|  |
| --- |
| Amsterdam UMC Research Cloud  SURFcumulus Research Cloud  HLD project 2018-032 |
|  |
|  |

|  |  |
| --- | --- |
| **Datum:** | **10-02-2020** |
| **Versie:** | 1.00 |
| **Auteur:** | Fons Ullings |

Documenthistorie

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** |  | **Datum** | **Wijzigingen** |
| 0.1 |  | 18-01-2019 | Initieel (Fons Ullings) |
| 0.7 |  | 17-09-2019 | Eerste draft release |
| 0.8 |  | 19-09-2019 | Feedback Christiaan Geertsma verwerkt |
| 0.9 |  | 30-09-2019 | Feedback Cédric en Stefan Hess verwerkt |
| 1.00 |  | 10-02-2020 | Laatste puntjes |
|  |  |  |  |

## Distributielijst

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Naam** | **Functie** | **0.7** | **0.8** | **0.9** |  | **1.0** | **1.1** |
| Christiaan Geertsman | OO&I Informatie Analist | X | X | X |  | X |  |
| Stefan Hess | Projectleider |  | X | X |  | X |  |
| Christiaan Luijt | ICT netwerkengineer |  | X | X |  | X |  |
| Simon Dedters | ICT netwerkengineer |  | X | X |  | X |  |
| Cédric Laurent | ICT virtualisatie engineer |  | X | X |  | X |  |
| René Thomassen | ICT functioneel/technisch beheerder |  | X | X |  | X |  |
| Arno Sinjewel | OO&I Manager |  |  | X |  | X |  |

## Issues

|  |  |  |
| --- | --- | --- |
| **#** |  | **Issues** |
| 001 | OK | Officiële productnaam op titelblad opvoeren |
| 002 |  |  |

## Referenties

* 20171011 Memo - Strategie Research Cloud 2018-2022 (Arno Sinjewel, Christiaan Geertsma, Fons Ullings)
* Plan van Aanpak 2018-032 - Lifecycle Vervanging Research Cloud v.1.0.pdf (Stefan Hess)
* 2018-032 Functioneel ontwerp - Research Cloud Lifecycle (Christiaan Geertsma)
* Amsterdam UMC Researchomgeving 1.2 (Hans van den Berg, Fons Ullings)
* PIA Amsterdam UMC Research Cloud 2018-032 - Lifecycle Vervanging Research Cloud\Werkdocumenten\PIA
* Dienstbeschrijving\_SURFcumulus\_okt-2018 (Michel Wets, SURFnet)
* Hub-spoke network topology in Azure (Microsoft 2019)

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke

* Naming conventions for Azure resources

https://docs.microsoft.com/en-us/azure/architecture/best-practices/naming-conventions

* CMP configuratie Amsterdam UMC workspace (Rutger Tromp)
* Azure naming convention worksheet V0.999 (research-cloud.nl team)
* LLD Research Cloud network infrastructuur (Christiaan Luijt, Simon Dedters)
* LLD LifeCycle Management Amsterdam UMC Research Cloud Platform (Cédric Laurent)

Inhoud

[1.1. Versiebeheer 2](#_Toc32220191)

[1.2. Distributielijst 2](#_Toc32220192)

[1.3. Issues 2](#_Toc32220193)

[1.4. Referenties 2](#_Toc32220194)

[2. Inleiding 4](#_Toc32220195)

[2.1. Doel 5](#_Toc32220196)

[2.2. Scope 5](#_Toc32220197)

[2.3. Fasering 5](#_Toc32220198)

[2.4. Informatie beveiliging 5](#_Toc32220199)

[3. Uitgangspunten 6](#_Toc32220200)

[4. Datastromen en zonering 9](#_Toc32220201)

[5. Infrastructuur 11](#_Toc32220202)

[5.1. Infrastructure as a Code 11](#_Toc32220203)

[5.2. Beschikbaarheid 13](#_Toc32220204)

[5.3. Monitoring 13](#_Toc32220205)

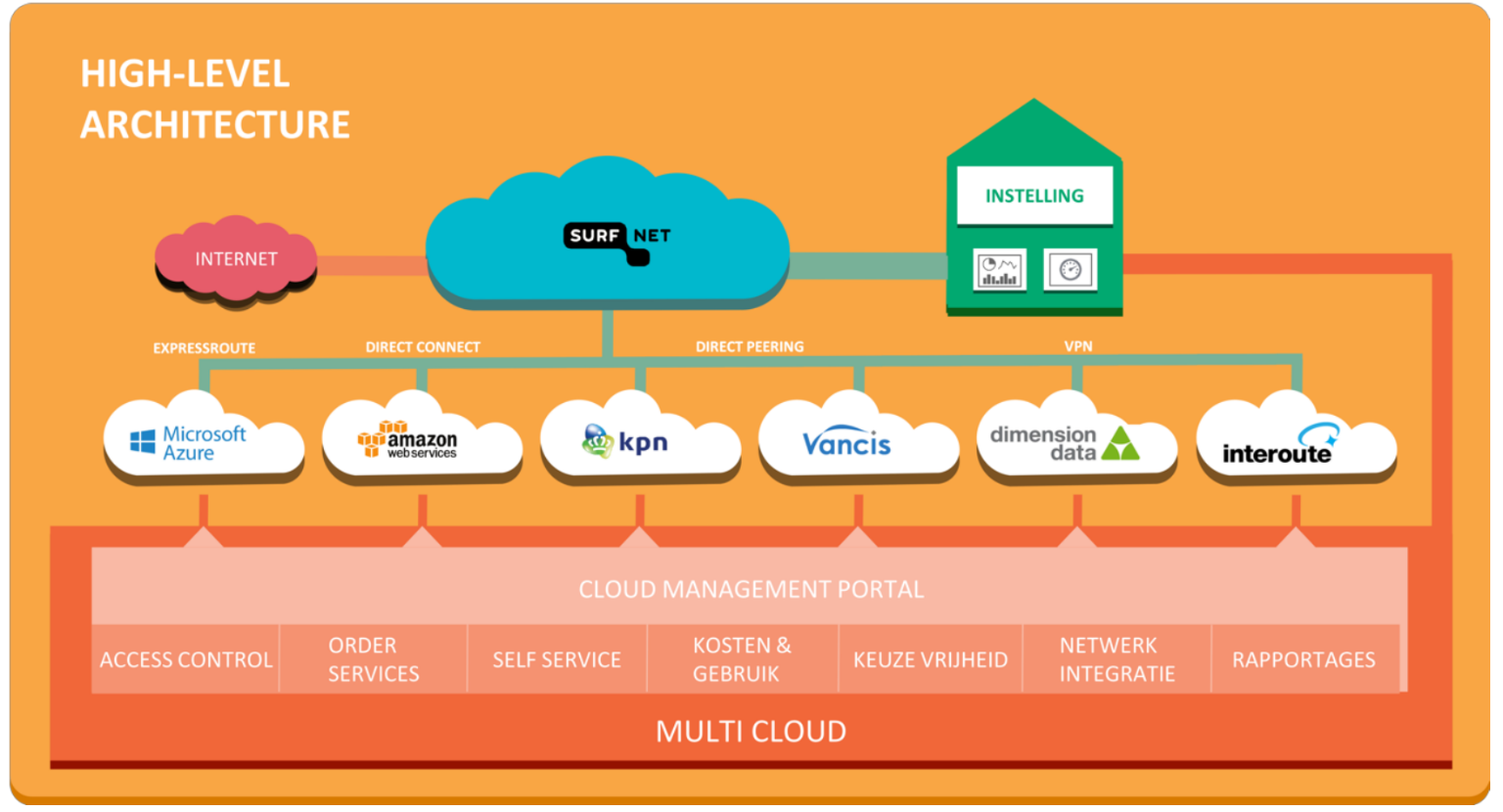
[5.4. Firewalling 13](#_Toc32220206)

# Inleiding

In de loop van 2012 is door de toenmalige dienst ICT van VUmc de SURFnet Campus Challenge subsidie verworven (Christiaan Geertsma, Johan Colijn, et.al.). Met hulp van deze funding is o.a. de VUmc Research Cloud ingericht: een toen on-premises Infrastructure as a Service (IaaS) omgeving, geïntegreerd met SURFteams, waar binnen research groepen geheel in selfservice Virtual Machine (VM) resources in eigen Virtuele Organisaties konden alloceren en exploiteren. Deze omgeving was in hoge mate gescheiden van de VUmc Enterprise ICT omgeving opgezet en bestond uit dedicated VMWare ESX hosts, Cisco Nexus switches en HP LeftHand storage nodes. Er werd gebruik gemaakt van een heel gebruikersvriendelijk Cloud Management Portal (CMP) avant la lettre, nl. GreenQloud Qstack. De kaders voor het gebruik waren afgestemd met de functionaris gegevensbescherming (FG) zodat volgens een standaard procedure compliancy geborgd wordt.

In de loop van 2017 verviel een flink deel van de onderhoudscontracten van de onderliggende hardware en software en is er op instigatie van het Informatie Management Research een vervangingsplan opgesteld. Uit acht verschillende on-premises en cloud oplossingen zijn vanuit een functionele weging drie oplossingen verder uitgewerkt. En begin oktober 2017 is door het MT aan de hand van een gedetailleerde beslisnotitie SURFcumulus multi-cloud (zie figuur 1) oplossing met voor alsnog Azure als resource laag geselecteerd. Na enige vertraging door financiële complicaties is vervolgens het eigenlijke vervangingstraject september 2018 onder leiding van Stefan Hess van start gegaan.

Dit document beschrijft in hoofdlijnen de uitgangspunten die vanaf oktober 2017 gehanteerd zijn.



Figuur 1 SURFcumulus multi-cloud architectuur

## Doel

Het doel van dit traject is om, conform de MT beslisnotitie oktober 2017, gebruikmakend van de SURFcumulus multi-cloud dienstverlening een Amsterdam UMC breed alternatief voor de on-premises VUmc GreenQloud Qstack Research IaaS omgeving aan te kunnen bieden. Conform de MT notitie is er voor gekozen om *initieel* Azure resources midden vertrouwelijk in te zetten. Maar qua (infrastructuur) design wél al geschikt voor hoog vertrouwelijk en voor multi-cloud (AWS, Google, etc.) op te zetten.

## Scope

De scope van *dit* document behelst de *as-is* transitie van de in 2012/2013 opgebouwde on-premises VUmc Qstack/GreenQloud Research IaaS omgeving naar een SURFcumulus multi-cloud gebaseerde Azure cloud opzet. Inclusief alle geformuleerde uitgangspunten en randvoorwaarden daarbij.

Buiten scope vallen:

* Hoog vertrouwelijke procesinrichting conform de Microsoft Azure richtlijnen.
* Effectief aanbieden van multi-cloud (AWS, Google, Vancis, KPN, etc.).
* Additionele diensten als Science Collaboration Zone (SCZ) deployments.

## Fasering

Dit traject wordt in één fase doorlopen. Wel zijn er in het kader van dit traject, om voor en tegen van verschillende oplossingsrichtingen uit te testen en kennis op te doen, diverse proeftuinen opgebouwd. Al deze artefacten zijn nu (eind augustus 2019) opgeruimd.

N.B. Azure is heel star in het hernoemen van resources: er zijn nog een aantal *centrale* componenten die bij een vervolg traject *research-cloud.nl hoog vertrouwelijk* hernoemd zouden moeten worden

## Informatie beveiliging

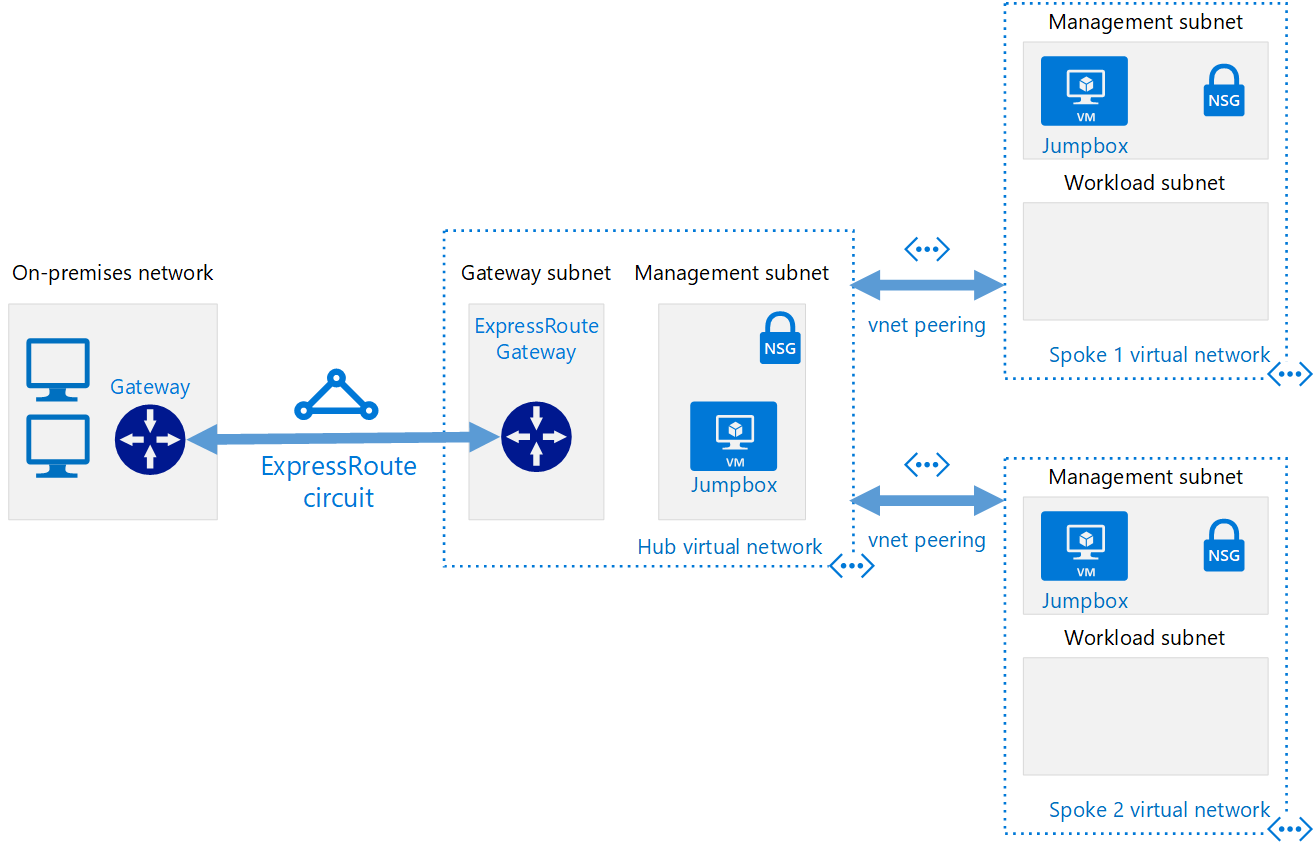
Alle netwerkdatastromen en aangrijppunten zijn conform de vigerende opzet en filtering van de on-premises VUmc Qstack/GreenQloud doorgezet (zie LLD Research Cloud network infrastructuur). Ook de scheiding tussen de research workspaces (VO’s) is binnen de Azure infrastructuur (hub/spoke) strikt gehandhaafd.

Wél is er, voor alsnog, functioneel qua informatie beveiligingsopties een veer gelaten: in tegenstelling tot de Qstack/GreenQloud opzet is er op Cloud Management Portal (CMP) niveau nog geen selfservice soft firewalling per VM of per workspace te definiëren.

# Uitgangspunten

De volgende uitgangspunten gelden voor dit SURFcumulus VRC research-cloud.nl traject:

* Voor dit traject wordt in samenspraak met de FG AMC en VUmc een PIA (Privacy Impact Analyse) opgesteld. En alle richtlijnen en maatregelen die in deze impact analyse zijn vastgesteld zijn *voor* het in productie nemen van VRC infrastructuur ook doorgevoerd.
* De uitgangspunten die bij de realisatie van de on-premises VUmc Qstack/GreenQloud omgeving zijn aangenomen (2013/2014) worden as-is overgenomen. Het project behelst dan ook expliciet de continuering van de VUmc Research Cloud dienstverlening richting de diverse Research community ’s, Virtuele Organisaties, VO’s.
  + Midden vertrouwelijk beveiligingsniveau.
  + Compliancy borging in intake procedure en duidelijke verantwoordelijkheden.
  + Hoge mate van selfservice.
  + Minimale beheerinspanning ICT.
  + Strike Infrastructure as a Service (IaaS).
  + Strikte scheiding tussen de infrastructuur van de diverse Research groepen (VO’s).
  + Qua netwerk, autorisatie en authenticatie ontkoppeld van de bestaande Enterprise infrastructuren.
  + Op basis van IPv4 gereguleerde toegang tot de Research data services, Store4Ever, licentieservers.
  + Gereguleerd Internet verkeer van en naar de VO omgevingen met op Enterprise niveau afgedwongen Next Gen Firewall (NGFW) rulesets.
* Dit traject is weliswaar onder het lopende locatie VUmc SURFnet contract uitgevoerd. Maar de VRC reseach-cloud.nl dienst is in élk aspect ook door locatie AMC Research community ‘s, equivalent aan locatie VUmc, in te zetten: het project resultaat is dan ook Amsterdam UMC dienst.
* De in te richten omgeving wordt qua *infrastructuur* al voorbereid om de verwerking van hoog vertrouwelijke data.
* Conform de geaccordeerde MT beslisnotitie oktober 2017 is de omgeving gebaseerd op de SURFcumulus multi-cloud Cloud Management Portal (CMP) propositie, waaronder in eerste instantie Azure resources worden ingezet. Maar waarbij binnen het ontwerpen het multi-cloud aspect gehandhaafd en mogelijk blijft (AWS, Google).
* Minimalisatie van de centraal te nemen kosten en investeringen/exploitatie binnen Azure, AWS, etc.
* Uitgangspunt voor de *Azure* infrastructuur is de Microsoft hub-spoke Azure datacentrum architectuur.
* Conform deze Microsoft architectuur en na uitgebreide consultatie van Microsoft is er voor gekozen om voor een één op één relatie tussen VO’s en *Azure* workspaces (subscriptions). Zie Figuur 2.
* Conform de VUmc on-premises Qstack/GreenQloud uitgangspunten wordt dan ook, gezien ook de Microsoft datacentrum en SURFcumulus architectuur, met een Azure ExpressRoute en SURFnet lichtpad *al* het netwerkverkeer door de on-premises FortiGate NGFW geleid.



Figuur 2 Microsoft Azure ExpressRoute hub-spoke virtual datacenter architectuur

* De on-premises FortiGate NGFW, en daarmee heel het achterliggende AMC/VUmc netwerklandschap, wordt *niet* met IPv4 adres ruimtes van de onderliggende cloud infrastructuren (Azure, AWS, Google, etc.) geconfronteerd. Er vindt binnen elk van deze cloud omgevingen IPv4 adres translatie plaats.
* Voor de IPv4 translaties worden vooralsnog FortiGate Azure appliances ingezet. Het door Microsoft binnen *Azure* aangeboden Firewall product bleek daar nog niet toe in staat.
* De per cloud ingerichte FortiGate appliances handelen alléén DNAT en SNAT translaties af: de netwerkverkeer regelende rulesets bevinden zich strikt in de on-premises FortiGate NGFW zodat al deze netwerk flows centraal te beheren zijn.
* De (Azure) FortiGate *appliance* is, op advies met de leverancier, niet dubbel uitgevoerd. Gezien de heel beperkte en statische functionaliteit (SNAT/DNAT translatie) levert het dubbel uitvoeren meer beschikbaarheid issues op dan het dubbel uitvoeren zou mitigeren.
* De betreffende SNAT/DNAT translaties worden voor een groter aantal workspace in één keer geconfigureerd zodat er niet steeds ad-hoc changes en beheer vereist zijn. De inrichting van de FortiGate appliances is dus qua configuratie geheel statisch en wordt als geheel bij een incident recovered.
* Er wordt voorkomen dat er IPv4 public space “snijverlies” ontstaat door per workspace public space mappings in groepen van vier IPv4 adressen uit te delen. Binnen een workspace kunnen virtueel onbeperkt aantal privat IPv4 adressen worden ingezet.
* De inkomende en uitgaande Internet verkeersstromen worden binnen de on-premises FortiGate NGFW infrastructuur (routering building block) conform de on-premises VUmc GreenQloud Qstack ruleset generiek voor alle workspaces/VO’s, maar wel “least privileged”, ingeregeld. Wel is deze ruleset tegen voortschrijdend inzicht gehouden en FTP als protocol geschrapt.
* De SURFnet naar Microsoft ExpressRoute infrastructuur, met inzet van Multi Service Port (MSP) paden vanuit de locatie VUmc routering building block, is redundant uitgevoerd.
* De SURFnet naar Microsoft ExpressRoute infrastructuur is fysiek 10Gbit enabled: door de beperkte capaciteit van de on-premises FortiGate NGFW is de bandbreedte nu (februari 2020) op 1Gbit geconfigureerd, passend binnen de oorspronkelijke begroting.
* De binnen een Azure tenant vereiste Azure Active Directory (Azure AD, AAD) wordt conform de uitgangspunten zo sober mogelijk, maar wél gebruikmakend van het Microsoft RBAC functionaliteit en “least privileged”, ingericht.
* In eerste en tweede lezing is het uitgangspunt om Azure AD RBAC gebaseerde toegang via een Azure AD groepen structuur en persoonlijke guest @amsterdamumc.nl work/school accounts multi factor (MFA) in te regelen. Gedurende het traject bleek dat de Azure @amsterdamumc.nl work/school infrastructuur nog niet op orde was. Er is dan ook voor de voortgang van het traject alsnog gekozen om de al gedefinieerde Azure AD groepen om te zetten in een handvol (zes) functionele Azure AD accounts.
* Recent (januari 2020) is MFA voor deze functionele Azure AD accounts in een pilot omgeving getest: deze MFA feature zal binnenkort ook in de productie omgeving worden uitgerold.
* Een eventuele andere opzet van de functionele accounts wordt in een vervolgtraject *research-cloud.nl hoog vertrouwelijk* opgepakt.
* De Azure omgeving is strikt rond de Azure Management Group systematiek ingericht zodat centraal voor alle workspaces de RBAC inrichting gegarandeerd gelijk is.
* Er is op basis van de Microsoft Azure naamconventie richtlijnen een strikte naamconventie voor alle resources gehanteerd. Het staat de research groepen (VO’s) alleen vrij om hun Virtual Machine namen binnen hun eigen workspace zelf te bepalen.
* Er is gestart met een *onmicrosoft.com* Azure AD domain. Dit Azure AD domain is in de loop van het traject omgezet naar research-cloud.nl. Voor dit domein is ook de DNS naam geregistreerd en binnen de locatie VUmc externe ICT DNS infrastructuur (SURFdomeinen) opgevoerd en geconsolideerd.
* Voor de migraties van VM’s uit de on-premises VMWare ESX omgeving wordt/is éénmalig de Microsoft Site Recovery Services ingericht en ingezet. De uitgeteste Veeam migratie optie was plan B. Na het voltooien van de migraties is de betreffende Site Recovery Services omgeving ontmanteld.
* Authenticatie naar SURFcumulus CloudBolt CMP wordt via SURFconext geregeld (AMC en VUmc): er zijn géén CloudBolt local accounts geconfigureerd.
* Voor alsnog kent het SURFcumulus CloudBolt CMP een eigen autorisatie model. aar ook die inrichting

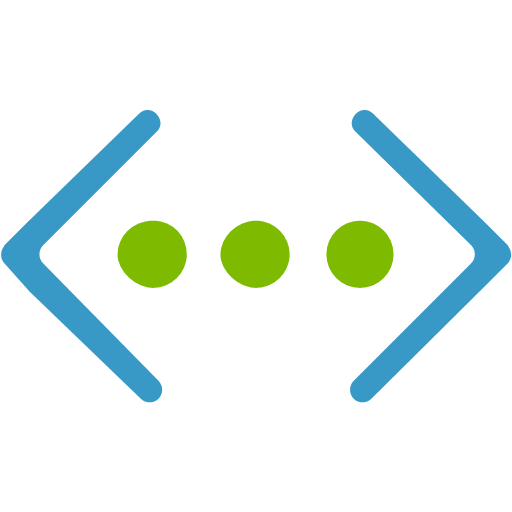
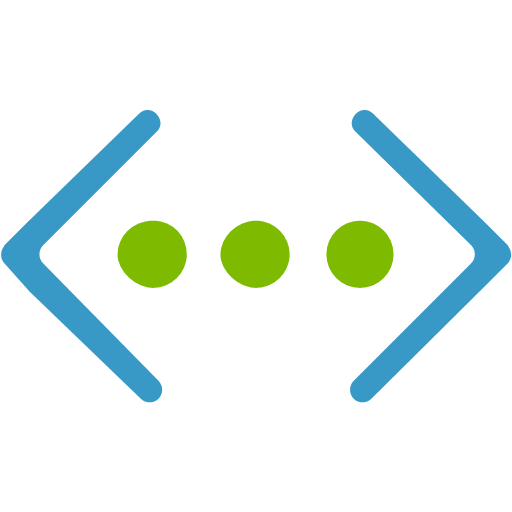
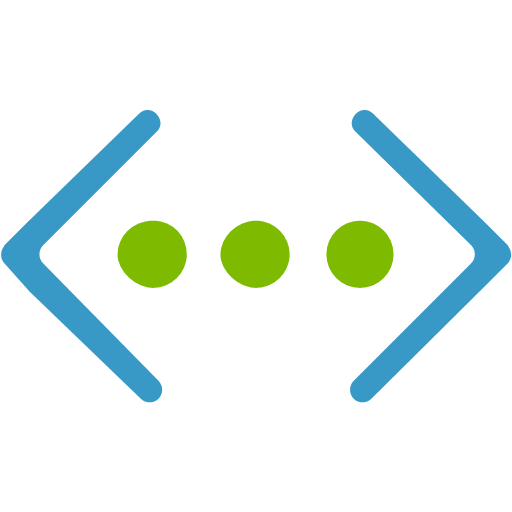
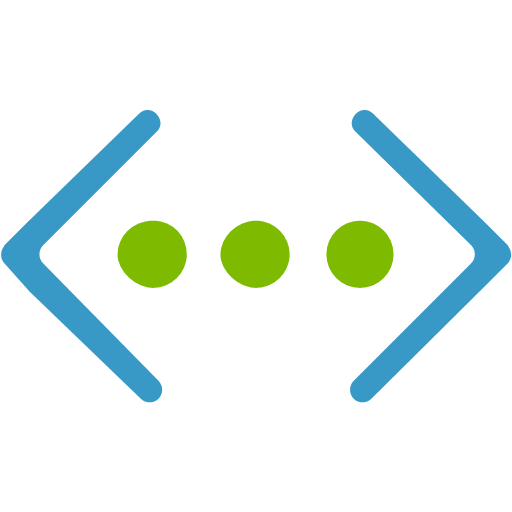
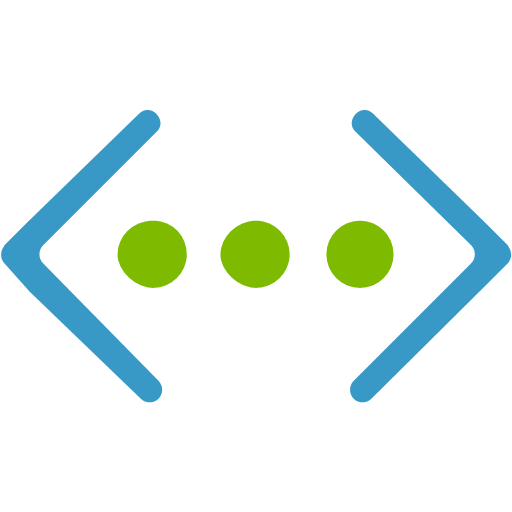
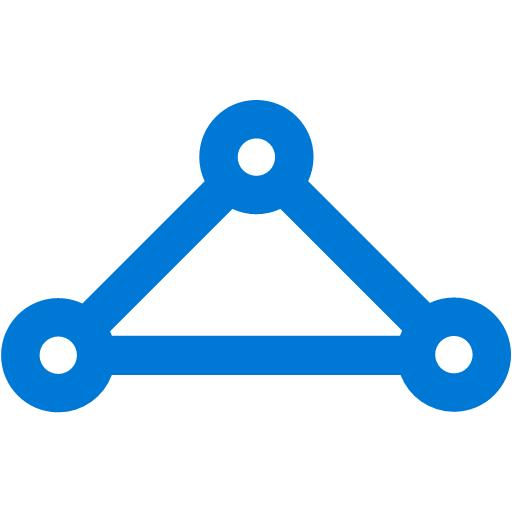
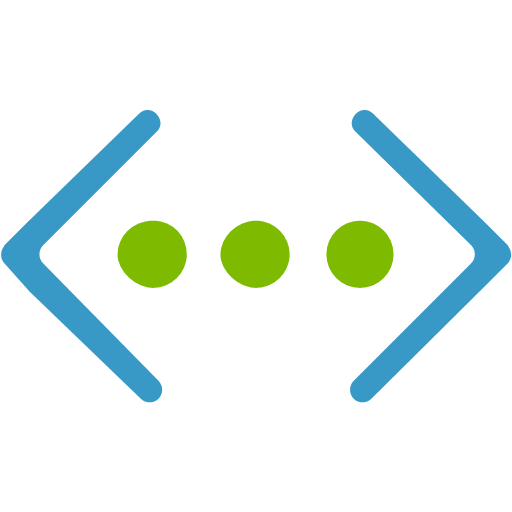
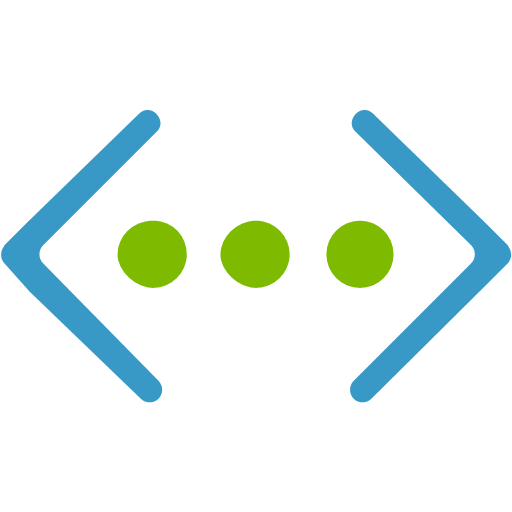
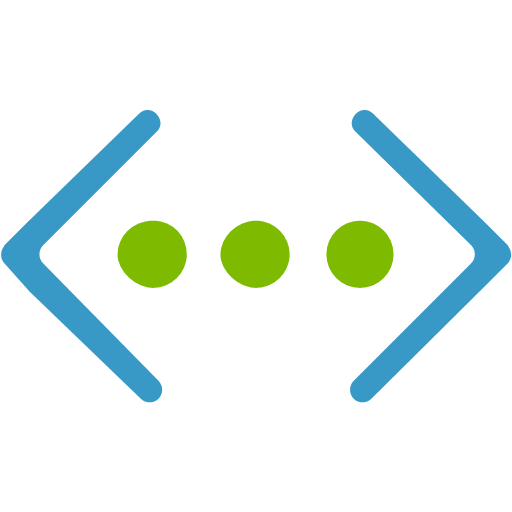
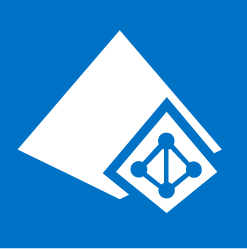
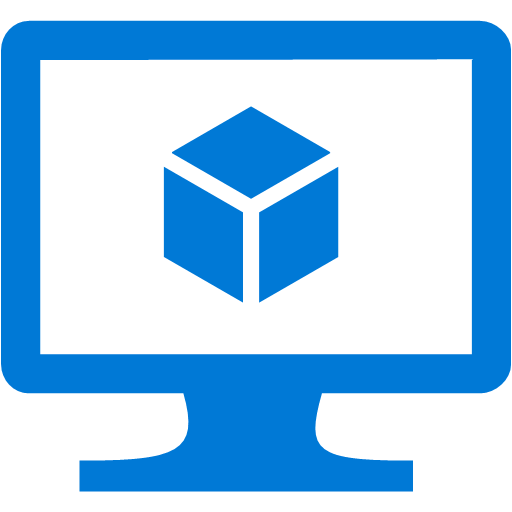
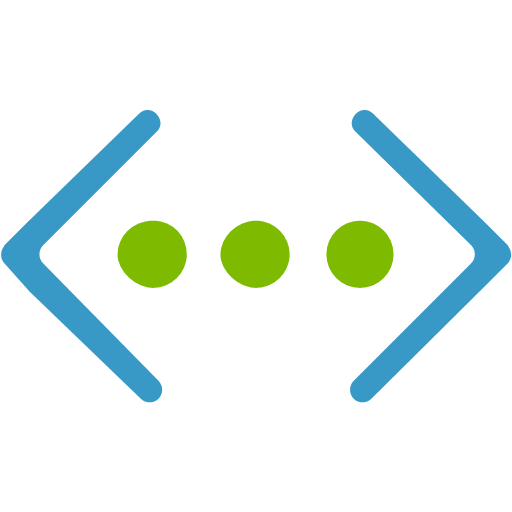
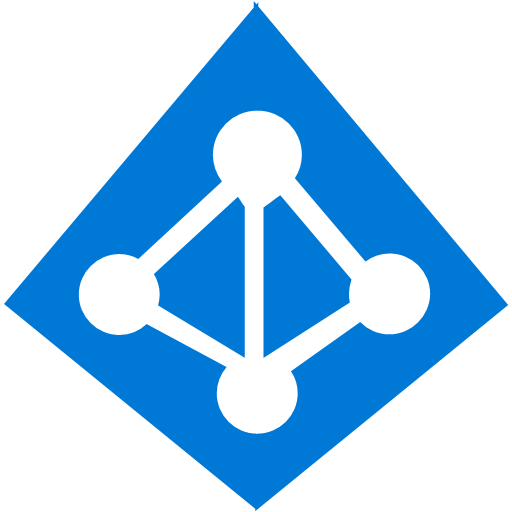
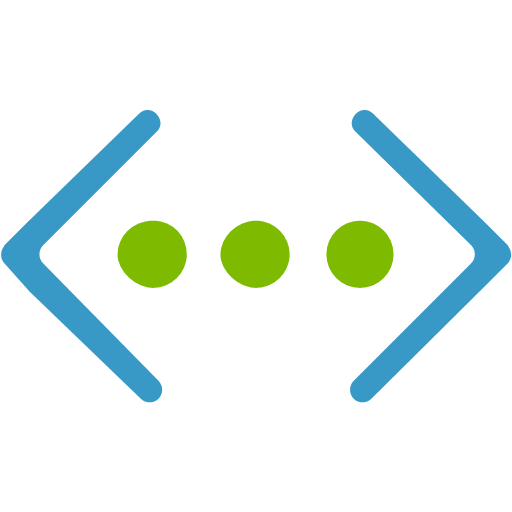
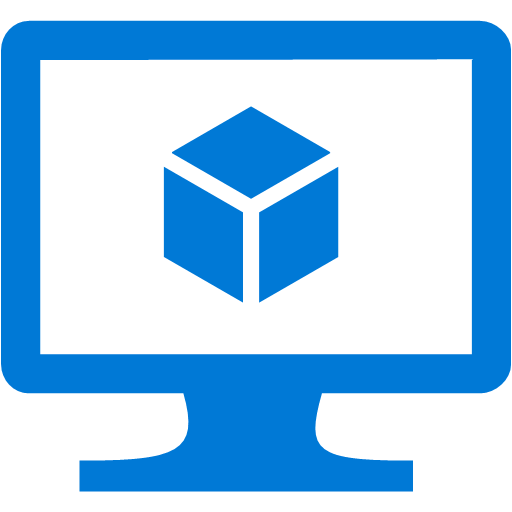
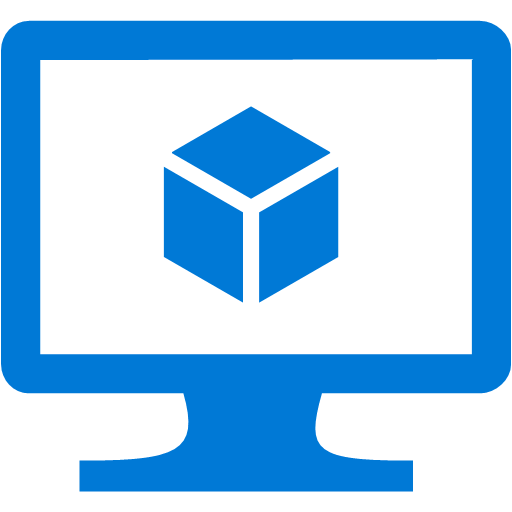
is in samenspraak met het SURFnet SURFcumulus team “least-privileged’ ingericht.

* Er is ten behoeve van de CloudBolt CMP aangrijping van de Azure resources een Application principal geregistreerd en een secret daarvan met SURFcumulus team uitgewisseld. Voor alsnog waren bij de eerste releases van CloudBolt Azure RBAC *Owner* rechten voor deze Principal vereist. Maar ook deze rechten zijn met de laatste release van CloudBolt (8.9 en hoger) “least privileged” ingeregeld.
* Recent (oktober 2019) is er in samenspraak met het SURFnet SURFcumulus team een CloudBolt CMP acceptatie omgeving met onderliggende dedicated acceptatie Azure workspaces en een dedicated acceptatie Azure Application principal ingericht. Hiermee kan de hele CMP naar Azure keten bij nieuwe releases worden getest en geaccepteerd.

# Datastromen en zonering

Voor elk van de Virtuele Organisatie (VO) workspaces zijn geautomatiseerd zogenaamde *Mapped* en *UnMapped* IPv4 private space netwerk subnets geconfigureerd. De UnMapped subnets zijn recht door zee: daarbinnen kan via het SURFcumulus CMP door de researcher zelf schier ongelimiteerd resources via CMP Blueprints (templates voor standaard Operating Systeem en XaaS/PaaS resources) aan worden gemaakt. Elk van deze UnMapped subnets manifesteert zich via SNAT translatie (private => public) met een (pér workspace) publiek IPv4 adres naar de rest van de netwerkinfrastructuur.

In het SURFcumulus CMP kan voor een resource ook het per VO Mapped subnet worden geselecteerd. Ook elk Mapped subnet kent zijn eigen SNAT translatie. Out-of-the-box worden daarnaast binnen elke VO workspace de eerste vier private IPv4 adressen met DNAT translaties (public => private). Via die vier publieke IPv4 adressen zijn die resources, uiteraard onder regie van de on-premises FortiGate NGFW policies, ook extern vanuit bijvoorbeeld CDW en VIEW benaderbaar. En zo zijn in selfservice ook bijvoorbeeld management servers, stepping stones en/of web services in te richten. Met deze opzet wordt de toch wel beperkt beschikbare publieke IPv4 ruimte optimaal benut zonder dat het aantal resources binnen de SURFcumulus beperkt wordt of de netwerkinfrastructuur vervuild wordt met (Azure, AWS, Google) private IPv4 adressen. Dit netwerkmodel past ook naadloos in de Microsoft hub en spoke opzet en is door Microsoft gevalideerd. Zie ook Figuur 3.

https://106c4.wpc.azureedge.net/80106C4/Gallery-Prod/cdn/2015-02-24/prod20161101-microsoft-windowsazure-gallery/Microsoft.NetworkSecurityGroup-ARM.1.0.5/Icons/Small.png

Figuur 3 SURFcumulus VRC netwerkinfrastructuur

Amsterdam UMC Azure Playgound

SNAT

DNAT

Workspace #N VRC VUmc\_ICT Production

Unmapped Subnet

10.250.1.0/24

Mapped Subnet

10.250.0.0/24

VM

vrc001-prod-rh01

10.250.0.4

VM

vrc001-prod-rh02

10.250.1.4

AADS VNet aads-vnet-01

10.1.0.0/24

default

10.1.0.0/24

FortiGate

Frontend

Subnet

145.121.124.0/22

FortiGate

Inside

Subnet

145.121.48.32/29

10.1.0.8

KMS

azure-kms01.research-cloud.nl

10.1.0.4

research-cloud.nl

research-cloud.local

Hub VNet TESTAUMC-vnet-01

Spoke VNet #N vrc001-prod-vnet-01

10.250.0.0/23

**AADDS-research-cloud.nl-NSG**

145.121.0.0/16

FortiGate

VUMC-FG01

145.121.63.142

145.101.114.0/24

145.121.124.125

145.121.48.36

FortiGate

azureplayfg01

On-Premises Network

ExpressRoute

Gateway

Peering

Peering

ldaps 663

SURFnet SCZ services

# Infrastructuur

## Infrastructure as a Code

Met vallen en opstaan en met in eerste lezing inzetten van creditcard accounts is de Azure omgeving met de ExpressRoute en FortiGate appliance (zie figuur 3) met de hand via de Azure portal opgezet. Maar al vroeg in het traject bleek, ook door aangeven van Microsoft architecten dat het hanteren van een strikte resources naamconventie vereist is. En dat het aantal workspaces zo zou oplopen, per februari 2020 zijn er meer dan 20 workspaces/Virtuele Organisaties actief) dat het dan al onvermijdelijk werd om Infrastructure as a Code (IaaC) technieken in te zetten. Er is dan ook zo een codering omgeving opzet dat workspaces geheel conform de vastgestelde naam conventie worksheet *geautomatiseerd* en *consistent* opgezet worden. Zie figuur 4, en de referentie Azure naming convention worksheet.

Ook voor het onderhoud van workspaces, bijvoorbeeld voor het toevoegen van User Defined Routes (UDR’s), Event Subscriptions en filtering e.d. is code ontwikkeld om vanuit de Azure *Management Group* de diverse workspace gestructureerd en eenduidig configuraties aan te kunnen passen en uit te kunnen rollen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Service or Entity** | **Scope** | **Suggested Pattern** | **Example** |
| Resource Group | Resource Group | Global | <service short name>-<environment>-rg | profx-prod-rg |
| Resource Group | Availability Set | Resource Group | <service-short-name>-<context>-as | profx-sql-as |
| General | Tag | Associated Entity | "key" : "value" | "department" : "Central IT" |
| Compute | Virtual Machine | Resource Group | <name>-<role>-<instance> | profx-sql-001 |
| Storage | Storage account name (data) | Global | <service short name><type><number> | profxdata001 |
| Storage | Storage account name (disks) | Global | <vm name without dashes>st<number> | profxsql001st0 |
| Storage | Container name | Storage account | <context> | logs |
| Storage | Blob name | Container | <variable based on blob usage> | <variable based on blob usage> |
| Storage | Queue name | Storage account | <service short name>-<context>-<num> | awesomeservice-messages-001 |
| Storage | Table name | Storage account | <service short name>-<context> | awesomeservice-logs |
| Storage | File name | Storage account | <variable based on blob usage> | <variable based on blob usage> |
| Networking | Virtual Network (VNet) | Resource Group | <service short name>-[section]-vnet | profx-vnet |
| Networking | Subnet | Parent VNet | <role>-subnet | gateway-subnet |
| Networking | Network Interface | Resource Group | <vmname>-<num>nic | profx-sql1-1nic |
| Networking | Network Security Group | Resource Group | <service short name>-<context>-nsg | profx-app-nsg |
| Networking | Network Security Group Rule | Resource Group | <descriptive context> | sql-allow |
| Networking | Public IP Address | Resource Group | <vm or service name>-pip | profx-sql1-pip |
| Networking | Load Balancer | Resource Group | <service or role>-lb | profx-lb |
| Networking | Load Balanced Rules Config | Load Balancer | descriptive context | http |
|  |  |  |  |  |
| **Environment** | **Full Name** |  |  |  |
| Production | Contoso SocialGaming AwesomeService Production |  |  |  |
| Dev | Contoso SocialGaming AwesomeService Dev |  |  |  |
| Production | Contoso IT InternalApps Production |  |  |  |
| Dev | Contoso IT InternalApps Dev |  |  |  |

Figuur 4 Microsoft Azure naming convention

## Beschikbaarheid

De DVO van de on-premises VUmc Research Cloud bedroeg richting de Research community 99.50%.

De beschikbaarheid van de in dit document beschreven Amsterdam UMC SURFcumulus Research Cloud wordt in hoofdlijnen door drie onderdelen bepaald:

* SURFcumulus CloudBolt infrastructuur (99.90%)
* Netwerkinfrastructuur *dubbel* uitgevoerd, hoog beschikbaar ingeregeld (99.99%):
  + SURFnet Internet opgang.
  + on-premises FortiGate NGFW.
  + SURFnet Multi Service Port (MSP).
  + Microsoft ExpressRoute.
* Microsoft Azure locatie West-Europe: SLA 99.95%
* De beschikbaarheid van de Azure FortiGate appliance wordt in hoge mate bepaald door de beschikbaarheid van Azure locatie West-Europe en is daarmee 99.95%.

Overall beschikbaarheid van deze SURFcumulus Research Cloud infrastructuur komt daarmee boven de 99.80% uit. Hierdoor is de doelstelling om in ieder geval de dienstverlening qua beschikbaarheid niet te verslechteren gerealiseerd. En is ook door toevoeging van redundantie het uitvoeren van onderhoud aan de onderliggende componenten en onderdelen behoorlijk gestroomlijnd.

## Monitoring

De monitoring van de on-premises FortiGate NGFW, de ExpressRoute en de FortiGate DNAT/SNAT appliance is door het netwerkteam binnen de standaard SolarWinds oplossing geregeld. De monitoring van de Azure infrastructuur, met name de beschikbaarheid en de back-ups van Virtual Machines, wordt door een ingericht Azure LogAnalytics platform geregeld (zie LLD LifeCycle Management Amsterdam UMC Research Cloud Platform).

## Firewalling

De on-premises redundant uitgevoerde FortiGate NGFW is ook voor deze SURFcumulus Research Cloud hét chokepoint waar alle (Enterprise) rulesets zijn bepaald en waar al het ingress en egress netwerkverkeer wordt gecontroleerd.

Er wordt wel overwogen om het intern gericht netwerkverkeer, zoals van en naar interne storage of andere diensten, via de al aangeschafte interne datacenter FortiGate NGFW te laten lopen.