eclypses

WHITE PAPER

Securing Transmissions in an Event-Driven Architecture with Eclypses MTE® Kafka

Authors: Joe Jeanjaquet & Tim Reynolds

Document ID: ECLYPSES - 1532395320-303
Version: 2.0

Contents

Introduction

Data security is an essential aspect of any organization's IT infrastructure. As the use of big data and real-time analytics continues to grow, data protection is increasingly important. It has become crucial for businesses to have a robust data security solution for their Kafka environment.

Kafka is a distributed event-streaming architecture widely used in various industries for data integration and processing. As Kafka is a real-time streaming platform, it requires efficient and secure data transmission. With the increasing amount of sensitive data being processed through the platform, securing transmissions has become a critical aspect of Kafka environment management.

The use of microservices architecture (MSA) has become increasingly popular in recent years due to its flexibility, scalability, and ability to support multiple programming languages. With MSA, individual microservices work together to create a larger application. However, the distributed nature of microservices also introduces security risks, especially when it comes to data transmission. Apache Kafka is a popular distributed streaming platform that has been widely adopted in MSA environments. In this white paper, we will focus on securing transmissions within a microservices architecture using Kafka and show how it can be implemented using MTE/MKE technology.

Data Sharing in a Kafka Environment

Before we dive into the different attack vectors and ways to secure transmissions within a Kafka environment, it's important to understand the three primary ways that data is shared within that environment:

1. Producing/subscribing to individual messages
2. Producing/consuming continuous data streams such as real-time analytics
3. Storing/retrieving stored data via ksqlDB

Attack Vectors

Attack vectors in MSA can come from several different sources. For example, the data that is gathered from the web service API and sent on to other microservices for processing and analysis can be the most likely place for an enterprise to use the Kafka solution. Eclypses' MTE Kafka toolkit is appropriate in this scenario to help mitigate potential attack vectors.

If payloads, which are the actual data, are protected with Eclypses MTE or MKE technology, even the internal replication of multiple Kafka brokers is protected.

Without security in place:

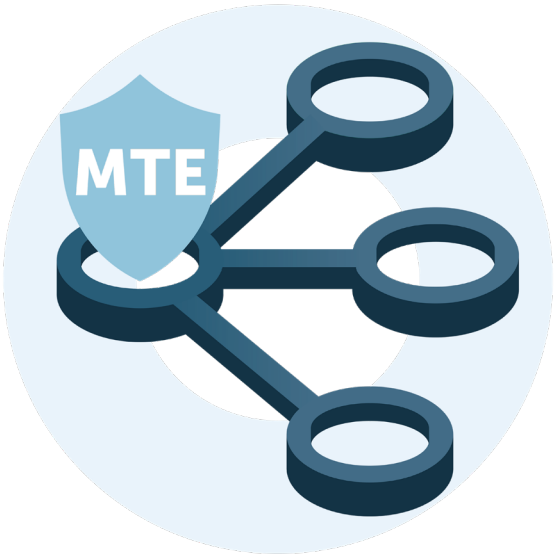
- As data moves, TLS is not enough to ensure protection against future threats
- Data-at-rest is where data is not encrypted in Kafka environments

With security in place:

- The Key Management Service (KMS) to distribute encryption keys exposes more attack vectors like RSA, TLS, and static encryption keys
- Packet inspection, injection and replay is utilized

Securing Kafka Event Streams within an MSA

In an event-driven architecture, microservices rarely send transmissions directly to one another but instead rely on broadcasting events when something noteworthy occurs. This decoupling of services allows business outcomes to be completed more efficiently and with more scalability. Security is also simplified because, rather than securing the transmission of data from service to service, the data itself can be secured end-to-end and will be secure both in transit and at rest.



MTE Kafka is a stateless, vault-less data encryption toolkit designed to secure Kafka messages within an MSA. It is protocol-agnostic and can work in the native environment of TCP or other

communication protocols as well. Kafka data can be secured at either message or field-level while still preserving the schema. Most importantly, MTE Kafka can be used in both Native and Cloud-Hosted Kafka environments – even those managed by third-party providers.

The use of MTE Kafka in an event driven Microservice Environment is simple:

Producing Data

- As data is being produced and is ready to be sent to Kafka, the toolkit will encode the message or field using Eclypses' patented technology in a process that ensures each message is uniquely secured.
- The message stream (with the encoded message) is created and sent to Kafka as it would normally.

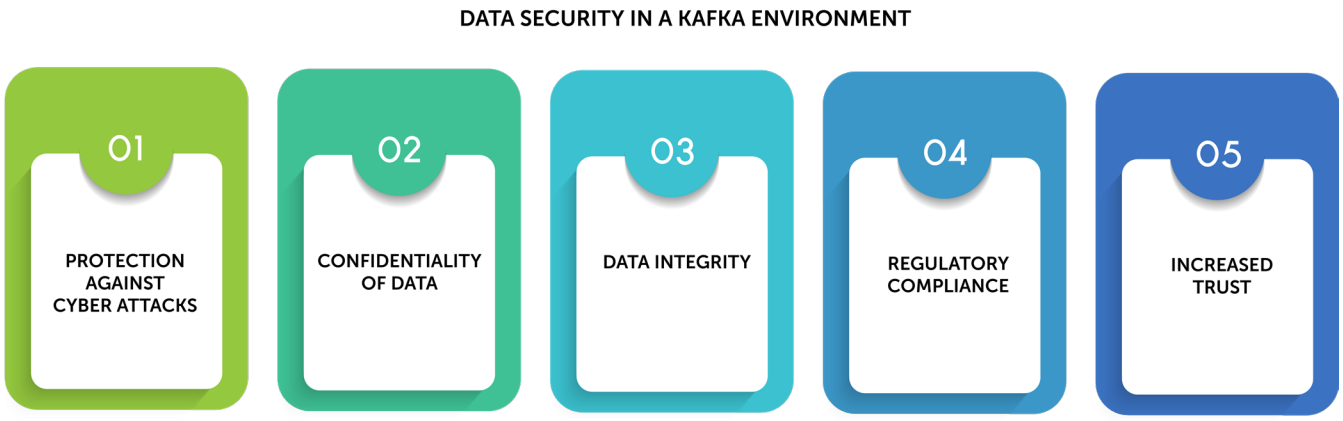
Consuming Data

- As it would normally, a microservice will request the (encoded) data from Kafka.
- The MTE Kafka toolkit will decode the data into plain text. The toolkit can be consumed directly or through low-code options like ksqlDB.

Data Security in a Kafka Environment

1. **Protection against Cyberattacks:** One of the significant benefits of having data security for a Kafka environment is protection against cyberattacks. The use of Kafka has increased significantly in recent years, and with it, the risk of cyberattacks has also increased. By implementing data security measures, organizations can protect themselves against cyberattacks such as data breaches, hacking, and other malicious activities.
2. **Confidentiality of Data:** Data security measures ensure that confidential information is kept private and protected from unauthorized access. This is essential for organizations that deal with sensitive information such as financial data or personally identifiable information (PII). Implementing data security measures ensures that only authorized personnel can access the data and maintain confidentiality.
3. **Data Integrity:** Data security measures also ensure data integrity, ensuring that data is not tampered with or altered in any way during transmission or storage. By ensuring data integrity, organizations can have confidence that the data they receive is accurate and has not been altered in any way.

4. **Regulatory Compliance:** Organizations that deal with sensitive information must comply with various regulations and data privacy laws. Implementing data security measures in a Kafka environment can ensure regulatory compliance and prevent any legal issues or penalties.
5. **Increased Trust:** Data security measures can also increase trust between an organization and its customers, partners, and other stakeholders. By ensuring that sensitive data is protected and secure, organizations can build trust and credibility with their stakeholders.



Conclusion

In conclusion, securing Kafka Streams within a Microservices Architecture is a critical aspect of ensuring the security of an enterprise's data. Eclypses MTE Kafka is a toolkit that can help secure Kafka data within MSA by offering end-to-end encryption. Its compatibility with TLS further enhances its security measures, making it a robust solution for enterprises looking to secure their microservices architecture.

MTE Kafka is the best way to ensure your MSA environment is absolutely secure. By implementing these data security measures in a Kafka environment, organizations can operate with confidence and focus on their core business operations.

For more information on Eclypses MTE Kafka, please email: contact@eclypses.com.

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, IoT devices, and Kafka environments. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

This technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT

contact@eclypses.com
www.eclypses.com
(719) 323-6680