KIICE 한국정보통신학회지 15권 2호
THE MAGAZINE OF KIICE
http://www.kiice.org

오픈스택 보안관리 방안

마상혁* · 이경환** · 이민규*** · 김종배***

*숭실대학교 대학원
**솔트웨어(주)
***숭실대학교 SW특성화대학원

목 차

Ⅰ. 서 론

IaaS형태의 클라우드 컴퓨팅 오픈소스 프로젝트로 탄생한 오픈스택은 현재 150여개 기업이 프로젝트에 참여하고 있으며, 2012년 창설된 비영리 단체인 OpenStack Foundation에서 유지, 보수를 하고 있고, 아파치 라이선스하에 배포되고 있다[1].

한편, 모든 사용자들의 데이터를 하나의 IDC(Internet Data Center)에 저장하는 클라우드 시스템의 주요 이슈 중 하나는 보안이다. 수천 혹은 수만이 사용하는 IDC가 보안에 취약하거나 침해사고가 발생한다면 고객의 신뢰를 잃음과 동시에 클라우드 서비스를 제공하는 기업의 매출 손실이 천문학 적일 것임이 자명하다. 클라우드 컴퓨팅 환경에서는 사용자의 데이터가 로컬이 아닌 클라우드 서버에 저장되기 때문에 해킹을 당하거나 악의적인 공격자에 의해 유출될 경우 많은 피해가 우려된다. 대표적인 사례로써 2014년 9월 애플의 아이클라우드가 해킹당하는 사태가 발생하여 개인정보 및 데이터가 유출되어 곤혹을 치렀다. 이에 따라 많은 전문가들은 클라우드서비스 활성화의 저해요인으로 보안문제를 지적하고 있다.

전세계적으로 많은 사용자가 채택하고 있는 오픈스택의 경우에도 마찬가지이다. 따라서 본 논문에서는 클라우드 컴퓨팅 오픈소스 프로젝트로 탄생한 오픈스택의 지속적인 보안 관리를 위한 방안으로 취약성 관리, 형상 관리, 안전한 백업 및 복구, 보안 감사를 제시한다.

Ⅱ. 오픈스택의 개념

2.1. 오픈스택의 정의

클라우드 컴퓨팅 환경 구축을 위한 오픈스택은 오픈소스로 만들어 졌다. NASA에서 Nebula 플랫폼을 오픈소스화 하고 Rackspace사에서 자사의 클라우드 스토리지 소프트웨어를 오픈소스화 하여 오픈스택의 개발이 시작되었다. 현재는 OpenStack Foundation으로 독립하였고 현재는 IBM, Intel, Cisco, Dell, HP, VMware, Redhat 등 150여개 기업이 프로젝트에 참여하고 있다. 최근 2014년 미국 샌프란시스코에서 열린 VMware의 대규모 행사인 VM월드 2014에서 VMware는 오픈소스 기반 클라우드 플랫폼인 오픈 스택을 적극 지원하겠다고 발표했다. 상용 소프트웨어 대표주자이면서 동시에 클라우드 플랫폼을 제공하는 VMware가 시장의 대세로 확실히 자리를 잡은 오픈스택 지원을 공식 선언하였다. 위와 같이 프로젝트에 참여하고 있는 기업들은 자사의 기술력을 동원해서 직접 개발에 참여하고 있다. 현재는 100여개 국가, 850여개 조직에서 8000여명의 멤버가 활발하게 활동 중이다[2].

오픈스택의 첫 번째 릴리즈는 프로젝트 시작 4개월 만인 2010년 10월 21에 공식 릴리즈 되었고 제품명은 Austin이었다. 이후 2011년 2월에 Bexar, 4월과 9월에는 Cactus 와 Diablo, 2012년 4월에 Essex, 9월에 Folsom을 선보였다. 또한 2013년 4월에 Greezly, 같은 해 10월에는 Havana를 선보이면서 프로젝트 안정화 단계에 접어들었다. 현재 오픈스택은 Juno 릴리즈를 준비하고 있다[3].

처음 릴리즈 된 Austin에서는 단순히 이미지 관리 서비스, 컴퓨트 서비스와 오브젝트 파일 스토리지 서비스만 선보였다. 이때는 각 하위 프로젝트에 이름이 없었다. Bexar에 이르러서야 컴퓨트 서비스는 노바(Nova), 오브젝트 파일 스토리지 서비스는 스위프트(Swift), 이미지 관리 서비스는 글랜스(Glance)라는 이름을 갖게 됐다. Essex 버전에서 오픈스택은 새로운 기능을 추가했는데, 노바와 글랜스, 스위피트 인증을 담당하는 프로젝트인 키스톤(Keystone)과 대시보드 기능을 제공하는 호라이존(Horizon)이 포함되었다.

이후 오픈스택은 클라우드 관리 기능을 추가하기 시작했다. Folsom을 선보일 땐 소프트웨어 정의 네트워크 관련한 퀀텀(Quantum) 프로젝트와 볼륨 스토리지를 관리할 수 있는 신더(Cinder) 프로젝트를 포함시켰다. Havana에 들어서서는 오케스트레이션 서비스인 '히트(Heat)'와 모니터링겸 미러링 서비스인 셀로미터(Ceilometer)을 추가했다. 최근 발표한 Icehouse에서는 데이터베이스 관리 기능인 트로브(Trove)를 새롭게 추가했다[4].

2.2. 오픈스택의 컴포넌트 및 보안 고려사항

2.2.1. 컴퓨트(Compute)

오픈스택 컴퓨트 서비스(프로젝트명 Nova)는 규모별로 VM 인스턴스 관리, 다-계층 어플리케이션을 관리하는 호스트, 개발과 테스트 환경, 빅데이터 고속처리 하둡(Hadoop) 클러스트 및 고성능 컴퓨팅을 지원하는 서비스를 제공한다. 또한 컴퓨트 서비스는 하이퍼바이저와 인터페이스하는 추상계층을 통하여 관리를 용이하게 해준다.

오픈스택 컴퓨트 서비스에 보안은 필수적이며 강화되어야 할 보안 기술은 강력한 인스턴스 분리, 컴퓨트의 하위컴포넌트 간에 안전한 통신과 공공-대응 API엔드포인트 회복성을 지원해야 한다.

2.2.2. 오브젝트 스토리지(Object Storage)

오픈스택 오브젝트 스토리지(프로젝트명 Swift)는 클라우드에서 데이터의 저장과 검색을 제공한다. 오브젝트 스토리지 서비스는 정적 데이터에 최적으로 사용된다. 또한 고유 API와 Amazon Web Services S3 호환 API 모두를 제공한다. 서비스는 데이터 복제를 통하여 높은 수준의 회복성을 제공하며 페타바이트 데이터를 처리할 수 있다[5].

오브젝트 스토리지의 보안은 접근 통제, 데이터를 전송할때 휴면 데이터의 암호화에 초점을 두어야 한다. 기타 고려사항으로는 시스템 오용, 불법이나 악의적인 컨텐트 스토리지 및 교차 인증 공격 벡터 등이다.

2.2.3. 블록 스토리지(Block Storage)

오픈스택 블록 스토리지 서비스(프로젝트명 Cinder)는 컴퓨트 인스턴스에 지속적인 블록 스토리지를 제공한다. 블록 스토리지 서비스는 블록-디바이스의 생성부터 인스턴스에 볼륨을 부착하고 해제하는 과정까지 라이프사이클 관리를 책임진다. 블록 스토리지의 보안 고려사항은 오브젝트 스토리지와 유사하다.

2.2.4. 오픈스택 네트워킹(OpenStack Networking)

오픈스택 네트워킹 서비스(Neutron)는 IP 주소 관리, DNS(Domain Name System), DHCP(Dynamic Host Configuration Protocol), 부하 조절 및 보안 그룹(네트워크 접근 룰, 방화벽 정책) 같은 다양한 네트워킹 서비스를 클라우드 사용자에게 제공한다. 다양한 네트워킹 솔루션과 플러그인 통합을 제공하는 SDN 프레임워크를 제공한다.

오픈스택 네트워킹을 통하여 클라우드 테넌트는 게스트 네트워크 구성을 관리할 수 있다. 네트워킹 서비스와 관련된 보안은 네트워크 트래픽 분리, 가용성, 무결성 및 신뢰성이다.

2.2.5. 대시보드(Dashboard)

오픈스택 대시보드 서비스(Horizon)는 클라우드 관리자와 클라우드 테넌트 양쪽을 위한 웹-기반 인터페이스를 제공한다. 이 인터페이스를 통하여 관리자와 테넌트는 클라우드 자원을 공급, 관리 및 모니터 할 수 있다. Horizon은 일반적으로 공공 웹 포탈의 모든 통상적인 보안 고려사항을 가지고 공공-대면 방식으로

적용된다.

2.2.6. 아이덴티티 서비스(Identity Service)

오픈스택 아이덴티티 서비스(Keystone)는 전체 클라우드 인프라 전반에 걸쳐 인증과 인가 서비스를 제공하는 공유 서비스이다. 아이덴티티 서비스는 여러 인증 형식을 지원한다.

보안 고려사항은 인증 신뢰, 인가 토큰 관리 및 안전한 통신 등이다.

2.2.7. 이미지 서비스(Image Service)

오픈스택 이미지 서비스(Glance)는 디스크 이미지 관리 서비스를 제공한다. 이미지 서비스는 필요 시 컴퓨트 서비스에 이미지 복구, 등록 및 공급 서비스를 제공한다.

데이터 보안에 대하여 이전에 언급된 모든 이슈처럼, 디스크 이미지 라이프사이클 관리에 대한 신뢰된 프로세스가 필요하다.

2.2.8. 기타 지원 기술

오픈스택은 여러 가지 서비스 간 내부 통신시 메시징에 의존하는데 기본적으로 AMQP을 기반으로 한 메시지 큐를 사용한다. 대부분 오픈스택 서비스와 유사하게 플러그인 컴포넌트를 지원한다. 현재 구현된 백엔드는 RabbitMQ, Qpid나 ZeroMQ가 될 수 있다. 대부분의 관리 명령이 메시지 큐잉 시스템을 통하여 흐르기 때문에, 모든 오픈스택 적용에서 우선적인 보안 고려사항이다.

Ⅲ. 오픈스택 보안 경계 및 위협

3.1. 보안 도메인

클라우드는 보안 도메인이라 부르는 기능, 사용자 및 공유된 보안 관심사에 의해 논리적 컴포넌트 모음집으로 추상화될 수 있다. 위협 액터와 위협 벡터는 자원접근과 동기를 기반으로 분류된다. 보안 도메인은 시스템 내에서 공통적인 신뢰 요구사항과 기대치를 공유하는 사용자, 어플리케이션, 서버나 네트워크로 구성된다. 일반적으로 동일한 인증 혹은 인가 요구사항과 사용자를 가진다.

보안 도메인은 오픈스택 클라우드를 적용하는데 필요한, 최소 요구사항으로 구성되는 공공(public), 게스트(guest), 관리(management), 데이터(data) 등 4 가지 개별 도메인으로 구분된다. 이러한 보안 도메인은 해당 오픈스택이 독립적으로 매핑될 수 있다. 예를 들어, 어떤 토폴로지는 게스트와 데이터 도메인을 묶어서 하나의 물리적 네트워크에 둘 수도 있고, 분리된 네트워크에 둘 수 도 있다. 두 가지 경우 모두 클라우드 운영자는 적절한 보안 관련사항을 인지해야 한다. 그리고 보안 도메인은 특정 오픈스택 적용 토폴로지에 대하여 매핑되어야 한다. 도메인과 신뢰 요구사항은 클라우드가 공공인지, 사설인지, 하이브리드인지에 따라 다르다.

3.2. 보안 도메인 종류

3.2.1. 공공도메인(Public Domain)

공공 도메인은 전체적으로 신뢰할 수 없는 클라우드 인프라 영역이다. 즉, 인가 받지 않는 인터넷으로 간주할 수 있다. 따라서 공공도메인은 항상 비신뢰로 취급되어야 하며 신뢰성이나 무결성 요구사항으로 이 도메인에 전송되는 데이터는 보정된 통제를 사용하여 보호되어야 한다.

3.2.2. 게스트도메인(Guest Domain)

게스트도메인도 공공 도메인과 마찬가지로 비신뢰로 간주된다. API 호출 같은 클라우드 운용을 지원하는 서비스는 아니고 일반적으로 컴퓨트 인스턴스-대-인스턴스 트래픽에 사용된다. 또한, 게스트 도메인은 클라우드 상의 인스턴스가 생성한 컴퓨트 데이터를 처리한다.

클라우드 공급자가 이 네트워크를 public 이 아닌 private 네트워크로 간주하고, 인스턴스와 모든 테넌트를 신뢰하도록 적절한 통제를 가질 때에만 신뢰할 수 있다.

3.2.3. 관리도메인(Management Domain)

관리 도메인은 통제 영역이라 불리며 서비스가 상호작용하는 곳이다. 이 도메인의 네트워크는 구성 파라미터와 사용자 이름 및 패스워드 같은 기밀성 데이터를 전송한다. 명령과 통제 트래픽이 이 도메인에 존재하며, 무결성 요구사항을 필요로 한다. 이 도메인 접근은 강력하게 제한되고 모니터 되어야 한다. 동시에 이 도메인은 지침에서 서술된 모든 보안 최상 사례를

적용해야 한다.

대부분 이 도메인 적용은 신뢰로 간주되지만, 오픈스택 적용의 경우, 이 도메인을 신뢰 수준이 낮은 다른 도메인과 브릿지하는 시스템이 많이 존재할 수도 있다.

3.2.4. 데이터도메인(Data Domain)

데이터 도메인의 신뢰 수준은 적용 의사결정에 따라 크게 다르며, 디폴트 신뢰 수준을 배정하면 안 된다.

데이터 보안 도메인은 오픈스택 내에서 스토리지 서비스와 관계된 정보와 관련된다. 이 네트워크에 걸친 대부분의 데이터는 높은 무결성과 신뢰성 요구사항을 가지며, 적용 유형에 따라 강력한 가용성 요구사항을 가질 수도 있다.

3.3. 보안 도메인 브릿지

브릿지는 하나 이상의 보안 도메인 내에 존재하는 컴포넌트이다. 이러한 브릿지가 네트워크 아키텍처의 취약점이 될 수 있기 때문에 다른 신뢰 수준이나 인증 요구사항을 가진 보안 도메인과 브릿지 하는 컴포넌트는 주의 깊게 구성되어야 한다. 브릿지는 브릿지 하는 도메인 중 최고 신뢰 수준의 보안 요구사항에 맞추어 구성되어야 한다. 브릿지의 보안 통제는 공격 가능성이 높기 때문에 최우선적으로 고려되어야 한다.

그림1은 데이터와 관리 도메인을 브릿지 하는 컴퓨트 노드를 보여 준다. 컴퓨트 노드는 관리 도메인 보안 요구사항에 맞추어 구성되어야 한다. 이 그림에서 API 엔드포인트는 비신뢰성인 공공 도메인과 관리 도메인을 브릿지 하며 공공 도메인을 통한 관리 도메인 공격을 보호하도록 구성되어야 한다.

3.4. 위협 분류

3.4.1. 위협 액터

위협 액터는 방어해야 하는 공격자를 분류하는 추상적 방식이다. 능력이 높은 공격자를 상대하려면 공격 완화와 예방에 더 많은 비용이 들어가는 보안 통제가 필요하다. 어떤 경우에는 3.4.2에서 언급되는 위협 액터에 대하여 클라우드 시스템 환경을 안전하게 유지하는 것이 불가능할 수도 있다.

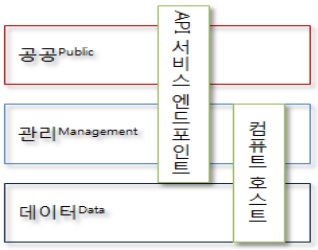

그림 1. 데이터와 관리도메인을 브릿지 하는 컴퓨트 노드

3.4.2. 위협 액터 종류

(1) 정보기관

가장 능력 있는 적대자로 간주되며 정보기관과 기타 상태 액터는 다양한 자원을 공격 목표로 정할 수도 있다. 다른 액터보다 더 높은 능력을 가지고 있으며 사람과 기술에 엄격한 통제 없이는 이런 액터를 방어하기 아주 어렵다.

(2) 심각한 조직 범죄

강력한 기술과 재정적 능력을 가진 공격 그룹으로 자체 악용 도구 개발과 공격 목표 연구가 가능하다. 최근의 대규모 사이버 범죄 기업인 Russian Business Network 같은 조직이 그 예이다.

(3) 고도 능력 그룹

서비스 공급자와 클라우드 오퍼레이터에게 심각한 위협이 될 수 있는 핵티비스트(Hacktivist) 유형의 조직으로 일반적으로 재정적 지원을 받지는 않는다.

(4) 동기를 가진 개인

불만을 가지거나 악의적인 직원, 불만을 품은 고객 및 소규모 산업 스파이 등의 유형으로, 이들은 단독으로 활동한다.

(5) 아마추어 해커

아마추어 해커는 대부분 성가신 정도이지만, 어떤 액터는 회사 명성에 심각한 위험을 유발하게 훼손할 수도 있다. 아마추어 해커는 자동화된 취약성 검색 혹은 악성 툴로 무작위 공격을 한다.

3.5. 공격 유형

그림2는 위협 액터로부터 예상되는 공격 유형을 보여준다. 어떤 위협 유형이 있으며, 어떤 위협 액터가 존재하며, 보호되어야 하는지를 의사 결정할 때 도움을 준다. 상용 공공 클라우드인 경우, 심각한 범죄 대응 예방도 포함될 수 있다. 정부에서 사설 클라우드를 적용할 경우, 시설망과 공급망에 대한 주의 깊은 보호를 포함하여 엄격한 보호 메커니즘이 준비되어야 한다.

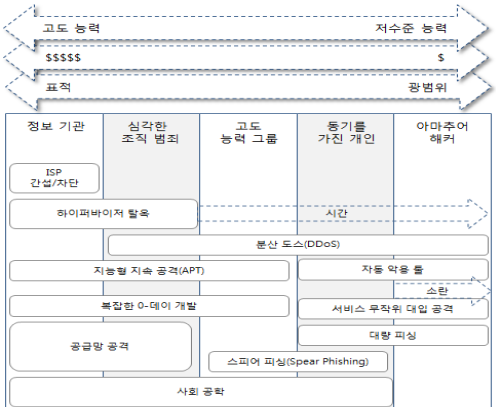

그림 2. 위협 액터로부터 예상되는 공격유형

3.6. 공공 클라우드와 사설 클라우드에서의 고려사항

사설 클라우드의 사용자는 일반적으로 클라우드를 소유한 조직의 직원이 클라우드를 사용하는 권한을 가진다. 대부분 사설 클라우드는 기업이나 단체 네트워크 내부나 방화벽 안에 구축되고 기업은 어떤 데이터가 네트워크에 나갈 수 있는지 엄격한 정책을 가지고 있어야 하며, 특별한 목적이 있는 경우 별개의 클라우드를 가질 수 있다. 직원은 클라우드에 접근하기 전에 교육을 받으며 정기적인 보안 교육에 참여해야 한다.

공공 클라우드의 공격 표면(Attack Surface)에서 큰 차이점은 서비스에서 인터넷 접근을 제공 해야만 한다는 것이다. 인스턴스 연결성과 인터넷을 통하여 파일을 접근하고 API 엔드포인트나 대시보드 같이 클라우드 통제 구조로 상호작용하는 능력은 공공 클라우드의 필수 조건이다.

공공 클라우드와 사설 클라우드에서 프라이버시 문제는 정반대이다. 사설 클라우드에서 생성되고 저장되는 데이터는 보통 클라우드 오퍼레이터가 소유한다. 클라우드 오퍼레이터는 DLP 예방, 파일 검사, 심도 깊은 패킷 검사 및 규범적인 방화벽 기술을 적용할 수 있다.

Ⅳ. 오픈스택 보안 관리 방안

4.1. 오픈스택 보안 관리 개요

클라우드 시스템을 적용한다는 것은 살아 숨쉬는 시스템을 만드는 것과 같다. 사람이 나이가 들면 몸의 기능이 저하 되듯이 기계가 오래되면 고장나고, 소프트웨어도 취약성이 드러난다. 소프트웨어에 에러나 누락이 발견되어 수정하고 업데이트 할 때, 이러한 변경은 안전한 방식으로 수행되어야 한다. 관리자는 다양하게 운용 가능한 기능들에 대하여 명령과 통제를 수행하고 숙지하여야 한다.

4.2. 취약성 관리

4.2.1. 취약성 관리 개요

오래된 소프트웨어는 시간이 흐른 만큼 취약성이 드러나므로 시스템에서 오픈스택의 컴포넌트를 최신 버전으로 유지하는 것이 중요하다. 클라우드 관리자는 보안관련 업데이트를 숙지할 수 있도록 메일링 리스트에 등록하는 것이 필수적이다.

4.2.2. 피해 분류

보안 업데이트를 확인한 다음 단계는 이 업데이트가 해당 클라우드 적용에 영향을 줄 것 인가 판단해야 한다. 특권 상승, 서비스 거부 및 정보 공개 등의 취약성 유형과 인프라에서 침해사고나 취약성이 발생한 위치를 이해하면, 합당한 대응 의사결정을 내릴 수 있다.

특권 상승이란 어떤 불법적 사용자가 시스템의 다른 사용자의 특권으로 활동하는 사용자 능력을 말한다. 예를 들어, 코드를 실행하거나 운용을 수행하는 표준 리눅스 사용자는 시스템 상에서 루트 권한으로 작업을 수행할 수도 있다.

서비스 거부는 서비스나 시스템 중지를 유발할 수 있는 악용된 취약성을 말한다. 네트워크 자원 전체에 걸친 분산 공격이나 단독 공격을 포함하며, 자원 할당 버그나 입력 유도 시스템 중지 결함을 통하여 유발된다.

취약성의 정보공개는 시스템이나 운용에 관한 정보를 노출한다. 정보공개된 취약성은 디버깅 정보부터 필수 보안 데이터 까지 다양하다. 이러한 여러 가지 변수를 고려하여 빠른 시간내에 클라우드를 업데이트 해야 한다.

4.2.3. 업데이트 테스트 및 적용

실행 중인 클라우드 환경에 업데이트를 적용하기 전에 업데이트를 테스트 해야 하는데 일반적으로 업데이트를 테스트 하기 위한 별개의 테스트 클라우드 환경이 필요하다. 이 클라우드의 소프트웨어와 하드웨어는 현재 실행중인 클라우드 환경과 유사해야 한다. 업데이트 테스트는 성능에 미치는 영향, 안정성, 어플리케이션에 미치는 영향 등을 고려하여 수행되어야 한다. 특히, 중요한 것은 특정 취약성 업데이트에 관해 이론적으로 해결한 문제가 실제로 고쳐졌는지 검증해야 한다.

업데이트가 완벽하게 테스트된 후에, 실행 환경에 적용될 수 있다. 이 적용은 형상 관리 툴을 사용하여 완전하게 자동화 되어야 한다.

4.3. 형상 관리

4.3.1. 형상 관리 개요

우수 실행 클라우드는 구성과 적용을 자동화 하는 툴을 항상 사용해야 한다. 사람이 직접 작업함으로써 발생할 수 있는 오류를 줄일 수 있으며, 클라우드를 보다 빠르게 확장이 가능하다.

오픈스택 클라우드 환경을 구축할 때, 형상 관리 툴이나 프레임워크를 염두에 두고 설계, 구현해야 한다. 형상 관리 툴을 통하여 오픈스택 같이 복잡한 인프라 구축, 관리 및 유지와 관련된 많은 어려움을 피할 수 있다. 형상 관리 유틸리티에 필요한 선언문, 사용서나 템플릿을 만들면, 여러 문서 및 규범 보고 요구사항을 만족시킬 수 있다. 게다가, 형상 관리는 BCP와 DR 계획의 일부분으로 동작될 수도 있다. DR 이벤트나 훼손 상태에서 안전하게 알려진 상태로 서비스나 노드를 복구할 수 있다. Git과 SVN 같은 버전 통제 시스템과 결합하면, 환경에서 계속해서 변경된 사항을 추적할 수 있고 인가 받지 않은 변경을 재교정 할 수 있다. 또한 형상 관리 툴은 업데이트를 적용하는데 사용될 수도 있는데, 이를 통해 보안 패치 프로세스를 단순화 한다. 클라우드를 안전하게 유지할 수 있는 주된 방법은 형상 관리 툴의 선택과 사용이다. 형상 관리 솔루션이 많지만, 오픈스택 환경에서 사용에 적합한 2 가지 툴은 Chef와 Puppet 등이 있다.

4.3.2. 정책 변경

정책이나 형상 관리가 변경될 경우, 이러한 변경을 로깅하고 신규 세트의 복사본을 백업하는 것이 좋다. 이런 정책과 형상은 git과 같은 버전 통제 리포지터리에 저장된다.

4.4. 안전한 백업과 복구

전체 시스템 보안 계획에 백업 절차와 정책을 포함시켜야 한다. 안전한 백업과 복구를 위해 네 가지 고려사항이 있는데, 첫 번째로는 정기적인 데이터 복구 옵션 테스트이다. 안전한 백업으로부터 재저장될 수 있는 형식 중 하나가 이미지이다. 훼손된 경우에는 즉시 실행 인스턴스를 종료하고 안전한 백업 리포지터리의 이미지로 인스턴스를 다시 개시하는 것이다. 두 번째는 백업 전송과 스토리지에 데이터 암호화 옵션을 사용하는 것 이다. 세 번째는 보안이 강화된 전용 백업 서버를 사용하고 백업서버의 로그를 매일 모니터링 고고 소수만이 접근 가능하게 하는 것이다. 네 번째는 인증 받은 사용자와 백업을 담당하는 직원만이 백업서버에 접근할 수 있도록 하는 것이다.

4.5. 보안 감사

보안 감사 툴은 형상 관리 툴을 보완할 수 있다. 보안 감사 툴은 대규모 보안 통제가 해당 시스템 구성을 만족하는가를 검증하는 프로세스를 자동화 한다. 예를 들어, SCAP는 미리 지정된 프로파일과 실행 시스템을 비교할 수 있다. SCAP는 프로파일에서 어떤 통제가 만족되는지, 무엇이 실패인지, 무엇이 점검되지 않았는지에 관한 상세 보고서를 출력한다.

감사 툴은 적용에 관련된 사항들에 초점을 둔다. 형상 관리 툴은 감사 관련사항을 해결하기 위해 각 시스템에 변경된 프로세스를 단순화 한다. 이런 방식으로 함께 사용하면 기본적으로 보안강화부터 컴플라이언스 검증까지 이르는 보안 요구사항을 만족하는 클라우드를 유지하는데 도움이 된다.

Ⅴ. 결론

세계적으로 많은 사용자가 오픈스택을 채택하고 프로젝트에 참가한 150여개 기업 8,000여명의 기술자들에 의해 제품이 성숙됨에 따라, 보안이 가장 중요한 문제로 부상하고 있다. 이에 따라 본 논문에서는 오픈스택 보안 관리 고려 사항을 제시하였다.

오픈스택이란 의미는 단순히 오픈소스 클라우드 플랫폼에 지나지 않으며, 전 세계 굴지의 IT기업들과 수천의 기술자들이 힘을 합쳐 만들어 나가는 건축물과 같다. 이제, 이러한 건축물이 무너지지 않도록 보안 전문가들이 힘을 합쳐 오픈스택의 보안을 한층 업그레이드시킬 필요가 있다.

참고문헌

[1] WiKiPedia, http://ko.wikipedia.org/wiki/%EC%98%A4%ED%94%88%EC%8A%A4%ED%83%9D
[2] 황진경, 안재석(2011), 오픈스택 클라우드 기술동향, 개방형컴퓨터통신연구회, pp.86-100.
[3] WikiPedia, 오픈스택http://ko.wikipedia.org/wiki/%EC%98%A4%ED%94%88%EC%8A%A4%ED%83%9D
[4] http://blog.naver.com/intelbiz/220107394156
[5] Nalee의 IT이야기, http://naleejang.tistory.com/90

마상혁(Sang-Hyeok Ma)

1990년: 강원대학교 산업공학과 졸업(학사)
1993년: 동대학원 공학석사
2008년~현재: 솔트웨어(주) 사업지원본부장
※관심분야: 소프트웨어 공학 유지보수 프로세스, 서비스기반 소프트웨어 등

이경환(Kyung-Hwan Lee)

1988년: 연세대학교 공과대학 건축공학(학사)
2004년: 연세대학교 공학대학원 컴퓨터공학(석사)
2008년~현재: 솔트웨어(주) 사업지원본부장
※관심분야: 보안, 클라우드 컴퓨팅

이민규(MinGyu LEE)

2014년: 동국대 정보통신공학부(학부)
2014년~현재: 숭실대 SW특성화대학원(석사)
※관심분야: 보안, 클라우드 컴퓨팅

김종배(Jong-Bae Kim)

2002년 8월 숭실대학교 정보과학대학원 석사
2006년 8월 숭실대학교 대학원 컴퓨터학과 박사
2001년~2012년 (주)이엔터프라이즈 대표이사
2012년~현재 숭실대학교 SW특성화대학원 교수
※관심분야 : 소프트웨어공학, 정보보호, 오픈소스소프트웨어