Service Certificate - STACKIT Server Update Management

Service Name
STACKIT Server Update Management

High level service description
The Server Update Management Service ("Server Update Management") permits customers to easily automate their operating system ("OS") update process. The service can be set up by the customer using the comprehensive and easy-to-use management interface or API. The Server Update Management allows the customer to reduce the risk of attacks and breaches by keeping the OS up to date. Automatically installed updates can increase the efficiency of the customer's IT department by reducing routine, manual update-related activities.

Key Features
- Automated cross-OS server update management. Currently supported operating systems:
    - Windows Server
    - Ubuntu
    - Debian
    - CentOS
    - Fedora
    - Rocky Linux
    - AlmaLinux
- Quick and easy enablement of default update schedules
- Advanced update schedules according to individual customer needs
- Possibility of Updates of the OS without the need to login
- Possibility to monitor the updates by the customer via remote

Metric
- Billing per started hour per server for which Server Update Management has been activated by the customer. Billing ends as soon as the customer terminates the Server Update Management or the server assigned to the Server Update Management is deleted.

SLA Specifics
Server Update Management is considered available insofar as the API for update management is accessible at the service delivery point.

Additional Terms
- The customer has to ensure that update schedules which can trigger a server restart after update installation are set according to the needs of the customer.

- The customer has to ensure that scheduled updates of a server do not overlap each other.
- The customer has to ensure that all necessary steps to activate the Server Update Management after the server is created are successfully executed according to the latest documentation
- If the customer uses its own image to create a server and does not use a public image provided by STACKIT, the customer has to check the proper functioning of the Server Update Management in conjunction with the own image.
- Customers are advised to check within the Server Update Management that automatically installed updates have been successfully installed and that the applications running on the VM works properly after the update has been carried out.
- The functions listed under Key Features for the Server Update Management can no longer be provided by STACKIT if:
  - the customer deactivates, deletes or changes the default settings of the STACKIT administration user
  - the customer deletes or changes the certificate/sshkey assigned to the STACKIT administration user
  - the customer changes the firewall settings and deactivates the connection from the local network or the user-defined WinRM-HTTPS listener
  - the customer deletes or changes the additional security groups (if any) associated with the server
  - the customer makes adjustments or changes that prevent STACKIT from accessing the servers
  - the customer deactivates or changes the STACKIT agents installed on the server
  - the customer changes the default update settings of the public images provided by STACKIT
  - the customer uses a server with an operating system which is not part of the supported operating systems listed above

Annex: Exportability (Online Register)

Data Type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data	Metadata of the updates and update schedules.	Yes	JSON	Updates and update schedules metadata can be queried via Server Update Management API.
User Accounts & Permissions	Access to STACKIT project	Yes	JSON	General access to the STACKIT project can be seen in the "IAM and Management" section in the STACKIT Portal.
System Metrics (Instances / Resources in Use)	Sizes and Capacities *Capacities of the available resources / instances*	No	-	STACKIT does not collect data for the size or capabilities of the updates.
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	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	-	STACKIT does not collect data for user activities

Version and start of validity
Version 1.1, valid from 12.09.2025