Risk Management

VKP

Service Level Agreements (SLA) need well-balanced infrastructures to maximize the Quality of Service (QoS) they offer and minimize the number of SLA violations.

- In service operation, risk assessment helps support the following: 1) from the end-user perspective, what is the SLA's failure risk?
- 2) similarly from the IP perspective what is the risk of failure of a specific SLA? of the cloud infrastructure?

- Here, IPs perform continuous risk assessment at service operation, monitoring low-level events from the infrastructure such as risk of failure of physical hosts/VMs, security, legal, and data management risk. On the other hand, end-users also perform continuous risk assessment, monitoring service level non-functional Quality of Service (QoS) metrics such as the availability of VMs. Risk assessment has been introduced.

RISK MANAGEMENT

- Risk is measured in terms of consequence (or impact) and the likelihood of the event. Qualitatively, the risk is considered proportional to the expected losses which can be caused by an event and to the probability of this event. Quantitatively, it is the product of the probability of the hazardous event and the consequences.

- A threat is a potential cause of an unwanted incident whereas a vulnerability is a weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset.

- Finally, risk is the likelihood of an unwanted incident and its consequence for a specific asset, and risk level is the level or value of a risk derived from its likelihood and consequence.

- A fundamental issue in the characterization and representation of risk is to properly and appropriately carry out the following steps:

→Analyse the triggering events of the risk, and by breaking down those events formulate adequately their accurate structure.

→Estimate the losses associated with each event in case of its realization.

→Forecast the probabilities or the possibilities of the events by using either statistical methods with probabilistic assessments, or subjective judgments with approximate reasoning.

After the possible risks have been identified, they are assessed in terms of their potential severity of loss andprobability or possibility of occurrence. This process is called Risk Assessment (RA).

A risk level can then be represented using for example a 7-point rating scale

1: Trivial

2: Minor (-),

3: Minor (+),

4: Significant (-)

5: Significant (+)

6: Major, and

7: Catastrophic.

RISK AWARE CLOUD COMPUTING – THE FRAMEWORK

The functional requirements include a requested performance profile, both in terms of hardware configuration, e.g., amount of physical memory and CPU characteristics for VMs as well as application-level Key Performance Indicators (KPIs) such as transaction rate, number of concurrent users, response time, which are used for elastic auto-scaling.

The assessment criteria are:

1) Past SLA Performance: this includes the number of past successful SLAs.

2) Geography Information: Geographic threat level, stability level, jurisdiction transparency level, jurisdiction overlapping level.

3) Certifications and Standards Compliance: facility related certification level, operation related certification level, and industry standard compliance level.

4) Business Stability: this includes for example the business history, the number of employees, and the number of customers.

5) General Infrastructure Practice: Available compute resources, available spare resources, average node availability, storage backup frequency.

6) General Security Practice: facility security level.

7) General Privacy Practice: facility and data access control level, personal data protection level.

A value between 0 and 1 is computed for each of the criterion by evaluating an IP with respect to a number of sub-criteria.

Therefore SPs are able to specify the importance of each of the criteria, e.g. on a scale of 0 to 10.

Service Provider Risk Assessment

1) Past SLA Performance: this includes the number of past successful SLAs deployed by the SP.

2) Business Stability: this includes for example the business history, the number of employees, and the number of customers.

3) General Security Practice: Facility Security Level.

The IP may also require to carry out a legal risk assessment for the benefit of legal compliance.

Some important points

- When an SLA negotiation takes place, an SP is able to assess the risk of dealing with IPs. It is useful for the SP to know which IP is less risky, as this brings the confidence that the SLA once signed has a good chance to be fulfilled.
- When an SLA negotiation takes place, an IP is able to assess the risk of dealing with an SP. Similarly, this is useful for the IP as it brings the confidence that once the SLA is signed the IP's assets are protected ensuring.g the SLA fulfilment.
- Prior to committing to an SLA, the IP carries out a risk assessment based on the service requirements. This is SLA dependent and may include assessing a security risk, a legal risk, the risk of failure of physical hosts, or the risk of failure of VMs. The risk of accepting an SLA request is seen as an aggregate of various risks.

- Prior to committing to an SLA, the SP carries out a risk of service unavailability by evaluating the IP's reliability with respect to past behavior. By doing so, the SP has the confidence that the SLA can be fulfilled by a reliable IP.
- Once a service is in operation, the SP constantly monitors the service execution and continuously performs risk assessment as part of the SLA fulfillment.
- Similarly, the IP constantly monitors its infrastructure in service operation and continuously performs risk assessment as part of the SLA fulfillment.