2020
한국정보보호학회 하계학술대회

CISC-S'20

Conference on Information Security and Cryptography - Summer 2020

07.15 WED
온라인 컨퍼런스
http://www.cisc.or.kr/

주최 주관 한국정보보호학회 Korea Institute of Information Security & Cryptology

후원 국가정보원 National Intelligence Service Korea · 과학기술정보통신부 · 행정안전부 · KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY · ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute · NSR 국가보안기술연구소 National Security Research Institute · cen 아이티센 ITcen

Immortal Cloud Service 제공을 위한 요구 사항 도출

김성진*, 최상훈*, † 박기웅

*세종대학교 시스템 보안 연구실, † 세종대학교 정보보호학과

Requirements for providing Immortal Cloud service

Seong-Jin Kim, Sang-Hoon Choi, Ki-Woong Park†

*SysCore Lab., Sejong University.

† Department of Computer and Information Security, Sejong University

요 약

클라우드를 이용하는 서비스들의 규모가 커짐에 따라 클라우드 환경에서 예기치 못한 사고에 대한 대응책의 중요성도 함께 증가하고 있다. 이런 사고에 대응하기 위해 사고 발생 시 운영되고 있던 서비스의 중단 없는 완전한 복구를 가능하도록 하는 방향으로 연구가 진행되고 있다. 하지만 기존의 대응책들은 저마다 극복해야 할 한계가 존재한다. 본 논문에서는 이와 같은 클라우드 환경에서의 예기치 못한 사고에 대한 기존의 대응책의 한계를 극복하는 보다 높은 수준의 대응책으로 클라우드 서비스에 대한 Real-Time Instance Clone을 유지하는 시스템을 실현하기 위한 요구 사항을 도출하고자 한다. 본 논문을 통해 예기치 못한 사고에 대한 대응책을 실현하는 데 필요한 기술들과 관련된 기존 연구의 내용과 한계에 대해 정리하고, Real-Time Instance Clone을 위해 수행되어야 할 연구의 방향을 제시한다.

I. 서론

시장조사회사 카날리스(Canalys)의 조사 결과에 따르면 클라우드 인프라 서비스 지출이 2020년 1분기에 또 다른 기록을 세우며 전년 동기 대비 34% 증가한 310억 달러를 기록했다고 한다[1]. 이처럼 비용 절감의 이점과 비즈니스 요구 사항의 변화에 따른 뛰어난 확장성 등의 여러 장점 때문에 많은 중요한 서비스들이 클라우드를 통해 제공되고 있고 그 수는 계속해서 증가할 것이다. 클라우드를 이용하는 서비스들의 규모가 기하급수적으로 커지고 있고, 이에 따라 클라우드 서비스에 예기치 못한 사고에 대한 대응책의 중요성도 함께 증가하고 있다. 예기치 못한 사고 발생 시에 사고 발생 직전의 데이터뿐만 아니라 클라우드 인스턴스의 상태(state)까지 모두 손실하지 않은 채로 서비스의 중단 없는 운영을 제공하기 위해 클라우드 인스턴스와 관련된 메모리, 디스크, 네트워크 등 모든 상태가 같은 Real-Time Instance Clone을 유지할 필요가 있다. 예를 들어서 클라우드 인스턴스에서 대규모의 연산을 처리하고 있을 때 예기치 못한 사고로 인해 작업이 중단된다면, 해당 작업을 처음부터 다시 수행해야 하므로 매우 많은 시간 낭비를 초래할 뿐만 아니라, 정상적인 서비스를 제공하지 못하게 할 것이다. 따라서 Real-Time Instance Clone을 유지하는 것은 원본 인스턴스가 사고로 인해 가용하지 않은 상황에서 원본 인스턴스를 대신해 중단 없는 서비스를 제공할 수 있게 해준다.

본 논문에서는 클라우드 환경에서의 예기치 못한 사고에 대한 보다 높은 수준의 대응책으로 클라우드 서비스에 대한 Real-Time Instance Clone을 유지하는 시스템을 실현하기 위한

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 2020년도 과학기술정보통신부의 재원으로 IITP 정보통신방송기술 개발 사업의 지원(No. 2018-0-00420, No. 2019-0-00273) 및 한국연구재단 연구과제(NRF-2020R1A2C4002737)의 지원을 받아 수행된 연구임.

요구 사항을 도출하고자 한다.

II. 관련 연구

클라우드 환경에서 예기치 못한 사고에 대응하는 방안에 관한 많은 연구가 있었다. 해당 연구들이 제안한 메커니즘을 기준으로 연구들을 분류하고 각 메커니즘의 특성 및 한계점에 대해 알아보고자 한다.

Mechanism	Related Work	
Checkpoint	[2], [3], [4], [5], [6]	[13], [14], [15], [16], [17]
Replication	[7], [8], [9], [10], [11], [12]	
Dynamic Service Scale Up/Down	[18], [19]	
Dual Role Operation	[20]	

<표 1>. 사고 대응 메커니즘에 따른 연구 분류

예기치 못한 사고에 대응하기 위한 기존 연구의 메커니즘은 크게 Checkpoint, Replication, Dynamic service scale Up/Down, Dual role operation의 네 가지 범주로 분류될 수 있다. 추가로, checkpoint-based replication 메커니즘을 제안한 연구들도 있었다[14-18]. 다음은 <표 1>에서 분류 기준으로 제시한 메커니즘에 대한 특징을 요약한 내용이다.

A. Checkpoint

Checkpoint는 사고 발생 시 시스템을 사고 발생 이전 시점으로 복구하기 위해 사용되는 system state에 대한 정보이다. Checkpoint를 이용하는 메커니즘은 복구를 위해 높은 빈도로 checkpoint를 저장해야 하는데, 이 연산은 과도한 오버헤드를 발생시킨다는 한계가 있다.

B. Replication

Replication은 사고 발생 시 서비스의 가용성을 보장하기 위해 시스템에 대한 Geographical redundancy를 이용하는 방법이다. 이 메커니즘은 지리적으로 분리된 복제본을 통해 시스템의 물리적 장애에 대응한다. Replication을 이용한 메커니즘은 WAN replication latency로 인한 서비스 performance 저하문제[10]와 복제본을 원본 시스템과 동기화하기가 매우 어렵다는 한계가 있다[9].

C. Dynamic Service Scale Up/Down

이 메커니즘은 현재 시스템 상태에 따라 서비스를 위한 자원 할당을 유동적으로 조절[18]하거나 output resolution의 조절[19]을 통해 시스템의 가용성을 최대한 보존한다. 이 메커니즘은 시스템의 물리적 장애에 대한 대응은 불가능하다는 한계가 있다.

D. Dual Role Operation

시스템이 복제본을 유지한다는 점에서 Replication 메커니즘과 유사하지만, 이 메커니즘은 각 노드가 일부 요청에 대해서는 primary node 역할을, 다른 요청에 대해서는 backup node 역할을 모두 수행할 수 있도록 허용한다는 차이점이 있다[20]. 이 메커니즘은 사고 발생 시 backup node가 장애 발생 노드의 서비스까지 대신 처리하기 위해 리소스를 더 사용해야 하므로 완벽한 성능을 보장하는 서비스 복구는 불가능하다는 한계가 있다.

III. Immortal Cloud Service를 위한 요구사항

이번 장에서는 2장에서 분석한 관련 연구 내용을 기반으로 Immortal Cloud Service를 위한 요구사항 및 한계에 대해 알아본다.

3.1 원본 인스턴스와 Clone의 지리적 분리

예기치 못한 다양한 사고와 다양한 장애에 대비하여 서비스를 제공하고 있는 클라우드 인스턴스와 그에 대한 Real-Time Instance Clone을 지리적으로 분리된 위치에서 관리하여야 한다. 사고 발생 시 지리적으로 분리된 곳에 위치하는 Real-Time Instance Clone이 원본 클라우드 인스턴스를 대신하여 서비스를 제공하도록 함으로써 중단 없는 서비스 제공이 가능하다.

3.2 네트워크 정보 변화에 따른 대책

클라우드 환경에서 예기치 못한 사고 발생 시 원본 인스턴스를 대신해서 서비스를 제공하는 Real-Time Instance Clone은 원본 클라우드

인스턴스와 지리적으로 분리된 위치에서 관리되므로 원본 인스턴스와 다른 IP 주소를 가질 것이다. 클라이언트에게 서비스를 제공하는 도중 서비스를 제공하는 주체가 Real-Time Instance Clone으로 바뀌더라도 중단 없는 서비스를 제공하기 위해서는 서비스를 제공하는 인스턴스의 IP 주소의 변화가 클라이언트와의 통신에 영향을 미치지 않도록 하여야 한다.

3.3 데이터 복제 기술

원본 클라우드 인스턴스와 같은 상태 및 데이터를 가지는 Real-Time Instance Clone을 유지하기 위해서 다음과 같은 원본 인스턴스의 상태 및 데이터를 복제하여야 한다.

A. CPU state

CPU의 현재 Program Counter, Control Unit, Arithmetic Logic Unit, 각종 레지스터 정보들에 대한 복제가 이루어져야 한다.

B. Memory

메모리 복제는 Virtual Machine(VM) Live Migration 분야에서 활발히 연구되고 있다. VM Live Migration이란 VM의 전원이 켜져 있는 상태로 하나의 물리적 호스트에서 다른 물리적 호스트로 VM을 복사하는 작업을 일컫는다[21]. Live Migration은 크게 pre-copy, post-copy의 두 가지 접근 방식으로 분류될 수 있다. 각 접근 방식은 메모리의 내용을 복제하여 destination host로 보내는 방식에 차이를 보인다. Pre-copy[22]는 페이지의 내용이 자주 변하지 않는 read-intensive 환경에서 좋은 성능을 보인다. 반면에 페이지의 내용이 매우 자주 변하는 write-intensive 환경에서는 좋은 성능을 보이지 못한다[23]. Post-copy[24]는 read-intensive 환경에서 좋은 성능을 보이지 못한다. 왜냐하면, 이런 환경에서는 VM이 과도한 page fault로 인해 network fault가 발생하여 response time을 느리게 만들기 때문이다[23]. VM Live Migration은 수행을 완료하기 위해 반드시 Source host의 동작이 중지되는 downtime을 겪어야 한다는 한계가 있다.

C. Disk

클라우드 환경에서 디스크 데이터의 관리의 좋은 예로 Amazon 사의 Simple Storage Service(S3)가 있다. Amazon S3는 데이터의 저장이 완료되었음을 알리는 SUCCESS 메시지를 반환하기 전에 하나의 Amazon S3 Region 내 최소 3개의 가용 영역에 걸쳐 여러 디바이스에 데이터를 중복 저장한다. 이 방식은 손실된 데이터를 신속하게 탐지 및 복구하여 디바이스 장애에 대응할 수 있는 서비스를 제공한다[25]. 이러한 방식의 데이터 관리 메커니즘은 원본 클라우드 인스턴스의 Real-Time Instance Clone을 유지하기 위한 Disk 데이터 복제 방식으로 사용하기 적합하다.

IV. 결론

본 논문에서는 클라우드 환경에서의 예기치 못한 사고에 대한 기존의 솔루션을 한계점을 분석하여 향후 효율적인 대응방안을 실현하는 데 필요한 요구사항을 도출하였다. 도출된 요구사항으로는 '원본 instance와 real-time instance clone의 지리적 분리', 'Gateway', '데이터 복제 기술'이 있었다. 특히 사고 발생시 서비스를 제공하는 물리 머신이 변경되면 IP 주소가 바뀌기 때문에 이에 대한 처리가 필요하다는 한계가 있었다. 또한, 메모리에 대한 데이터 복제 기술에 있어서 반드시 머신의 동작이 중지되는 단계를 거쳐야 한다는 한계가 있었다. 추후 연구는 본 논문의 요구사항 도출에서 드러난 위와 같은 한계점들을 극복할 방안들을 도출해 내기 위한 연구를 진행할 것이다.

[참고문헌]

[1] Canalys, Global cloud services market Q1 2020, https://www.canalys.com, April 2020
[2] E.N.Elnozahy, L.Alvisi, Y.M.Wang and D. B.Johnson, A Survey of Rollback-Recovery Protocols in Message-Passing Systems, ACM Computing Surveys (CSUR), 2002
[3] M.Fu, L.Zhu, L.Bass and A.Liu, Recovery for failures in rolling upgrade on clouds, 2014 44th Annual IEEE/IFIP International Conferen

ce on Dependable Systems and Networks. IEEE, June, 2014
[4] A.B.Brown and D.A.Patterson, Rewind, repair, replay: three R's to dependability, Proceedings of the 10th workshop on ACM SIGOPS European workshop, July, 2002
[5] I.Weber, H.Wada, A.Fekete, A.Liu and L.Bass, Supporting undoability in systems operations, The 27th Large Installation System Administration Conference, 2013
[6] M.Fu, Recovery for Sporadic Operations on Cloud Applications, ASWEC Doctorial Symposium, 2014
[7] M.Pokharael, S.Lee and J.S.Park, Disaster recovery for system architecture using cloud computing, 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, July, 2010
[8] J.Behl, T.Distler, F.Heisig, R.Kapitza and M.Schunter, Providing fault-tolerant execution of web-service-based workflows within clouds, The 2nd International Workshop on Cloud Computing Platforms, April, 2012
[9] M.Ji, A.C.Veitch and J.Wilkkes, Seneca: remote mirroring done write, USENIX Annual Technical Conference, June, 2003
[10] T.Wood, H.A.Lagar-Cavilla, K.K.Ramkrishnan, P.Shenoy and J.Ven der Merwe, PipeCloud: using causality to overcome speed-of-light delays in cloud-based disaster recovery, The 2nd ACM Symposium on Cloud Computing, October, 2011
[11] A.Lenk and S.Tai, Cloud standby: disaster recovery of distributed systems in the cloud, European Conference on Service-Oriented and Cloud Computing, September, 2014
[12] Y.Tamura, K.Sato, S.Kihara and S.Moriai, Kemari: Virtual machine synchronization for fault tolerance, USENIX Annu. Tech. Conf, June, 2008
[13] S.Rajagopalan, B.Cully, R.O'Conner and A.Warfieeld, SecondSite: disaster tolerance as a service, The 8th ACM SIGPLAN/SIGOPS conference on Virtual Execution Environments, March, 2012
[14] B.Cully, G.Lefebvre, D.Meyer, M.Feeleey, N.Hutchinson, and A.Warfield, Remus: High availability via asynchronous virtual machine replication, The 5th USENIX symposium on networked systems design and implementation, April, 2008
[15] M.C.Caraman, A.S.Moraru, S.Dan and D.M.Kristaly, ROMULUS: DISASTER TOLERANT SYSTEM BASED ON KERNEL VIRTUAL MACHINES, Annals of DAAAM & Proceedings, 2009
[16] J.Zhu, Z.Jiang, Z.Xiao and X.Li, Optimizing the performance of virtual machine synchronization for fault tolerance, IEEE Transactions on Computers, 2010
[17] B.Silva, P.Maciel, E.Tavares, and A.Zimmermann, Dependability models for designing disaster tolerant cloud computing systems, 013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2013
[18] Y.Nakajima, H.Masutani, W.Shen, H.Tanaka, O.Kamatani, K.SHimano, M.Fukui and R.Kawamura, Design and implementation of virtualized ICT resource management system for carrier network services toward cloud computing era, ITU Kaleidoscope: Building Sustainable Communities, April, 2013
[19] H.Naccache, G.C.Gannod and K.A.Gray, A self-healing web server using differentiated services, International Conference on Service-Oriented Computing, December, 2006
[20] N. Aghdaie and Y.Tamir, Fast transparent failover for reliable web service, International Conference on Parallel and Distributed Computing and Systems, November, 2003
[21] A.Strunk, Costs of virtual machine live migration: A survey, 2012 IEEE Eighth World Congress on Services, June, 2012
[22] C.Clark, K.Fraser, S.HanS, J.G.Hansen, E.Jul, C.Limpach, I.Pratt and A.Warfield, Live migration of virtual machines, The 2nd conference on Symposium on Networked Systems Design & Implementation, May, 2005
[23] S.Sahni and V.Varma, A hybrid approach to live migration of virtual machines, 2012 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), October, 2012
[24] M.R.Hines, and K.Gopalan, Post-copy based live virtual machine migration using adaptive pre-paging and dynamic self -ballooning, The 2009 ACM SIGPLAN/ SIGOPS international conference on Virtual execution environments, March, 2009
[25] Amazon AWS, Amazon S3 FAQ, https://aws.amazon.com, 2020