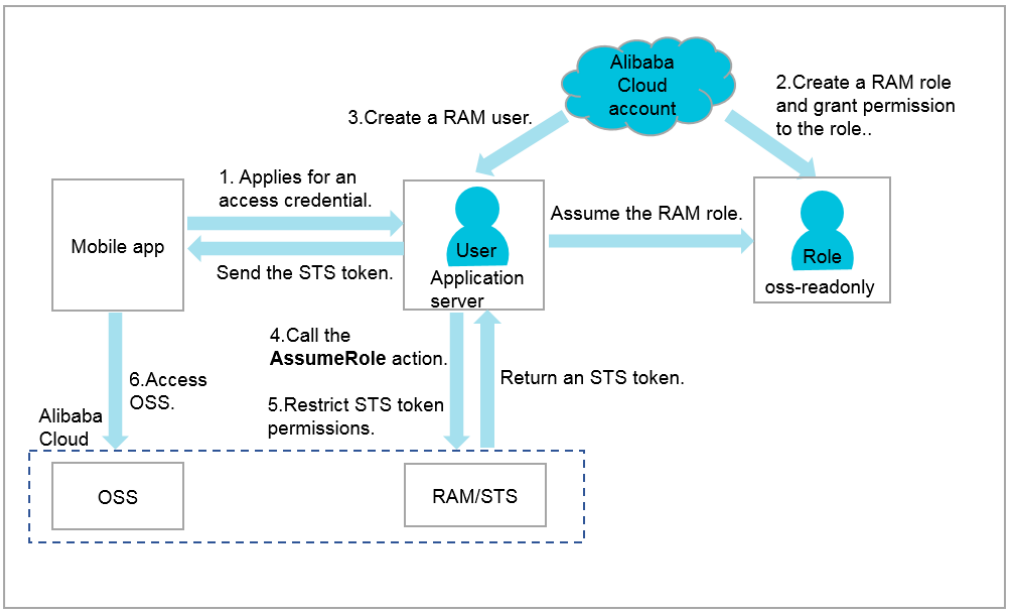

Figure 21:Alibaba RAM Roles

MISK's will deploy Services accounts that connect the webservers in the India region with the databases there.

To allow MISK to manage temporary credentials to our Alibaba Cloud resources. A RAM role can only be assumed by using an issued STS token to access Alibaba Cloud resources. When the STS token is issued, we will specify a validity period and access permissions for the STS token. We will use an STS token to assume a RAM role. An authorized RAM user can use an AccessKey pair to call the theAssumeRole operation.

This way, the RAM user obtains an STS token of a RAM role and can use the STS token to access Alibaba Cloud resources. This method is used to implement cross-account access and temporary authorization for our employees in MISK. we will obtain an STS token for role-based single sign-on (SSO).

We will call the AssumeRoleWithSAML operation to obtain an STS token of a RAM role to implement a role-based SSO. That would help MISK to reduce the risks of AccessKey pair leaks. An AccessKey pair is a long-term credential for a RAM user. We can specify the validity period for STS tokens. After STS tokens expire, they become invalid. Therefore, we do not need to rotate the STS tokens regularly. Also, we can attach custom policies to STS tokens for flexible and fine-grained authorization.

We will set up, configured, provision, and secure our RAM users in MISK applications by deploying ECS instances to use AccessKey pairs (AKs) to access other Alibaba Cloud services. An AK allows you to access Alibaba Cloud APIs with full permissions for our accounts. To facilitate the management of the AK by applications, we must store the AK in the application configuration files or otherwise store the AK in an ECS instance.

These operations make it more complicated to manage the AK and keep it confidential. We need consistent deployment across regions. So, the AK is spread along with the images or instances created from the images. In these cases, we will update and redeploy each instance and image individually whenever we make changes to the AK.

We will attach a RAM role to an ECS instance, and use an STS temporary credential to access other cloud services from the applications within the instance. STS temporary credentials are generated and updated automatically. Applications can obtain the STS temporary credentials by using the instance metadata URL. We will use RAM roles and authorization policies to grant ECS instances with different or identical permissions to access other cloud services.

MISK’S BACKUPS AND FAILOVER

First of all, we will back up MISK’s database. The data will be backed up every day at 2:00 am in the Saudi time zone. We will keep our backups for 5 years minimum. When a system failure occurs, the database can automatically switch services from the primary node to a read-only mode. We will specify a read-only node as the new primary node to switch services from the primary node to the read-only mode.
We will set automatic failover active-active architecture that ensures high availability. If the primary node that supports reads and writes is faulty, services are automatically switched to the read-only mode that is elected by the system as the new primary node.
A failover priority is assigned by the system to each node in a cluster. During a failover, a node is elected as the primary node based on the probability that is determined by this priority. The probability of being elected as the primary node is the same for the nodes that are assigned the same failover priority we will save our data in (OSS) as an offsite backup storage solution. Data will be backed up by a simple bash script that gets executed regularly Client will be used to transfer the backups to OSS. Alibaba Cloud OSS is a suitable backup storage solution. Rarely accessed objects such as backups can be stored reliably, cheaply, and securely. The first 5 GB of storage can be used completely free of charge.

And to back up our disks we will use a snapshot which is a data file that captures the point-in-time status of a disk. Snapshots are often used to back up and restore data or to create custom images. When snapshots are used for data backup, the first snapshot of a disk is a full backup, and subsequent snapshots are incremental backups. Incremental snapshots can be created quickly and have small sizes. The amount of time required for backup depends on the amount of incremental data to be backed up. Also, Elastic Block Storage (EBS) devices offer high performance and reduce latency, persistent, and highly reliable Block-level random Storage for ECS instances. Block storage supports automatic replication of our data in the zone to prevent the unavailability of data caused by unexpected hardware failures and protect your business from the threat of hardware failures.

To secure our backup we will deploy a security group that acts as a virtual firewall for our backup files. Web Application Firewall (WAF) is a security service that protects our website and app services. WAF identifies malicious traffic, scrubs, filters the traffic, and then forwards normal traffic to our web server. WAF protects our web server against attacks and ensures the security of our data and business.

In addition, we will deploy Anti-DDoS: which is on Alibaba Cloud's global scrubbing centers, combined with intelligent DDoS detection and protection systems developed at Alibaba, automatically mitigates attacks and

reinforces the security of MISKs applications, reducing the threat of malicious attacks and Server Load Balancer (SLB): SLB is a service that distributes network traffic across groups of backend servers to increase the throughput of our applications. we can use SLB to prevent service disruptions caused by single points of failure (SPOFs) and improve the availability of applications.

Any cloud might fail due to unexpected reasons, such as a device or power failure in the data center. In this case, our disaster recovery plan can help MISK to ensure data consistency and service availability. ApsaraDB for Redis provides a variety of disaster recovery solutions to meet the MISK's requirements

Cross-region disaster recovery solution: In MISK database architecture of Global Distributed Cache for Redis, a distributed instance consists of multiple child instances that synchronize data among each other in real-time by using synchronization channels. The channel manager monitors the health status of child instances and handles exceptions that occur on child instances, such as a switchover between the primary and secondary databases.

Global Distributed Cache for Redis is applicable in scenarios such as geo-disaster recovery, active geo-redundancy, nearby application access, and load sharing.

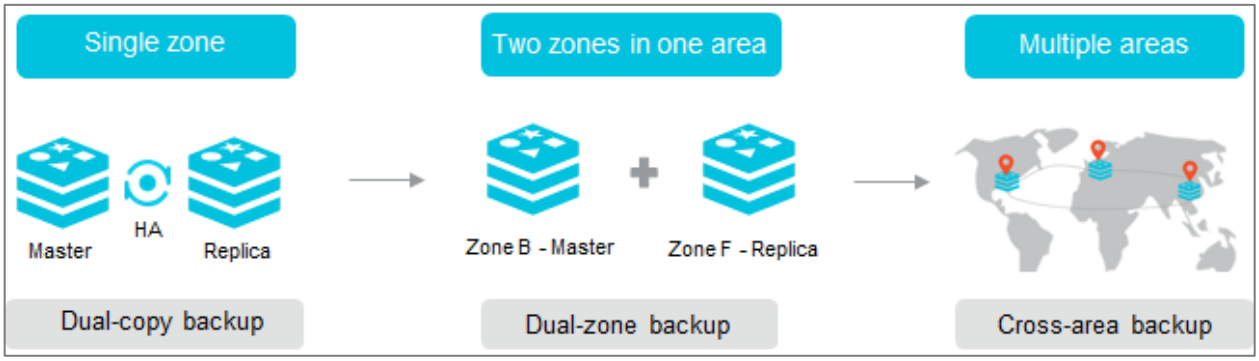

Figure 22:Cross-region disaster recovery

When the system detects a failure in an Express Connect circuit, the system performs a failover. The time required to complete a failover is approximately 5 seconds because when MISK takes a long time to recover after a disaster that would cost MISK a lot of money. We will deploy Hybrid Backup Recovery all the backup effort is performed in the appliance without consuming extra resources. It implements a backup and recovery solution easily and acts as a bridge between MISK's on-premises servers and the public cloud. The HBR Appliance has a dual power source, dual network ports, hot-backup disks, etc, providing a safe and stable backup operating environment. After obtaining the backup data automatically, the HBR appliance encrypts, deduplicates, and uploads it to the cloud.

In this way, it perfectly balances the security and the network efficiency during the backup and protects critical data of the enterprises. Each HBR appliance has a one-year software license for file and virtual machine backup. The period starts after the activation of the license. After the license expires, MISK can renew it online in the Alibaba Cloud console.

Using HBR's unique data deduplication and compression, customers can achieve a data reduction ratio of up to 30:1. This can save storage space and cloud traffic and improve data storage and transmission efficiency.

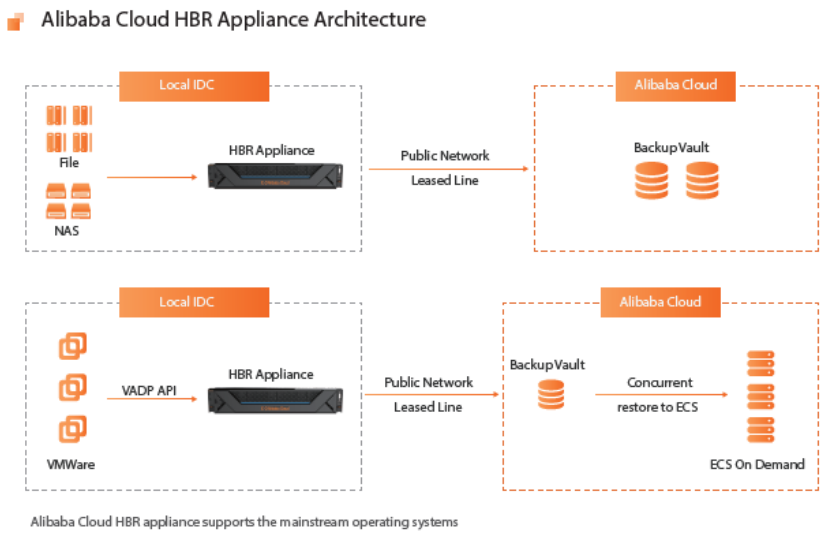

Figure 23:Alibaba HBR

All the data is deduplicated and compressed before being uploaded to the cloud, which saves bandwidth and consumes less cloud storage space. The cost is up to 70% lower than traditional backup solutions. In disaster recovery scenarios, only storage resources are usually consumed, and only servers on the cloud are pulled up as needed when disaster recovery takes over. This is 90% lower than traditional disaster recovery solutions.

Category	Configuration	DR208INTL
Data Source	Max. Files	200 M
	Max. VMs	200
Cloud	Cloud Backup Storage	300 TB
	Max. Upload Speed	1TB / Hour
	Cloud Monitoring	Yes
Computing	CPU	Xeon 6130 * 2
	Memory	256 GB
Storage	RAW Disk Space	configurable, 2 TB-96 TB
	Disks Quantity	configurable, 4 -12
	Disk Type & Capacity	SATA HDD, 4 TB-8 TB
		SSD, 960 GB
	RAID Protection	RAID 5
Network	On Board: 10GbE	configurable, 0 - 2
	On Board: 1 GbE	configurable, 0 - 2
	16Gb HBA	configurable, 0 - 2

Table 2:backup solutions

The process of backup and failover recovery to MISK will be automated according to the following steps:

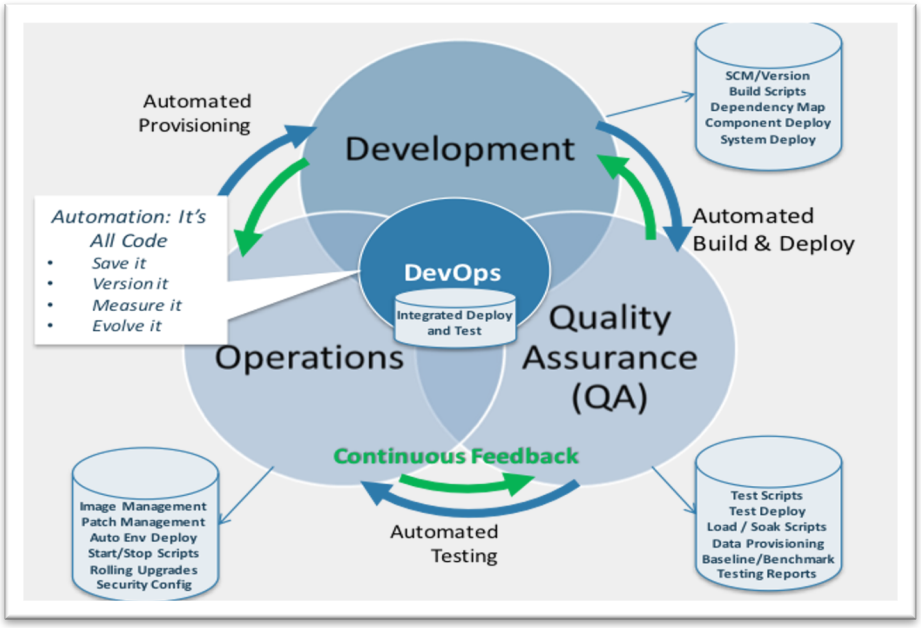

Figure 24:DevOps

Infrastructure as Code (IaC): Alibaba Cloud IAC is a server environment that provides a complete server backend to facilitate deployment. Alibaba Cloud IAC Alibaba Cloud IAC works with Terraform that enables MISK to adjust resources depending on usage. It can also be implemented for automating resource scaling. IAC can be reused multiple times at different stages of the DevOps practice. It could be for testing or building the code, sandboxing, or maintaining the application in a production environment.

Continuous Integration (CI): Depending on the metrics collection and user feedback, new features or improvements are constantly integrated into the application. These form new versions or iterations of the application. The Alibaba Cloud CI-CD pipeline provides support for version control and instant rollbacks.

Continuous Delivery (CD): Continues Delivery pipelines ensure that automatic delivery is not hampered throughout the practice, and all the required resources are provisioned automatically. The application is pushed into production as soon as the testing is completed. This process is completed without any manual interception of the process and doesn't interrupt the end-user experience.

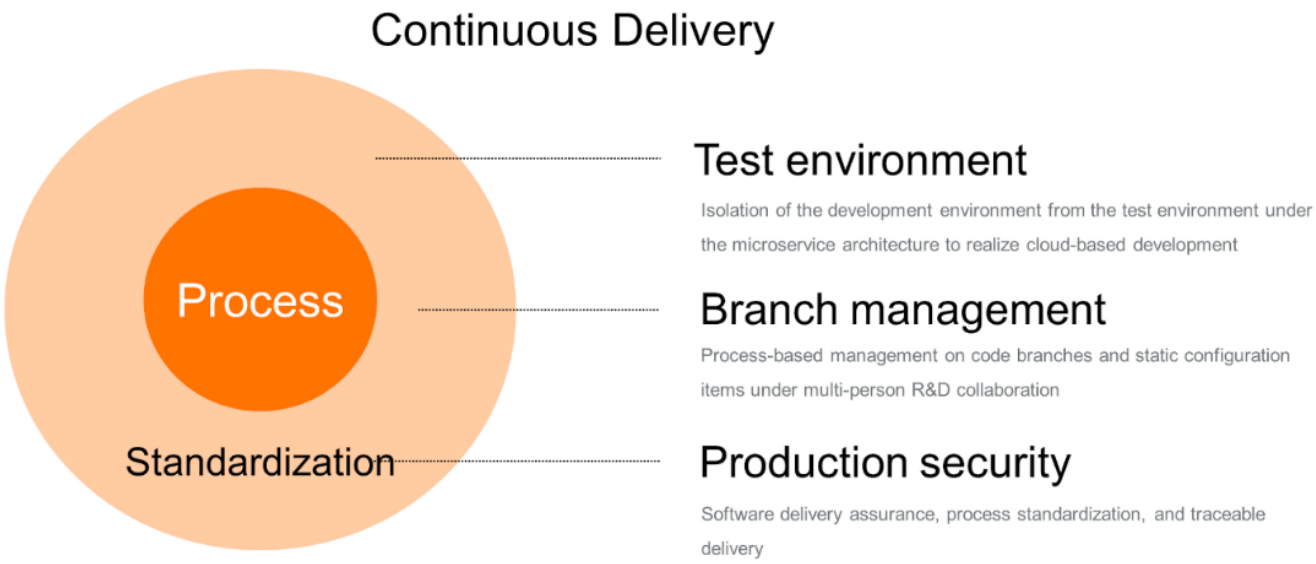

Figure 25:Continuous Delivery

Microservices – Containers No downtime is achieved by implementing Alibaba Cloud Microservices using the Container Service for Kubernetes (ACK). Microservices have provided functionality where inter-dependability is now non-existent. When modules (microservices) will not depend on each other and with containers, most of the configuration and operational details are integrated. Changes to one module will not affect another.

To conclude, in this paper, we discussed many important steps that would help MISK to consider Alibaba Cloud products and solutions to leverage Cloud Computing benefits and migrate their whole resources to Alibaba Cloud.

We started our paper by illustrating the overview of our cloud solutions that we recommend MISK to follow. We described the services in the diagram component by component and how each service communicates with the other services with a short overview of the services and how it works.

We discussed the database we are going to deploy which is MySQL and in which region and zone. We explain how to connect it to the ECS instance via a services account. We mention what kind of data MISK stores in their database including students' pieces of information and meta-data and more.

We explained our security services to protect our database and how to back up these data and recover it and restore it in no time. For more clarity, we attached a database overview diagram.

Then, we discussed the ECS instance that we need. We determine what type of instance and memory meets our requirements. We explain how to backup out instances using snapshots and block storage and how to scale our instances so we don't waste our resources. We discuss our big data services and attached an ECS's instants diagram.

We demonstrate MISK's networking that includes VPC and VPN. We discussed the failover group that consists of two virtual border routers (VBRs). And we attached a network overview diagram.

We interpreted MISK RAM users and their policies. We explain RAM accounts to the users and the administers .and how to secure them with multi-factor authentication (MFA) device for a Resource Access Management (RAM)

Finally. We demonstrate our plan of backups and disaster recovery and how to restore our resources and data in no time.

Nevertheless, as the cloud service models evolve at a fast pace and new solutions appear every day, companies may find it difficult to choose the right option for them and the migration to the cloud may be an intricate and challenging procedure. Considering the SaaS and PaaS models, this document tries to enlighten some misconceptions and to deliver a migration model with distinct phases, which aims to recommend MISK to go on and migrate to Alibaba Cloud for best practice and a brighter future.

REFERENCES

https://www.alibabacloud.com/blog/how-to-automate-backups-with-alibaba-cloud-object-storage-service_580252

https://www.alibabacloud.com/solutions/hosting/Disaster-Recovery

https://www.alibabacloud.com/help/en/doc-detail/100734.htm?spm=a3c0i.23458820.2359477120.1.ce717d3fzKzEUF

https://www.alibabacloud.com/blog/devops-team-building-define-and-collaborate-in-the-real-world_597054

https://www.alibabacloud.com/blog/devops-team-building-define-and-collaborate-in-the-real-world_597054

https://www.alibabacloud.com/product/ram

https://online.visual-paradigm.com/diagrams/templates/alibaba-cloud-architecture-diagram/architecture-transformation-of-oltp-type-relational-databases/

https://www.alibabacloud.com/help/en/doc-detail/201882.html