|  |  |
| --- | --- |
|  |  |
| Projectnaam: | Lifecycle Management Amsterdam UMC Research Cloud Platform |
| Projectnummer: | 2018-032 |
| Auteur: | Cédric Laurent / Fons Ullings |
|  |  |
| Gewijzigd door: | Fons Ullings |
| Datum: | 20-07-2020 |
| Versie: | 1.1 |
| Status document: | Final |

Inhoud

[1. Inleiding 3](#_Toc46151943)

[2. azure-play-OnVMcreate 4](#_Toc46151944)

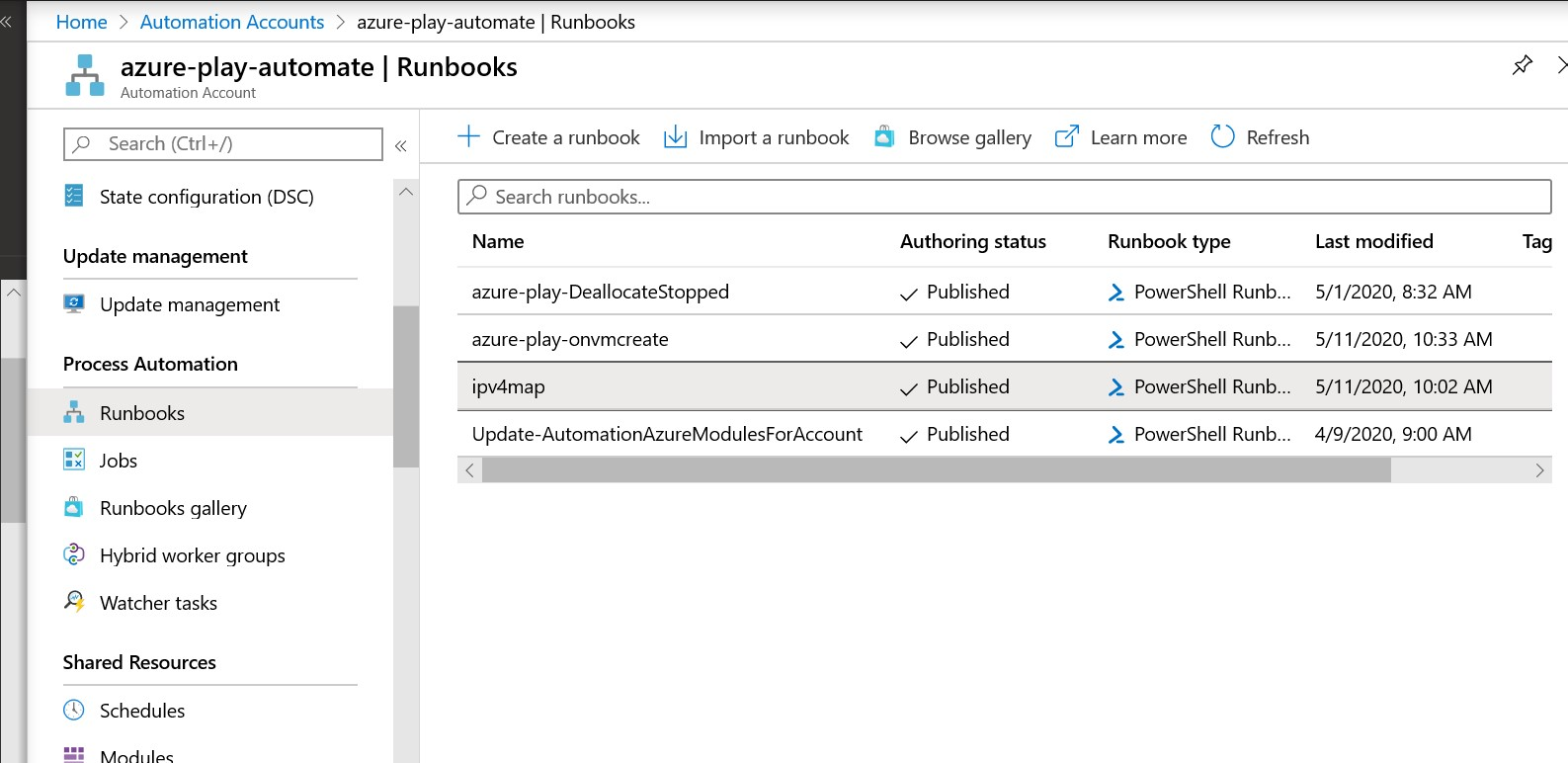
[3. ipv4map 4](#_Toc46151945)

[4. azure-play-DeallocateStopped 4](#_Toc46151946)

[5. Update-AutomationAzureModulesForAccount 5](#_Toc46151947)

# Inleiding

Een aantal van de functionele eisen die binnen het Amsterdam UMC Research Cloud traject zijn geformuleerd, zijn niet out-of-the-box door Azure configuraties te bestendigen. Dit document beschrijft een tweetal Power Shell Runbooks die binnen het Azure Automation framework zijn ontwikkeld. Deze Automation Runbooks zijn binnen de “hub” workspace *azure-play-automate* geïmplementeerd (zie HLD en LLD) en maken gebruik van een Azure “run as” account dat out-of-the-box opgezet is. Dit “run-as” account heeft via de centrale Azure Management Group 'SURFcumulus-Amsterdam-UMC-VRC-Production’ inherited Contributor rechten op alle workspaces die binnen deze Management Group ondergebracht zijn.



Dit document geeft van elk van deze Automation Runbooks een technisch/functionele beschrijving. De Power Shell code van deze Automation Runbooks is self-documented met toevoeging van comments opgeschreven.

# azure-play-OnVMcreate

De Automation Runbook *azure-play-OnVMcreate* wordt vanuit elk van de workspaces Automation Account via een webhook getriggerd meteen nadat er een succesvol een Virtual Machine is aangemaakt (“write success” filter). Dit biedt de optie om allerlei noodzakelijk post-processing uit te voeren.

In de huidige versie heeft deze Automation Runbook twee belangrijke rollen:

1. DNS registratie(s) van de VM waarbij de IPv4 NAT translatie wordt meegenomen bij het bepalen van het DNS A record. En dat ook het Cloud Management Portal (CMP) CloudBolt deze DNS registratie(s) kent en naar de Researchers kan representeren.
2. Het aanzetten (enable) van back-up policy LocalPolicy zodat altijd (!), onafhankelijk van de interacties van de Researchers, van de VM’s back-ups t.b.v. disaster recovery worden gemaakt.

Maar deze Automation Runbook kan natuurlijk voor een diversiteit aan andere post-processing worden ingezet. En kan ook via CloudBolt parameters (Tag’s) meekrijgen zodat deze post-processing ook weer door de Researchers (zonder toegang tot Azure) zelf gestuurd kan worden.

N.B. *OnVMcreate* is een legacy naamgeving (geworden) en zou nu zoiets als *OnVMcreate* moeten zijn. Maar dit zou voor een volgende lifecycle van de Research Cloud op de agenda kunnen staan.

N.B. SURFdomeinen heeft géén API (…) en het is dan ook niet mogelijk om deze DNS informatie vanuit een stuk Automation in SURFdomeinen op te voeren.

# ipv4map

Is een Automation child Runbook die vanuit *azure-play-OnVMcreate* wordt aangeroepen en waarin de netwerk NAT vertaaltabel staat.

N.B. het is beslist de ontwikkelambitie om deze NAT vertaling via de FortiGate API automatisch op te halen zodat er een single source of truth is.

# azure-play-DeallocateStopped

Bij de eerste experimentele live-gang van deze Research Cloud liepen de kosten voor een aantal Research groepen onverwacht hoog op: deze Researchers waren gewend om na een intense reken job de betreffende VM bijvoorbeeld vanuit de applicatie een *shutdown* te geven. Door zo een *shutdown* raakt deze VM in Azure in *Stopped* state en blijven de Azure kosten gewoon doorlopen. Deze Automation Runbook gaat met een Automation Schedule elk uur alle workspaces en alle VM’s daarin af om *Stopped* state machines in *Deallocated* state te brengen. Waardoor alleen nog maar de vaak beperkte storage kosten voor deze VM’s doorlopen.

N.B. Het is zeker denkbaar om net als azure-play-OnVMcreate een vergelijkbare Webhook trigger bij het stoppen van een VM te laten uitvoeren. Maar dit is nog voer voor ontwikkeling.

# Update-AutomationAzureModulesForAccount

Tot voorkort was in de Azure portal de versioning van Azure Az Power Shell Modules te managen. Maar Microsoft heeft dit hele proces nu in een Automation Runbook ondergebracht.

Zie: <https://docs.microsoft.com/en-us/azure/automation/automation-update-azure-modules>