STUDY OF FAULT TOLERANCE METHODS FOR CLOUD INFRASTRUCTURE WITH NESTED VIRTUALIZATION ARCHITECTURE

Bondarenko Maksym, Tarasiants Alina
Scientific advisor - Candidate of Technical Sciences, Associate Professor
Tkachev Vitalii
Kharkov National University of Radioelectronics
14 Nauky ave., Kharkov, 61166
Department of Electronic Computers, tel. (057) 702-13-54
E-mail: bondarenko@ieee.org

The abstracts are devoted to research of known methods of providing fault-tolerance of cloud infrastructure with the architecture of nested virtualization by setting of model experiments in order to determine the degree of consistency of established approaches to the dynamically developing technologies of nested virtualization, which are the basis of regional technologies

To date, the task of investigating established fault tolerance methods for cloud infrastructure with nested virtualization architecture is relevant [1-2]. This is due both to rapid technological advances, in particular the emergence of new virtualization technologies [3], and because of purely technical aspects [4], for example, the failure or failure of a major node leads to the collapse of the entire nested architecture.

As a subject of research, the methods described in are considered [5]. Generally, cloud infrastructure involves more than a single physical or virtual server. Data stored in the cloud is distributed among these servers automatically and transparently to the user, i.e. a load balancing strategy of individual servers is implemented.

Another method that was investigated was to ensure the resilience of the cloud infrastructure by periodically maintaining the state of computing processes based on 'checkpoints'. Studies have shown that this method allows processes to recover state in case of failure, with processes exchanging messages to monitor each other's states.

As the resilience of cloud infrastructure is based on improving the individual reliability of each individual server. As each process runs in an isolated environment, a specialised software module, located outside the investigated structure and responsible for the correctness of its operation, is used to monitor the state of the process.

The external location of the module with respect to the process under study ensures that the process is not distorted, and the accumulated heuristics allow the decision to create the next checkpoint. System recovery involves rolling back the state of the computational process to the last known correct checkpoint.

Research shows that the most interesting method for fault-tolerant cloud infrastructure operation is the message retention method. The method is based on

the assumption that any change in the state of the entire system can be described as a sequence of messages. These messages change the state of one of the system components. Such messages are recorded asynchronously (without affecting the computational process itself) in the form of a queue located in a separate memory area, which allows to restore the system state after failures by replaying the stored messages.

Thus, the issue of fault tolerance of cloud infrastructure should be considered holistically, with mandatory consideration of computer network bandwidth.

The issue of assessing the system-wide reliability of the cloud infrastructure in relation to the consumer is of considerable interest with further formalisation of the reliability baselines (host and intermediate hardware, software, etc.) and new methods for such assessment.

Refernces:

1. Tkachov V., Hunko M., Volotka V. Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In Proc. 2019 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2019, 08-11 October 2019, Kyiv, Ukraine, pp. 769-773.

2. Ткачов В.М. Аналіз методів забезпечення відмовостійкості оверлейних мереж / В.М. Ткачов, К.П. Гвоздецька // Проблеми інформатизації : тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків, 2020. – С. 44.

3. Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv.

4. Ruban I.V. Structural-functional reconfiguration of computer systems with reconstruct structure / I.V. Ruban, G.I. Churyumov, V.V. Tokariev, V.M. Tkachov // Проблеми інформатики та моделювання (ПІМ–2019): тези 19-ї міжнар. наук.-техн. конф., 11-16 вересня 2019 р. / Харків; Одеса: НТУ "ХПІ", 2019. – С. 71-72.

5. Судани Х. Х., Абросимов М. Б. Отказоустойчивость и безопасность доступа в облачных вычислениях //Южно-Сибирский научный вестник. – 2019. – №. 2. – С. 55-59.