wortell

Service Description

Mission Critical Azure

7 december 2021

Table of contents

1 Introduction

1.1 Constantly in motion

Microsoft Azure is a service from Microsoft that is constantly in motion. We are constantly adapting our services to the services of Microsoft Azure. As a result, we may have to adjust our service description during the period that we provide our services to you. Our starting point is that we always offer a service that remains at least the same or offers an equal experience.

1.2 References

1.2.1 Quote

This document is part of the agreement between Wortell and your organization. The modules that are included in the quote issued by Wortell are part of the scope of the service. Modules from the Service Description that are not mentioned in the quotation are not part of the service. Additional modules can be added via your Account Manager, who will provide you with an additional quote.

2 Mission Critical Azure

Mission Critical Azure also known as MCA is a secure, managed and automated cloud product based on Microsoft Azure. Mission Critical Azure provides a secure, up-to-date, cost and performance optimized Azure Datacenter for all your infrastructure systems and applications (IaaS and PaaS) on the Microsoft Azure platform.

The solutions developed by MCA, such as update management, start/stop systems, monitoring and alerting, etc. are designed, built and implemented from an "infrastructure as a code" perspective. The core value of all these solutions are: Fast, reliable, quality, uniformity and optimized for performance. The management will therefore mainly be done from Azure DevOps. This ensures more grip on the environment. Where possible, we will also apply IaC when deploying existing and new resources.

MCA includes the Pulse module. Pulse is the smart monitoring, automation and surveillance system that enables the management team to provide up to 24x7 supervision of the managed resources, so that the continuity of the environment is guaranteed. MCA offers different choices on the Pulse module whereby it is possible to classify resources according to their importance for your organisation.

MCA provides a secure environment where the IaaS environment is always up-to-date and protected against external vulnerabilities for both Windows OS and Linux OS. With the support of Microsoft Defender for Cloud, the environment is tested for vulnerabilities. The environment will be tested on a regular basis on the most important standards such as the CIS Framework, where MCA ensures that the environment always has a secure and compliant infrastructure.

MCA provides a continuous cost and performance optimized environment. Systems are evaluated on sizing and usage. This will ensure that you don't pay too much for the purchased resources, and that the systems and applications perform as efficiently as possible.

Wortell provides technical support for MCA. This technical support consists of troubleshooting if the services described in this Service Description no longer function as expected.

What we don't do:

- Functional management on databases
- Functional application management
- Investigating cyber attacks or security monitoring alerts
- Managing Azure Active Directory

MCA consists of a number of components:

- Azure out of the box management
- Subscription Management
- CIS baseline testing
- Microsoft Defender for Cloud Management
- Network management
- Backup management
- Patch management

- Monitoring - Wortell Pulse
- Resource management
- Azure SQL management
- App Service Management
- Azure Kubernetes Service Management
- Data Factory management
- Azure Service Bus Management
- Azure cache for Redis management
- Azure firewall management
- Azure Frontdoor Management
- Application Gateway (WAF) management
- Azure Loadbalancer management
- VPN Gateway management
- Express Route Circuit Management
- Virtual WAN management

3 Azure out of the box management

The Landing zone in Azure is the foundation of the Azure environment, the bare data center. Wortell has a standard way of creating a Landing Zone called "Azure out of the Box". This way we make sure the foundation is secure and compliant with the requirements of the customer, all based on Microsoft's best practices.

With our Landing zone management we ensure that an environment remains safe and compliant. Landing zone management is the basis for managing the environment in Azure.

Subscription management, CIS Baseline, security center and network management fall under Landing zone management.

3.1 What do we do for you?

Landing zone management includes the following activities:

- Security management (including arranging IAM, Policies and Management Groups, PIM for Azure resources)
- Capacity planning (including Azure reservations, right-sizing advice)
- Cost management (including right-sizing advice, orphaned resources, Azure reservations, start-stop automation)

Monthly meeting with an engineer to discuss reports from CIS, security center and Azure advisor.

3.2 What else do you do?

Together with our engineers, assess which reports and changes have the highest priority.

3.3 Added value

The landing zone managed by Wortell is maintained in accordance with security, governance and compliancy best practices. This means that if in the future better practices are advised by, for example, Microsoft, we will also implement these improvements (in consultation with the customer) on the environment managed by us.

4 Subscription Management

An Azure subscription is an agreement with Microsoft for the use of one or more Microsoft cloud platforms or services, for which charges are made on the basis of per-user license fees or on resource consumption on the Cloud.

Microsoft Azure Subscriptions are the logical entities within which Azure resources can be deployed. Azure subscriptions are always associated with one Azure Active Directory tenant, but an Azure Active Directory tenant can have multiple Azure subscriptions under it.

4.1 What do we do for you?

Part of Azure subscription management includes the following activities:

- Escalation to Microsoft (including use of Wortell premier support if customer is registered as DPOR)
- Subscription provisioning (including creating new subscriptions under the Wortell CSP contract.

4.2 What else do you do?

If subscriptions have to be purchased via EA or PAYG, you arrange these subscriptions yourself and delegate the further management of these subscriptions to Wortell's MCA team.

4.3 Added value

The subscriptions managed by Wortell are designed and maintained according to security, governance and compliancy best practices. Together with the landing zone, changes in best practices will be implemented in consultation with the customer. Well-organized subscriptions are the most important basis for further success in the Microsoft Azure Cloud.

5 CIS Baseline

The Center for Internet Security (CIS) is a non-profit organization whose mission is to identify, validate, promote and maintain best-practice solutions related to cybersecurity. CIS has published a "CIS MS Azure Foundations Benchmark" for users who want to develop, deploy, assess or secure secure solutions in Azure. If the guidelines of this.

5.1 What do we do for you?

On a frequent basis we make a report regarding the status of the CIS compliancy within your subscriptions. This report is then discussed by the Product Delivery Manager from team MCA with for example IT responsible or CISO. We advise on all points found and make suggestions on which steps the environment can become fully compliant.

5.2 What else do you do?

Make the IT manager, CISO or similar available for periodic consultation on the CIS baseline. Review and discuss findings and approve possible (non-standard) changes that arise from CIS baseline advice. You can also indicate which exceptions you want to make to the CIS baseline and are therefore no longer required for further reporting.

5.3 Added value

As a customer, you always have an environment that meets the CIS security guidelines. The percentage of compliance does of course depend on the choices you make as to which measures you choose to implement or not. The periodic report also provides for audit assessments by external parties.

6 Security Center Management

Microsoft uses a wide range of physical, infrastructure, and operational controls to secure Azure, but there are additional actions you should take to protect your workloads. Enable Azure Security Center to improve the status of your cloud security. Use Azure Defender in Azure Security Center to secure your hybrid cloud workloads.

6.1 What do we do for you?

We assess the secure score given by Security Center on a monthly basis and will act pro-actively or in an advisory capacity when findings are made. If this results in non-standard changes, this will always be discussed with the customer by an MCA Product Delivery Manager and provided with context.

6.2 What else do you do?

Reviewing the recommended improvements and approving (non-standard) changes to improve the secure score.

6.3 Added value

We always strive to keep a customer's environment as secure and compliant as possible. Security advice is therefore of great importance to both the customer and the management party in order to keep the environment safe and available.

7 Network management

Azure Virtual Network (VNet) is the basic building block for your private network in Azure. VNet allows many types of Azure resources, such as virtual Azure machines, to securely communicate with each other, the Internet, and on-premises networks. VNet is similar to a traditional network you would run in your own data center, but it also offers the benefits of Azure's infrastructure, such as scale, availability, and isolation.

7.1 What do we do for you?

We manage the configured virtual networks in the Azure subscription(s), as well as the subnets within those networks and the Network Security Groups that can be set up on them.
We also manage any User-Defined Route tables and Service endpoints.

7.2 What else do you do?

Management of local and/or other networks connected to the Azure VNET(s). Request changes if the design of the Azure VNET(s) needs to be adjusted, for example extension of Subnets or adjustments in Network Security Groups.

7.3 Added value

Wortell is fully responsible for the operation of the VNET(s) in Azure. No knowledge is required from the customer regarding the operation of Virtual Networks in Azure.

7.4 Pricing

Includes with Landing zone and subscription management module.

7.5 Standard changes

- Request changes on Network Security Groups
- Request changes on Subnet (add, delete or modify)
- Requesting or adding changes to Service Endpoints
- Requesting changes to VNET Peering/VNET to VNET connectivity

8 Backup Management

We use Azure Backup to provide stable and secure backups of your workloads. Azure Backup is a cost-effective, secure, one-click backup solution that scales based on your backup storage needs. The centralized management interface makes it easy to define backup policies and secure a wide range of enterprise workloads, including Azure Virtual Machines, SQL and SAP databases, and Azure file shares.

8.1 What do we do for you?

We provide correctly designed backup policies, based on the wishes of the client. Furthermore, we monitor the progress of these backups and will intervene/report on the moment a backup failed unexpectedly. Furthermore, we have periodic checks of backup/restore functionalities by performing (automated) backup/restore tests. You can also request a restore of a machine over or next to the existing machine at any time, for example in case of loss of individual files within a server.

8.2 What are you still doing up?

In consultation with Wortell you take care of the retention and recovery requirements.

8.3 Added value

Your backups are executed by Wortell MCA, monitored and restored when necessary.

9 Patch management

Software Updates in Azure Automation Update Management provides a set of tools and resources that allow Wortell to manage the complex task of tracking and applying software updates to machines in Azure and hybrid Cloud. An effective software update management process is required to maintain operational efficiency, resolve security issues and reduce the Risk of Cyber-attacks. Due to the changing nature of technology and the constant emergence of new security threats, effective management of software updates requires consistent and continuous attention.

9.1 What do we do for you?

- Review and install Operating System Hotfixes
- Review and installation of monthly security patches
- Daily Windows Defender updates
- Actively monitor the success of the above updates through our monitoring system

9.2 What else do you do?

You will install application specific hotfixes and patches (with or without vendor support). If the applications are managed by Wortell Services, then Wortell will take care of these tasks.

9.3 Added value

An up-to-date environment where 'malware' cannot exploit security vulnerabilities in Windows Software.

10 Monitoring - Wortell Pulse

Wortell Pulse is our smart monitoring and automation platform. The resources within Azure that are used to build your environment, are monitored 24x7 for signals and alerts from Azure, based on the policies and tools we set up.

Pulse uses algorithms to spot any peculiarities and/or deviations. Such an anomaly is immediately brought to the attention of our standby team, who can then determine whether this could potentially become an incident. If this is the case, an incident can be prevented or at least detected in time.

10.1 What do we do for you?

A report is sent out proactively and picked up when Pulse detects something. This enables us to solve (potential) incidents quickly, sometimes even before they occur. In this way we can optimally guarantee the continuity of the environments we manage.

We also automatically check our monitoring platform every night and resolve any anomalies. This ensures that if resources are added that do not comply with our policy, they are automatically brought in line with our monitoring standards.

10.2 What else do you do?

Sign off on incidents or changes.

10.3 Added value

Wortell is constantly working to identify potential disruptions before they occur. We also continue to develop the platform.

11 Resource management

11.1 IAAS VM

A virtual machine is a computer file (usually called an installation copy) that behaves like a real computer. In other words, a computer is created within another computer. Azure offers a wide variety of types of VMs as well as configuration options. From simple single VMs to complex high-availability Virtual Machine in availability zones and sets. For every type of workload there is a fitting VM.

11.1.1 What do we do for you?

- We set up Azure VMs according to best-practices in the field of logging/monitoring, configuration, disk encryption etc.
- We deploy the VM according to the standard naming convention.
- We deploy the VM in a Subnet of the customer's choice
- We monitor the VM for compliance with the Secure Baseline from CIS (from an IaaS perspective).
- We monitor the VM for compliancy with the Microsoft Secure Baseline for content design of the VM itself.

We always provide a compliant/hardened VM image upon initial delivery of the VM.

11.1.2 What else do you do?

You are responsible for everything from OS level upwards. This means the functional and applicative setup of the server, setting and adjusting security settings within the server etc. It is also possible to purchase this service from Wortell Services/WORK.

11.1.3 Added value

Virtual Machines delivered by Wortell always meet the agreed naming convention and security baseline. After that you are free to configure the server as you wish. We then include the VM in monthly assessments in the area of security & compliancy, capacity management etc.

Standard changes

- Expanding existing Azure VM Data disks
- Restart, shutdown or enable existing Virtual Machines
- Restoring an existing VM (see also backup data management)
- Adjusting the sizing of an existing VM (vertical scaling)

11.2 Azure SQL Server

Azure SQL Database server, part of the Azure SQL family, is the intelligent, scalable, relational database service built for the cloud. The evergreen database service is always up-to-date, with AI-powered and automated features that optimize performance and sustainability for you.

11.2.1 What do we do for you?

- We set up the Azure SQL server according to best practices in the field of logging/monitoring, configuration, encryption of data and any auditing rules.
- We deploy the Azure SQL server according to the standard naming convention.
- We provide the Azure SQL server with network configuration as required: Public, Private endpoint or Service Endpoints
- We monitor the Azure SQL server for compliance with the secure Baseline and from the CIS framework.
- We take care of the backup frequency and retention (in consultation)

11.2.2 What else do you do?

In consultation with Wortell you agree on a good backup strategy.

11.2.3 Value added

Azure SQL servers that are delivered by Wortell always meet the agreed naming convention and best practices in the field of security & compliancy. The servers are then managed by Wortell and may or may not include auto-scaling settings to grow with the customer's usage needs.

11.2.4 Standard changes

- Adjustments in auditing settings
- Adjustments in the (server side) encryption settings
- Creating a new Azure SQL Database Server (excluding databases
- Adjustments in SQL Server network/firewall settings

11.3 Azure SQL Database

Azure SQL Database is a fully managed PaaS (platform as a service) database engine that automates most database management functions, such as upgrades, patches, backups and monitoring.

11.3.1 What do we do for you?

We set up empty databases and ensure that these databases end up under the correct Azure SQL Database server.

11.3.2 What else do you do?

Entering/importing the correct data into the empty databases.

11.3.3 Added value

Azure SQL databases delivered by Wortell always comply with the agreed naming convention and best practices in the field of security & compliancy.

11.3.4 Standard changes

- Adjustments to Geo-replica settings
- Adjustments in the sizing/SKU (horizontal, vertical or elastic pole)
- Adjustments in Auditing Settings
- Adjustments to the encryption settings

11.4 Azure Cosmos DB

Azure Cosmos DB is a fully managed NoSQL database service (platform as a service) that automates most database management functions such as upgrades, patches, backups and monitoring.

11.4.1 What do we do for you?

- We set up the Azure Cosmos DB resource according to best-practices in the field of logging/monitoring and infrastructural configuration.
- We deploy the Azure Cosmos DB resource according to standard naming convention.
- We set up empty database collections
- We activate global data replication if required
- We arrange any network integration and / or private endpoint configuration

11.4.2 What else do you do?

Entering/importing the correct data into the empty database collections

11.4.3 Added value

Azure Cosmos DB databases delivered by Wortell always comply with the agreed naming convention and best-practices in the field of security & compliancy. ,

11.4.4 Standard changes

- Adjustments to Geo-replica settings
- Adjustments in the Sizing/SKU (Throughput)
- Adjustments in Backup & Restore settings
- Adjustments in Network/Private endpoint configuration

11.5 App Service Plans

Azure App Service Plans is the definition of a set of computer resources suitable for running web apps. You can compare an App Service Plan to a virtual machine, specified in a certain size, with Microsoft-managed software on it to run web apps.

11.5.1 What do we do for you?

- We set up the Azure App Service Plans according to best practices in the field of logging/monitoring, configuration and possible VNET integration.
- We deploy the Azure App Service Plans according to standard naming convention.
- We monitor the App Service Plans on compliancy with the Secure baseline and from the CIS framework.

11.5.2 What else do you do?

Wortell takes care of everything concerning App Service Plans.

11.5.3 Added value

Azure Apps Service Plans that are delivered by Wortell always meet the agreed naming convention and best practices in the field of security & compliancy. The App Service Plans are then managed by Wortell and may or may not include auto-scaling settings to grow with the customer's usage needs.

11.5.4 Standard changes

- Adjustments in the sizing/SKU (horizontal or vertical)
- Adjustments in Network Settings (integration with e.g. Azure VNET)

11.6 App Services

App Services is probably the most widely used resource type in the Azure Cloud. A webapp makes it possible to host web applications in Azure. Both frontend and backend applications are possible.

11.6.1 What do we do for you?

- We set up the Azure App Services in accordance with best practices in the field of logging/monitoring, configuration and possible VNET integration.
- We deploy the Azure App Services in accordance with the standard naming convention.
- We monitor the App Services for compliance with the Secure baseline and from the CIS framework.
- Setting up backup processes
- Adding custom domain name settings
- Adding and replacing SSL Certificates

11.6.2 What else do you do?

- Release or deploy the web application to the Azure App Service. Making adjustments to server side configuration parameters (e.g. .NET version, connection strings etc).
- The optional monitoring of Application Performance (APM) by deploying, for example, Azure Application Insights or another APM solution.
- Requesting and delivering to Wortell the SSL certificates for the web applications in PFX format.

11.6.3 Added value

Azure Apps Services delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the App Service.

11.6.4 Standard changes

- Adjustments in backup settings
- Adjustments to TLS/SSL settings
- Adjustments in Size/SKU (horizontal or vertical)
- Creating (extra) Deployment slots

11.7 Azure Kubernetes Service (per instance)

Azure Kubernets Service is a managed Kubernetes service that allows you to quickly deploy and manage Kubernetes clusters.

11.7.1 What do we do for you?

- We set up the Azure AKS according to best-practices in the field of logging/monitoring and configuration (including namespaces, node pools etc.)
- We deploy the AKS in accordance with the standard naming convention.
- We monitor AKS for compliance with the Secure baseline and from the CIS framework.

11.7.2 What else do you do?

Deploying the workloads to the AKS cluster. Building and maintaining the containers themselves.

11.7.3 Added value

Azure Kubernets Service(s) delivered by Wortell always meet the agreed naming convention and best practices in the field of security & compliancy. The AKS are then managed by Wortell, with or without auto-scaling settings to grow along with the customer's usage needs. The AKS infrastructure is managed and monitored by Wortell (including the nodes).

11.7.4 Standard changes

- Adjustments to the Cluster Configuration/Kubernetes release
- Adjustments in Size/SKU/Scale
- Adjustments in Network settings (http application routing, IP whitelisting)
- Adjustments in Storage settings (Volumes)
- Adjustments to Services & Ingress settings

11.8 Data Factory

Azure DataFactory is a fully managed, serverless data integration solution for ingesting, preparing and transforming all your data at scale.

11.8.1 What do we do for you?

- We set up Azure DataFactory resource according to best practices in logging/monitoring and infra configuration.
- We deploy the Azure DataFactory according to the standard naming convention.
- We monitor the Azure DataFactory for compliance with the Secure baseline and from the CIS framework.

11.8.2 What else do you do?

Functional design of the Azure DataFactory.

11.8.3 Added value

Azure DataFactory that are delivered by Wortell always meet the agreed naming convention and best-practices in the field of security and compliancy. We also monitor the infrastructural performance of the Azure DataFactory, including Integration Runtime CPU & Memory and any deviations from expected pipeline runs.

11.9 Azure Service Bus

Azure ServiceBus is the trusted messaging as a service (MaaS) in the cloud, providing easy hybrid integration. Use Service Bus when you need a highly reliable cloud messaging service between applications and services, even when they are offline.

11.9.1 What do we do for you?

- We set up Azure ServiceBus resource according to best practices in logging/monitoring and infra configuration.
- We deploy the Azure ServiceBus in accordance with the standard naming convention.
- We monitor the Azure ServiceBus for compliancy with the Secure baseline and from the CIS framework.

11.9.2 What else do you do?

The functional set up of the Azure Service Bus

11.9.3 Added value

Azure ServiceBus that are delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the Azure ServiceBus, including server/User errors, abandoned messages etc.

11.10 Azure cache for Redis

Azure Cache for Redis provides data storage in memory based on the Redis software. Redis improves the performance and scalability of applications that use back-end data stores. It can handle large volumes of application requests by storing frequently used data in server memory for fast writing and reading. Redis is an essential low-latency, high-throughput data storage solution for modern applications.

11.10.1 What do we do for you?

- We set up the Azure Cache for Redis resource according to best-practices in the field of logging/monitoring and infra configuration.
- We deploy the Azure Cache for Redis according to the standard naming convention.
- We monitor the Azure Cache for Redis resource for compliance with the Secure baseline and from the CIS framework.

11.10.2 What else do you do?

Functional design of the Azure Cache for Redis. Think of TLS version, memory policies, Scale and Cluster sizes. Of course Wortell can help you with this.

11.10.3 Added value

Azure Cache for Redis delivered by Wortell always complies with the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of Azure Cache for Redis, including CPU, Used Memory, Errors and Server Load.

12 Connectivity and Firewall components

Within Azure there are several possibilities to arrange connectivity and firewalling. Within MCA-management, we use the Microsoft solutions, which are described below.

12.1 Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a full stateful firewall as a service with built-in high availability and unlimited cloud scalability.

12.1.1 What do we do for you?

- We set up the Azure Firewall in accordance with best practices in the field of logging/monitoring, configuration
- We deploy the Azure Firewall according to the standard naming convention.
- We monitor the Azure Firewall for compliance with the Secure baseline and from the CIS framework.
- We manage any assigned Azure Firewall Policies

12.1.2 What else do you do?

Functional management: evaluating Threat alerts from the Threat Intelligence option of the firewall as well as composing the application firewall rules. The management and follow-up of alerts can also be performed by Wortell's Managed Detection & Response (MDR) team.

12.1.3 Added value

Azure Firewall that are delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the App Service.

12.1.4 Standard Changes

- Adjustments to the Rules (Classic)
- Adjustments to the Firewall Manager/Firewall Policies
- Modifications to the Public IP configuration

12.2 Azure Frontdoor

Azure Frontdoor is a - on Microsoft global edge network - deployed entrance to a.o. web applications. Azure Frontdoor is infinitely scalable, fast and has additional Web Application Firewall functionalities and Content Caching close to the users of the application.

12.2.1 What do we do for you?

- We set up the Azure Frontdoor according to best-practices in the field of logging/monitoring, configuration
- We deploy the Azure App Services in accordance with the standard naming convention.
- We monitor the App Services for compliance with the Secure baseline and from the CIS framework.
- We manage any assigned Web Application Firewall rules

12.2.2 What else do you do?

Helping decide on the design/requirements for the front door, with regard to the backend, distribution of traffic flows and supplying the necessary SSL certificates. In addition, also thinking about the design of any Web Application Firewall rulesets.

12.2.3 Added value

Azure Frontdoor(s) delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. The Frontdoor(s) are then managed and monitored by Wortell.

12.2.4 Standard changes

- Replacement of SSL Certificates
- Adjustments in Front Door designer (backend/frontend/rule configuration)
- Modifications to assigned WAF rules.

12.3 Application Gateway (WAF)

Azure Application Gateway is a web traffic load balancer that allows you to manage traffic to your web apps. Traditional load balancers operate at the transport layer (OSI Layer 4 - TCP and UDP) and route traffic based on IP source address and a source port to a destination IP address and port. Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example, URI path or host headers (OSI layer 7)

12.3.1 What do we do for you?

- We set up Azure Application Gateway in accordance with best practices in the field of logging/monitoring, configuration
- We deploy the Azure Application Gateway according to the standard naming convention.
- We monitor the Azure Application Gateway for compliance with the Secure baseline and from the CIS framework.

12.3.2 What else do you do?

- Request and delivery of required SSL certificates in PFX format
- Participate in deciding the (possible) Web Application Firewall rules

12.3.3 Added value

Azure Application Gateway that are delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the Application Gateway and the backend pools.

12.3.4 Standard Changes

- Adjustments in backend pools
- Adjustments in http settings
- Adjustments in Listeners
- Adjustments in Frontend IP configuration
- Adjustments to AGW routing rules

12.4 Azure Loadbalancer

Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. This is the single point of contact for clients. The Load Balancer distributes incoming flows that arrive at the front-end of the load balancer for back-end address group. These flows are based on configured load balancing rules and status checks. The instances of the back-end address group can be Azure virtual machines or instances in a scale-set for virtual machines.

12.4.1 What do we do for you?

- We set up Azure LoadBalancer in accordance with best practices in the field of logging/monitoring, configuration
- We deploy the Azure Loadbalancer according to the standard naming convention.
- We monitor the Azure LoadBalancer for compliance with the Secure baseline and from the CIS framework.

12.4.2 What else do you do?

Nothing

12.4.3 Standard Changes

- FrontendIP configuration changes
- Backend Pool configuration changes
- Adjustments to load balancing rules
- Adjustments to Inbound NAT rules

12.4.4 Added value

Azure Loadbalancer(s) delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the LoadBalancer and the backend pools.

12.5 VPN Gateway (including VPN connection)

A VPN gateway is a special type of virtual-network gateway that is used to send encrypted traffic between a virtual Azure network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

12.5.1 What do we do for you?

- We set up Azure VNET/VPN gateway according to best-practices in the field of logging/monitoring, configuration
- We deploy the Azure VNET/VPN gateway according to the standard naming convention.
- We monitor the Azure VNET/VPN gateway for compliance with the Secure baseline and from the CIS framework.

12.5.2 What else do you do?

- Creating new Site-to-Site tunnels on the on-premises side of the tunnel; and/or
- Arranging contact details of other third parties with whom tunnels between Azure and that particular site(s) must be established

12.5.3 Standard Changes

Creation of new Site-to-Site tunnels on the Azure side

12.5.4 Added value

Azure VPN Gateway(s) delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the Application Gateway and the availability of defined Site-to-Site VPN tunnels.

12.6 Express Route Circuit & Connections

Azure ExpressRoute is used to create private connections between Windows Azure data centers and infrastructure at your site or in a co-location environment. ExpressRoute connections do not run over the public Internet and offer greater reliability, faster speeds, and shorter latencies than typical Internet connections.

12.6.1 What do we do for you?

We monitor the availability of the Express Route Circuit & Connections that run over the Express Route Circuit. We can also measure (maximum) usage to ensure that no bottlenecks occur in the selected connection speed of the ExpressRoute connections.

12.6.2 What else do you do?

Arranging any on-premises or non-Azure data center connectivity. Monitoring the connectivity from that side of the connection.

12.6.3 Added value

Azure ExpressRoute circuit(s) and connections delivered by Wortell always meet the agreed naming convention and best practices in the field of security & compliancy. We monitor the availability of the connection(s) and fulfil the SPOC role in case of connectivity incidents.

12.7 Virtual WAN

Azure Virtual WAN is a network service that brings together a wide range of network, security and routing functions to provide a single operational interface. These features include branch connectivity (via connectivity automation of Virtual WAN Partner devices such as SD-WAN or VPN CPE), site-to-site VPN connectivity, connectivity via VPN for remote users (point-to-site), personal connectivity (ExpressRoute), intra-cloud connectivity (transitive connectivity for virtual networks), VPN-ExpressRoute interconnectivity, routing, Azure Firewall and encryption for personal connectivity.

12.7.1 What do we do for you?

- We set up the Azure Virtual WAN in accordance with best-practices in the field of logging/monitoring, configuration
- We deploy the Azure Virtual WAN in accordance with the standard naming convention.
- We monitor the Azure Virtual WAN for compliancy with the Secure baseline and from the CIS framework.
- We monitor VWAN connections including Site-to-Site, ExpressRoute connections and Hub-to-VNET connections

12.7.2 What else do you do?

Arranging any on-premises or non-Azure data center connectivity. Monitoring connectivity from that side of the connection. Setting up point-to-site VPN tunnels if they are needed by users.

12.7.3 Added value

Azure Virtual WAN delivered by Wortell always meet the agreed naming convention and best practices in the field of security and compliancy. We also monitor the infrastructural performance of the service.

13 Service levels on Resources

The content of this Service Description follows the agreements that are made in the general SLA/XLA that was made between Wortell and your organization. In the SLA/XLS you will find the service windows and response times.

The resources that we monitor for you are offered in 3 tiers. These tiers are described below. The 3 tiers are equal to the priorities 1, 2 and 3 from the SLA/XLA.

13.1 SLA Gold

This SLA is for business-critical production workloads that are important to the organisation 24x7. The resources with this SLA are proactively monitored 24x7 by Pulse and in the event of an incident or notification where an engineer is required, the engineer on duty will receive an alert from Pulse to resolve the incident.

The response- and lead times are equivalent to a Prio 1 as laid down in the SLA/XLA.

13.1.1 What do we do for you?

In the event of an incident on a Gold resource, Pulse automatically forwards the notification to the engineer on duty who confirms the notification and then starts working on it.

13.1.2 Added value

A quick response from a skilled Azure engineer who solves the problem with the business critical resource.

13.2 SLA Silver

This SLA is for critical workloads that are important to the organisation during business hours. The resources with this SLA are proactively monitored by Pulse 24x7 and in the event of an incident or notification where an engineer is required, the engineer will receive an alert from Pulse during business hours to resolve the incident.

The response- and lead times are equivalent to a Prio 2 as laid down in the SLA/XLA.

13.2.1 What do we do for you?

In the event of an incident on a Silver resource, Pulse automatically forwards the notification to the engineer on duty. The engineer confirms the report and starts working on it.

13.2.2 Added value

A quick reponse from a skilled Azure engineer who solves the problem with the critical resource within office hours.

13.3 SLA Bronze

This SLA is for standard and/or non-critical (development/test) workloads during business hours. The resources with this SLA are proactively monitored 24x7 by Pulse and in the event of an incident or report that requires an engineer, the engineer receives an alert from Pulse during office hours to resolve the incident.

The response- and lead times are equivalent to a Prio 2 as laid down in the SLA/XLA.

13.3.1 What do we do for you?

In the case of an incident on a Bronze resource, Pulse automatically forwards the notification to the engineer on duty and he acknowledges the notification. The maximum resolution time we aim for is equal to the level 3 incident n

13.3.2 Added value

A reponse from a skilled Azure engineer who solves the problem with the resource within office hours. A substantive response is provided within 2 working days and the maximum resolution time we aim for is 5 working days.