HIGH AVALABULITY

1)**Redundancy**: High-availability systems often incorporate redundancy in critical components. This redundancy ensures that if one component fails, another can take over seamlessly, minimizing downtime.

2)**Failover**: The ability to automatically switch to a backup or secondary system when a failure is detected. This ensures continuous operation and reduces the impact of failures on end-users.

3)**Load Balancing**: Distributing incoming network traffic across multiple servers or resources to ensure no single point of failure and optimal resource utilization.

4)**Monitoring and Alerting:** Continuous monitoring of system health and performance, coupled with alerts or notifications that inform administrators of potential issues. Proactive monitoring allows for quick responses to problems before they escalate.

5)**Scalability**: The system should be designed to scale horizontally to handle increased demand. This could involve adding more servers, resources, or instances dynamically.

6)**Data Replication:** Replicating data across multiple locations or servers to ensure data availability and integrity. This can involve techniques such as database replication or distributed file systems.

7)**Geographic Redundancy**: Having redundant systems located in geographically diverse locations to mitigate the impact of regional outages or disasters.

MONITORINGS ===>

system observation and measurement of various aspects of system performance behaviour or state primary Mona rating is ensure the reliability availability and optimal performance of application services and infrastructure

1**) metrics** -- monitoring involves collecting analysing various performance matrices such as CPU using memory utilization network traffic disk response times these metrices provides insights into the health and efficiency os system

2)**AVAILABILITY UP TIME** -- monitoring the availability of service and system often measured as uptime percentage it help to identify the down time events understand their causes and work towers mini service disruption

3)ALERTING -- monitoring system are often configured with alerting mechanisms alerts notifies administrator team

4**)LOGGING --** monitoring the often invalues the collecting annualizing of logs detailed records of events errors and activities with in the system

OBSERVABILITY ======>

SYSTEM REFERS TO THE ABILITY To understand mesurfe and gain insight into the internal state of system by analyzing its out puts logs events etc ..it crusial aspect of monitoring and managing complex systems helpingdevelopers and opertor to detect diagnose and resolve isssue efficently

1)**METRICS ---** quantitative meserments that provides information about system behavior metrics could in cloude cpu memory utilizzation network trafic responce times error ratres thse meserments help in understing the overall health and performance of system

2**)LOGS** --- detailed records or enterieas generayted by the system system capcrting events action errors messages logs are valabule to troble shooting and identify specific issues with in thwe system

3)TRECE -- destibuting tracing involes tracking the flow of request as it travers through various components and compomnts and services in system trace help in uderstang the performance and dependencies b/w diffrent part of distubuted system

4)ALERTS -- notifiction triggered by perdifind conditions alerts are used to notify operator administator when certain metrices events rech level that require attentipon they play crucial role proactive monatering issue resolution

5)Dashboards: Visualization tools that present a consolidated view of key metrics and data in real-time. Dashboards help users monitor the system's status at a glance and quickly identify any anomalies or issues.

6)Anomaly Detection: Algorithms and techniques that analyze data to identify unusual patterns or deviations from expected behavior. Anomaly detection is valuable for identifying potential issues or irregularities in the system.

AUTOSCALING ====>

cloud computing feature that allow s system to automatically adjust its computing resorce resorce based on current demand gole is autoscaling the applictiing right amout(computr power ,storage or network bandwidth)avalable to handle varing work loads efficintly .. autoscaling env infrastrure scale up or down dynamically in responce to change in demand

1)LOAD BALANCING -- aworks in conjunction with load balancing as deamand incress new instance or virtual mechines are added to the pool The load balncer distubute incomming trafic accross the instance and optimal performace

2)METRICS AND TRIGGERS --- aautomatically decession are based on pre defined mertics and trigger it inclodes CPU memory network traffic .. trigger are conditin when met

3)SCALING policies --- autoscalling policises define how the infrastruer should scale in or out based on specific conditon

4)MANUAL AND AUTOMATIC SCALING --- automatically based on predefind condition or rules manually trigger by admistator in responce to certain events

5)INSTANCE TEMPLATE OR IMAGE --- whennscalling up automatically system use the predefined template or images then lanch the new instance with the reqired configuration and software

OSI

open system interconnection model

1)APPLICATION --- this is the top most layeer where commeniction between end -user software applicatin and the network occures it provides newtwork services directoly to end -user

2)PRESENTATION -- deal with data format translation encription and conpression

.the data send by the appliction layer of one system can be properly interpreted by the application layer of another

3) SESSION -- manage session or connetion b/w applicton allowing them to establish maintain and terminate commeniction

4)TRANSPORT -- end to end communiction error recovery and flow control b/w device Transmission Control Protocal(TCP) User DataGram Proctoal (UDP) operate at this layer

5)NETWORK -- manages the routing of data packets b/w diffrent networks addressing and logical addresing The Internet Protocal(IP)

6)DATALINk -- responsible for crating realiable link b/w two directly connected node and dealing with issue like framing addressing and errror detection

7)PHYCAL -- deal with the phycal connection b/w devices and the transmission of raw binary data over a phycial medium

RTO===>>

Recovery Time Objective (RTO): ---In the context of disaster recovery and business continuity planning, RTO refers to the maximum acceptable downtime for a system, service, or process. It represents the targeted duration within which a business process

RPO =====>

Recovery Point Objective (RPO)---: In the context of data recovery and backup strategies, the term "Recovery Point Objective" (RPO) is often used. RPO refers to the point in time to which you want to recover data after a system failure or data loss incident. It represents the acceptable amount of data loss measured in time.