다중 클러스터 환경에서의 서비스 간 상호인증 및 통신 암호화 체계 구축

류경표 [1], 남재현 [2]
[1] 단국대학교 컴퓨터공학과 학부생
[2] 단국대학교 컴퓨터공학과 교수

32191441@dankook.ac.kr, namjh@dankook.ac.kr

Development of Inter-Service Mutual Authentication and Communication Encryption in Multi-Cluster Environments

Kyungpyo Ryu[1], Jaehyun Nam[2],
[1]Dept. of Computer Engineering, Dankook University (Undergraduate Student)
[2]Dept. of Computer Engineering, Dankook University (Professor)

요 약

컨테이너 기반 애플리케이션 개발의 증가와 마이크로서비스 아키텍처의 보급으로 컨테이너 클러스터 내 워크로드 간 안전한 통신이 중요해지고 있다. 또한, 최근에는 단일 클러스터 환경이 아닌 멀티 클라우드 등의 도입과 함께 다중 클러스터 환경이 점차 증가하면서 서로 다른 클러스터의 서비스 간 통신에 대한 보안 역시 강조되고 있다. 따라서, 본 논문에서는 이러한 요구사항을 충족시키기 위해 다중 클러스터 환경에서의 서비스 간 상호 인증 및 통신 암호화를 구현하고자 한다. 특히, 서비스 간 상호 인증이 가능한 mTLS (Mutual TLS)를 SPIFFE/ SPIRE 를 이용하여 구현하고, 이를 다시 확장하여 단일 클러스터 뿐만 아니라 다중 클러스터에서도 동일한 상호 인증 체계 및 통신 암호화를 사용할 수 있도록 하므로 컨테이너 환경 전반에 걸친 보안성과 신뢰성을 향상시키고자 한다.

1. 서론

최근 컨테이너 기반의 애플리케이션 개발이 급속도로 증가하고 있으며, 이와 동시에 마이크로서비스 아키텍처가 기존의 소프트웨어 개발 방식을 재정의하고 있다. 마이크로서비스 아키텍처는 작고, 모듈화 된 서비스로 시스템을 구성함으로써 높은 수준의 확장성과 유연성을 제공한다. 하지만, 이러한 마이크로서비스 사이의 워크로드 통신은 시스템의 안정성과 효율성에 직접적인 영향을 미친다[1]. 따라서, 컨테이너 클러스터 내에서의 워크로드 간 안전한 통신은 필수적이다.

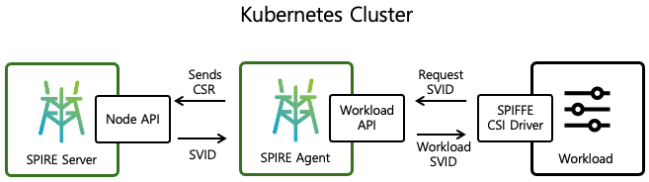
이와 더불어, 최근에는 단일 클러스터 환경에만 의존하지 않고 멀티 클라우드 및 다중 클러스터 환경의 도입이 증가하고 있다. 이러한 환경은 다양한 클라우드 서비스 제공업체의 리소스를 통합하여 사용함으로써 비즈니스 연속성과 재해 복구, 글로벌 확장성을 보장한다. 하지만, 다중 클러스터 환경에서의 서비스 간 안전한 통신 문제는 복잡해지며, 서로 다른 클러스터 간의 데이터 일관성 유지, 안전한 통신 채널의 확립, 그리고 인증 및 권한 부여 메커니즘의 구축이 주요한 도전 과제로 등장하였다[2, 3].

따라서, 본 논문에서는 다중 클러스터 환경에서 서비스 간의 통신이 안전하게 이루어질 수 있도록, 상호 인증 및 통신 암호화에 초점을 맞추어 연구를 진행한다. 이를 위해, 양방향 TLS, 즉 mTLS (Mutual TLS) 프로토콜과 SPIFFE/SPIRE 시스템을 활용하여 서비스 간 상호 인증이 가능하도록 하고, 이를 통해 데이터의 기밀성과 무결성을 확보한다. 특히, 본 연구에서는 단일 클러스터 뿐만 아니라 다중 클러스터 환경에서도 동일한 상호 인증 체계 및 통신 암호화를 적용할 수 있도록 설계하여 컨테이너화 된 환경 전반에 걸친 보안성과 신뢰성을 향상시키고자 한다.

2. SPIFFE/SPIRE 동작 원리 및 구조

SPIFFE (Secure Production Identity Framework for Everyone)는 소프트웨어 아이덴티티를 일관되게 관리하는 명세서이며, SPIRE (SPIFFE Runtime Environment)[4]는 SPIFFE의 사양을 실제로 구현한 오픈소스 소프트웨어

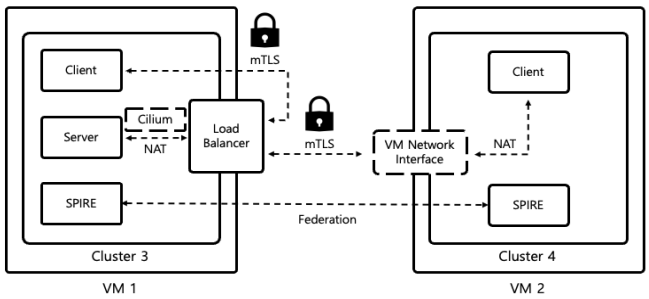
시스템이다. SPIRE 시스템은 SPIRE Server와 Agent로 구성되어, 서비스 아이덴티티를 중앙에서 관리하고 각 노드에서 인증한다.



(그림 1) SPIRE/SPIFFE 구조

워크로드가 클러스터 내에 배포될 때, Cluster SPIFFE ID CRD (Custom Resource Definition)에 정의된 라벨에 따라, 해당 워크로드에 대한 등록 엔트리가 SPIRE Server 내에 생성된다. 이후, SPIFFE CSI (Container Storage Interface) Driver가 포함된 볼륨이 워크로드에 마운트 되고, 이 Driver는 SPIRE Agent의 Workload API를 통해 해당 워크로드를 위한 SVID를 요청한다. SPIRE Agent는 Kubernetes Workload Attestor를 이용해 워크로드의 메타데이터를 수집하고, 이를 토대로 Selector를 생성하여 SPIRE Server에 CSR (Certificate Signing Request)을 보낸다. SPIRE Server는 요청 받은 Selector와 미리 등록된 엔트리를 비교하여 일치 여부를 확인한 후, 일치하면 워크로드에 SVID를 발급한다. 이렇게 발급된 SVID를 사용하여 클러스터 내에서 워크로드 간에 mTLS를 통한 안전한 통신이 가능해진다. 이러한 방식으로, SPIFFE/SPIRE는 클러스터 내의 서비스들이 상호 인증을 수행하고, 암호화된 채널을 통해 데이터를 안전하게 교환할 수 있는 환경을 구축한다.

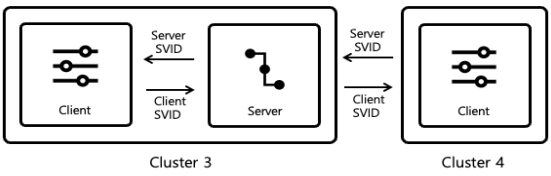
3. SPIRE/SPIFFE 를 사용한 mTLS 구현



(그림 2) mTLS 통신 과정에 대한 설계

본 논문에서는 단일 클러스터 및 다중 클러스터 설정을 기반으로 하는 두 가지 아키텍처 모델을 개념화하고 있다. 그림 2 에서 볼 수 있듯이, 단일 클러스터 환경인 클러스터 3 에서는 mTLS 통신이 클라이언트가 서버에게 패킷을 보내면서 시작되며, 이 패킷은 CNI (Container Network Interface)를 통해 NAT (Network Address Translation) 과정을 거쳐 서버의 내부 IP 로 변환되어 전달된다.

다중 클러스터 환경, 즉 클러스터 4 에서는 클라이언트가 패킷을 서버에 보낼 때 다른 접근 방식을 사용한다. 이 경우, VM (Virtual Machine)의 네트워크 인터페이스를 통해 NAT 가 수행되며, 클라이언트의 내부 IP 주소가 VM2 의 IP 주소로 변환되어 패킷이 전송된다. 이 과정은 단일 클러스터의 NAT 과정과 유사하게 진행된다.



(그림 3) mTLS 를 위한 SVID 교환

멀티 클러스터 환경에서의 추가적인 단계로, 서로 다른 SPIRE 서버 간에 신뢰를 구축하는 Federation 절차가 포함된다. 워크로드는 mTLS 통신을 시작하기 전에 서로의 SVID 를 교환하고 검증하여 상호 인증을 수행한다. SVID 의 서명은 발급한 SPIRE 서버가 하며, 신뢰 번들에 포함된 공개 키를 사용하여 이 서명의 무결성과 신뢰성을 검증한다. 서명이 검증되면 SVID 가 해당 SPIRE 서버의 신뢰할 수 있는 개인 키로 서명된 것으로 확인되고, 이를 통해 mTLS 통신에 필요한 워크로드 간의 신뢰를 구축한다.

4. 결론

본 논문에서는 SPIFFE/SPIRE를 이용하여 단일 클러스터와 다중 클러스터 환경 모두에 적용 가능한 서비스 간의 상호 인증과 mTLS 기반으로 한 통신 암호화 체계를 구현하였다. 향후 연구로는, Istio와 같은 서비스 메시 환경에서의 워크로드 상호 인증 및 암호화 체계 구축 방법에 대한 연구를 진행할 예정이다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터사업의 연구결과로 수행되었음 (IITP-2024-RS-2023-00258649)

참고문헌

[1] Tetiana Yarygina, "Overcoming Security Challenges in Microservice Architectures" IEEE Symposium on Service-Oriented System Engineering, (2018)

[2] Jelena Curguz, "Vulnerabilities of the SSL/TLS Protocol" Journal of Network Security, 248-249 (2016).

[3] Yutian Yang, "Security Challenges in the Container Cloud" IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (2021)

[4] E Falcão, M Silva, A Luz, A Brito, "Supporting Confidential Workloads in SPIRE", IEEE International Conference on Cloud Computing Technology and Science, (2022)