Service Specifications & Additional Terms and Conditions for Managed Cloud Services for Azure

Last revised: March 26, 2019

Publication details

Published by

T-Systems International GmbH

Hahnstrasse 43d

60528 Frankfurt am Main, Germany

WEEE Reg.No. DE50335567

hereinafter referred to as "Telekom"

www.t-systems.de/pflichtangaben/

CONTENTS

1 INTRODUCTION

Azure is a globally available public cloud platform from Microsoft. This platform is currently available in 54 regions worldwide. Telekom provides the customer with Managed Cloud Services for Azure (hereinafter referred to as MCS Azure). This makes it easier for the customer to manage, configure, and operate the customized applications on Azure.

2 OVERVIEW

Telekom Managed Cloud Services for Azure consist of two modules:

"MCS Azure – Foundation": Telekom commissions an Azure policy framework agreed with the customer and manages Azure core resources (virtual network, routing, peering, KeyVault, and – if required – additional resources by agreement) for each defined Azure region in all managed subscriptions. The provisioning and instantiation of managed Azure resource groups and cost reporting is included.

"MCS Azure – Advanced": This is an extension of the "MCS Azure – Foundation" service. Telekom provides and manages Azure Virtual Machines (VM)/operating system instances (OS). The customer can deploy the specified Azure resources via self-service using the Azure Portal or a customized provisioning API (provisioning based on the ARM templates). "MCS Azure Advanced" is activated for each managed subscription.

Telekom deploys managed resource groups on behalf of the customer. With the deployment of the managed resource group, at least two customer AAD identities with agreed authorizations in the IAM function are added to the respective managed resource group. All resources deployed in this managed resource group are given access to the virtual network (if supported by the Azure resource).

MCS Azure is not available in the following Azure regions (Sovereign Cloud Regions): Azure based on Microsoft Cloud Germany (regions: Germany North East and Germany Central), Azure Government, Azure China.

Telekom consulting services and other optional service extensions can be added. These are billed in accordance with the price list (usually on a time and materials basis), see below in the "Optional services" chapter.

3 TELEKOM MCS AZURE – FOUNDATION

3.1 Provisioning/onboarding

3.1.1 Start of project

At the beginning of the provisioning, the setup of the MCS Azure services will be defined by mutual agreement in a workshop and recorded in an engagement plan. The customer defines the customer-specific content here (e.g., policy rules/policies, subscription structure, scope of "Deploy if not exist," and the resources permitted for deployment).

Telekom provides the customer with a script for the initial setup of the managed subscriptions. This gives Telekom access to the Azure Active Directory and managed subscriptions on an administrative level. With the help of this role, Telekom configures all necessary Azure resources in the Azure tenant/subscription. Furthermore, Telekom will create further roles in the Azure tenant/subscription in consultation with the customer. These roles have limited privileges and are used by Telekom (for automatisms).

3.1.2 Setting up standard monitoring

Telekom defines a standard monitoring system and agrees how and with what measures Telekom should react to certain notifications from the monitoring system. Extended, customer-specific monitoring can be ordered as an optional service.

3.1.3 Setting up standard reporting

Telekom defines a standard reporting system. Costs in managed subscriptions and MCS Azure costs are mapped in Azure Cost Control. Standard reporting is based on the collected monitoring data from standard monitoring. An Azure Dashboard represents the standard reporting. The compliance status of policies is shown in the standard reporting.

Extended, customer-specific reporting can be ordered as an optional service.

3.1.4 Subscription configuration – basic setup (landing zone)

For each managed subscription, Telekom deploys the Azure policies agreed with the customer and defines the rights and naming conventions for the managed subscription. Management resources follow a fixed naming scheme, and so do resource groups. Telekom manages the subscription and configures Azure AD/IAM subscription in the sense of "on behalf." The configuration takes place in the customer-specific Azure tenant.

Microsoft operates Azure in different regions. Telekom configures these different regions in consultation with the customer. This includes providing management resources used and managed by MCS Azure (Recovery Vault, KeyVault, vNets, peerings, network security groups, Azure Automation, and others). Access to these resources – after mutual agreement by the customer or by Telekom – is secured via Azure AD roles and subscription rights & role assignment.

All Azure resources provided to the customer are defined as Infrastructure as Code and are stored in a secure, verified environment that complies with Telekom security standards.

3.1.5 Provision of MCS Azure services

Telekom's service begins with the customer setting up the access rights in the managed subscriptions. The MCS Azure Services will be deemed to have been provided when the access rights are set up in the managed subscriptions and will be invoiced from the date the aforementioned access rights have been set up.

3.2 Foundation operation

The "MCS Azure – Foundation" framework regularly checks the compliance of deployed resources with the defined policies. In the event of non-compliance, Telekom initiates measures to remedy the non-compliance.

Telekom uses Azure Log Monitor to monitor the vNet function in the managed subscriptions. If errors occur during vNet operation, Telekom starts troubleshooting during service times.

Furthermore, Telekom provides managed resource groups during the service times shown below.

4 TELEKOM MCS AZURE – ADVANCED: MANAGEMENT OF VIRTUAL VM/OS

"Telekom MCS Azure – Advanced" is an extension to the "Telekom MCS Azure – Foundation" module and therefore requires the "Telekom MCS Azure – Foundation" for each managed subscription. The module is provided and configured per managed subscription.

4.1 Provisioning/onboarding

Telekom provides managed Azure virtual machines (VM)/operating system (OS) instances in a managed resource group. When the managed VM/OS instances are provided, Azure plugins are installed for the secure operation by Telekom of those VM/OS instances. For Windows systems, the Azure Antimalware extension is also installed.

The inclusion of VM/OS instances in MCS Azure can be ordered by the customer subject to the following specifications:

- Microsoft supports Windows and Linux OS instances as described under the links below: Windows/Linux.
- Within the framework of MCS Azure Advanced, Telekom only provides Windows OS/Linux OS instances for which Microsoft/Linux distributors offer an Azure Marketplace image.
- The customer can only order the provision of such Windows OS/Linux OS instances (or the plugins for them) if these are compatible in accordance with the Terms and Conditions for Microsoft Support.
- The following link shows the Linux images that are supported by Microsoft Azure: Linux

Additional functions can be included as an option, see the following chapter on optional services.

The linked documents are always valid in the most current version.

Customer applications should be compatible with Azure Availability Sets and Azure Availability Zones so that the customer can claim the standard credits promised by Microsoft in the event of non-compliance with the SLAs. Therefore, managed VM/OS are provided by Telekom for virtual machines in line with the Azure platform SLA i.e., in accordance with the following table. Data and OS disks always use the Managed Disk feature.

Microsoft defines the following three SLA classes for its services. Accordingly, the number of OS instances and the appropriate storage type are defined as follows in the respective Telekom template:

VM SLA	Min. no. of VM/OS instances	Memory type
99.9%	1	Premium SSD
99.95%	2	Standard SSD
99.99%	2	Standard SSD

The Windows administrator account name/Linux root account name and associated passwords are stored in an Azure KeyVault and are protected by access rules.

Managed Azure VM/OS are assigned automated tags for differentiation. The tags to be used are agreed with the customer. Telekom reserves 10 tags for its own operation. The managed resource group passes on the tags to the managed VM/OS.

Telekom will provide the VM/OS after the customer has commissioned it to do so.

Telekom's "MCS Azure – Advanced" service begins with the customer setting up the access rights in the managed subscriptions. The MCS Azure Advanced services will be deemed to have been provided when the access rights are set up in the managed subscriptions and will be invoiced from the date the aforementioned access rights have been set up.

4.2 VM/OS backup

Managed Azure VM/OS are automatically added to an Azure Recovery vault and an Azure backup plan. The default backup plan is agreed in advance with the customer and implemented in the managed subscriptions. A dedicated Azure Recovery vault is created for each managed resource group. The standard plan is defined in the managed subscription.

Telekom monitors the execution of the planned backups and initiates troubleshooting in the event of an incident.

4.3 Access to virtual networks and the internet

Telekom ensures that managed OS/VM have access to a subnet (only to the resources suitable for this) and that name resolution and IP routing work are agreed with the customer. VM/OS instances receive dynamic IP addresses from this subnet. The DNS server configuration defined at the time of provisioning is used. Internet access (outbound) cannot be restricted. Access to the subnet is only possible via port 3389 (for Windows) or port 22 (for Linux).

Further required ports can be ordered as part of a change and/or modified by authorized users (at the customer).

4.4 VM/OS patching with Azure Automation Patch Management

Telekom ensures that the managed VM/OS receive quality and security updates in accordance with the policies published by Microsoft/the respective Linux distributor. Telekom adds the managed VM/OS instances to a specific patch plan. There is no pre-qualification (application compatibility) or patch selection. For Windows VM/OS, Telekom starts the Windows Update function at specified intervals. For Linux, the distribution-specific update mechanism is configured with Azure Patch Management and the OS update function is started at specified intervals.

Possibly necessary reboots of the OS are always executed after the installation by the Windows Update/Linux Update mechanism. Emergency patches are not included in the price as a standard service, but are ordered as an optional service in consultation with the customer and billed separately.

The customer can carry out his patch management independently by arrangement.

4.5 Provision of Windows/Linux provisioning templates and API interface

Telekom provides Azure ARM templates for use by the customer. These templates simplify self-service provisioning of Windows/Linux VM/OS. Furthermore, these templates will ensure that the infrastructure is provided in compliance with the Azure platform SLA, including in the self-service in Azure. In the Standard version, up to 15 OS templates can be defined for the customer. All defined templates are also available via an authenticated API. Telekom manages access to the API.

5 STANDARD MONITORING AND REPORTING

5.1 Standard monitoring

Telekom uses Azure Log Monitor to monitor VM/OS values (heartbeat/availability, vCPU utilization, memory utilization, disk IOPS, disk fill level), backup statuses, patch compliance status, framework compliance status, and the virtual network in Azure and defines thresholds as well as responses to threshold violations.

For VM/OS, the Azure Log Monitor extension for Windows/Linux is installed for each instance and connected to a Log Monitor Workspace in the managed subscription. The above monitoring and associated log records are collected in the same Log Monitor Workspace.

In consultation between Telekom and the customer, an additional 20 values or values deviating from the standard can be monitored and responded to.

Standard monitoring can be extended as an optional service.

5.2 Standard reporting

5.2.1 Dashboard

Telekom provides a simple view of the collected standard monitoring data via the Azure Dashboard functionality.

5.2.2 Cost reporting

Telekom provides 10 user accounts for "Azure Cost Control." The customer receives full cost transparency about his spend in Azure. "Azure Cost Control" does not require Azure RBAC user rights in the managed subscriptions. Costs can be easily analyzed and measures can be derived. The following standard scope of services is provided:

- Azure Cost Control application access for 10 AAD identities
- Standard views of spend
- Filter on the views
- Memory function for view filter
- Team administration
- Cost alerts
- Daily email report

Costs are displayed on the basis of the contract currency. "Azure Cost Control" is included and the product's scope of service within the framework of these Service Specifications cannot be changed. Telekom reserves the right to provide the cost reporting with another product/SaaS solution.

6 OPERATIONS SUPPORT

6.1 Reporting incidents/changes/orders

Reports can be addressed to the Service Desk in German and English on a 24/7 basis. The following options are available:

- By email to: cloud-products@telekom.de
- By phone: +49 391 5976 2433

6.2 Processing of reported incidents

Incidents are classified by Telekom and processed according to criticality, taking into account the following service KPIs:

- Critical incident/event: impact on the availability of an MCS Azure service and critical business impact at the customer
- Non-critical event: all other requests

Telekom reserves the right to change the criticality if the preliminary classification made by the customer does not comply with the above requirements.

Service KPIs:

Service parameter		Description
Response time		4 hours
Resolution time		as soon as possible
Service hours	Critical events	Non-critical events
	Mon - Sun 24/7 (CET/CEST)	Mon. - Fri. 8:00 a.m. - 5:00 p.m. (CET/CEST)

7 CHANGE MANAGEMENT

7.1 Standard changes

Change requests can be ordered via the Service Desk as shown above. The following standard changes are included in the "MCS Azure – Foundation" module per month.

Standard change	Included
Provide managed resource group	All

The following standard changes are included in the "MCS Azure – Advanced" module per month.

Standard change	Included
Provide managed VM/OS	All
Disk change/disk addition*	10
Patch plan change	3
Backup plan change	3
Change network security group	3
Change size of instance (SKU/VM size)	11

*The customer is responsible for increasing the size of file systems in the OS. A reboot is always required after the change.

Additional changes will be invoiced separately (see price sheet).

7.2 Restore

"MCS Azure – Advanced" supports the restore of VM backups held in Azure Backup/Recovery Vault.

- Complete restore including VM definition

- Disk restore
- Folder/file restore per disk

Restore operations are ordered via the Service Desk. Restore orders are charged separately in accordance with the price sheet.

8 REQUIREMENTS AND OBLIGATIONS TO COOPERATE

By commissioning MCS Azure services, the customer agrees to the following measures and specifications:

- Consent to the automated, software-defined provision of Azure resources and provision of necessary authorizations in the customer's Azure tenant and in the associated MCS Azure-managed subscriptions by Telekom
- Use of Azure services and the associated costs in all managed subscriptions by Telekom
- Deposit of the Microsoft Partner ID of Telekom, as well as access and rights assignment to all Azure API interfaces (authorization) in all managed tenants/subscriptions by the customer
- Use, registration, and administration of additional groups/function users/applications by Telekom
- Use of Azure Cost Control
- Administration of the subscriptions by Telekom so that Telekom can configure the Azure AD/IAM subscription in the sense of "on behalf" in the customer's own Azure tenant
- Cross-tenant management and data transfer between customer tenants and Telekom administration tenants
- Change of technologies to manage the tenant/subscriptions during the term of the contract

In all other respects, the customer undertakes to cooperate in order to ensure proper provision of the required services; in particular, he is obligated to provide the following services free-of-charge, on-time, and to the required extent:

- The customer ensures the sufficient licensing of all OS instances at Microsoft/the Linux distributors.
- The customer concludes a support contract with Microsoft for Azure (Premier Support). The customer enables Telekom to use Microsoft's support services.
- The customer names contacts who can make the necessary decisions and apply settings.
- The customer provides all information about the existing infrastructure (IP address ranges, network connections, DNS, Active Directory. and others) immediately from the beginning of the project and answers Telekom's inquiries immediately.
- If the customer has a local Windows Active Directory, he will synchronize it with Azure Active Directory.
- The customer is not entitled to delete authorizations/resource groups/AAD groups/service principles/configurations set up by Telekom or for Telekom during the term of the contract.
- The customer assigns access rights (roles & authorizations) to the Azure Portal/API in consultation with Telekom.
- Together with Telekom and for each managed subscription, the customer defines Azure Policies, rights relating to the managed subscription, and naming conventions.
- The customer ensures the uniqueness of virtual machine names and associated host names across regions in his ordering process.

- All changes are requested or commissioned by the customer in accordance with the agreed change process.
- The customer is responsible for checking whether the data transferred by him in connection with the use of the service is personal data and whether processing this personal data is permissible. To the extent that the customer wishes personal data to be processed, the customer will sign an agreement on the processing of personal data based on the Telekom sample agreement, which Telekom will provide to the customer upon request.

9 AZURE FRAMEWORK CONDITIONS

The prerequisite for the provision of services by Telekom is an existing Azure contractual relationship between the customer and Microsoft. Telekom's MCS Azure Services are based on the Microsoft Public Cloud Azure and its platform functions provided by Microsoft. Telekom's performance is therefore dependent on Microsoft's performance; in this regard, reference is made to the applicable Microsoft Azure Online Service Terms and/or the service level agreements described by Microsoft. The services provided by the public cloud service provider (Microsoft) and the logical and physical services below the public cloud platform, including the hypervisor layer and the hardware devices making up the public cloud platform, are not the subject of Telekom's performance and any failures or malfunctions are not the responsibility of Telekom.

Microsoft reserves the right to limit the functionality of the Microsoft platform temporarily or permanently. The platform also defines threshold values/maximum execution intervals that cannot be exceeded. Microsoft documents these restrictions and limitations here: https://docs.microsoft.com/de-de/azure/azure-subscription-service-limits . Telekom's services are subject to the framework conditions specified by Microsoft. Adjustments to performance by Microsoft may also lead to the need to adjust Telekom's performance.

The customer can also obtain the Azure platform service from Telekom. This service is not part of MCS Azure and would have to be ordered by the customer within the framework of a separate contractual relationship.

10 OPTIONAL SERVICES

10.1 Billing on a time-and-materials basis

The customer can order the following optional services/extension of the scope of services from Telekom. These are invoiced monthly on the basis of the hourly rates stated in the price sheet.

- Azure Solution Architect consulting services
- Migration and transformation consulting and implementation of migration and transformation projects
- Emergency patch installation
- Extensions of MCS Azure standard monitoring and reporting
- Customer-specific provision of a Windows OS/Linux OS image not available in Azure Marketplace
- Azure cost optimization service
- Other customized templates for Windows/Linux
- Administration of application software (prerequisite: the customer ensures sufficient licensing of the application software used in Azure and concludes support agreements with the manufacturers, which Telekom can use).
- Extension of the MCS Azure Services by additional functions:
  - Windows: automatic Active Directory/Azure Active Directory Domain Services Join
  - Linux: SSH/Azure Active Directory user authentication

10.2 Additional user accounts for cost reporting

Additional user accounts for cost reporting will be charged in accordance with the fee stated in the price sheet.

11 RIGHTS OF USE FOR AUTOMATION TOOLS

The customer only receives a simple, non-transferable, non-sublicensable right to use the automation tools/scripts created by Telekom for MCS Azure, including all extensions specially created for the customer, for the contractually intended purposes limited to the term of the contract.

12 INVOICE

The customer will receive a monthly invoice from Telekom for the MCS Azure service on the basis of the charges shown in the price sheet.

13 TERM

A minimum lease period, which ends one calendar year after the end of the calendar month in which the respective module was provided, applies to the two MCS Azure modules (i.e., the "MCS Azure – Foundation" and "MCS Azure – Advanced" modules respectively).

The ordered modules can be terminated by the customer in writing for the first time by observing a period of notice of 2 (two) calendar months with effect from the end of the minimum lease period. Otherwise, the term of the respective module will be extended indefinitely and may then be terminated in writing by giving 2 (two) calendar months' notice with effect from the end of a calendar month.

14 GLOSSARY

A
AAD: Azure Active Directory AD: Windows Server Active Directory Administrator: user account with high-level administrative rights Azure Marketplace: a function of Azure. Platform for the publication of services and software products ARM: Azure Resource Manager ARM template: description files for the deployment/administration/update of Azure resources Azure: public cloud service of Microsoft Azure Cost Control: Telekom SaaS Service to present current Azure spend
B
C
D
Dashboard: configurable Azure resource type for the presentation/reporting of Azure resource states Deployment: provision, instantiation of Azure resources Disk/vHD: file that stores the contents of a (virtual) hard disk and is stored in Azure

E

F

Framework: see Policies/Framework

G

H

I

IaC/Infrastructure as Code: files, software that map the infrastructure in Azure in code
IAM: Identity and Access Management
Instantiation: putting into operation, providing in Azure

J

K

KeyVault: Azure resource type for secure storage of secrets

L

M

MCS: Managed Cloud Services

N

NSG/Network Security Group: Azure resource type for the restriction of vNets and activation on IP ports

O

OS: Operating System

P

Patch/Patch management: quality or function updates for operating systems. Orderly process for applying patches
Policies/framework: summary of individual rules in a framework. Technical term: policy
Provisioning: see Deployment

Q

R

Framework: see Policies/framework
RBAC/Role-Based Access Control: Azure authorization concept for controlling access to Azure resources
Rights: see RBAC
Recovery Vault: storage area in Azure that is used for backup data
Region(s): Microsoft data center locations where Azure resources can be provided
Resources: all functions/features in Azure are referred to an Azure resources
Resource group: Azure administration unit. Bundles Azure resources
Restore: Data restore
Roles: see RBAC
root: Linux: highest-level administrative user in a Linux OS

S

Secret: Key values
SKU/Stock Key Unit: order number
Subscription: security and cost container in Azure, administration unit
SLA: Service Level Agreement

T

Tags: short descriptions/values to classify/identify an Azure resource more easily
Tenant: Azure Active Directory namespace and administration unit of AAD

U

V

VM: Virtual Machine
VNIC: Virtual Network Interface Controller
vNet: Virtual network in Azure

X

Y

Z