AccessReal

System Monitor Process Flow

Version 1.0

i-Sprint

Trust without Boundaries

Table of Contents

1 Overview

Monitor AccessReal infrastructure 24x7 to ensure the services are continuous, and always available without disruption or downtime to the customers. When a failure is detected, administrators can be alerted to take necessary actions.

Purpose

This flow is applicable to the production server, databases, and devices of AccessReal deployed on AliCloud platform.

2 Duty and Privileges

This flow involves below departments (roles) duty and privileges.

2.1 IT Business System Manager

i. Create and implement a policy for monitoring based on the business requirements and company relative instructions.
ii. Review and modify monitoring targets, methods, and policies based on the business requirements or company instructions.
iii. Arrange resources to carry on the daily monitoring tasks.

2.2 System Administrator

i. Setup the network devices, servers, system service parameters, alarm value, alarm receivers, alarm frequency, and its methods.
ii. Monitor targets including operations, devices, and services in real-time, and take actions for any failure alarm.
iii. Review and modify monitoring parameters.
iv. Upgrade monitoring tools.
v. Optimize monitoring methods according to the business requirements.
vi. Perform failure simulation practice for different systems regularly.

3 Details

3.1 Monitoring Purpose

- Monitor the server, database, app, and others of AccessReal production environment on the AliCloud.
- Inform the system administrator by email or SMS if any alarm/failure is detected.
- Compile the issues into documents for history record to do further analysis of the failure trend.

3.2 Monitoring Flow

i. **Data Collection** - It is implemented by using the monitoring tool via SNMP, Agent, ICMP, SSH, and IPMI.

ii. **Data Storage** -The data will be stored at the monitoring server's database by using the monitoring tool.

iii. **Data Analysis** - For data analysis, the monitoring tool can provide related failure information such as the failed event/time for troubleshooting.

iv. **Alarm** - According to the alarm policy setting, the monitoring system will send the alarm information to the system administrator by email or SMS when an alarm/failure is detected.

v. **Action** - IT department receives the alarm, assesses the failure level, and takes action or works with other colleagues to solve the problems.

vi. **Document** – Compile the alarm/failure events into historical record.

3.3 Monitoring Objects

A System

i. CPU Usage Rate
ii. Physical Memory Usage Rate
iii. Hard Disk Space Usage Rate
iv. Disk I/O Throughput
v. Network Port Throughput

B Apps

i. Nginx
ii. Tomcat
iii. MySQL Database
iv. MongoDB

C Flow

i. Server Load Balancer (SLB).
ii. The throughput of the network that forwards the loads.

D API

The monitoring tool will automatically send requests (e.g. GET, POST, PUT, HEAD, and OPTIONS etc.) to API according to the schedules to test the availability, accuracy and response time.

E Logs

System and app generate different logs, such as system logs, access logs, error logs, running logs, network logs. IT department would monitor those logs by using the monitoring tools and collect log information. For the exceptions or errors, the monitoring tool will analyze and report to the system administrator.

F Security

i. System vulnerability and backdoor detection
ii. Unusual logins
iii. DDoS attacks

G Performance

i. Monitor the webpage performance, DNS response time, successful HTTP connection time, webpage performance rates, response time, availability and the element size and more.
ii. Monitor the CPU database and memory usage rate, connection counts, I/O throughput and the SQL statements that run for a long time.

H AliCloud Service

Monitor the AliCloud account balance, expiration date, and send alarms for recharge or account extension.

3.4 Monitor Configuration File & Logs Management

The administrator shall regularly export the monitored configuration files as logs to the storage path for backup. Only with permission, the logs are available for project team members, or to be the reference object of system performance/service.

3.5 Feedback Monitor Results

A General Alarm (refer to failure level 2-4 below). The monitoring system will notify the related system administrators and head of IT department once the alarm/failure is detected.

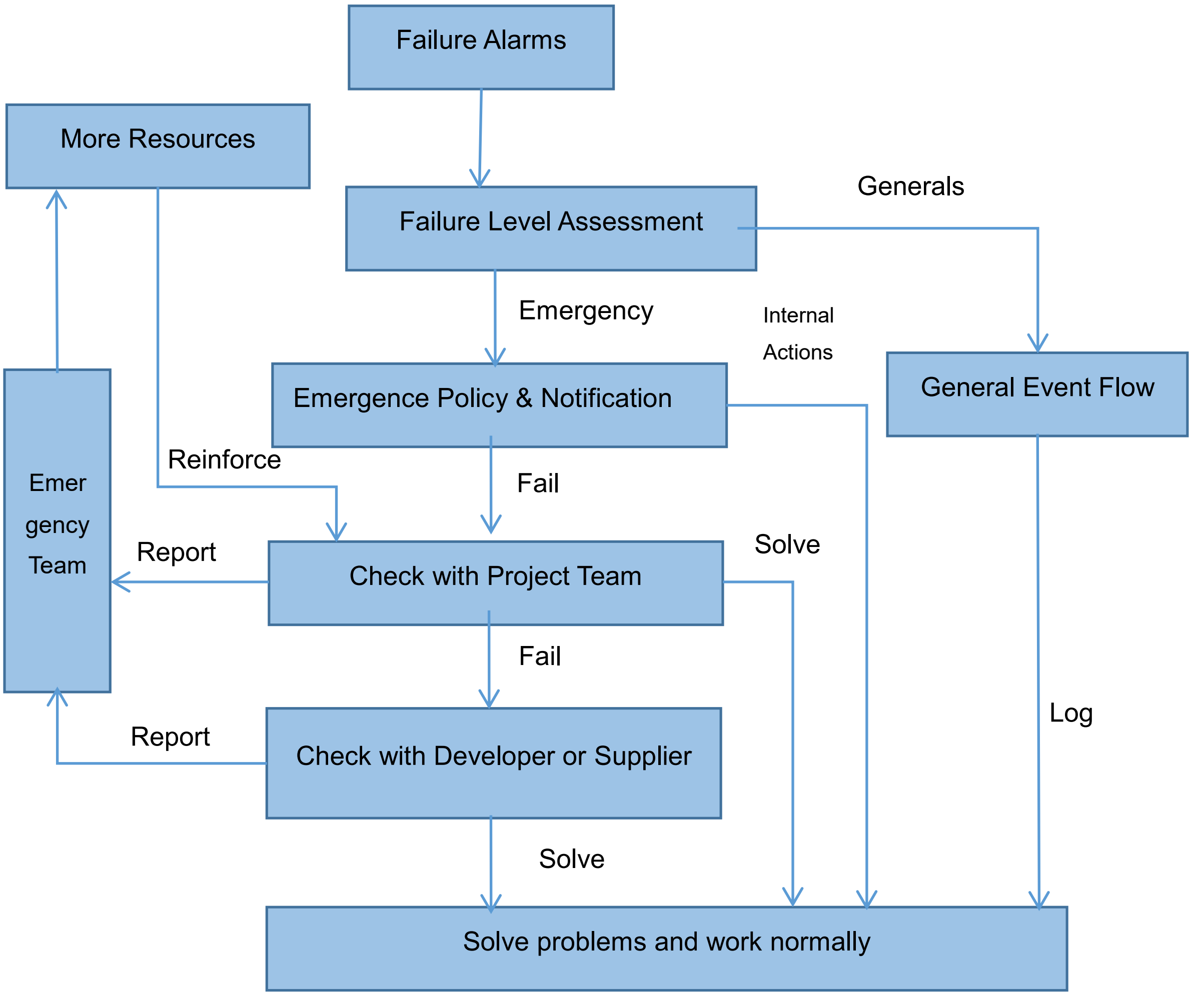
B Serious Alarm (refer to failure level 1 below). The monitoring administrator will send email to the heads of IT department and system users (other departments or project teams).

C Feedback Channel & Action

i. The system administrators shall keep the mobile and emails client available to receive the alarm notification. The email administrator shall make sure the alarm email can be sent to the target emails in time.
ii. Once the alarm emails were sent to the receivers, immediate actions shall be taken to solve the failures. At the same time, they have to report to the heads of department about the failures to seek for more help and resources if needed.

4 Alarm/failure Process Flow

4.1 Alarm/failure process flow chart



4.2 Emergence Failure Process Policy

The monitor administrator shall analyze the failure, point out the failure location/object (e.g. server problem), and follow the event until it is back to normal.

In general, the monitor administrator shall confirm the failure within 10mins, i.e. to judge its type to be a general or emergency event and take actions accordingly (referring to the flowchart above and failure list below).

The monitor administrator shall report to the leaders for more help or resources, or contact the developer or supplier for technical support.

4.3 Failure Levels & Guides

A Failure Levels

Level	Response Time	Complete Time
I Emergency: System crash causes data lost and the business flow stops running.	10mins. Provide solution within 30mins.	Within 3 hours
II Serious: some component failures decrease the system performance, but the system is running and the business flow is working normally.	10mins. Provide solution within 30mins.	Within 6 hours
III Less Serious: System reports errors or warning, but the system performance and running are not affected, and the business flow is working normally.	10mins. Provide solution within 30mins.	Within 12 hours
IV General: Exceptions. However, the system deployment, configurations, and functions are OK, and the business flow is working normally.	10mins. Provide solution within 2hours.	Within 24 hours

B Action Guides

i. Follow all the requirements or guides in this file.

ii. Work with other colleagues, departments or third party to solve the problems as soon as possible.

iii. Report to the leaders in time about the troubles, technical difficulties or any other important information.

iv. Confidentiality - All staff is responsible to keep all data of AccessReal confidential, and is not allowed to copy or distribute without written permissions of i-Sprint. The data of AccessReal are listed but not limited to the production network, server, system, app, monitoring information and logs.