wortell

Service Description

Mission Critical Azure

7 december 2021

Inhoudsopgave

1 Inleiding 7

1.1 Constant in beweging 7

1.2 Verwijzingen 7

1.2.1 Prijsopgave 7

2 Mission Critical Azure 8

3 Azure out of the box beheer 10

3.1 Wat doen we voor je? 10

3.2 Wat doe je nog zelf? 10

3.3 Toegevoegde waarde 10

4 Subscription beheer 11

4.1 Wat doen we voor je? 11

4.2 Wat doe je nog zelf? 11

4.3 Toegevoegde waarde 11

5 CIS Baseline 12

5.1 Wat doen we voor je? 12

5.2 Wat doe je nog zelf? 12

5.3 Toegevoegde waarde 12

6 Security Center beheer 13

6.1 Wat doen we voor je? 13

6.2 Wat doe je nog zelf? 13

6.3 Toegevoegde waarde 13

7 Netwerk beheer 14

7.1 Wat doen we voor je? 14

7.2 Wat doe je nog zelf? 14

7.3 Toegevoegde waarde 14

7.4 Prijsstelling 14

7.5 Standaard changes 14

8 Backup Management 15

8.1 Wat doen we voor je? 15

8.2 Wat doen je nog zelf? 15

8.3 Toegevoegde waarde 15

9 Patch management 16
9.1 Wat doen we voor je? 16
9.2 Wat doe je nog zelf? 16
9.3 Toegevoegde waarde 16

10 Monitoring – Wortell Pulse 17
10.1 Wat doen we voor je? 17
10.2 Wat doe je nog zelf? 17
10.3 Toegevoegde waarde 17

11 Resource beheer 18
11.1 IAAS VM 18
11.1.1 Wat doen we voor je? 18
11.1.2 Wat doe je nog zelf? 18
11.1.3 Toegevoegde waarde 18
11.2 Azure SQL Server 19
11.2.1 Wat doen we voor je? 19
11.2.2 Wat doe je nog zelf? 19
11.2.3 Toegevoede waarde 19
11.2.4 Standaard changes 19
11.3 Azure SQL Database 20
11.3.1 Wat doen wij voor je? 20
11.3.2 Wat doe je nog zelf? 20
11.3.3 Toegevoegde waarde 20
11.3.4 Standaard changes 20
11.4 Azure Cosmos DB 21
11.4.1 Wat doen wij voor je? 21
11.4.2 Wat doe je nog zelf? 21
11.4.3 Toegevoegde waarde 21
11.4.4 Standaard changes 21
11.5 App Service Plans 22
11.5.1 Wat doen wij voor je? 22
11.5.2 Wat doe je nog zelf? 22

11.5.3 Toegevoegde waarde 22
11.5.4 Standaard changes 22
11.6 App Services 23
11.6.1 Wat doen we voor je? 23
11.6.2 Wat doe je nog zelf? 23
11.6.3 Toegevoegde waarde 23
11.6.4 Standaard changes 23
11.7 Azure Kubernetes Service (per instance) 24
11.7.1 Wat doen we voor je? 24
11.7.2 Wat doe je nog zelf? 24
11.7.3 Toegevoegde waarde 24
11.7.4 Standaard changes 24
11.8 Data Factory 25
11.8.1 Wat doen we voor je? 25
11.8.2 Wat doe je nog zelf? 25
11.8.3 Toegevoegde waarde 25
11.9 Azure Service Bus 26
11.9.1 Wat doen we voor je? 26
11.9.2 Wat doe je nog zelf? 26
11.9.3 Toegevoegde waarde 26
11.10 Azure cache for Redis 27
11.10.1 Wat doen we voor je? 27
11.10.2 Wat doe je nog zelf? 27
11.10.3 Toegevoegde waarde 27

12 Connectivity en Firewall componenten 28
12.1 Azure Firewall 28
12.1.1 Wat doen we voor je? 28
12.1.2 Wat doe je nog zelf? 28
12.1.3 Toegevoegde waarde 28
12.1.4 Standaard Changes 28
12.2 Azure Frontdoor 29
12.2.1 Wat doen we voor je? 29

12.2.2 Wat doe je nog zelf? 29
12.2.3 Toegevoegde waarde 29
12.2.4 Standaard changes 29
12.3 Application Gateway (WAF) 30
12.3.1 Wat doen we voor je? 30
12.3.2 Wat doe je nog zelf? 30
12.3.3 Toegevoegde waarde 30
12.3.4 Standaard Changes 30
12.4 Azure Loadbalancer 31
12.4.1 Wat doen we voor je? 31
12.4.2 Wat doe je nog zelf? 31
12.4.3 Standard Changes 31
12.4.4 Toegevoegde waarde 31
12.5 VPN Gateway (inclusief VPN connectie) 32
12.5.1 Wat doen we voor je? 32
12.5.2 Wat doe je nog zelf? 32
12.5.3 Standard Changes 32
12.5.4 Toegevoegde waarde 32
12.6 Express Route Circuit & Connections 33
12.6.1 Wat doen we voor je? 33
12.6.2 Wat doe je nog zelf? 33
12.6.3 Toegevoegde waarde 33
12.7 Virtual WAN 34
12.7.1 Wat doen we voor je? 34
12.7.2 Wat doe je nog zelf? 34
12.7.3 Toegevoegde waarde 34

13 SLA – Service levels op Resources 35
13.1 SLA Gold 35
13.1.1 Wat doen we voor je? 35
13.1.2 Toegevoegde waarde 35
13.2 SLA Silver 35
13.2.1 Wat doen we voor je? 35

13.2.2 Toegevoegde waarde 35
13.3 SLA Bronze 35
13.3.1 Wat doen we voor je? 36
13.3.2 Toegevoegde waarde 36

1 Inleiding

1.1 Constant in beweging

Microsoft Azure is een dienst van Microsoft die constant in beweging is. Wij passen onze dienstverlening dan ook constant aan op de diensten van Microsoft Azure. Hierdoor kan het zijn dat wij onze dienstbeschrijving gedurende de periode dat wij onze diensten aan u leveren aan moeten passen. Onze uitgangspositie is dat wij daarbij altijd een dienst bieden die minimaal gelijk blijft of een gelijke ervaring biedt.

1.2 Verwijzingen

1.2.1 Prijsopgave

Dit document is onderliggend aan de overeenkomst tussen Wortell en uw organisatie. De modules die zijn opgenomen in de prijsopgave die Wortell heeft uitgebracht, zijn onderdeel van de scope van de dienstverlening. Modules uit de Service Description die niet zijn vermeld in de prijsopgave, zijn geen onderdeel van de dienstverlening. Additionele modules kunnen via uw Accountmanager worden toegevoegd, deze zal daarvoor een aanvullende prijsopgaaf uitbrengen.

2 Mission Critical Azure

Mission Critical Azure ook wel MCA genoemd is een veilig, beheerd en geautomatiseerd cloud-product op basis van Microsoft Azure. Mission Critical Azure zorgt voor een veilig, up-to-date, kosten en performance geoptimaliseerd Azure Datacenter voor al uw infrastructurele systemen en applicaties (IaaS en PaaS) op het Microsoft Azure platform.

De door MCA ontwikkelde oplossingen, zoals updatemanagement, start/stop systeem, monitoring en alerting etc. worden vanuit een “infrastrucure as a code” gedachtegoed ontworpen gebouwd en geïmplementeerd. De kernwaarde van al deze oplossingen zijn: Snel, betrouwbaar, kwaliteit, uniformiteit en geoptimaliseerd voor performance. Het beheer zal dan ook voornamelijk worden uitgeoefend vanuit Azure DevOps. Dit zorgt voor meer grip op de omgeving. Waar mogelijk zullen wij ook IaC toepassen bij het deployen bij bestaande en nieuwe resources.

MCA bevat de module Pulse. Pulse is het slimme monitoring, automation en bewakingssysteem dat het beheerteam in staat stelt om tot 24x7 toezicht op de beheerde resources te verzorgen, zodat de continuïteit van de omgeving wordt gewaarborgd. MCA biedt verschillende keuzes aan op de module Pulse waarbij het mogelijk is om op maat resources in te delen in de mate van het belang voor uw organisatie.

MCA verzorgt een veilige omgeving waarbij de IaaS-omgeving altijd up-to-date is en beveiligd tegen kwetsbaarheden vanuit buitenaf voor zowel het Windows OS als het Linux OS. Met ondersteuning van Microsoft Defender for Cloud wordt de omgeving getoetst op kwetsbaarheden. De omgeving zal op regelmatige basis getoetst worden op de meest belangrijke normen zoals het CIS Framework, waarbij MCA zorgt dat de omgeving altijd een zo secure en compliant mogelijke infrastructuur heeft.

MCA verzorgt continue een kosten en performance geoptimaliseerde omgeving. Waarbij systemen worden beoordeeld op sizing en verbruik. Hiermee zal er niet te veel betaald worden voor de afgenomen resources, en zal er zorg worden gedragen dat de systemen en applicaties zo efficiënt mogelijk performen.

Wortell levert technische ondersteuning voor MCA. Deze technische ondersteuning bestaat uit het oplossen van problemen indien de in deze Service Description beschreven diensten niet meer naar verwachting functioneren.

<u>Wat doen we niet:</u>

- Functioneel beheer op databases
- Functioneel applicatie beheer
- Het onderzoeken van cyber aanvallen of security monitoring alerts
- Het beheer van de Azure Active Directory

MCA bestaat uit een aantal onderdelen:

- Azure out of the box beheer
- Subscription beheer
- CIS baseline toetsing
- Microsoft Defender for Cloud beheer

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

3 Azure out of the box beheer

De Landing zone in Azure is het fundament van de Azure omgeving, het kale datacenter. Vanuit Wortell hebben we een standaard manier van het neerzetten van een Landing zone genaamd “Azure out of the Box”, hiermee zorgen we dat deze basis veilig en compliant is aan de eisen van de klant en alles op basis van best-practises van Microsoft.

Een omgeving is bij oplevering veilig en compliant, met ons Landing zone beheer zorgen we ervoor dat deze omgeving veilig en compliant blijft. Landing Zone beheer is de basis voor het beheer van de omgeving in Azure.

Subscription beheer, CIS Baseline, security center en netwerkbeheer vallen onder Landing zone beheer.

3.1 Wat doen we voor je?

Onderdeel van landing zone management zijn o.a. de volgende activiteiten:

- Beveiligingsmanagement (waaronder het regelen van IAM, Policies en Managementgroups, PIM voor Azure resources)
- Capaciteitsplanning (waaronder Azure reservations, right-sizing advies)
- Kosten management (waaronder right-sizing advies, orphaned resources, Azure reservations, start-stop automation)

Maandelijkse bespreking met een engineer om meldingen van CIS, security center en Azure advisor te bespreken.

3.2 Wat doe je nog zelf?

Samen met onze engineers beoordelen welke meldingen en wijzigingen het meeste prioriteit hebben.

3.3 Toegevoegde waarde

De door Wortell gemanagede landing zone wordt conform security, governance en compliancy best practices onderhouden. Dat wil zeggen dat als er in de toekomst betere practices worden geadviseerd vanuit bijvoorbeeld Microsoft wij die verbeteringen ook (in overleg met de klant) zullen doorvoeren op de door ons beheerde omgeving.

4 Subscription beheer

Een Azure subscription is een overeenkomst met Microsoft voor het gebruik van een of meer Microsoft cloudplatformen of-services, waarvoor kosten worden berekend op basis van licentiekosten per gebruiker of op het resourceverbruik op de Cloud.
Microsoft Azure Subscriptions zijn de logische entiteiten waarbinnen Azure resources ge-deployed kunnen worden. Azure subscriptions zijn altijd gekoppeld aan één Azure Active Directory tenant, maar een Azure Active Directory tenant kan meerdere Azure subscriptions onder zich hebben.

4.1 Wat doen we voor je?

Onderdeel van Azure subscription management zijn o.a. de volgende activiteiten:

- Escalatie naar Microsoft (waaronder gebruik van Wortell premier support indien klant geregistreerd staat als DPOR)
- Subscription provisioning (waaronder het aanmaken van nieuwe subscriptions onder het Wortell CSP contract.

4.2 Wat doe je nog zelf?

Indien de subscriptions via EA of PAYG aangeschaft moeten worden, regelt u deze subscriptions zelf en delegeert u het verdere beheer van die subscriptions aan team MCA van Wortell.

4.3 Toegevoegde waarde

De door Wortell gemanagede subscription worden conform security, governance en compliancy best practices ingericht én onderhouden. Samen met de landing zone zullen veranderingen in best-practises ook hier worden doorgevoerd in overleg met de klant. Goed ingerichte subscriptions zijn de belangrijkste basis voor een verder succes in de Microsoft Azure Cloud.

5 CIS Baseline

De Center for Internet Security (CIS) is een non-profit organisatie met als missie om best-practice oplossingen m.b.t cybersecurity te identificeren, valideren, promoten en onderhouden. CIS heeft een “CIS MS Azure Foundations Benchmark” gepubliceerd voor gebruikers die veilige oplossingen in Azure willen ontwikkelen, neerzetten, beoordelen of beveiligen. Als de richtlijnen van dit.

5.1 Wat doen we voor je?

Op frequente basis maken wij een rapportage m.b.t. de status van de CIS compliancy binnen uw subscriptions. Deze rapportage wordt vervolgens besproken door de Product Delivery Manager vanuit team MCA met bijvoorbeeld IT verantwoordelijke of CISO. Wij adviseren op alle gevonden punten en doen suggesties aan de hand van welke stappen de omgeving volledig compliant kan zijn/worden.

5.2 Wat doe je nog zelf?

IT verantwoordelijke, CISO of soortgelijke verantwoordelijke beschikbaar stellen voor periodiek overleg m.b.t. de CIS-baseline. Beoordelen en bespreken van bevindingen en goedkeuren van mogelijke (non-standard) changes die voortvloeien vanuit CIS-baseline advies. Tevens kunt u aangeven welke uitzonderingen u op de CIS-baseline wil maken en dus niet meer benodigd zijn voor verdere rapportages.

5.3 Toegevoegde waarde

Als klant heeft u altijd een omgeving die voldoet aan de CIS-security richtlijnen. Het percentage van compliant zijn hangt uiteraard wel af van de keuzes die u maakt welke maatregelen u wel of niet kiest om te implementeren. Het periodieke rapport voorziet verder in audit beoordelingen vanuit externe partijen.

6 Security Center beheer

Microsoft gebruikt een breed scala aan fysieke, infrastructurele en operationele besturingselementen om Azure te beveiligen, maar er zijn extra acties die u moet ondernemen om uw werkbelastingen te beschermen. Schakel Azure Security Center in om de status van uw cloudbeveiliging te verbeteren. Gebruik Azure Defender in Azure Security Center om uw hybride cloud workloads te beveiligen.

6.1 Wat doen we voor je?

Wij beoordelen op maandelijkse basis de secure score die vanuit Security Center wordt gegeven en zullen proactief of adviserend handelen bij bevindingen. Indien dit resulteert in non-standard changes, zal dit altijd door een MCA Product Delivery Manager met de klant worden besproken en van context worden voorzien.

6.2 Wat doe je nog zelf?

Het beoordelen van de geadviseerde verbeteringen en goedkeuren van (non-standard) changes om de secure score te verbeteren.

6.3 Toegevoegde waarde

Wij streven er altijd naar om een omgeving van een klant zo secure en compliant mogelijk te houden. Security adviezen zijn dus zowel voor klant als beheerpartij van groot belang om op te voeren om de omgeving veilig en beschikbaar te houden.

7 Netwerk beheer

Azure Virtual Network (VNet) is de basisbouwsteen voor uw privénetwerk in Azure. Via VNet kunnen veel soorten Azure-resources, zoals virtuele Azure-machines, veilig communiceren met elkaar, internet en on-premises netwerken. VNet is vergelijkbaar met een traditioneel netwerk dat u in uw eigen datacentrum zou uitvoeren, maar biedt daarnaast de voordelen van de infrastructuur van Azure, zoals schaal, beschikbaarheid en isolatie.

7.1 Wat doen we voor je?

Wij beheren de geconfigureerde virtuele netwerken in de Azure subscription(s), evenals de subnets binnen die netwerken en de Network Security Groups die daarop ingesteld kunnen worden.
Ook beheren wij eventuele User-Defined Route tables en Service endpoints.

7.2 Wat doe je nog zelf?

Management over lokale en/of andere netwerken welke gekoppeld zijn aan de Azure VNET(s). Veranderingen aanvragen indien het design van de Azure VNET(s) moet worden aangepast, bijvoorbeeld uitbreiding Subnets of aanpassingen in Network Security Groups.

7.3 Toegevoegde waarde

Wortell is volledig verantwoordelijk voor de werking van de VNET(s) in Azure. Er is geen kennis nodig bij de klant m.b.t. de werking van Virtuele netwerken in Azure.

7.4 Prijsstelling

Inclusief bij Landing zone- en subscription beheer module.

7.5 Standaard changes

- Wijzigingen aanvragen op Network Security Groups
- Wijzigingen aanvragen op Subnet (toevoegen, verwijderen of aanpassen)
- Wijzigingen aanvragen op Service Endpoints of toevoegen hiervan
- Wijzigingen aanvragen op VNET Peering/VNET to VNET connectivity

8 Backup Management

Wij maken gebruik van Azure Backup om op een stabiele en veilige manier uw workloads van backups te voorzien. Azure Backup is een voordelige, veilige back-upoplossing met één klik die schaalbaar is op basis van wat u nodig hebt aan back-upopslag. Met de gecentraliseerde beheerinterface kunt u eenvoudig back-upbeleid definiëren en een breed scala aan bedrijfswerkbelastingen beveiligen, met inbegrip van Azure Virtual Machines, SQL- en SAP-databases en Azure-bestandsshares.

8.1 Wat doen we voor je?

Wij verzorgen correct ingerichte backup policies, op basis van de wensen van de klant. Verder monitoren wij het verloop van deze backups en zullen wij ingrijpen/rapporteren op het moment dat een backup onverhoopt niet gelukt is. Verder hebben we periodieke controles van backup/restore functionaliteiten door het uitvoeren van (geautomatiseerde) backup/restore tests. U kunt tevens te allen tijde een restore van een machine aanvragen over of naast de bestaande machine heen, bijvoorbeeld bij verlies van individuele bestanden binnen een server.

8.2 Wat doen je nog zelf?

In overleg met Wortell zorgt u voor de retentie en recovery vereisten.

8.3 Toegevoegde waarde

Uw backups worden door Wortell MCA uitgevoerd, gemonitord en ge-restored indien nodig.

9 Patch management

Software-updates in Azure Automation Updatebeheer biedt een set hulpprogramma's en resources waarmee Wortell de complexe taak voor het bijhouden en toepassen van software-updates op machines in Azure en hybride Cloud kunt beheren. Er is een effectief beheerproces van software-updates nodig om operationele efficiëntie te behouden, beveiligingsproblemen op te lossen en de Risico's van verhoogde beveiligingsrisico's voor Cyber-aanvallen te verminderen. Wegens de veranderende aard van technologie en het permanent opduiken van nieuwe veiligheidsbedreigingen, vergt effectief beheer van software-updates consistente en continue aandacht.

9.1 Wat doen we voor je?

- Beoordeling en installatie van Operating System Hotfixes
- Beoordeling en installatie van maandelijkse security patches
- Dagelijkse Windows Defender updates
- Actief monitoren van het slagen van bovenstaande updates via ons monitoringsysteem

9.2 Wat doe je nog zelf?

Je doet de installatie van applicatie specifieke hotfixes en patches (al dan niet met ondersteuning van een leverancier). Indien de applicaties door Wortell Services worden beheerd, dan zal Wortell deze taken op zich nemen.

9.3 Toegevoegde waarde

Een up-to-date omgeving waarbij ‘malware’ geen gebruik kan maken van beveiligingslekken in Windows Software.

10 Monitoring – Wortell Pulse

Wortell Pulse is ons slimme monitoring en automation platform. De resources binnen Azure waarmee jullie omgeving is opgebouwd, worden op basis van door ons ingestelde policies en tools 24x7 bewaakt op signalen en meldingen uit Azure. Pulse maakt gebruik van algoritmes om hier in bijzonderheden en of afwijkingen te zien. Zo'n afwijking wordt direct onder de aandacht gebracht van ons stand-by team, die dan kan bekijken of dit potentieel een incident kan worden. Is dit het geval zal een incident kunnen worden voorkomen of in ieder geval tijdig gesignaleerd.

10.1 Wat doen we voor je?

Er wordt pro-actief een melding uitgestuurd en opgepakt wanneer Pulse iets signaleert. Hierdoor kunnen we (potentiële) incidenten spoedig oplossen soms zelfs voor ze ontstaan. Op deze manier kunnen we de continuïteit van de door ons beheerde omgevingen optimaal waarborgen.

Ook controleren we automatisch iedere avond ons monitoring platform en worden afwijkingen daarop opgelost. Hierdoor zorgen we ervoor, dat als er resources worden toegevoegd welke niet aan ons beleid voldoen, dat deze dan automatisch in lijn worden gebracht met onze monitoring standaarden.

10.2 Wat doe je nog zelf?

Sign off geven van incidenten of changes.

10.3 Toegevoegde waarde

Wortell is constant bezig om potentiële verstoringen te signaleren voor ze ontstaan. Tevens blijven we het platform door ontwikkelen.

11 Resource beheer

11.1 IAAS VM

Een virtuele machine is een computerbestand (meestal een installatiekopie genoemd), dat zich als echte computer gedraagt. Er wordt met andere woorden een computer gemaakt binnen een andere computer. Azure biedt een grote verscheidenheid aan type VM's alsmede configuratie mogelijkheden aan. Van simpele enkelvoudige VM's tot complexe hoog-beschikbare Virtuele Machine in beschikbaarheidszones en sets. Voor iedere type workload is er wel een bijpassende VM te vinden.

11.1.1 Wat doen we voor je?

- Wij richten Azure VM's in conform best-practices op het gebied van logging/monitoring, configuratie, diskencryptie etc.
- Wij deployen de VM conform standard naming convention
- Wij deployen de VM in een Subnet naar keuze van de klant
- Wij monitoren de VM op compliancy met de Secure Baseline vanuit CIS (vanuit IaaS perspectief)
- Wij monitoren de VM op compliancy met de Microsoft Secure Baseline voor inhoudelijke inrichting van de VM zelf.

Wij zorgen bij initiële oplevering van de VM altijd voor een compliant/hardened VM-image.

11.1.2 Wat doe je nog zelf?

Je bent zelf verantwoordelijk voor alles vanaf OS-niveau. Dat wil zeggen functionele en applicatieve inrichting van de server, het instellen en aanpassen van security settings binnen de server etc. Eventueel is deze dienst ook af te nemen van Wortell Services/WORK.

11.1.3 Toegevoegde waarde

Virtuele Machines die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en security baseline. Daarna heb je de vrijheid om de server naar eigen smaak af te configureren. Wij nemen de VM vervolgens mee in maandelijkse beoordelingen op het gebied van security & compliancy, capacity management etc.

Standaard changes

- Uitbreiden van bestaande Azure VM Data disks
- Herstarten, uit of inschakelen van bestaande Virtuele machines
- Restoren van een bestaande VM (zie ook backup datmanagement)
- Aanpassen van de sizing van een bestaande VM (verticale schaling)

11.2 Azure SQL Server

Azure SQL Database server, een onderdeel van de Azure SQL-familie, is de intelligente, schaalbare, relationele databaseservice die is gebouwd voor de cloud . De 'evergreen' databaseservice is altijd up-to-date, met AI-aangedreven en geautomatiseerde functies waarmee de prestaties en duurzaamheid voor u worden geoptimaliseerd.

11.2.1 Wat doen we voor je?

- Wij richten de Azure SQL server in conform best-practices op het gebied van logging/monitoring, configuratie, versleuteling van data en eventuele auditing rules.
- Wij deployen de Azure SQL server conform standard naming convention
- Wij voorzien de Azure SQL server naar wens van netwerkconfiguratie: Public, Private endpoint of Service Endpoints
- Wij monitoren de Azure SQL server op compliancy met de secure Baseline en vanuit het CIS framework
- Wij verzorgen (in overleg) de backup frequentie en retentie

11.2.2 Wat doe je nog zelf?

In overleg met Wortell stem je een goede backup strategie af.

11.2.3 Toegevoede waarde

Azure SQL-servers die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy. De servers worden vervolgens door Wortell gemanaged en al dan niet voorzien van auto-scaling instellingen om mee te groeien met de gebruiksbehoeftes van de klant.

11.2.4 Standaard changes

- Aanpassingen in auditing instellingen
- Aanpassingen in de (server side) encryptie instellingen
- Het aanmaken van een nieuwe Azure SQL Database Server (exclusief databases
- Aanpassingen in SQL Server netwerk/firewall instellingen

11.3 Azure SQL Database

Azure SQL Database is een volledig beheerde PaaS-database-engine (platform as a service), waarmee de meeste databasebeheerfuncties, zoals upgrades, patches, back-ups en controle worden geautomatiseerd.

11.3.1 Wat doen wij voor je?

Wij richten lege databases in en zorgen ervoor dat deze databases onder de juiste Azure SQL Database server terecht komen.

11.3.2 Wat doe je nog zelf?

Het invoeren/importeren van de juiste data in de lege databases.

11.3.3 Toegevoegde waarde

Azure SQL-databases die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy.

11.3.4 Standaard changes

- Aanpassingen aan Geo-replica instellingen
- Aanpassingen in de sizing/SKU (horizontaal, verticaal of elastic pool)
- Aanpassingen in Auditing instellingen
- Aanpassingen in de encryptie instellingen

11.4 Azure Cosmos DB

Azure Cosmos DB is een volledig beheerde NoSQL-databaseservice (platform as a service), waarmee de meeste databasebeheerfuncties, zoals upgrades, patches, back-ups en controle worden geautomatiseerd.

11.4.1 Wat doen wij voor je?

- Wij richten de Azure Cosmos DB resource in conform best-practices op het gebied van logging/monitoring en infrastructurele configuratie
- Wij deployen de Azure Cosmos DB resource conform standaard naming convention
- Wij richten lege database collections in
- Wij activeren global data replication indien gewenst
- Wij regelen eventuele netwerkintegratie en/of private endpoint configuratie

11.4.2 Wat doe je nog zelf?

Het invoeren/importeren van de juiste data in de lege database collections

11.4.3 Toegevoegde waarde

Azure Cosmos DB databases die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy.,

11.4.4 Standaard changes

- Aanpassingen aan Geo-replica instellingen
- Aanpassingen in de sizing/SKU (Throughput)
- Aanpassingen in Backup & Restore settings
- Aanpassingen in Netwerk/Private endpoint configuratie

11.5 App Service Plans

Azure App Service Plans is de definitie van een set computeresources welke geschikt zijn om webapps in te draaien. Je kunt een App Service Plan vergelijken met een virtuele machine, gespecificeerd in een bepaalde grootte, met daarop door Microsoft gemanagede software om webapps te draaien.

11.5.1 Wat doen wij voor je?

- Wij richten de Azure App Service Plans in conform best-practices op het gebied van logging/monitoring, configuratie en eventuele VNET-integratie
- Wij deployen de Azure App Service Plans conform standard naming convention
- Wij monitoren de App Service Plans op compliancy met de Secure baseline en vanuit het CIS framework.

11.5.2 Wat doe je nog zelf?

Wortell regelt alles m.b.t. App Service Plans.

11.5.3 Toegevoegde waarde

Azure Apps Service Plans die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy. De App Service Plans worden vervolgens door Wortell gemanaged en al dan niet voorzien van auto-scaling instellingen om mee te groeien met de gebruiksbehoeftes van de klant

11.5.4 Standaard changes

- Aanpassingen in de sizing/SKU (horizontaal of verticaal)
- Aanpassingen in Netwerkinstellingen (integratie met bijv. Azure VNET)

11.6 App Services

App Services is waarschijnlijk het meest gebruikte resourcetype in de Azure Cloud. Een webapp maakt het mogelijk om webapplicaties in Azure te hosten. Zowel frontend als backend applicaties zijn mogelijk.

11.6.1 Wat doen we voor je?

- Wij richten de Azure App Services in conform best-practices op het gebied van logging/monitoring, configuratie en eventuele VNET-integratie
- Wij deployen de Azure App Services conform standard naming convention
- Wij monitoren de App Services op compliancy met de Secure baseline en vanuit het CIS framework.
- Backup processen inrichten
- Het toevoegen van custom Domainname settings
- Het toevoegen en vervangen van SSL Certificaten

11.6.2 Wat doe je nog zelf?

- De webapplicatie releasen of deployen naar de Azure App Service toe. Aanpassingen maken aan server side configuratie parameters (bijv. .NET versie, connectie strings etc).
- Het optionele monitoren van de Applicatie Performance (APM) door middel van het inzetten van bijvoorbeeld Azure Application Insights of een andere APM-oplossing.
- Het aanvragen van en aanleveren aan Wortell van de SSL-certificaten voor de webapplicaites in PFX-formaat.

11.6.3 Toegevoegde waarde

Azure Apps Services die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de App Service.

11.6.4 Standaard changes

- Aanpassingen in Backup instellingen
- Aanpassingen in TLS/SSL settings
- Aanpassingen in Size/SKU (horizontaal of verticaal)
- Het aanmaken van (extra) Deployment slots

11.7 Azure Kubernetes Service (per instance)

Azure Kubernets Service is een gemanagede Kubernetes service, welke het mogelijk maakt om op een snelle manier kubernetes clusters te deployen en beheren.

11.7.1 Wat doen we voor je?

- Wij richten de Azure AKS in conform best-practices op het gebied van logging/monitoring en configuratie (o.a. namespaces, node pools etc)
- Wij deployen de AKS conform standard naming convention
- Wij monitoren AKS op compliancy met de Secure baseline en vanuit het CIS framework.

11.7.2 Wat doe je nog zelf?

Het deployen van de workloads naar het AKS cluster. Het bouwen en onderhouden van de containers zelf.

11.7.3 Toegevoegde waarde

Azure Kubernets Service(s) die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy. De AKS worden vervolgens door Wortell gemanaged en al dan niet voorzien van auto-scaling instellingen om mee te groeien met de gebruiksbehoeftes van de klant. De AKS infrastructuur wordt vervolgens door Wortell gemanaged en gemonitord (ook de nodes)

11.7.4 Standaard changes

- Aanpassingen in de Clusterconfiguratie/Kubernetes versie
- Aanpassingen in Size/SKU/Scale
- Aanpassingen in Network settings (http application routing, IP whitelisting)
- Aanpassingen in Storage settings (Volumes)
- Aanpassingen in Services & Ingress settings

11.8 Data Factory

Azure DataFactory is een volledig beheerde, serverloze oplossing voor gegevensintegratie voor het op schaal opnemen, voorbereiden en transformeren van al uw gegevens.

11.8.1 Wat doen we voor je?

- Wij richten Azure DataFactory resource in conform best-practices op het gebied van logging/monitoring en infra configuratie
- Wij deployen de Azure DataFactory conform standard naming convention
- Wij monitoren de Azure DataFactory op compliancy met de Secure baseline en vanuit het CIS framework

11.8.2 Wat doe je nog zelf?

Het functioneel inrichten van de Azure DataFactory

11.8.3 Toegevoegde waarde

Azure DataFactory die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de Azure DataFactory waaronder Integration Runtime CPU & Memory en eventuele afwijkingen van verwachtte pipeline runs.

11.9 Azure Service Bus

Azure ServiceBus is de betrouwbare MaaS (Messaging as a Service) in de cloud en verzorgt eenvoudige hybride integratie. Gebruik Service Bus wanneer u een uiterst betrouwbare cloudberichtenservice tussen toepassingen en services nodig hebt, zelfs wanneer ze offline zijn.

11.9.1 Wat doen we voor je?

- Wij richten Azure ServiceBus resource in conform best-practices op het gebied van logging/monitoring en infra configuratie
- Wij deployen de Azure ServiceBus conform standard naming convention
- Wij monitoren de Azure ServiceBus op compliancy met de Secure baseline en vanuit het CIS framework

11.9.2 Wat doe je nog zelf?

Het functioneel inrichten van de Azure Service Bus

11.9.3 Toegevoegde waarde

Azure ServiceBus die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de Azure ServiceBus waaronder Server/User errors, abandoned messages etc.

11.10 Azure cache for Redis

Azure Cache voor Redis biedt gegevensopslag in het geheugen op basis van de Redis-software. Redis verbetert de prestaties en schaalbaarheid van toepassingen die gebruik maken van back-end-gegevensarchieven. Het kan grote hoeveelheden toepassingsaanvragen verwerken door vaak gebruikte gegevens in het servergeheugen te bewaren zodat deze snel kunnen worden geschreven en gelezen. Redis is een essentiële oplossing voor gegevensopslag met lage latentie en hoge doorvoer voor moderne toepassingen.

11.10.1 Wat doen we voor je?

- Wij richten de Azure Cache for Redis resource in conform best-practices op het gebied van logging/monitoring en infra configuratie
- Wij deployen de Azure Cache for Redis conform standard naming convention
- Wij monitoren de Azure Cache for Redis resource op compliancy met de Secure baseline en vanuit het CIS framework

11.10.2 Wat doe je nog zelf?

Het functioneel inrichten van de Azure Cache for Redis. Denk hierbij aan TLS versie, memory policies, Scale en Cluster sizes. Vanuit Wortell kunnen wij uieraard wel meedenken over deze inrichting.

11.10.3 Toegevoegde waarde

Azure Cache for Redis die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de Azure Cache for Redis waaronder CPU, Used Memory, Errors en Server Load

12 Connectivity en Firewall componenten

Binnen Azure zijn er verschillende mogelijkheden om connectivity en firewalling in te regelen. Binnen MCA-beheer, gaan we uit van de Microsoft oplossingen, welke hieronder beschreven staan.

12.1 Azure Firewall

Azure Firewall is een beheerde, cloudgebaseerde netwerkbeveiligingsservice die uw Azure Virtual Network-resources beschermt. Het is een volledige stateful firewall als een service met ingebouwde hoge beschikbaarheid en onbeperkte cloudschaalbaarheid.

12.1.1 Wat doen we voor je?

- Wij richten de Azure Firewall in conform best-practices op het gebied van logging/monitoring, configuratie
- Wij deployen de Azure Firewall conform standard naming convention
- Wij monitoren de Azure Firewall op compliancy met de Secure baseline en vanuit het CIS framework.
- Wij beheren eventueel toegewezen Azure Firewall Policies

12.1.2 Wat doe je nog zelf?

Functioneel beheer: dat wil zeggen het beoordelen van Threat alerts afkomstig uit o.a. Threat intelligence optie van de firewall alsmede het samenstellen van de applicatie firewall rules. Het beheer en opvolging van alerts kan ook door het Managed Detection & Response (MDR) team van Wortell uitgevoerd worden.

12.1.3 Toegevoegde waarde

Azure Firewall die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de App Service.

12.1.4 Standaard Changes

- Aanpassingen in de Rules (Classic)
- Aanpassingen in de Firewall Manager/Firewall Policies
- Aanpassingen in de Public IP configuratie

12.2 Azure Frontdoor

Azure Frontdoor is een – op Microsoft globale edge netwerk – gedeployde ingang tot o.a. webapplicaties. Azure Frontdoor is oneindig schaalbaar, snel en beschikt over additionele Web Application Firewall functionaliteiten en Content Caching dicht bij de gebruikers van de applicatie.

12.2.1 Wat doen we voor je?

- Wij richten de Azure Frontdoor in conform best-practices op het gebied van logging/monitoring, configuratie
- Wij deployen de Azure App Services conform standard naming convention
- Wij monitoren de App Services op compliancy met de Secure baseline en vanuit het CIS framework.
- Wij beheren eventueel toegewezen Web Application Firewall rules

12.2.2 Wat doe je nog zelf?

Meebeslissen over de inrichting/eisen aan de frontdoor, met betrekking tot backend, verdeling van de verkeersstromen en het aanleveren van benodigde SSL-certificaten. Daarnaast ook het meedenken over het inrichten van eventuele Web Application Firewall rulesets.

12.2.3 Toegevoegde waarde

Azure Frontdoor(s) die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming conventie en best-practices op het gebied van security & compliancy. De Frontdoor(s) worden vervolgens door Wortell gemanaged en gemonitord.

12.2.4 Standaard changes

- Vervangen van SSL-certificaten
- Aanpassingen in Front Door designer (backend/frontend/rule configuratie)
- Aanpassingen in toegewezen WAF regels.

12.3 Application Gateway (WAF)

Azure Application Gateway is een load balancer voor webverkeer waarmee u het verkeer naar uw webapps kunt beheren. Traditionele load balancers werken op de transportlaag (OSI-laag 4 - TCP en UDP) en routeren verkeer op basis van IP-bronadres en een bronpoort naar een IP-doeladres en doelpoort. Application Gateway kan routeringsbeslissingen nemen op basis van extra kenmerken van een HTTP-aanvraag, bijvoorbeeld URI-pad of hostheaders (OSI-laag 7)

12.3.1 Wat doen we voor je?

- Wij richten Azure Application Gateway in conform best-practices op het gebied van logging/monitoring, configuratie
- Wij deployen de Azure Application Gateway conform standard naming convention
- Wij monitoren de Azure Application Gateway op compliancy met de Secure baseline en vanuit het CIS framework

12.3.2 Wat doe je nog zelf?

- Het aanvragen en aanleveren van benodigde SSL Certificaten in PFX-formaat
- Meebeslissen over de (eventuele) Web Application Firewall rules

12.3.3 Toegevoegde waarde

Azure Application Gateway die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de Application Gateway en de backend pools.

12.3.4 Standaard Changes

- Aanpassingen in Backend pools
- Aanpassingen in http settings
- Aanpassingen in Listeners
- Aanpassingen in Frontend IP configuratie
- Aanpassingen in AGW-routing rules

12.4 Azure Loadbalancer

Azure Load Balancer werkt op laag 4 van het OSI-model (Open Systems Interconnection). Dit is het enige contactpunt voor clients. De Load Balancer verdeelt inkomende stromen die binnenkomen bij het front-end van de load balancer voor back-endadresgroep. Deze stromen zijn gebaseerd op geconfigureerde taakverdelings regels en status controles. De exemplaren van de back-endadresgroep kunnen virtuele Azure-machines of exemplaren in een scale-set voor virtuele machines zijn.

12.4.1 Wat doen we voor je?

- Wij richten Azure LoadBalancer in conform best-practices op het gebied van logging/monitoring, configuratie
- Wij deployen de Azure Loadbalancer conform standard naming convention
- Wij monitoren de Azure LoadBalancer op compliancy met de Secure baseline en vanuit het CIS framework

12.4.2 Wat doe je nog zelf?

Niets

12.4.3 Standard Changes

- Aanpassingen in FrontendIP configuratie
- Aanpassingen in Backend Pool configuratie
- Aanpassingen in Loadbalancing rules
- Aanpassingen in Inbound NAT rules

12.4.4 Toegevoegde waarde

Azure Loadbalancer(s) die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de LoadBalancer en de backend pools.

12.5 VPN Gateway (inclusief VPN connectie)

Een VPN-gateway is een speciaal soort virtueel-netwerkgateway die wordt gebruikt om versleuteld verkeer te verzenden tussen een virtueel Azure-netwerk en een on-premises locatie via het openbare internet. U kunt een VPN-gateway ook gebruiken om versleuteld verkeer tussen virtuele Azure-netwerken te verzenden via het Microsoft-netwerk.

12.5.1 Wat doen we voor je?

- Wij richten Azure VNET/VPN gateway in conform best-practices op het gebied van logging/monitoring, configuratie
- Wij deployen de Azure VNET/VPN gateway conform standard naming convention
- Wij monitoren de Azure VNET/VPN gateway op compliancy met de Secure baseline en vanuit het CIS framework

12.5.2 Wat doe je nog zelf?

- Het aanmaken van nieuwe Site-to-Site tunnels aan on-premise zijde van de tunnel; en/of
- Het regelen van contactgegevens van overige derde partijen waarmee tunnels tot stand moeten worden gebracht tussen Azure en die betreffende locatie(s)

12.5.3 Standard Changes

Het aanmaken van nieuwe Site-to-Site tunnels aan Azure zijde

12.5.4 Toegevoegde waarde

Azure VPN Gateway(s) die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de Appliation Gateway en de beschikbaarheid van gedefinieerde Site-to-Site VPN tunnels

12.6 Express Route Circuit & Connections

Azure ExpressRoute wordt gebruikt om particuliere verbindingen te maken tussen Windows Azure-datacenters en infrastructuur op uw locatie of in een co-locatieomgeving. ExpressRoute-verbindingen lopen niet via het openbare internet en bieden een grotere betrouwbaarheid, hogere snelheden en kortere wachttijden dan gebruikelijke internetverbindingen.

12.6.1 Wat doen we voor je?

Wij monitoren de beschikbaarheid van de Express Route Circuit & Connecties die over het express route circuit lopen. Daarnaast kunnen we ook (maximaal) verbruik meten om ervoor te zorgen dat er geen bottlenecks ontstaan in de gekozen verbindingssnelheid van de ExpressRoute connecties.

12.6.2 Wat doe je nog zelf?

Het regelen van eventuele on-premise of non-Azure datacenter connectivity. Het monitoren van de connectivity vanaf die zijde van de verbinding.

12.6.3 Toegevoegde waarde

Azure ExpressRoute Circuit(s) en connections die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Wij monitoren de beschikbaarheid van de connectie(s) en vervullen de SPOC-rol bij connectivity incidenten.

12.7 Virtual WAN

Azure Virtual WAN is een netwerkservice die een groot aantal netwerk-, beveiligings- en routeringsfuncties samenbrengt om één operationele interface te bieden. Deze functies omvatten vertakkingsconnectiviteit (via connectiviteitsautomatisering van Virtual WAN Partner-apparaten zoals SD-WAN of VPN CPE), site-naar-site-VPN-connectiviteit, connectiviteit via VPN voor externe gebruikers (punt-naar-site), persoonlijke connectiviteit (ExpressRoute), intra-cloud-connectiviteit (transitieve connectiviteit voor virtuele netwerken), VPN-ExpressRoute-interconnectiviteit, routering, Azure Firewall en versleuteling voor persoonlijke connectiviteit.

12.7.1 Wat doen we voor je?

- Wij richten de Azure Virtual WAN in conform best-practices op het gebied van logging/monitoring, configuratie
- Wij deployen de Azure Virtual WAN conform standard naming convention
- Wij monitoren de Azure Virtual WAN op compliancy met de Secure baseline en vanuit het CIS framework
- Wij monitoren de VWAN-connecties waaronder Site-to-Site, ExpressRoute verbindingen en Hub-naar-VNET-verbindingen

12.7.2 Wat doe je nog zelf?

Het regelen van eventuele on-premise of non-Azure datacenter connectivity. Het monitoren van de connectivity vanaf die zijde van de verbinding. Het instellen van Point-to-site VPN-tunnels indien deze nodig blijken te zijn voor gebruikers.

12.7.3 Toegevoegde waarde

Azure Virtual WAN die door Wortell worden opgeleverd voldoen altijd aan de afgesproken naming convention en best-practices op het gebied van security & compliancy. Tevens monitoren wij de infrastructurele performance van de dienst.

13 Service levels op Resources

De inhoud van deze Service Description volgt de afspraken die zijn vastgelegd in de algemene SLA/XLA welke is afgesloten tussen Wortell en uw organisatie. In de SLA/XLS treft u de service windows en responstijden.

De resources die wij voor u monitoren, bieden wij aan in 3 tiers. Deze tiers staan hieronder beschreven. De 3 tiers staan gelijk aan de prioriteiten 1,2 en 3 uit de SLA/XLA.

13.1 SLA Gold

Deze SLA is voor bedrijfskritieke productie workloads, welke 24x7 belangrijk zijn voor de organisatie. De resources met deze SLA worden 24x7 proactief bewaakt door Pulse en in het geval van een incident of melding, waar een engineer nodig is, ontvangt de dienstdoende engineer een waarschuwing van Pulse om het incident te verhelpen.

De reactie- en responstijden staan gelijk aan een Prio 1 zoals vastgelegd in de SLA/XLA.

13.1.1 Wat doen we voor je?

In het geval van een incident op een Gold resource, stuurt Pulse de melding automatisch door naar de dienstdoende engineer en deze bevestigt de melding en begint er vervolgens aan te werken.

13.1.2 Toegevoegde waarde

Een snelle response van een skilled Azure engineer die het probleem met de bedrijfskritische resource oplost.

13.2 SLA Silver

Deze SLA is voor kritieke workloads, die belangrijk zijn voor de organisatie tijdens kantooruren. De resources met deze SLA worden 24x7 proactief gemonitord door Pulse en in het geval van een incident of melding, waar een engineer nodig is, ontvangt de engineer tijdens kantooruren een waarschuwing van Pulse om het incident te verhelpen.

De reactie- en responstijden staan gelijk aan een Prio 2 zoals vastgelegd in de SLA/XLA.

13.2.1 Wat doen we voor je?

In het geval van een incident op een Silver resource, stuurt Pulse de melding automatisch door naar de dienstdoende engineer. Deze bevestigt de melding en begint er vervolgens aan te werken.

13.2.2 Toegevoegde waarde

Een snelle reponse van een skilled Azure engineer die het probleem met de kritische resource binnen kantoortijden oplost.

13.3 SLA Bronze

Deze SLA is voor standaard- en/of niet-kritische (ontwikkel-/test) workloads tijdens kantooruren. De resources met deze SLA worden proactief 24x7 gemonitord door Pulse en in het geval van een incident of melding, waar een engineer nodig is, ontvangt de engineer tijdens kantooruren een waarschuwing van Pulse om het incident te verhelpen.

De reactie- en responstijden staan gelijk aan een Prio 2 zoals vastgelegd in de SLA/XLA.

13.3.1 Wat doen we voor je?

In het geval van een incident op een Bronze resource, stuurt Pulse de melding automatisch door naar de dienstdoende engineer en deze bevestigt de melding. De maximale resolutietijd die we nastreven is gelijk aan het level 3 incident n

13.3.2 Toegevoegde waarde

Een reponse van een skilled Azure engineer die het probleem met de resource binnen kantoortijden oplost. Binnen 2 werkdagen is er een inhoudelijke reactie en de maximale resolutietijd die we nastreven is 5 werkdagen.