빅데이터기반의 로그분석을 통한 통합 관리 솔루션 개발

강선경[*] · 이현창[**]· 신성윤[***]

[*]원광대학교 컴퓨터소프트웨어공학과

[**]원광대학교 디지털콘텐츠공학과

[***]군산대학교

Development of integrated management solution through log analysis based on Big Data

Sun-Kyoung Kang[*] · Hyun-Chang Lee[**] · Seong-Yoon Shin[***]

[*]Department of Computer(Software) Engineering, Wonkwang University, Iksan, 54538, South Korea

[**]Department of Digital Contents Engineering, Wonkwang University, Iksan, 54538, South Korea

[***]Scool of Computer Information & Communication Engoneering, Kunsan National University, Kunsan 54150, South Korea

E-mail :{doctor10, hclglory}@wku.ac.kr, s3397220@kunsan.ac.kr

요 약

본 논문에서는 복잡하고 다양한 클라우드 환경을 통합하여 간편하게 운영할 수 있는 통합관리 솔류션을 개발하고자 한다. 이는 빅데이터 기반의 정형로그데이터와 비정형로그데이터를 수집하고 분석하여 실시간으로 통합 모니터링이 가능하여 사용자와 관리자가 편리하게 문제를 해결할 수 있다는 장점을 가지고 있다. Hypervisor 로그패턴 분석 기술을 통해 기존의 복잡하고 다양한 클라우드 환경을 좀 더 효율적으로 운용 관리할 수 있는 솔루션이라 하겠다.

ABSTRACT

In this paper, we intend to develop an integrated management solution that can be easily operated by integrating complex and various cloud environments. This has the advantage that users and administrators can conveniently solve problems by collecting and analyzing fixed log data and unstructured log data based on big data and realizing integrated monitoring in real time. Hypervisor log pattern analysis technology will be able to manage existing complex and various cloud environment more efficiently.

키워드

빅데이터, 클라우드, 정형로그, 비정형로그, 모니터링

Ⅰ. 서 론

클라우드 서비스는 자원의 공동이용, 인터넷을 이용한 정보서비스, 다양한 미디어 환경, 정보시스템의 아웃소싱 등의 특징들로 구성되어져 있기 때문에 외부로부터의 위험요소와 침입등으로 인한 피해에 대한 보안문제가 서비스를 활성화 시키는데 가장 큰 문제점으로 야기되고 있다. 또한 클라우드 서비스 구축시 가상화 영역의 보안 요구사항은 제공하는 서비스의 범위, 제공방법, 구현방법에 따라 다양하게 변경될 수 있다는 문제점으로 인해 보안위협이 가해짐으로 인해 클라우

드 서비스의 활성화시키기 위한 대책마련이 시급한 것이 현실이다[1][2]. 본 논문에서는 이런 문제를 해결하기 위한 근본적인 방법을 찾기 위해 빅데이터기반의 로그분석을 통한 통합관리 솔루션을 개발하고자 한다.

II. 통합관리 시스템

기존의 가상화 관리 솔루션은 가상 데스크탑 환경 구축과 가상 인프라 자원 모니터링이라는 두 가지 기능을 중심으로 이루어져 있어 통합관리가 어려웠으며, 이러한 기본적인 기능 이외에 복잡하고 다양한 클라우드 환경을 보다 효율적으로 운용하고 분석하는 기능을 시스템 관리자들에게는 필요한 중요한 기술개발 요소로 작용하게 되었다. 이런 기술개발 요소는 관리자에게 외부로부터의 침입을 보다 빠르게 인지할 수 있도록해주는 도우미 역할을 담당하는 중요한 요소라 할 수 있다. 그림 1은 본 논문에서 제안하는 통합관리 시스템의 아키텍처를 보여주고 있다. 그림1에서 보이는 것과 같이 Self Service 기반 가상PC 신청 및 관리, 자동 배포 관리, 자원관리, 레포팅 관리, IP자원 관리, 마스터 VM 및 시스템 설정 관리, 데스크탑 그룹관리로 이루어져 있다.

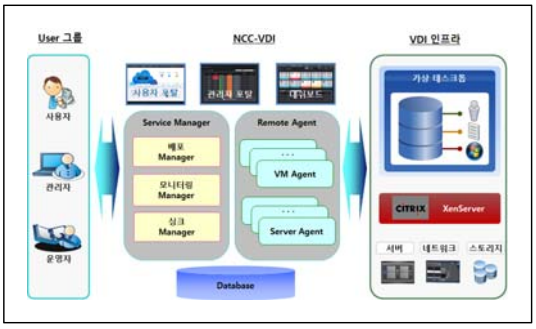

그림 1. 통합관리 시스템 아키텍처

III. 로그분석

현재 사용되어지고 있는 상용 가상화 엔진에서 생성되는 로그를 실시간으로 분석하여 장애 감지 및 중요 시스템 오류를 인지하고 이에 대한 적절한 통합관리 시스템에 취합하여 관리자가 이를 쉽고 빠르게 시스템을 지원할 수 있다. 본 솔루션에서 사용되는 로그분석기법은 클라우드 인프라를 구성하는 이러한 기법은 Hypervisor 및 Virtual Machine에서 생성되는 로그를 실시간으로 분석할 뿐만아니라, 비정형 텍스트 기반의 패턴 분석에도 주로 사용된다. 이러한 기법을 이용하여 검출된 패턴은 소켓통신을 통해 웹포탈에 전달되고 수집된 패턴은 웹소켓을 통해 관리자 브라우저에 실시간으로 전송되는 형태로 이루어져 있다. 아래 그림2는 로그 파일 패턴 검출 시스템의 구성을 보여주고 있다.

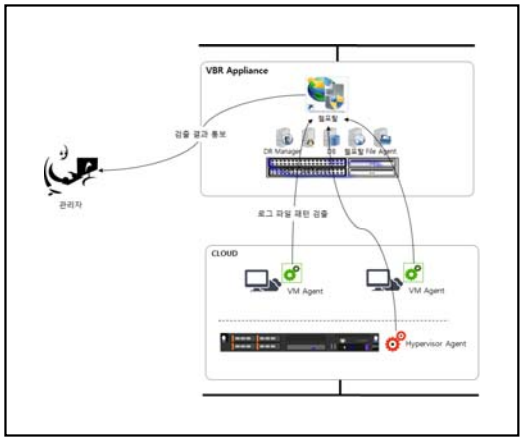

그림 2. 로그 패턴 시스템 구성

IV. 결 론

급속도로 성장하고 있는 클라우드 서비스인프라에 대해서 기술적인 측면의 클라우드 구축에 기술력이 집중되어 있어 관리자의 효율적인 통합운영관리에 필요한 운영 안정성이 확보된 솔루션 개발이 필요하다. 이를 위해 본 논문에서 빅데이터 기반의 Hypervisor 로그패턴 분석 기술을 통해 기존의 복잡하고 다양한 클라우드 환경을 좀 더 효율적으로 운용 관리할 수 있도록 하였다.

ACKNOWLEDGMENTS

This paper was supported by Ministry of SMEs and Startups. [Innovative Technology Development Project]

참고문헌

[1] 최도현, 유한나, 박태성, 도경화, 전문석, “클라우드 서비스 가상화 내부 환경을 위한 BareMetal Hypervisor 기반 보안 구조 설계”, 한국통신학회논문지, v.38B no.7, pp.526-534, 2013.

[2] KISA(Korea Internet Security Agency) Research and Developer Team, “Cloud Service Information Security Guideline,” KISA Guideline and Explanation, Oct. 2011.