schwarz digits

Leistungsschein

STACKIT Secrets Manager

Version und Geltungsbeginn	
Version 1.4	Gültig ab 12.09.2025

Leistungsschein | STACKIT Secrets Manager

Servicename

STACKIT Secrets Manager

Kurzbeschreibung

STACKIT Secrets Manager („Secrets Manager“) ist ein gemanagter Service, der einen sicheren Key-Value-Store für sensible Daten (wie Kennwörter, Konfigurationsdateien und Text) bereitstellt. Er ermöglicht den Schutz und die Verwaltung von Secrets. Der Secrets Manager bietet eine API, die eine einfache Integration in Anwendungen und Arbeitsabläufe ermöglicht. So ist eine Trennung von Quellcode und Secrets möglich und Compliance Vorgaben können umgesetzt werden.

Wesentliche Merkmale

- Speicherung von Secrets entsprechend den Sicherheitsvorgaben (z. B. Trennung von Quellcode und Secrets)
- Über die Self-Service-Benutzeroberfläche im STACKIT Portal kann der Kunde schnell und einfach einen Secrets Manager bestellen
- Secrets können über eine benutzerfreundliche Konfigurationsoberfläche und API verwaltet werden
- Nachvollziehbarkeit von Änderungen durch Versionierung einzelner Secrets
- Hochverfügbarkeit gewährleistet den sicheren Betrieb des Secrets Managers
- Vorkonfigurierte Auto-Update-Funktionen halten Komponenten auf dem neuesten Stand

Servicepläne

Der Secrets Manager skaliert automatisch in der Anzahl der Secrets, Secret-Versionen und den Benutzern.

Es gibt folgende Beschränkungen:

- die Anzahl der API-Zugriffe ist je Secrets Manager auf 10.000 Zugriffe pro Stundebeschränkt
- es können je Secrets Manager bis zu 100 Benutzer angelegt werden

- je Secret Version können bis zu 1 MB Text in Form von Key-Value-Paaren hinterlegt werden

Metriken

- Die Abrechnung erfolgt stundengenau nach Anzahl Secret-Versionen.

SLA-Spezifika

- Secrets Manager gilt als verfügbar, sofern die API und die Konfigurationsoberfläche am Leistungsübergabepunkt erreichbar sind.

Backup

- Es findet kein kundenindividuelles Backup statt. Der Secrets Manager speichert automatisch eine vorkonfigurierte Anzahl von Secret-Versionen (standardmäßig unbegrenzt). Wird ein Versionslimit eingestellt und dieses überschritten, werden die ältesten Versionen gelöscht.

Zusätzliche Bedingungen

- Der Kunde ist für die Konfiguration des Secrets Managers verantwortlich (insb. für die Verwaltung von Accounts und vom Versionslimit)

Anhang | Exportierbarkeit

(Online Register)

Datentyp	Beschreibung	Exportierbar (Ja/Nein)	Format	Zusätzliche Anmerkungen
Kundendaten (Datenbank-inhalte)	Daten, die vom Kunden in der Datenbank (sofern vorhanden) bzw. innerhalb des Produktes/Services gespeichert werden	Ja	JSON	Datenexport ist möglich über die Hashicorp Vault kompatible API möglich
Benutzer-konten & Berechtigungen	Informationen über Nutzer und deren Berechtigungen	Ja	JSON	Das Passwort kann nicht exportiert werden
System-Metriken (Instanzen/ Ressourcen in Nutzung)	Leistungsdaten der Instanz/ genutzten Ressource (z. B. CPU-Auslastung, Speichernutzung)	Nein. Betriebsinternum STACKIT.	-	-
	Größen und Kapazitäten *Kapazitäten der vorhandenen Ressourcen / Instanzen*	Ja	JSON	Anzahl Secrets und Versionen
System-eigenschaften (Instanzen/ Ressourcen in Nutzung)	Versionen und Informationen, die notwendig sind, um Kompatibilität prüfen zu können	Nein. Betriebsinternum STACKIT.	-	-
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. Betriebsinternum STACKIT.	-	-
	Log Daten (nicht personalisiert und personalisiert)	Nein. Betriebsinternum STACKIT.	-	-

System-Status, Technical-events, etc.			
Log Daten (nicht personalisiert und personalisiert) *Login/Logout der Nutzer, Nutzeraktivitäten*	Ja	JSON	Events können über die STACKIT Audit Log API exportiert werden