기술 브리프

퓨어스토리지 인크립트리듀스 (EncryptReduce)

완전한 경로 암호화 및 데이터 절감 기능의 혜택을 누리세요.

퓨어스토리지 솔루션의 주요 장점 중 하나는 작은 공간 안에 많은 양의 데이터를 넣을 수 있다는 것입니다. 압축과 중복 제거를 실행하고 패턴을 제거해 많은 비용을 절감할 수 있습니다. 하지만 절감 기능은 작은 공간 안에 데이터를 넣는 것에서 멈추지 않습니다.
플래시 미디어에 대한 쓰기 볼륨을 줄임으로써 플래시 드라이브의 수명을 여러 번 연장할 수 있습니다. 즉, 상당한 유지보수 비용을 절감하고 안정성을 얻을 수 있습니다.

이미 널리 알려진 데이터 절감의 이점을 반복해 설명하는 이유는 무엇일까요? 서버가 암호화된 데이터를 퓨어스토리지 플래시어레이(FlashArray™)에 쓸 때 데이터 절감의 이점이 사라지기 때문입니다.

해당 문제는 한동안 저장 데이터 암호화에 대한 새로운 접근 방식을 통해 해결되어 왔습니다. 어레이의 모든 데이터는 FIPS 140-2 인증 AES256 암호화를 사용하여 암호화되지만, 적어도 지금까지는 데이터 절감의 혜택을 누리기 위해선 수신 데이터를 암호화할 수 없었습니다.

퓨어스토리지 인크립트리듀스(EncryptReduce)는 이 문제를 해결합니다. Thales와의 파트너십을 기반으로, 인크립트리듀스(EncryptReduce)는 네트워크를 통해 호스트에서 플래시어레이(FlashArray)로의 완전한 전송 중 암호화(inflight encryption)를 지원합니다.

이는 다음과 같은 이점을 제공합니다.

- 네트워크를 통한 전송 중 암호화 지원
- 플래시어레이(FlashArray)에서 표준 데이터 절감 기능 실행
- KMIP(Key Management Interoperability Protocol)를 통해 물리적 보안 제공

이 솔루션은 데이터 절감을 지원하는 전송 중 암호화를 실현하기 위한 네 가지 구성 요소를 필요로 합니다. Thales는 호스트 소프트웨어인 Thales VTE(Vormetric Transparent Encryption)와 Thales DSM(Data Security Manager)이라는 두 가지 구성 요소를 제공합니다. 다른 두 구성 요소는 플래시어레이(FlashArray)와 퓨리티//FA(Purity//FA) 소프트웨어(버전 5.3 이상)입니다.

전송 중 암호화

전송 중 데이터를 암호화하면서 데이터를 압축하고 데이터 중복을 제거할 수 있습니다.

물리적 보안

인크립트리듀스는 KMIP(Key Management Interoperability Protocol)를 통해 물리적 보안 기능을 제공합니다.

표준 준수

어레이의 모든 데이터는 FIPS 140-2 인증 AES256 암호화를 사용하여 암호화됩니다.

인크립트리듀스(EncryptReduce)의 핵심, 키 공유

기본 기술은 복잡하겠지만, 인크립트리듀스(EncryptReduce)의 작동 방식의 개념은 간단합니다. Thales DSM은 호스트와 플래시어레이(-FlashArray) 사이에서 호스트와 플래시어레이(FlashArray)에서 사용되는 키를 보관합니다. 플래시어레이(FlashArray)의 경우, 사용자는 DSM을 KMIP 리소스로 정의한 다음 플래시어레이(FlashArray)와 DSM 간에 인증서를 교환합니다. 이 프로세스는 잘 알려진 프로토콜인 KMIP로 정의되므로 내부에서 특이 사항은 발생하지 않습니다. 호스트는 또한 자신과 DSM 간에 키를 교환합니다. 호스트와 플래시어레이(FlashArray)는 이제 동일한 키를 공유하고 호스트가 플래시어레이(FlashArray)에 데이터를 쓸 때 퓨어스토리지는 메모리에서 키를 해독한 다음 표준 데이터 절감 프로세스를 적용합니다. 이러한 접근 방식으로 플래시어레이(FlashArray) I/O 경로를 최소한으로 수정할 수 있습니다. 인크립트리듀스(EncryptReduce)는 여전히 저장 데이터 암호화를 유지하고 감소된 데이터를 AES256 알고리즘으로 기록합니다.

인크립트리듀스(EncryptReduce) 적용 예시

그림 1은 인크립트리듀스(EncryptReduce)가 지원하는 플래시어레이(FlashArray)에 있는 볼륨을 보여줍니다. 암호화되지 않은 볼륨은 다른 호스트의 데이터와 동일합니다. 여기서는 신뢰성 높은 절감 기능을 제공하고 테스트 및 검증용으로 공개되어 있는 Enron Email Corpus를 사용했습니다.

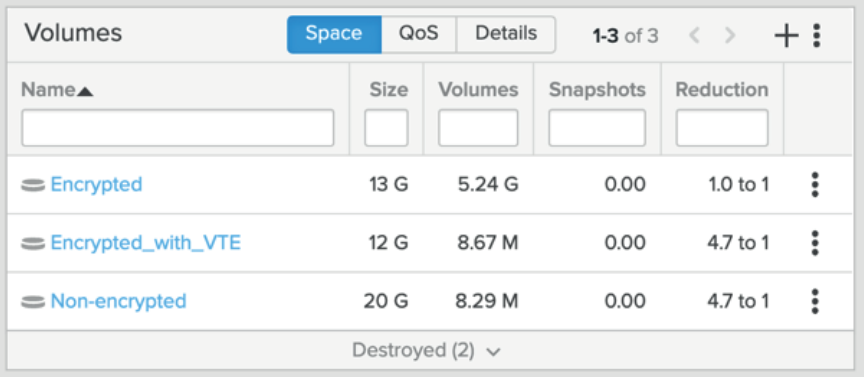

그림 1. 인크립트리듀스(EncryptReduce) 지원 플래시어레이(FlashArray)의 볼륨.

볼륨 이름으로도 충분히 알 수 있겠지만, VTE 암호화 볼륨을 사용하면 암호화되지 않은 볼륨과 정확히 동일한 데이터 감소의 이점을 누릴 수 있습니다. 두 볼륨이 절감된 방식에는 차이가 없습니다.

퓨어스토리지는 실용적인 기술을 사용할 때 어느 정도는 타협해야 한다는 주장을 믿지 않습니다. 다시 말해, 오른쪽에 있는 것을 얻기 위해 왼쪽에 있는 것을 포기해야 한다고 생각하지 않습니다. 퓨어스토리지는 에버그린(Evergreen) 서브스크립션 모델, 포괄적인 라이선싱, 무중단 하드웨어 및 소프트웨어 기능 업그레이드를 통해 이 점을 지속적으로 증명하고 있습니다. 이 접근 방식은 데이터센터의 전반적인 보안에도 적용하고 있는 중입니다. 여전히 전송 중 데이터를 암호화할 수 있으며 작은 공간 안에 많은 데이터를 저장할 수 있습니다. 이 모두 퓨리티 인크립트리듀스(Purity EncryptReduce)와 파트너사 Thales 간의 협력으로 가능한 일입니다.

Thales의 Vormetric Data Security Platform은 확대되는 암호화 및 규정 준수 요구 사항을 해결하는 데 필요한 확장성, 유연성 및 효율성을 제공하는 동시에 비용과 복잡성을 줄일 수 있습니다. Thales Cloud Protection and Licensing은 Thales Group에 속합니다.

purestorage.com/kr
+82 2 6001-3330

PURESTORAGE®

ps EncryptReduce_technical-brief