Managing Redis - Security

생성일	@2022년 12월 27일 오후 10:09
태그	

Redis security

> 레디스 보안모델 및 기능

Security model

신뢰할 수 없는 클라이언트가 직접 접근하는 것은 옳지 않음. 신뢰할 수 없는 접근은 ACL을 구현하고 사용장 ㅣㅂ력을 검증하며 Redis 인스턴스에 대해 수행할 작업을 결정하는 계층에 의해 조정되어야 한다.

Network security

직접 Redis를 사용하는 애플리케이션을 구현하는 컴퓨터에 사용해야한다. EC2 가상화 인스턴스 사용시 방화벽으로 외부에서 액세스 할 수 없도록 해야한다.

❓ 루프백 인터페이스가 뭘까.

Protected mode

암호 없이 기본 구성으로 실행될 때 보호 모드라는 특수 모드에 들어간다. 이 모드는 루프백 인터페이스의 쿼리에만 응답하고 다른 주소에서 연결하는 클라이언트에 문제와 Redis를 올바르게 구성하는 방법을 설명하는 오류로 응답한다.

그럼에도 보호모드를 비활성화 하거나 모든 인터페이스를 수동으로 바인딩 가능하다.

Authentication

클라이언트를 인증하는 두가지 방법이 있다.

- IAM처럼 명명된 사용자를 생성하고 세분화된 권한을 할당할 수 있는 액세스 제어 목록 사용(Redis version 6 ~)

- redis.conf 파일을 편집하고 requirepass 설정을 사용하여 데이터베이스 암호를 제공하여 활성화된다.

암호는 길면 길수록 좋다. 방화벽 같은 기타 시스템도 병행되어야 한다. AUTH명령어는 암호화되지 않은 상태로 전송되기 때문에 도청당할 수 있다.

TLS support

Redis는 모든 통신 채널에서 TLS를 선택적으로 지원함

> ❓ TLS가 뭘까.

Disallowing specific commands

명령을 허용하지 않거나, 지정된 명령 집합으로만 제한되도록 할 수 있다.

Attacks triggered by malicious inputs from external clients

외부에서 악의적으로 알고리즘 복잡성을 유발하는 데이터를 Redis에 넣을 수 있다. 이를 방지하기 위해 Redis는 해시 함수에 대해 실행별 의사 난수 시드를 사용한다.

Redis는 qsort 알고리즘을 사용해 SORT 명령을 구현한다. 현재 알고리즘으로는 무작위화되지 않으므로 올바른 입력 집합을 선택해 2차 최악의 경우 동작을 트리거할 수 있다.

> ❓ qsort 알고리즘이 뭘까.

String escaping and NoSQL injection

문자열 이스케이프 개념이 없어서 일반적으로는 주입이 불가능하다. 완전 안전! 하지만 Lua 스크립트 사용시에는 주의하자.

Code security

클라이언트는 모든 명령 집합에 대한 액세스가 허용된다. 하지만 인스턴스 액세스로 Redis를 제어할 수 있으면 안된다. redis사용자로 실행을 하던지 해서 조심하도록 하자. 루트권한 주지 않기!

ACL

> Redis Access Control List - 레디스 접근 제어 리스트

실행할 수 있는 명령과 액세스할 수 있는 키 측면에서 특정 연결을 제한할 수 있는 기능이다. 사용자 이름과 유효한 암호를 통해 인증된다. 별도 설정이 없으면 “기본” 사용자로 임명된다.

- Redis 6 이후

```
AUTH <username> <password>
```

- Redis 6 이전 (기본 사용자)

```
AUTH <password>
```

When ACLs are useful

언제 사용할까용

1. 신뢰할 수 있는 클라이언트에게만 제한된 명령을 사용하도록 할 때
2. Redis 작업을 하는 사람이 필요 이상의 명령어를 사용할 수 없도록 할 때

> 💡 어떻게 사용하는지 궁금하다면 문서 찾아보기!

TLS

> TLS 지원

SSL/TLS는 Redis 6부터 컴파일 시 활성화해야 하는 선택적 기능이다.