SERVICE SPECIFICATIONS AND ADDITIONAL CONDITIONS MANAGED CLOUD OPERATING SYSTEM

T-Systems International GmbH

Hahnstr. 43

60528 Frankfurt

Version: 1.44o

Stand: March 5th, 2018

Status: final

Publication Details

Published by

T-Systems International GmbH
Hahnstrasse 43d
60528 Frankfurt am Main, Germany

WEEE reg. no.: DE50335567

Information required by law: https://www.t-systems.com/de/en/compulsory-statement

hereinafter referred to as "Telekom"

Copyright

Confidentiality notice

The customer is obliged to treat the information as well as the knowledge made available to them by way of this document, which they obtain from cooperation based upon this document, for example through matters of a technical, commercial or organizational nature, as confidential and not to use the information and knowledge otherwise or make it accessible to third parties during as well as after the cooperation.

The customer shall ensure that submitted proposals, sample contracts, and individual contracts with their respective appendices, including edited versions, are not fully or partially disclosed to third parties without prior written consent from the publisher.

Table of Contents

1 INTRODUCTION

With the *Managed Cloud Operating System* (MCOS), Telekom provides a managed and IT-supported administration service for server operating systems on cloud platforms. The MCOS service is run largely automatically via a central management zone (CMZ) and additionally by an experienced team of administrators.

The following cloud platforms are supported:

- Open Telekom Cloud (OTC)
- Microsoft Azure (Azure)
- Amazon Web Services (AWS)
- DSI local vCloud

MCOS is a service for server administration, which is independent of the respective cloud platform used and billed separately by Telekom.

2 SERVICES PROVIDED BY TELEKOM

Overview of the MCOS service:

- Registration of the customer for the MCOS service
- Provision of the MCOS operating system image to the customer
- System monitoring, security monitoring, and incident management
- Integrity monitoring for an MCOS instance
- Provision of operating system patches
- Provision of updated MCOS images for new installations
- Granting of temporary privileges to specific customer employees
- International service desk
- Customized meta data via customer tags
- Customized configurations via customer profiles
- Customer Operating Portal

2.1 Provision of MCOS Service and Images

2.1.1 Initial Registration for the MCOS Service

To be able to use the MCOS service, an initial registration process (onboarding) is required, which the customer will complete jointly with its Telekom contact (Service Delivery Manager, Sales Manager). The MCOS activation key (credentials) required for the installation of the MCOS instances will be generated by the Telekom Service Delivery Manager/Sales Manager and made available to the customer. The activation key must be treated as confidential and must not be passed on to third parties.

2.1.2 Provision of the MCOS Images

The MCOS images provided for the installation and/or deployment are "hardened". This means they have been optimized in relation to their security configuration and are provided to the customer via the MCOS download server (if the Microsoft Azure platform technology is used as well as DSL local (vCloud)) or via image sharing (only possible if the Open Telekom Cloud platform technology or the Amazon Web Services platform technology is used). The customer must provide the images in its cloud platform.

The scope of the MCOS service does not include operating system licenses. In other words, the customer must ensure that it has the necessary usage rights (licenses) for the respective operating systems. MCOS supports the following operating system versions:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- SUSE Linux Enterprise 11
- SUSE Linux Enterprise 12
- Red Hat Enterprise Linux 7

These MCOS images can be used on the relevant cloud platform. With help of the MCOS activation key (credentials) the customer can register image-based instances at the MCOS service ("MCOS instances").

2.2 System Monitoring, Security Monitoring, and Incident Management

Telekom will monitor every MCOS Instance of the customer regarding weak points and occurring security events.

Telekom has defined specific thresholds and events for the MCOS services. Thanks to the MCOS service compliance with the services can be monitored as well as events that are important for the servers and operating systems. If there is an event, or if a threshold defined for MCOS is exceeded, an incident (ticket) will opened and the named customer contact is notified by e-mail or phone.

Every instance running under MCOS is monitored for possible vulnerabilities and security events that may occur. The following activities are performed for the running MCOS instances:

- MCOS Windows and Linux instances are:
  - monitored for system and security-related hardware and software configurations and for critical system settings. System and security-related activities are logged.
- MCOS Windows instances additionally run anti-virus protection.

If an event occurs, or if a threshold defined for MCOS is exceeded, an Incident (Ticket) will be opened. Identified misconfigurations on the operating system level are removed by T-Systems. If there is no misconfiguration of the operating system, the customer is provided – if available – with information about the restriction of the malfunction.

Regarding an Incident with the level „critical“ and „high“, the named contact partner of the customer is informed per e-mail or by telephone. The classification is done according to the Incident Management Process of T-Systems.

2.3 Monitoring of the MCOS Instances' Integrity

Furthermore, the MCOS instances are continually monitored by another monitoring system for malicious attacks and unauthorized access, threats, and changes. The following activities are performed:

- Log analysis
- Windows Registry monitoring (Windows Server only)
- Rootkit detection
- Monitoring and logging of the addition and deletion of system files

If a critical event occurs, a ticket is opened. Identified misconfigurations on the operational system level are removed by T-Systems. If there is no misconfiguration of the operational system, the customer - if available – is provided with information used to limit the disorder.

Regarding an Incident of the level „critical“ and „high“ the designated contact partner of the customer is informed by e-mail or by telephone. The classification is done according to the Incident Management Process of T-Systems.

2.4 Provision of Patches

Telekom will provide patches for the MCOS instances on a regular basis. These patches must be installed independently by the customer immediately after they have been provided by Telekom. If need be, the customer can configure an automation of the patch installation by himself.

The patches for the MCOS instances will be made available to the customer via corresponding software distribution servers.

a) Linux patch provision
   - On the first day of every month, all current patches that are published by SUSE will be provided for the relevant operating system.
   - Patches for the removal of operating system vulnerabilities classified as critical by Telekom CERT will be made available directly after they have been released by CERT. The customer must install them immediately in accordance with Telekom's specifications.

b) Windows patch provision
   - The latest Microsoft security patches will be provided every month.
   - Patches for the removal of operating system vulnerabilities classified as critical by Telekom CERT will be made available directly after they have been released by Telekom CERT. The customer must install them immediately in accordance with Telekom's specifications.

2.5 Provision of Updated MCOS Images for New Installations

Updated MCOS images will be provided regularly for new installations of MCOS instances.

a) Linux
   - Updated MCOS images are provided every three months.

b) Windows
   - Updated MCOS images are provided every six months.

2.6 Temporary Privileges

All MCOS instances will be initially provided with standard user rights. The customer may request *temporary privileges* (administrator or root rights) to perform administration tasks. These will be provided for 10 hours from the time of their request.

During the period in which *temporary privileges* are assigned to the customer for an MCOS instance, the SLAs for the MCOS instance will be suspended (i.e., the contractual service quality as described in the next section will not be assured by Telekom) and the monitoring of the instance will be deactivated. During this period, the customer will be responsible for the stability of its MCOS instances and/or for eliminating any problems that may arise in conjunction with the relevant MCOS instance.

If the customer performs activities, that impair or obstruct the operation of the MCOS instance during the period for which it was assigned *temporary privileges*, or should the MCOS instance be impaired or disrupted after this period, Telekom will not provide any further MCOS service for the affected MCOS instance initially until the system has been restored. The SLAs will remain suspended (i.e., the service quality described in the section below will no longer be assured). The activities performed by the customer are deemed the cause of the impairment and/or disruption of the MCOS instance if the impairment and/or disruption occur in a close temporal connection with the assignment of *the temporary privileges* to the customer or if the impairment or disruption is likely to be due to the measures performed by the customer. The customer is free to prove that its activities did not cause the impairments.

In this case, restoring the MCOS instances or eliminating the impairments is not in the scope of services provided by Telekom. The customer can order support services for the restoration of the MCOS instances from Telekom for a separate charge.

2.7 Service Desk

The customer can open incident tickets for one or more of its MCOS instances via Telekom's International Service Desk (ISD).

The service desk can be accessed via the following input channels:

- Telephone: +49 391 5976 2433
- E-mail: cloud-products@telekom.de

When an incident ticket is opened, the customer must keep the following information at hand:

- User details (last name, first name, e-mail address, phone number, company name, department)
- Product name/designation (MCOS, operating system version)
- System affected including the MCOS host name (e.g., mcos998000398xxx)
- Cloud platform used (Open Telekom Cloud, Microsoft Azure, Amazon Web Services, etc.)
- Description of the incident
- Screenshot(s), if available

The service language of the International Service Desk is English.

The tickets opened by the customer are processed according to the incident management process described above.

2.8 Use of the Customer's own Active Directories

The MCOS instances can be integrated into the customer's own Active Directories subject to the requirements listed below:

- The customer must disable the block inheritance, also at GPO level ("block GBP inheritance), of the organizational unit (OU) for all MCOS instances.
- The customer must also ensure that the local administrator ID that is required by Telekom for supporting purposes is not overwritten or impaired by OU rules.
- The customer must in no way override the system management accounts using customer rules.

2.9 MCOS-Support Operating System

The MCOS Service of Telekom is only maximally provided for the respective operating system version of an MCOS Instance on the customer side as long as the manufacturer offers the support for the respective operating system as standard service (i.e. the operating system is still located under “Basic Support” or „General Support“).

2.10 Start and End of the MCOS Service for an MCOS Instance

The MCOS service will be available immediately after the installation of an MCOS instance, i.e., the contractual services will be provided from this date and must be paid for by the customer.

The customer can terminate the MCOS service at any time by running the service deactivation script, see also the "Method for calculating charges" section.

Note: When the MCOS service of a MCOS instance is deactivated, only the provision of services for this MCOS instance will be stopped. The (server) instance and its application data will **not** be deleted by the service deactivation. Nevertheless, Telekom recommends backing up the data for an MCOS instance on other systems before the MCOS service is deactivated.

For technical reasons, it is not possible to reactivate the MCOS service for a MCOS instance that has been terminated.

2.11 Customized Meta Data on Customer Tags

For a better management of the MCOS instances, meta data can be handed over in form of Customer Tags to every instance. Every Customer Tag consists of a name and a value. Thus, explanatory information can be assigned to every MCOS instance. Thus it is e.g. possible to assign every MCOS instance to a cost unit with the help of the assigned Tag (Tag-Name = ”Cost Centre“, Tag-Value = „1123581321“).

2.12 Customized Configurations via Customer Profiles

Customers have the possibility to configure MCOS instances by means of an automation script individually and to carry out software installations automatedly. For this purpose, customers can create automation scripts independently.

After being created, these scripts must be handed over to the International Service Desk per email. Thus, the Service Desk checks the scripts for compliance with the security requirements for MCOS and provides the automation script, if they are compliant, centrally so that the automation scripts can be used on all MCOS instances of the customer.

After the provision of an automation script, the customer can use this on existing or new MCOS instances. If errors should occur during this execution, the customer must correct the automation script and it must be handed over again to the International Service Desk for review and provision.

For the installation of software on the customer-owned MCOS instances by means of the automation script, it is required that the software is available in the customer environment for the executing instance (e.g. via a customer-owned Software Repository).

The support, the review, authorization and installation of the automation scripts will be charged depending on time and effort.

Requirements for the automation scripts are described in the current MCOS User Documentation. Advice for the creation of the automation scripts as well as an error analysis and handling are not part of the Managed Cloud Operating System Service. Appropriate support can be ordered by the customer separately, if need be.

2.13 Customer Operating Portal

Via a Customer Operating Portal, the customer can get an overview of his MCOS use by means of Web Browser. In the following all MCOS instances are listed with

- Host Name
- Status
- Cloud Infrastructure
- Operating System
- IP-Address
- Customer Tags (comp. chapter 2.11)
- Contract ID

The Customer Operating Portal can be reached via the following URL: https://ws-ext.mcos.t-systems-service.com/mcos-customer-portal/

Please use the MCOS activation key (comp. chapter 2.1.1) for login.

3 METHOD FOR CALCULATING CHARGES

3.1 MCOS Instance

The use of the MCOS service will be billed for each individual MCOS instance. Billing of a single MCOS instance starts with the installation of an MCOS instance, which is performed by the customer. In the month of the installation, the monthly usage charge will be billed on a pro rata basis (number of days to the end of the month).

The agreement concerning the individual MCOS instances is concluded indefinitely (but for at least one month) for each MCOS instance and may be terminated by either party at any time from the second month for each individual MCOS instance. The customer gives notice by running the deactivation script while Telekom gives notice by sending an e-mail to the contact appointed by the customer. The charge shall be payable until the end of the month for the month in which the MCSO service has been terminated for the relevant instance.

The charge for the relevant MCOS instance must be paid by the customer during the term of the relevant MCOS instance, irrespective of whether the instance is still being used or has been shut down.

3.2 Temporary Privileges (Admin and Root Rights)

Temporary privileges (granting of 10 hours of admin and root rights) will be charged on a one-time basis per request. The first extension (for another 10 hours) that is requested during the relevant period will be free of charge. Each additional extension will be charged additionally as a one-time amount.

After the relevant time range has ended, the temporary privileges will be deactivated automatically.

3.3 Customized Configurations via Customer Profiles

The support for the creation and testing of automation scripts via Customer Profiles as well as the testing, approval and installation of the automation scripts will be charged according to the effectively carried out working hours.

4 SERVICE QUALITY

4.1 Scope of the MCOS Service

The Telekom services described apply to the MCOS services. The quality of the underlying cloud platform (Open Telekom cloud, Azure cloud platform, Amazon Web Services cloud platform or DSI local vCloud and/or their availability are not considered. In other words, downtimes of the cloud platforms are not considered in relation to the service quality of the MCOS service. Agreements to this effect are the subject matter of separate customer contracts concerning the relevant cloud platform it has chosen.

4.2 Quality Attributes of the MCOS Service

Service Parameters	**Value**
Uptime	Monday – Sunday 24/7
Attended operation time	Monday – Sunday 24/7
Availability of the MCOS service	99.7 per calendar year

4.3 Definition of the Quality Attributes

Definition of operating time:
Period during which the MCOS service is basically available (except for maintenance windows)

Definition of attended operating time:
Period during which the customer can contact Telekom via the hotline (International Service Desk) and during which operating system administrators are basically available for the customer.

Definition of MCOS service availability per calendar year [average availability]	
Calculation of availability as a percentage	The percentage value for the availability of the MCOS service is calculated as follows: $\frac{Planned\ uptime - Downtime\ \ during\ the\ planned\ uptime}{Planned\ uptime} \times 100$ Review period: 1 calendar year, starts on the first day of every calendar year. The following times are not deemed to be downtimes: Maintenance window: three times a year, maintenance windows for twenty-four hours each are permitted for the central MCOS management zone (announced in advance). During this time, the MCOS service functions may not be available or may only be available to a limited extent. Operational security and the functionality of the MCOS instances remain unaffected by this. It may not be possible to newly install or deactivate the MCOS service of an MCOS instance during this time. The availability of the central MCOS Service Zone is decisive. The availability of the central Service Zone is measured and documented by a Business Service Monitoring (BSM) of Telekom.

5 THE CUSTOMER'S DUTIES TO COOPERATE

The customer is obligated to render all cooperation services required for the proper provision of services, particularly however, the following, free of charge, on time, and in the required scope.

5.1 Duties to Cooperate in the Initial Provision

The customer will independently perform the initial MCOS onboarding (see "Registration for the MCOS service" section) together with Telekom Sales or the Service Delivery Manager. The customer will provide all the information required for the onboarding.

5.2 Duties to Cooperate in Terms of Licenses

The customer will obtain all necessary software licenses (e.g., for operating systems, applications, etc.) and other rights to protected content from the licensors or software vendors independently unless Telekom has explicitly taken over the provision of the relevant content and/or licenses as per the contractual documentation.

5.3 Duties to Cooperate during the Usage

- The customer provides the infrastructure resources (CPU, RAM, and storage) on the relevant cloud platform for the MCOS service.
- The customer provides the network bandwidth and/or data volumes required for the provision of the service on the cloud platform.
- The customer provides a permanent Internet connection for every instance that uses the MCOS service.
- The customer provides a dedicated public IP address for each MCOS instance.
- The customer opens the following IP addresses and ports for every MCOS instance for the necessary VPN communication in the direction of the CMZ (everything outgoing from MCOS instances):

IP Addresses	Ports
46.29.97.43	443/tcp
93.188.243.19	1194/udp + 1194/tcp
93.188.243.20	1194/udp + 1194/tcp

- The customer will be responsible for backup activities and, if required, for restore activities relating to the MCOS instance(s).
- Patches must be installed independently by the customer immediately after they have been provided by Telekom. If required, the MCOS instance must be restarted to activate the patches. If these regular patches and boots are not performed, Telekom will be entitled to terminate the provision of the MCOS services for this MCOS instance if any risks occur.
- The customer will appoint one or more qualified contacts for customer support. The nomination will be kept up to date by the customer (fax, e-mail).
- The customer shall only use secure passwords, change them regularly, store them with care, and especially he shall not pass them on to third parties.

- The customer will be responsible for checking and ensuring compliance with any/all legal provisions, laws, regulations, and industry-specific provisions that are relevant and applicable in conjunction with the use of the service. This particularly also includes compliance with confidentiality obligations, for example those resulting from a professional activity. The customer confirms that data or personal data of relevance to confidentiality will only be stored where there is an effective approval.
- If personal data is processed on the customer's behalf (commissioned data processing), the customer will be responsible for concluding CDP agreement with Telekom. Telekom will provide the customer with an agreement for commissioned data processing, if required.

5.4 Maintaining the Integrity of MCOS Instances by the Customer

The subsequent requirements will be met and complied with by the customer, so that the MCOS Services can be provided by Telekom as agreed, and the MCOS Instances will not be damaged. These requirements aim at both stability and integrity of the MCOS Instances. It is crucial for the MCOS Service that the customer meets these requirements. In case of non-compliance by the customer, the quality parameters mentioned in the chapter below „Service Quality“ will not be applicable („SLA-Suspension“).

- The customer must not change the operating system configurations.
- The customer will not make any changes at the local administrator accounts of Telekom, at the MCOS System Management Services, at the system partitions of the servers and the security configurations.
- The customer will not take any measures within the period during which he is assigned *temporary privileged rights* for an MCOS Instance, which enable him to still exercise root- and administrator rights. That means the customer will not create further administrators or respective users, who have permanent root and administrator rights.
- The customer will not install rootkits if changes are made at an MCOS Instance (e.g. regarding installations of software or applications) and sees to it that thus system configurations at this Instance are not changed, which may violate system integrity of the MCOS Instance.
- The customer will not change the MCOS operating system images provided by Telekom, i.e. especially the customer will not integrate or insert files which have not been provided by the MCOS Service into the Operating System Image.

If the preceding requirements are not met, there will be system impairments which are removed by Telekom only upon agreement and against an additional compensation, these do not form part of the MCOS Service.

6 MCOS PRICE LIST

Preiselemente	Preis *	Abrechnungseinheit
MCOS	69,00 €	Monthly remuneration per MCOS Instance
Temporary Privileged Rights	94,50 €	One-time remuneration per call
Support for Customer Profiles	54,00 €	Per hour

* all quotations exclusive currently valid added VAT.

7 GLOSSARY

Term	Description
Activation Key	Also called User Data or Credentials. A pair of values consisting of one value for User and one for Secret, which serves as an activation key during MCOS Server deployment.
CDP	Commissioned data processing (German: ADV/Auftragsdatenverarbeitung)
CPU/vCPU	(virtual) Central Processing Unit
Credentials	Also called User Data or Activation Key. A pair of values consisting of one value for User and one for Secret, which serves as an activation key during MCOS Server deployment.
Deployment	As well OS deployment – this refers to the installation of an operating system (see also OS image) that can run after the deployment, e.g., as a virtual server
GPO	Group Policy Object
IaaS	Infrastructure as a Service
IP	Internet Protocol
ISD	Telekom International Service Desk
MCOS	Managed Cloud Operating System
MCOS Instance	The respective customer operating system running with activated MCOS service
MCOS Onboarding	One-time registration for the MCOS service Must take place together with the Service Delivery Manager or Sales Manager appointed for the customer.
OS	Operating System
OS Image	An operating system with specific configurations that can be installed, copied, or subsequently run (e.g., ISO image)
OU	Organizational unit, e.g., in an Active Directory
RAM/vRAM	(virtual) Random Access Memory. Main memory
SDM	Service Delivery Manager (customer adviser)
SLA	Service Level Agreement
Telekom CERT	Telekom Cyber Emergency Response Team. Internationally responsible for the management of security incidents for all information and network technologies of Deutsche Telekom Group.
User Data	Also called Activation Key or Credentials. A pair of values consisting of one value for User and one for Secret, which serves as an activation key during MCOS Server deployment.