aklivity

How KONE Uses Zilla Plus to Securely Bridge Amazon MSK with SAP Cloud & Beyond

Headquarters

Espoo, Finland

Industry

Indusrial & Manufacturing

Challenge

Needed a way to securely expose its MSK cluster to external systems such as SAP Cloud

Solution

Deployed Zilla Plus for Amazon MSK and established secure, publicly reachable entry points for its MSK cluster without exposing underlying brokers to the internet

Results

- Securely connect MSK from anywhere without placing brokers in public subnets
- Accelerate integration delivery—cutting time-to-market for projects involving external data consumers
- Reduce development overhead by eliminating the need for custom publisher/subscriber applications in the integration layer

The Challenge: Secure Connectivity to a Global Ecosystem

KONE operates a vast ecosystem of applications, many of which require secure, reliable, real-time data exchange with their Amazon Managed Streaming for Apache Kafka (MSK) clusters. These MSK clusters were deliberately placed in private AWS subnets to mitigate security risks.

The main challenge was connecting approximately **20 distinct applications and teams** hosted outside KONE's internal network, including critical vendor and third-party systems. Key external consumers include:

- **SAP BTP IS (BTPIs):** The core SAP Integration Suite, responsible for publishing and reading messages to/from MSK and converting data to/from SAP formats (e.g., IDOC). The BTPIs system is treated as a single consumer, despite supporting 30-40 underlying integrations.
- **My Kone (Mobile Apps):** Applications used for building mobile services, which consume data like service orders via the internet.
- **Monitoring Team:** Consumes MSK topics to provide end-to-end monitoring across source, integration, and target systems.
- **Other Systems:** Salesforce CRM, EWA, R&D AWS applications, PLM, GoodSign, PIP, and E2Open.

Connecting these systems via the internet without placing Kafka brokers in public subnets required a secure, Kafka-native solution that could enforce security at the edge.

The Solution: Zilla Plus as a Kafka-Native Security Gateway

KONE selected Aklivity Zilla Plus Gateway as the critical component to securely expose their private MSK clusters to internet consumers.

" Zilla Plus gave us exactly what we needed—secure, Kafka-native connectivity to our private MSK clusters from anywhere, without compromising security or building custom integrations. It's accelerated our project delivery and simplified how we connect critical business systems across our ecosystem."

- *Karthik Rajendran, Platform Owner – AWS Cloud Integration/Data Movement at KON*

Zilla Plus functions as a Kafka-native proxy, allowing KONE to:

1. **Maintain Private Infrastructure:** Keep all MSK clusters securely isolated in private subnets.
2. **Enforce Strong Authentication:** Authenticate and authorize internet clients using **mutual TLS (mTLS)**, which is KONE's preferred and most secure method for external connections, rather than simpler API keys or SASL/SCRAM.
3. **Support Flexible Integration Patterns:** Zilla Plus seamlessly supports all four primary integration patterns KONE employs:
    - **Direct Publisher:** Source systems (like BTPIs) push data directly to MSK.
    - **KONE Publisher:** KONE's custom integration code pulls data from a source system and pushes it to MSK.
    - **Direct Consumer:** Consumers read data directly from MSK.
    - **KONE Subscriber:** KONE's custom integration code pulls data from MSK, transforms it, and pushes it to the consumer's API.

KONE's central integration team is responsible for managing the Zilla Gateway and owning any custom publisher/subscriber code written to bridge systems that cannot connect to MSK directly.

Results: Accelerated Delivery and Robust Security

By adopting Zilla Plus, KONE successfully achieved its core objectives:

- **Secured Access:** MSK is securely accessible from anywhere using mTLS, without compromising security by placing brokers in public subnets.
- **Accelerated Delivery:** Time-to-market for projects involving external data consumers has been significantly cut.
- **Reduced Overhead:** The reliance on KONE's custom publisher/subscriber code for basic bridging has been minimized, reducing development and maintenance overhead.

This unified, secure approach enables KONE to support critical data flows—including financial, supply chain, and R&D data—from numerous systems while maintaining robust security and a flexible integration model.

Learn More About KONE

https://www.kone.com/en/