Leistungsschein Version 1.2 gültig ab 01.12.2025:

Leistungsschein STACKIT Confidential Kubernetes

Servicename
STACKIT Confidential Kubernetes

Kurzbeschreibung
STACKIT Confidential Kubernetes ist eine Confidential Cloud Computing Plattform basierend auf der Software „Constellation“ des STACKIT-Partners Edgeless Systems GmbH, Stadionring 1, 44791 Bochum („Edgeless Systems„). STACKIT Confidential Kubernetes dient der sicheren Bereitstellung und Verwaltung von containerisierten Anwendungen durch den Kunden. STACKIT Confidential Kubernetes ermöglicht es dem Kunden, benutzerdefinierte und selbstverwaltete STACKIT Confidential Kubernetes-Cluster zu erstellen. Mit STACKIT Confidential Kubernetes bleiben alle Kundendaten verschlüsselt – auch während der Laufzeit. Kunden können zudem überprüfen, ob die Integrität des Workloads sichergestellt ist. STACKIT Confidential Kubernetes kann ausschließlich im Zusammenhang mit dem STACKIT Confidential Server betrieben werden. Wenn der Kunde STACKIT Confidential Kubernetes abonniert, erhält er Confidential Virtual Machines (CVMs) zusammen mit einer Lizenz der Constellation Software, der Constellation CLI, dem Terraform-Provider und BetriebssystemImages für die Kubernetes-Control-Plane und Worker-Nodes. Der Kunde ist in der Lage, eigenständig Kubernetes-Cluster zu erstellen und zu betreiben, die durch Confidential Computing-Mechanismen geschützt sind.

Wesentliche Merkmale

- Laufzeitverschlüsselung: Mit Constellation werden alle Kubernetes-Knoten in CVMs ausgeführt. Dies stellt die Laufzeitverschlüsselung des kompletten Clusters sicher.
- Netzwerk und Speicherverschlüsselung: Constellation ergänzt die Laufzeitverschlüsselung um eine transparente Verschlüsselung von Netzwerk und Speicher.
- Transparentes Key Management: Constellation verwaltet die kryptografischen Schlüssel innerhalb der CVM automatisch und sorgt so für eine einfache und sichere Nutzung.
- Note-Attestierung und -Verifizierung: Die Integrität jedes neuen CVM-basierten Knotens im Cluster wird vor der Inbetriebnahme mittels „remote attestation“ geprüft. Nur Knoten, die erfolgreich verifiziert wurden und ein signiertes, Confidential Computing-optimiertes Constellation-Image verwenden, erhalten die kryptographischen Schlüssel, um auf das Netzwerk und den Speicher des Clusters zugreifen zu dürfen.
- „Whole-Cluster-Attestierung“: Kunden können die Sicherheit und Integrität eines gesamten Clusters mittels eines einzigen an Hardware-gebundenen Zertifikates überprüfen.
- Constellation CLI and Terraform: Das Constellation CLI bzw. Terraform unterstützen Kunden beim eigenständigen Betrieb von Confidential Kubernetes Clustern inkl. Day-2-Operations (Restore, Upgrades).

Servicepläne
Der Kunde kann aus allen verfügbaren STACKIT Confidential Servers in den angebotenen Verfügbarkeitsklassen wählen.

Metrik

- Die Lizenzgebühr für Confidential Kubernetes wird auf Basis der Anzahl der vom Kunden erstellten vCPUs der CVM und pro gestarteter Stunde berechnet.
- Berechneter Zeitraum: Erstellung der CVM bis Löschen der CVM.
- Für weitere vom Kunden im Verbund mit STACKIT Confidential Kubernetes genutzten Ressourcen wie bspw. Block Storage, Floating IP und Loadbalancer erfolgt eine gesonderte Berechnung zu den in dem jeweiligen Leistungsschein genannten Bedingungen.

SLA specifics

- STACKIT Confidential Kubernetes gilt als verfügbar, wenn die jeweilige CVM, auf der der Service läuft, verfügbar ist.
- Es wird eine Verfügbarkeit von 99,5% im Kalendermonatsmittel vereinbart.
- CVM die aufgrund einer Störung des Block Storage auf Zugriff auf ihre Disk warten, gelten als verfügbar.
- Fehler von Kubernetes Knoten, Volumes oder Pods innerhalb von STACKIT Confidential Kubernetes-Clustern werden bei der Berechnung der Verfügbarkeit als ausgeschlossene Ereignisse im Sinne der allgemeinen Servicebeschreibung behandelt und wirken sich dementsprechend nicht auf die Berechnung der Verfügbarkeit aus.
- Die Verfügbarkeitsangaben beziehen sich auf die Verfügbarkeit der CVM, die sich im Betrieb befinden. Nicht erfasst sind konfigurations- oder kundenseitig bedingte Umstände für eine Nichtverfügbarkeit (z.B. ein Herunterfahren der CVM).
- STACKIT stellt einen First-Level support für den Kunden von STACKIT Confidential Kubernetes bereit. Für Supportanfragen seitens des Kunden, die STACKIT nicht im firstlevel beantworten kann, wird STACKIT falls notwendig die entsprechende Anfrage an Edgeless Systems weiterleiten. Die Bearbeitung von Second-Level Anfragen findet im Zeitraum Montag bis Freitag (Werktage, bundeseinheitliche Feiertage ausgeschlossen) zwischen 9 und 17 Uhr (MEZ) statt. Ein darüber hinaus gehender Second-Level Support ist nur durch eine separate Vereinbarung zwischen STACKIT und dem Kunden möglich.
- Soweit STACKIT zur Beseitigung eines Mangels oder Fehlers verpflichtet ist, kann STACKIT als kurzfristige Maßnahme eine Ersatz- oder Umgehungslösung zur vorübergehenden Beseitigung oder Umgehung der Auswirkungen eines Mangels oder Fehlers bereitstellen, soweit dies möglich und im Hinblick auf die Auswirkungen des Mangels oder Fehlers zumutbar ist. Die Verpflichtung zur vollständigen Beseitigung des Mangels oder Fehlers bleibt hiervon unberührt.

Backup

- Backup und Wiederherstellung liegen im Verantwortungsbereich des Kunden.

Zusätzliche Bedingungen

- STACKIT Confidential Kubernetes wird konstruktionsbedingt ausschließlich als selfmanaged Service angeboten: Um den Ausschluss eines Zugriffs von STACKIT als Cloud Provider sicherzustellen, liegen das Erstellen sowie das Management von STACKIT Confidential Kubernetes Clustern vollständig im Verantwortungsbereich des Kunden. Dies umfasst auch Day-2 Operations, wie bspw. Backup, Recovery oder Upgrades von Clustern.
- STACKIT Confidential Kubernetes CVMs können ausschließlich mit den von STACKIT unterstützten Images verwendet werden.
- Es gelten zusätzlich die nachfolgenden Bedingungen:
    - 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

- In Bezug auf die Constellation Software erhält der Kunde ein nicht ausschließliches, nicht übertragbares, nicht unterlizenzierbares und auf die Laufzeit des Abonnements des jeweiligen STACKIT Confidential Kubernetes Cloud Service beschränktes Recht, die Constellation Software ausschließlich in Verbindung mit und zum Zweck des Betriebs des STACKIT Confidential Kubernetes auf von STACKIT gehosteten CMVs zu nutzen. Jede andere Art der Nutzung, Verbreitung oder ähnliches ist untersagt.
- Die Constellation-Software wird lizenziert, nicht verkauft. Der Urheberrechtsinhaber der Constellation-Software ist Edgeless Systems. Der Kunde ist nicht berechtigt, Copyright-und Urheberrechtsvermerke von Edgeless Systems zu verändern oder zu entfernen.
- Verstößt der Kunde im Zusammenhang mit der Nutzung der Constellation Software gegen die sich aus dem Abonnement des STACKIT Confidential Kubernetes Service ergebenden Pflichten und Obliegenheiten oder gegen gesetzliche Bestimmungen und wird der Verstoß nicht innerhalb einer angemessenen Frist abgestellt oder beseitigt, ist STACKIT berechtigt, die Lizenz mit Wirkung für die Zukunft zu widerrufen und dieses Abonnement mit sofortiger Wirkung zu kündigen.
- Der Kunde hat angemessene Vorkehrungen zur Datensicherung, Fehlerdiagnose und Ergebniskontrolle zu treffen, es sei denn, STACKIT stellt dem Kunden diese Leistungen nach Maßgabe dieses Leistungsscheins zur Verfügung.
- Cilium: https://github.com/cilium/cilium/blob/master/LICENSE

Annex: Exportability (Online Register)

Datentyp	Beschreibung	Exportierbar (Ja/Nein)	Format	Zusätzliche Anmerkungen
Kundendaten (Datenbankinhalte)	Daten, die vom Kunden in der Datenbank (sofern vorhanden) bzw. innerhalb des Produktes/Services gespeichert werden	Nein	Gepacktes Verzeichnis (z.B. ZIP, rar, tar.gz)	Blockspeicher mit Kundendaten (Persistent Volumes): Daten sind auf einer confidential virtual machine encrypted abgelegt und durch STACKIT nicht exportierbar. Nur der Kunde kann die Daten unencrypted lesen und muss demnach selbst einen

				Export vornehmen.
		Nein	-	Kubernetes Cluster Konfigurations daten (etcd): Cluster Konfigurations daten liegen encrypted auf einer confidential virtual machine, STACKIT kann die Daten nicht entschlüsselt exportieren. Dies muss bei Bedarf Kunde selbst vornehmen.
Benutzerkonten & Berechtigungen	*Informationen über Nutzer und deren Berechtigungen*	Ja	JSON	Authorisierung des Cluster Zugriffs: Nutzer mit Zugriff auf das zugehörige STACKIT Projekt und mit Editor-Rolle im 'IAM und Management' in diesem Projekt können auf den confidential Kubernetes Cluster zugreifen.
System Metriken (Instanzen /	Leistungsdaten der Instanz/genutzte Ressourcen	Nein	-	STACKIT Confidential Kubernetes sendet keine

Ressourcen in Nutzung)	(z. B. CPU-Auslastung, Speichernutzung)			Metriken zu äußeren Telemetrie Systemen.
	Sizes and Capacities	Ja	JSON / YAML	Die Größen der Cluster Nodes sind durch Auswahl der entsprechenden confidential virtual machine Flavors beim Anlegen der Cluster konfigurierbar und automatisierbar (Terraform), d.h. diese Konfiguration ist exportierbar.
Systemeigenschaften (Instanzen / Ressourcen in Nutzung)	Versionen und Informationen, die notwendig sind um Kompatibilität prüfen zu können	Nein	-	Versionsinformationen sind in der Dokumentation zu finden: https://docs.stackit.cloud/stackit/en/image-version-table-confidential-kubernetes-213254309.html
Produkt / Servicebezogene Daten (kundenunabhängige Produkteigenschaften)	Konfigurationsdaten und Source Code	Nein. Betriebsinternum STACKIT.	-	-

	Log Daten (nicht personalisiert und personalisiert) Nein. Betriebsinter num STACKIT. -- System-Status, Technische Events, etc.	Nein. Betriebsinter num STACKIT.	-	-
	Log Daten (nicht personalisiert und personalisiert) Login/Logout der Nutzer, Nutzeraktivität en	Nein. Betriebsinter num STACKIT.	-	-

Leistungsschein Version 1.1 gültig bis 30.11.2025:

Leistungsschein STACKIT Confidential Kubernetes

Servicename
STACKIT Confidential Kubernetes

Kurzbeschreibung
STACKIT Confidential Kubernetes ist eine Confidential Cloud Computing Plattform basierend auf der Software „Constellation“ des STACKIT-Partners Edgeless Systems GmbH, Stadionring 1, 44791 Bochum („Edgeless Systems„). STACKIT Confidential Kubernetes dient der sicheren Bereitstellung und Verwaltung von containerisierten Anwendungen durch den Kunden. STACKIT Confidential Kubernetes ermöglicht es dem Kunden, benutzerdefinierte und selbstverwaltete STACKIT Confidential Kubernetes-Cluster zu erstellen. Mit STACKIT Confidential Kubernetes bleiben alle Kundendaten verschlüsselt – auch während der Laufzeit. Kunden können zudem überprüfen, ob die Integrität des Workloads sichergestellt ist. STACKIT Confidential Kubernetes kann ausschließlich im Zusammenhang mit dem STACKIT Confidential Server betrieben werden. Wenn der Kunde STACKIT Confidential Kubernetes

abonniert, erhält er Confidential Virtual Machines (CVMs) zusammen mit einer Lizenz der Constellation Software, der Constellation CLI, dem Terraform-Provider und BetriebssystemImages für die Kubernetes-Control-Plane und Worker-Nodes. Der Kunde ist in der Lage, eigenständig Kubernetes-Cluster zu erstellen und zu betreiben, die durch Confidential Computing-Mechanismen geschützt sind.

Wesentliche Merkmale

- Laufzeitverschlüsselung: Mit Constellation werden alle Kubernetes-Knoten in CVMs ausgeführt. Dies stellt die Laufzeitverschlüsselung des kompletten Clusters sicher.
- Netzwerk und Speicherverschlüsselung: Constellation ergänzt die Laufzeitverschlüsselung um eine transparente Verschlüsselung von Netzwerk und Speicher.
- Transparentes Key Management: Constellation verwaltet die kryptografischen Schlüssel innerhalb der CVM automatisch und sorgt so für eine einfache und sichere Nutzung.
- Note-Attestierung und -Verifizierung: Die Integrität jedes neuen CVM-basierten Knotens im Cluster wird vor der Inbetriebnahme mittels „remote attestation“ geprüft. Nur Knoten, die erfolgreich verifiziert wurden und ein signiertes, Confidential Computing-optimiertes Constellation-Image verwenden, erhalten die kryptographischen Schlüssel, um auf das Netzwerk und den Speicher des Clusters zugreifen zu dürfen.
- „Whole-Cluster-Attestierung“: Kunden können die Sicherheit und Integrität eines gesamten Clusters mittels eines einzigen an Hardware-gebundenen Zertifikates überprüfen.
- Constellation CLI and Terraform: Das Constellation CLI bzw. Terraform unterstützen Kunden beim eigenständigen Betrieb von Confidential Kubernetes Clustern inkl. Day-2-Operations (Restore, Upgrades).

Servicepläne

Der Kunde kann aus allen verfügbaren STACKIT Confidential Servers in den angebotenen Verfügbarkeitsklassen wählen.

Metrik

- STACKIT Confidential Kubernetes wird pro erstellter CVM und pro angefangener Stunde berechnet.
- Berechneter Zeitraum: Erstellung der CVM bis Löschen der CVM.
- Für weitere vom Kunden im Verbund mit STACKIT Confidential Kubernetes genutzten Ressourcen wie bspw. Block Storage, Floating IP und Loadbalancer erfolgt eine gesonderte Berechnung zu den in dem jeweiligen Leistungsschein genannten Bedingungen.

SLA specifics

- STACKIT Confidential Kubernetes gilt als verfügbar, wenn die jeweilige CVM, auf der der Service läuft, verfügbar ist.
- Es wird eine Verfügbarkeit von 99,5% im Kalendermonatsmittel vereinbart.
- CVM die aufgrund einer Störung des Block Storage auf Zugriff auf ihre Disk warten, gelten als verfügbar.
- Fehler von Kubernetes Knoten, Volumes oder Pods innerhalb von STACKIT Confidential Kubernetes-Clustern werden bei der Berechnung der Verfügbarkeit als ausgeschlossene Ereignisse im Sinne der allgemeinen Servicebeschreibung behandelt und wirken sich dementsprechend nicht auf die Berechnung der Verfügbarkeit aus.
- Die Verfügbarkeitsangaben beziehen sich auf die Verfügbarkeit der CVM, die sich im Betrieb befinden. Nicht erfasst sind konfigurations- oder kundenseitig bedingte Umstände für eine Nichtverfügbarkeit (z.B. ein Herunterfahren der CVM).
- STACKIT stellt einen First-Level support für den Kunden von STACKIT Confidential Kubernetes bereit. Für Supportanfragen seitens des Kunden, die STACKIT nicht im firstlevel beantworten kann, wird STACKIT falls

notwendig die entsprechende Anfrage an Edgeless Systems weiterleiten. Die Bearbeitung von Second-Level Anfragen findet im Zeitraum Montag bis Freitag (Werktage, bundeseinheitliche Feiertage ausgeschlossen) zwischen 9 und 17 Uhr (MEZ) statt. Ein darüber hinaus gehender Second-Level Support ist nur durch eine separate Vereinbarung zwischen STACKIT und dem Kunden möglich.

- Soweit STACKIT zur Beseitigung eines Mangels oder Fehlers verpflichtet ist, kann STACKIT als kurzfristige Maßnahme eine Ersatz- oder Umgehungslösung zur vorübergehenden Beseitigung oder Umgehung der Auswirkungen eines Mangels oder Fehlers bereitstellen, soweit dies möglich und im Hinblick auf die Auswirkungen des Mangels oder Fehlers zumutbar ist. Die Verpflichtung zur vollständigen Beseitigung des Mangels oder Fehlers bleibt hiervon unberührt.

Backup

- Backup und Wiederherstellung liegen im Verantwortungsbereich des Kunden.

Zusätzliche Bedingungen

- STACKIT Confidential Kubernetes wird konstruktionsbedingt ausschließlich als selfmanaged Service angeboten: Um den Ausschluss eines Zugriffs von STACKIT als Cloud Provider sicherzustellen, liegen das Erstellen sowie das Management von STACKIT Confidential Kubernetes Clustern vollständig im Verantwortungsbereich des Kunden. Dies umfasst auch Day-2 Operations, wie bspw. Backup, Recovery oder Upgrades von Clustern.
- STACKIT Confidential Kubernetes CVMs können ausschließlich mit den von STACKIT unterstützten Images verwendet werden.
- Es gelten zusätzlich die nachfolgenden Bedingungen:
    - 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
- In Bezug auf die Constellation Software erhält der Kunde ein nicht ausschließliches, nicht übertragbares, nicht unterlizenzierbares und auf die Laufzeit des Abonnements des jeweiligen STACKIT Confidential Kubernetes Cloud Service beschränktes Recht, die Constellation Software ausschließlich in Verbindung mit und zum Zweck des Betriebs des STACKIT Confidential Kubernetes auf von STACKIT gehosteten CMVs zu nutzen. Jede andere Art der Nutzung, Verbreitung oder ähnliches ist untersagt.
- Die Constellation-Software wird lizenziert, nicht verkauft. Der Urheberrechtsinhaber der Constellation-Software ist Edgeless Systems. Der Kunde ist nicht berechtigt, Copyright-und Urheberrechtsvermerke von Edgeless Systems zu verändern oder zu entfernen.
- Verstößt der Kunde im Zusammenhang mit der Nutzung der Constellation Software gegen die sich aus dem Abonnement des STACKIT Confidential Kubernetes Service ergebenden Pflichten und Obliegenheiten oder gegen gesetzliche Bestimmungen und wird der Verstoß nicht innerhalb einer angemessenen Frist abgestellt oder beseitigt, ist STACKIT berechtigt, die Lizenz mit Wirkung für die Zukunft zu widerrufen und dieses Abonnement mit sofortiger Wirkung zu kündigen.
- Der Kunde hat angemessene Vorkehrungen zur Datensicherung, Fehlerdiagnose und Ergebniskontrolle zu treffen, es sei denn, STACKIT stellt dem Kunden diese Leistungen nach Maßgabe dieses Leistungsscheins zur Verfügung.
- Cilium: https://github.com/cilium/cilium/blob/master/LICENSE

Annex: Exportability (Online Register)

Datentyp	Beschreibung	Exportierbar (Ja/Nein)	Format	Zusätzliche Anmerkungen
Kundendaten (Datenbankinhalte)	Daten, die vom Kunden in der Datenbank (sofern vorhanden) bzw. innerhalb des Produktes/Services gespeichert werden	Nein	Gepacktes Verzeichnis (z.B. ZIP, rar, tar.gz)	Blockspeicher mit Kundendaten (Persistent Volumes): Daten sind auf einer confidential virtual machine encrypted abgelegt und durch STACKIT nicht exportierbar. Nur der Kunde kann die Daten unencrypted lesen und muss demnach selbst einen Export vornehmen.
		Nein	-	Kubernetes Cluster Konfigurationsdaten (etcd): Cluster Konfigurationsdaten liegen encrypted auf einer confidential virtual machine, STACKIT kann die Daten nicht entschlüsselt exportieren. Dies muss bei Bedarf Kunde selbst vornehmen.
Benutzerkonten & Berechtigungen	*Informationen über Nutzer und deren Berechtigungen*	Ja	JSON	Authorisierung des Cluster Zugriffs: Nutzer mit Zugriff auf das zugehörige STACKIT Projekt und mit Editor-Rolle im 'IAM und Management' in diesem Projekt können auf den confidential Kubernetes Cluster zugreifen.
System Metriken (Instanzen / Ressourcen in Nutzung)	Leistungsdaten der Instanz/genutzte Ressourcen (z. B. CPU-Auslastung, Speichernutzung)	Nein	-	STACKIT Confidential Kubernetes sendet keine Metriken zu äußeren Telemetrie Systemen.
	Sizes and Capacities	Ja	JSON / YAML	Die Größen der Cluster Nodes sind durch Auswahl der entsprechenden confidential virtual machine Flavors beim Anlegen der Cluster konfigurierbar und

				automatisierbar (Terraform), d.h. diese Konfiguration ist exportierbar.
Systemeigenschaften (Instanzen / Ressourcen in Nutzung)	Versionen und Informationen, die notwendig sind um Kompatibilität prüfen zu können	Nein	-	Versionsinformationen sind in der Dokumentation zu finden: https://docs.stackit.cloud/stackit/en/image-version-table-confidential-kubernetes-213254309.html
Produkt / Servicebezogene Daten (kundenunabhängige Produkteigenschaften)	Konfigurationsdaten und Source Code	Nein. Betriebsinter num STACKIT.	-	-
	Log Daten (nicht personalisiert und personalisiert) Nein. Betriebsinter num STACKIT. -- System-Status, Technische Events, etc.	Nein. Betriebsinter num STACKIT.	-	-
	Log Daten (nicht personalisiert und personalisiert) Login/Logout der Nutzer, Nutzeraktivitäten	Nein. Betriebsinter num STACKIT.	-	-