

Service certificate

STACKIT
Confidential
Kubernetes

Version and start of validity

Version 1.2	Valid from 2025-12-01
-------------	-----------------------

Service certificate | STACKIT Confidential Kubernetes

Service name

STACKIT Confidential Kubernetes

High level service description

STACKIT Confidential Kubernetes is a confidential cloud computing platform based on the “Constellation” software (“Constellation”) of STACKIT-Partner Edgeless Systems GmbH, Stadionring 1, 44791 Bochum (“Edgeless Systems”). STACKIT Confidential Kubernetes is used for the secure provision and management of containerized applications by the customer. STACKIT Confidential Kubernetes enables the customer to create user-defined and user-managed STACKIT Confidential Kubernetes clusters. With STACKIT Confidential Kubernetes, all customer data remains encrypted – even at runtime – and users can verify that the integrity of the workloads is maintained. STACKIT Confidential Kubernetes runs on STACKIT Confidential Server only. When subscribing to STACKIT Confidential Kubernetes, Customer is provided with Confidential Virtual Machines (CVMs) together with a license of Constellation software, the ready-to-use Constellation CLI, Terraform provider and operating system images for Kubernetes control-plane and worker nodes. The customer is able to independently create and operate Kubernetes clusters protected by Confidential Computing mechanisms.

Key features

- Runtime encryption: Constellation runs all Kubernetes nodes inside CVMs. This provides runtime encryption for the entire cluster.
- Network and storage encryption: Constellation augments runtime encryption with transparent encryption of the network and persistent storage.
- Transparent key management: Constellation manages the corresponding cryptographic keys inside CVMs.
- Node attestation and verification: Constellation verifies the integrity of each new CVM-based node using remote attestation. Only nodes, verified with a positive result and running a signed, Confidential Computing-optimized Constellation node image receive the

cryptographic keys required to access the network and storage of a cluster.

- “Whole cluster” attestation: Towards the customer, Constellation software is able to provide a single hardware-rooted certificate to verify that the integrity of the cluster incl. workload is maintained.
- Constellation Command-Line-Interface (CLI) and Terraform: Constellation CLI and Terraform support customers in managing Confidential Kubernetes Cluster incl. Day2-Operations (Restore, Upgrades).

Service plans

The customer can select from all available STACKIT Confidential Servers in the provided availability classes.

Metrics

- A STACKIT Confidential Kubernetes licensing fee is charged based on the number of vCPUs of the CVM created by the Customer and per hour started.
- Metering period: Creation of the CVM until deletion of the CVM.
- For other resources used by the customer in conjunction with STACKIT Confidential Kubernetes, such as Block Storage, Floating IP and Load Balancer, a separate charge is made according to the conditions specified in the respective Service Certificates.

SLA specifics

- STACKIT Confidential Kubernetes is considered available when the CVM on which it is running is available.
- An availability of 99.5% on a calendar month average is agreed.
- CVMs that are waiting for access to their disk due to a Block Storage failure are rated as available.
- Failures in Kubernetes nodes, volumes, or pods within STACKIT Confidential Kubernetes clusters are treated in the calculation of availability as excluded events in the sense outlined in the general service description and as such do not affect the calculation of availability.
- The availability information refers to the availability of the CVMs that are in operation. Configuration-related or customer-related

circumstances for unavailability (e.g. a shutdown of the CVMs) are not covered.

- STACKIT provides first-level support for the customer for STACKIT Confidential Kubernetes. For support requests from the customer which STACKIT cannot answer in first-level support, STACKIT will forward the respective support request to Edgeless Systems as second-level support if required. The service hours for second-level support for answering support requests are Mondays to Fridays (business days, excluding national holidays) between 9 a.m. and 5 p.m. (CET); outside the above service hours, second-level support is only available by separate agreement between STACKIT and the customer.
- Insofar as STACKIT is obliged to remedy a defect or error, STACKIT may, as a short-term measure, provide a substitute or workaround solution to temporarily remedy or circumvent the effects of a defect or error, insofar as this is possible and reasonable with regard to the effects of the defect or error. The obligation to completely remedy the defect or error remains unaffected.

Backup

Backup and restore are sole responsibility of the customer.

Additional terms

- STACKIT Confidential Kubernetes is provided as a pure self-service, per design: To ensure that STACKIT as the cloud provider is excluded from accessing the cluster, provisioning and managing of STACKIT Confidential Kubernetes clusters is sole responsibility of the customer. This includes Day-2 operation such as Backup, Recovery, or Upgrades.
- STACKIT Confidential Kubernetes CVMs can only be used with images supported by STACKIT
- For the use of STACKIT Confidential Kubernetes by customer, the following additional rules apply:
 - Edgeless Constellation EULA:
https://www.edgeless.systems/eulas/Edgeless_Systems_Standard_EULA.pdf
 - Edgeless Constellation:
<https://www.edgeless.systems/licenses/>

- Fedora Core OS:
<https://fedoraproject.org/wiki/Legal:Licenses/LicenseAgreement>
- Cilium:
<https://github.com/cilium/cilium/blob/master/LICENSE>
- With regard to the Constellation Software, the customer receives a non-exclusive, non-transferable, non-sublicensable right, limited to the term of the subscription to the respective STACKIT Confidential Kubernetes Cloud Service, to use the Constellation Software exclusively in connection with and for the purpose of operating the STACKIT Confidential Kubernetes on CVMs hosted by STACKIT. Any other kind of use, distribution, or the like is prohibited.
- With regard to the Constellation Software, the customer receives a non-exclusive, non-transferable, non-sublicensable right, limited to the term of the subscription to the respective STACKIT Confidential Kubernetes Cloud Service, to use the Constellation Software exclusively in connection with and for the purpose of operating the STACKIT Confidential Kubernetes on CVMs hosted by STACKIT. Any other kind of use, distribution, or the like is prohibited.
- The Constellation software is licensed, not sold. The copyright owner to the Constellation software is Edgeless Systems. The customer is not allowed to change or remove copyright and copyright notices of Edgeless Systems.
- If the customer violates the duties and obligations arising from the Subscription of the STACKIT Confidential Kubernetes service or statutory provisions in connection with the use of the Constellation software and the violation is not remedied or eliminated within a reasonable period of time, STACKIT is entitled to revoke the license with effect for the future and to terminate this Subscription with immediate effect.
- The customer shall take appropriate precautions for data backup, error diagnosis and result control, unless STACKIT provides these services to the customer in accordance with this Service Certificate.
- Cilium: <https://github.com/cilium/cilium/blob/master/LICENSE>

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	No	Packed directory (e.g ZIP, rar, tar.gz)	Block storage with customer data (persistent volumes): Data is stored encrypted on a confidential virtual machine and cannot be exported via STACKIT. Only the customer can read the unencrypted data and must therefore export it themselves.
		No	-	Kubernetes cluster configuration data (etcd): Cluster configuration data is stored encrypted on a confidential virtual machine; STACKIT cannot export the data in decrypted form. This must be done by the customer themselves if necessary
User Accounts & Permissions	Information about users and their permissions	Yes	JSON	Authorization of cluster access: Users with access to the associated STACKIT project and with editor role in 'IAM and Management' in this project can access the confidential Kubernetes cluster.
System Metrics (Instances /	Performance data of the instance / resource in use	No	-	STACKIT Confidential Kubernetes does not

Resources in Use)	(e.g., CPU usage, memory usage)			send metrics to external telemetry systems.
	Sizes and Capacities	Yes	JSON / YAML	The sizes of the cluster nodes can be configured and automated (Terraform) by selecting the appropriate confidential virtual machine flavors when creating the cluster, i.e. this configuration is exportable.
System properties (Instances / Resources in use)	Versions and information necessary to check compatibility	No	-	Version information can be found in documentation only: https://docs.stackit.cloud/stackit/en/image-version-table-confidential-kubernetes-213254309.html
Product / service related data (product properties)	Configuration data and source code	No. Company confidential STACKIT.	-	-
	Log Data (non personalized and personalized) <i>System-status, Technical-events, etc.</i>	No. Company confidential STACKIT.	-	-
	Audit Log Data (non personalized and personalized) Login/Logout of User, User activities SCF Audit Events for	No. Company confidential STACKIT.	-	-

	CF User, Organization, Space, Service Instance, App Instance Lifecycles			
--	--	--	--	--