schwarz digits

Leistungsschein

STACKIT VPN

Version und Geltungsbeginn	
Version 1.0	Gültig ab 05.05.2026

Leistungsschein | STACKIT VPN

Servicename

STACKIT VPN

Kurzbeschreibung

Das Produkt **STACKIT VPN** ermöglicht es Kunden, sichere, skalierbare und flexible virtuelle private Netzwerkverbindungen (VPN) in der STACKIT Cloud-Umgebung bereitzustellen. Mit STACKIT VPN können Kunden ihre On-Premises-Datenzentren oder ihre Bürostandorte mit ihren STACKIT Cloud-Ressourcen verbinden, um eine verschlüsselte Datenübertragung und robuste Netzwerksicherheit zu gewährleisten. Der Kunde kann zwischen verschiedenen VPN-Konfigurationen wählen, darunter Site-to-Site, Site-to-Multisite, und Active-Active-Verbindungen, um den spezifischen Anforderungen seines Unternehmens gerecht zu werden. Die Bereitstellung, Verwaltung und Konfiguration des VPN erfolgt durch den Kunden selbst über die STACKIT API sowie das STACKIT Portal oder die STACKIT Developer Tools.

Wesentliche Merkmale

- **Flexible VPN-Konfigurationen:** Unterstützung von verschiedenen VPN-Typen, darunter Site-to-Site, Site-to-Multisite und Active-Active VPNs, um unterschiedliche Anwendungsfälle und Unternehmensanforderungen abzudecken.
- **Sichere Datenübertragung:** End-to-End-Verschlüsselung aller Daten, die über das VPN übertragen werden, zur Gewährleistung höchster Sicherheitsstandards.
- **Hohe Verfügbarkeit:** Möglichkeit zur Implementierung redundanter VPN-Verbindungen und Active-Active-Setups zur Maximierung der Ausfallsicherheit und Minimierung von Downtime.
- **Self-Service-Bereitstellung:** Verwaltung, Konfiguration und Überwachung des VPN über die STACKIT API oder das STACKIT Portal.
- **Skalierbarkeit:** Dynamische Anpassung der VPN-Verbindungen entsprechend dem wachsenden Bedarf, ohne dass umfangreiche Infrastruktur Änderungen erforderlich sind.

Servicepläne

Der Kunde hat die Möglichkeit im Rahmen der Bestellung aus verschiedenen Konfigurationen des Service auszuwählen. Diese unterscheiden sich vornehmlich in ihrer maximalen Bandbreite und Anzahl möglicher Verbindungen.

Metrik

- **Abrechnung:** Betriebsstunden pro angelegten VPN Gateway je angefangener Stunde entsprechend dem gewählten Serviceplan.
- **Berechneter Zeitraum:** Anlage der VPN Gateway bis Löschen der entsprechenden Ressource.
- Für zusätzliche, vom Kunden im Zusammenhang mit STACKIT VPN genutzte Ressourcen, wie z.B. STACKIT Observability, erfolgt eine gesonderte Berechnung zu den in den jeweiligen Leistungsschein genannten Bedingungen.

SLA-Spezifika

Das STACKIT VPN-Dienstangebot unterliegt den allgemeinen SLA-Bestimmungen, wie sie in der STACKIT Servicebeschreibung festgelegt sind. Ergänzende, spezifische Service-Level-Vereinbarungen für STACKIT VPN sind nachfolgend aufgeführt:

- Der SLA gilt ausschließlich für VPN Gateways, die im Active-Active Modus konfiguriert sind. Es obliegt dem Kunden, beide im VPN Gateway bereitgestellten Instanzen (Tunnel 1 und Tunnel 2) auf seinem lokalen Gateway (Customer Gateway) redundant anzubinden und zu konfigurieren.
- Eine VPN Verbindung gilt als verfügbar, sofern mindestens eine der beiden STACKIT VPN Gateway Instanzen betriebsbereit ist und Traffic über einen aufgebauten Tunnel verarbeiten kann.
- Die Verbindung wird als nicht verfügbar gewertet, wenn beide Instanzen des VPN Gateways von STACKIT gleichzeitig keine externe Konnektivität herstellen können und dies auf die STACKIT Infrastruktur zurückzuführen ist. Dies ist gegeben, wenn:
  - Keine der beiden STACKIT VPN Instanzen über das öffentliche Netzwerk erreichbar ist.
  - STACKIT-seitige Fehler den Aufbau beider Tunnel trotz korrekter kundenseitiger Konfiguration verhindern.

Backup

Backup und Wiederherstellung der VPN-Konfigurationen und -Daten obliegen dem Kunden und sind nicht im Service enthalten. Dies bezieht sich insbesondere auf:

- Die Konfiguration des VPN Gateways und der VPN-Verbindungen, einschließlich aller vom Kunden festgelegten Eigenschaften und Einstellungen.
- Die Protokolldaten und Verbindungsinformationen, die im Zusammenhang mit der Nutzung des VPN-Dienstes entstehen.
- Sicherungen von Zugangsdaten und Zertifikaten, die zur Authentifizierung und Verschlüsselung der VPN-Verbindungen verwendet werden.

Zusätzliche Bedingungen

- Die vom Kunden konfigurierten VPN-Einstellungen und -Verbindungen sind nicht Teil des Service Umfangs von STACKIT VPN und unterliegen der alleinigen Verantwortung des Kunden.

- Der Kunde ist für das Management der VPN-Konfigurationen, einschließlich der Verwaltung von Zugangsdaten und Zertifikaten, verantwortlich. Dazu gehören insbesondere die Erstellung, Wartung, Aktualisierung und Sicherung der VPN-Einstellungen.
- STACKIT bietet Support für technische Probleme im Zusammenhang mit der VPN-Infrastruktur selbst, nicht jedoch für die spezifische Konfiguration oder den Betrieb des VPN auf Kundenseite.
- Der Kunde trägt die Verantwortung für die Sicherheit seiner VPN-Verbindungen und die Einhaltung der geltenden Sicherheitsrichtlinien. Dies umfasst insbesondere die Sicherstellung, dass keine unbefugten Zugriffe auf das VPN oder die über das VPN übertragenen Daten erfolgen. STACKIT gewährleistet die Sicherheit der VPN-Infrastruktur gemäß den Anforderungen der §§ 165 ff. TKG.
- Die aktuellen Informationen zu unterstützten VPN-Protokollen, Verschlüsselungsstandards und Konfigurationsmöglichkeiten sind in der STACKIT Knowledgebase verfügbar. STACKIT behält sich das Recht vor, die angebotenen VPN-Funktionen und -Konfigurationen zu ändern oder zu erweitern. Änderungen werden in der Dokumentation entsprechend aktualisiert. Wesentliche Änderungen werden dem Kunden mindestens einen Monat vor Wirksamwerden im Rahmen der STACKIT Release-Notes mitgeteilt; § 57 TKG bleibt unberührt.
- Der Kunde verpflichtet sich, alle gesetzlichen Anforderungen und regulatorischen Vorschriften, die im Zusammenhang mit dem Einsatz des VPN-Dienstes für die Zwecke des Kunden bestehen, einzuhalten. STACKIT erfüllt die einem Anbieter von Telekommunikationsdiensten obliegenden regulatorischen Pflichten (insbesondere nach dem TKG und dem TDDDG).
- Der Kunde ist verpflichtet, regelmäßige Sicherheitsüberprüfungen durchzuführen und die Integrität der VPN-Verbindungen zu gewährleisten.

Anhang | Exportierbarkeit (Online Register)

Datentyp	Beschreibung	Exportierbar (Ja/Nein)	Format	Zusätzliche Anmerkungen
Kundendaten (Datenbank-inhalte)	*VPN Gateway & VPN Connection Konfigurationsdaten*	Ja	JSON	Alle vom Kunden erstellten Konfigurationen, abgesehen von Passwörtern (PSK), sind über die STACKIT VPN API exportierbar oder über das STACKIT Portal auslesbar.
	Verbindungsdaten	Nein	-	Bei einem VPN-Dienst ist der primäre "Dateninhalt" der durchgeleitete Datenverkehr. Dieser Verkehr wird nicht gespeichert.
Benutzer-konten & Berechtigungen	Informationen über Nutzer und deren Berechtigungen	Nein	-	Der STACKIT VPN Service speichert keine Konten oder Berechtigungen. Auth erfolgt vollständig über STACKIT IAM.
System-Metriken (Instanzen/ Ressourcen in Nutzung)	Leistungsdaten der Instanz/ genutzten Ressource (z. B. CPU-Auslastung, Speichernutzung)	Ja	JSON	Beinhaltet Daten wie Anzahl der aktiven Verbindungen und Datenvolumen. Werte können über die STACKIT VPN API abgefragt oder im STACKIT Portal eingesehen werden. Der Kunde kann (zukünftig, optional) eine eigene Observability Instanz konfigurieren, an die diese und weitere Leistungsdaten der VPN Instanzen geschickt werden können. Diese Instanz unterliegt der Kontrolle des Kunden.
	Größen und Kapazitäten *Kapazitäten der vorhandenen Ressourcen / Instanzen*	Ja	JSON	Dies sind die vertraglich vereinbarten oder gebuchten Leistungsgrenzen, z. B. maximale Bandbreite, maximal zulässige Anzahl an Verbindungen oder die Anzahl der gebuchten VPN-Gateways. Werte ergeben sich aus dem vom Kunden gebuchten VPN

				Plan und Projekt Quotas und können über die STACKIT VPN API oder im STACKIT Portal eingesehen werden.
System-eigenschaften (Instanzen/ Ressourcen in Nutzung)	Versionen und Informationen, die notwendig sind, um Kompatibilität prüfen zu können	Ja	JSON	Die Daten sind im STACKIT Portal und über die STACKIT VPN API einsehbar, z.B. aktuell erstellte VPN Gateways & Connections sowie verwendete Verschlüsselungsalgorithmen und Authentifizierungs-methoden. Von STACKIT VPN unterstützte VPN Protokolle, Verschlüsselungsalgorithmen und Authentifizierungs-methoden sind in der STACKIT Dokumentation, dem STACKIT Portal und STACKIT VPN API Docs einsehbar.
Produkt / Service-bezogene Daten (Produkt-eigenschaften)	Konfigurationsdaten und Source Code *Configuration of IT-Systems/ rudimental IT, Settings, Customizing, IP's, VLAN, Interfaces, Software Code, Scripts*	Nein. Betriebs-internum STACKIT		
	Log Daten (nicht personalisiert und personalisiert) *System-Status, Technical-events, etc.*	Ja	-	Der Kunde kann (zukünftig, optional) eine eigene Observability Instanz konfigurieren, an die Log Daten der VPN Verbindungen (Verbindungsaufbau, -abbruch, -status) der VPN Instanzen geschickt werden können. Diese Instanz unterliegt der Kontrolle des Kunden.
	Log Daten (nicht personalisiert und personalisiert) *Login/Logout der Nutzer, Nutzeraktivitäten*	Ja	JSON	Alle API-Calls zur STACKIT VPN API via STACKIT Telemetry Router.