schwarz digits

Service certificate

STACKIT Telemetry Router

Version and start of validity	
Version 1.0	Valid from 2026/06/02

Service certificate | STACKIT Telemetry Router

Service name

STACKIT Telemetry Router

High level service description

The STACKIT Telemetry Router (“Telemetry Router”) is a managed service that acts as a central ingestion and distribution point for telemetry data. It collects standardized audit logs and service logs from STACKIT services according to the parameters set by the Customer. Audit and service logs collected in this way can be forwarded by the Customer to other services provided by STACKIT or to external destinations.

Key features

- **Central Aggregation:** Collects audit and service logs from various STACKIT services in a central location.
- **Standardized Ingestion:** Receives telemetry data uniformly via the OpenTelemetry Protocol (OTLP).
- **Flexible Routing:** Forwards data to other obtained and compatible STACKIT cloud services (e.g., STACKIT Object Storage, STACKIT Logs, STACKIT Observability) or to external OTLP- and S3-compatible target systems according to the parameters set by the Customer.
- **Security & Compliance:** Data transmission and temporary storage are encrypted. The service enables "at-least-once" delivery through retry mechanisms.
- Option for the Customer to create a standardized log stream for audits (security & traceability) and operational service logs (debugging & monitoring) for forwarding to central analysis systems or storage.

Service plans

The Telemetry Router automatically scales compute and storage resources based on the volume of log data specified by the Customer.

The following restrictions apply to the service:

- **Supported sources:** Only customer-procured & compatible STACKIT cloud services can send telemetry data (audit and service logs) to the telemetry router.
- **Audit logs:** are cached by the system for a maximum of 90 days after collection.
- **Service logs:** Are only buffered briefly (volatile) for delivery and forwarded asynchronously; persistent storage does not take place.

Metrics

Billing is usage-based per megabyte (MB) depending on the volume of the Customer's outgoing (forwarded) log data. The data volume is continuously summed up within the billing period and billed per started outgoing MB.

SLA specifics

- The telemetry router is considered available as long as the telemetry data is successfully transferred at the service transfer point. Any non-availability of customer-side target systems has no influence on the calculation of the availability of the telemetry router.

Backup

- STACKIT does not create backups of the data processed by the Telemetry Router. The system-side retention (90 days for audit logs or volatile buffering for service logs) serves purely to secure data delivery and does not replace long-term data backup by the Customer. The Customer is responsible for archiving and any archiving requirements for all log data.

Additional terms

- The customer is solely responsible for configuring the Telemetry Router service (especially the management of access tokens and the configuration of destinations).If the Customer routes data to external systems (outside of STACKIT), the legal conformity of the forwarding and for ensuring, for example, compliance with data protection regulations (e.g. third country transfer) for these external destinations is the sole responsibility of the Customer.
- After the 90-day period has expired, the buffered audit logs are automatically and irrevocably deleted from the system. If the contractual relationship between the parties regarding the Telemetry Router ends, all logs remaining with the service will be deleted 90 days after the end of the contract.

Annex | Exportability

(Online Register)

Data type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data (database content)	Data stored by the customer in the database (if available) or within the product/service	Yes	OTLP	Customer data can be retrieved per instance via the API.
User accounts & permissions	Information about users and their permissions	Yes	JSON	Access tokens are managed per instance via the API. Only metadata that does not allow any conclusions to be drawn about the token itself can be called up via this interface. The actual token is not stored for security reasons and is only accessible to the customer at the moment of generation
System metrics (instances / resources in use)	Performance data of the instance / resource in use (e.g., CPU usage, memory usage)	No. Company confidential STACKIT	-	
System properties (instances / resources in use)	Versions and information necessary to check compatibility	No. Company confidential STACKIT	-	
Product / service-related data (product properties)	Configuration data and source code *Configuration of IT-systems / rudimental IT, settings, customizing, IP's, VLAN, interfaces, software code, scripts*	No. Company confidential STACKIT	-	
	Log data (non personalized and personalized) *System-status, technical-events, etc.*	No. Company confidential STACKIT	-	

	Log data (non personalized and personalized) *Login/logout of user, user activities*	No. Company confidential STACKIT	-