



PLAN VAN AANPAK STAGE

VANROEY.BE | 22/04/2021

PHILIPPE BOETS | GIANNI JORDENS

R0744284@student.thomasmore.be | r0738258@student.thomasmore.be



INHOUD

Inleiding	2
Beschrijving stageopdracht	2
Motivatatie en business value	2
1. cloud adoption framework	3
2. Plan	4
2.1. inventariseren en analyseren	4
2.1.1. Inventaris analyseren	5
2.1.2. Workloads definiëren en prioriteren	5
2.1.3. Volgorde bepalen	5
2.2. Nieuwe tenant plannen	6
2.2.1. CAF Foundation Blueprint	6
2.2.2. RBAC	8
3. Ready	9
3.1. Identity en access control security	9
3.1.1. RBAC best practices	9
3.1.2. pim best practices	10
3.2. Cost management	10
3.3. Security en monitoring	11
4. Adopt	12
4.1. Security policies toepassen	12
4.2. RBAC	13
4.3. Policies	13
4.4. Testen	14
5. Besluit	14



INLEIDING

BESCHRIJVING STAGEOPDRACHT

Vanroey.be beschikt over verschillende Azure tenants, hierdoor is het overzicht op vlak van financiën, rechten en resources in alle klantgerichte tenants en test omgevingen zoek. Als stageopdracht hebben wij de opdracht gekregen om deze Azure tenants te analyseren en een nieuwe tenant aan te maken waarop we alle subscriptions, resources en gebruikers van de eerder gemaakte tenants samenvoegen. Deze 'master' tenant richten we in volgens het Cloud Adoption Framework. Hierdoor is er een overzichtelijke structuur binnen de tenant waar in de toekomst ook verder op gebouwd kan worden.

MOTIVATIE EN BUSINESS VALUE

In de huidige situatie is het overzicht zoek, er zijn veel verschillende tenants waardoor navigeren tussen deze tenants moeizaam wordt. Ook is het onduidelijk welke rechten bepaalde gebruikers hebben binnen deze tenants, wat een securityprobleem kan zijn. Er kunnen bepaalde resources dubbel aangemaakt zijn en er is geen duidelijk overzicht van alle kosten die gemaakt worden in deze tenants.

Bij één enkele goed uitgewerkte Azure tenant kan er een duidelijke structuur opgesteld worden waarbij gebruikers de juiste rechten toegekend krijgen zodat ze enkel toegang hebben tot de middelen die ze nodig hebben om hun werk te doen. In die structuur kan er een duidelijke onderverdeling gemaakt worden zodat de verantwoordelijke van financiën een duidelijk overzicht heeft van alle kosten in de tenant. Door alles in één tenant samen te voegen zal het ook duidelijk worden welke resources er allemaal zijn, en kan er efficiënter aan kost management gedaan worden.

Het uiteindelijke doel van de opdracht is dus één overzichtelijke, goed gemanagede tenant te creëren met als doel een duidelijk overzicht te krijgen van alle resources, rechten en kosten.



1. CLOUD ADOPTION FRAMEWORK

Om deze opdracht tot een goed einde te brengen gaan we gebruik maken van het Cloud Adoption Framework van Microsoft (CAF). Dit framework bestaat uit een aantal strategieën, tools, best practices en documentatie om een organisatie voor te bereiden en te helpen hun cloud infrastructuur te implementeren en uit te breiden. Dit allemaal in een goed opgebouwde en gemanagede omgeving. Cloud Governance is een belangrijke term in dit geheel. Cloud Governance is een verzamelterm voor alle tools en best practices om een cloud omgeving efficiënt te monitoren, beheren, beveiligen en om cost controls in te voeren.

Het Cloud Adoption Framework bestaat uit een aantal stappen die uiteindelijk leiden tot een uniforme, beveiligde en goed gemanagede omgeving. Bij elk van deze stappen wordt er rekening gehouden met Governance en het overzichtelijk managen van alle cloud resources.

Stappen CAF:

1) Plan:

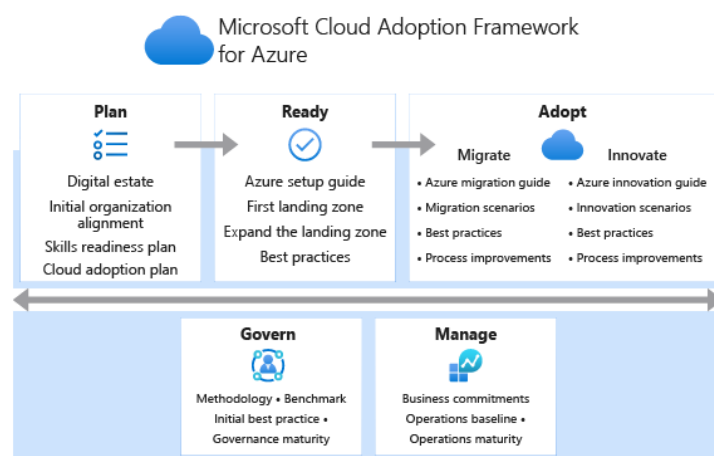
- a) Eerst moet er een plan gemaakt worden waarin beschreven wordt welke resources allemaal bestaan, welke user er welke rechten hebben, welke policies van toepassing zijn, Er wordt beschreven welke resources naar waar moeten verplaatsen en hoe dit aangepakt gaat worden.

2) Ready:

- a) De tweede stap is het voorbereiden van de cloud omgeving. Er moet een basis gemaakt worden waarop alle workloads uiteindelijk gaan draaien. We bedoelen hiermee een goede organisatorische structuur aanbrengen waarop we Role Based Acces Control (RBAC), policies en management groups. Verder zorgen we dat alles klaar staat voor security, monitoring en cost-monitoring.

3) Adopt:

- a) De derde stap is het eigenlijke migreren van alle workloads naar de nieuwe omgeving. Best practice is beginnen met de minst mission critical workload zodat de impact op de werking van de organisatie miniem is en er al getest kan worden of de omgeving robuust is.



Figuur 1: De stappen van het Cloud Adoption Framework



2. **PLAN**

Tijdens de planningsfase gaan we de bestaande tenants eerst analyseren zodat we een goed beeld krijgen waar deze tenants voor dienen en wat er allemaal van subscriptions, resources, RBAC rollen, policies, security, structuur (management/resource groups, ...) en gebruikers aanwezig is. Daarna gaan we kijken hoe we de nieuwe tenant volgens het CAF kunnen opzetten.

2.1. **INVENTARISEREN EN ANALYSEREN**

De eerste stap van deze fase zal het inventariseren en analyseren van alle bestaande tenants en hun inhoud zijn. We gaan per tenant volgende zaken opsommen:

- Structuur:
 - o Welke management groups bestaan er?
 - o Welke actieve subscriptions zijn er?
 - o Welke resource groups bestaan er?
- Resources:
 - o Welke resources bestaan er en waarvoor dienen deze?
 - o Dependencies van elke resource
- RBAC:
 - o Welke custom roles zijn er aangemaakt?
 - o Welke groepen zijn er aangemaakt en welke soort (Security, O365 ,...)?
 - o Welke rechten en rollen zijn toegekend aan gebruikers en op welke scope (subscription, resource group of specifieke resource)?
- Gebruikers:
 - o Welke gebruikers zitten in welke groepen?
- Monitoring:
 - o Welke resources worden hoe gemonitord?
 - o Bestaan er eventueel alerts?
- Data:
 - o Wat voor data wordt er verwerkt of bijgehouden?
 - o Hoe vertrouwelijk of belangrijk is deze data?
 - o Waar en hoe wordt deze data opgeslagen(sql database, blob storage,...)?
- Security:
 - o Welke policies met betrekking tot security bestaan er?
 - o Welke tools worden al gebruikt: Azure Sentinel, ... ?
- Policies:
 - o Welke policies bestaan er?
 - o Hoe worden deze toegepast?
- Welke applicaties runnen op welke resources?
- Wordt er gewerkt met Azure DevOps, Github, ... ?



2.1.1. **INVENTARIS ANALYSEREN**

Nadat we een grondige inventaris van alle assets uit elke tenant gemaakt hebben kunnen we deze data gaan analyseren. Dit zodat we weten waar alle assets voor dienen en ook zodat we eventueel een aantal dingen kunnen optimaliseren. We gaan dus kijken of resources efficiënt gebruikt worden bv: een virtual machine die 8 vCPU's en 16gb RAM heeft, maar er eigenlijk maar 6vCPU's en 8gb RAM nodig heeft.

Het is ook belangrijk dat we per tenant samenzitten met alle partijen die met de tenant iets te maken hebben. Zo kunnen we een beeld vormen waarvoor elke tenant dient en hoe belangrijk deze zijn. We gaan dus een meetings organiseren per tenant met de perso(o)n(en) die deze tenant opgezet hebben of beheren.

Door de inventaris op deze manier te analyseren gaan we dus een beter inzicht krijgen naar de werking van elke tenant, en kunnen we dus efficiënter deze tenants gaan migreren en optimaliseren.

2.1.2. **WORKLOADS DEFINIËREN EN PRIORITEREN**

Een tweede doel van onze analyse is het definiëren van workloads binnen elke tenant. Een workload is één duidelijk afgebakend proces dat binnen de tenant draait, en alle resources die daarbij horen om dat proces mogelijk te maken. Een workload kan bijvoorbeeld een webapplicatie zijn, daarbij horen dan enkele resources zoals een webserver, een database, app insights, een vnet, We moeten dus binnen onze inventaris resources gaan groeperen per workload.

Het is ook mogelijk dat twee workloads van elkaar afhankelijk zijn, of dat bijvoorbeeld één workload input verwacht van een andere workload. Daarom is het belangrijk per tenant de workloads te definiëren en ook de dependencies per workload bijhouden.

2.1.3. **VOLGORDE BEPALEN**

Aan de hand van deze analyse gaan we de volgorde van de migratie bepalen. Volgens prioriteit gaan we eerst de minst belangrijke workloads migreren. Hierbij is het belangrijk dat alle betrokken partijen op de hoogte zijn van de migratie, zodat bijvoorbeeld developers ineens zonder resources zitten. Er moet dus per tenant correct afgesproken worden met alle gebruikers van de workloads die in een tenant draaien.



2.2. NIEUWE TENANT PLANNEN











Nadat we een inventaris en een goed inzicht hebben van de bestaande tenants kunnen we beginnen met het plannen van de centrale tenant. Hier gaat het dan over de structuur (management groups, user groups, ...) en policies die overkoepelend over de hele tenant nodig zijn.

We gaan kijken welke subscriptions bij elkaar gegroepeerd moeten worden.. Door onze analyse zal het duidelijker worden of al dan niet bepaalde tenants samengevoegd of zelfs helemaal verwijderd kunnen worden. Daarnaast gaan we ook monitoring en beveiliging

2.2.1. CAF FOUNDATION BLUEPRINT

Als basis van deze tenant gaan we gebruik maken van de CAF Foundation blueprint die in Azure ingebouwd is. Deze blueprint vormt al een goede basis voor het aanmaken van een nieuwe tenant. In deze blueprint worden een aantal policies uitgerold die ervoor zorgen dat er volgens best practices en industrie standaarden gewerkt wordt.

Volgende policies zitten al in de CAF blueprint, we kunnen uiteraard na onze analyse nog policies toevoegen maar deze blueprint vorm een goede basis:

 Append CostCenter TAG & its value from the Resource Group	Policy assignment	1 out of 1 parameters populated	***
 Append CostCenter TAG to Resource Groups	Policy assignment	1 out of 2 parameters populated	***
 Enable Monitoring in Azure Security Center	Policy assignment	105 out of 105 parameters populated	***
 Allowed locations	Policy assignment	0 out of 1 parameters populated	***
 Allowed locations for resource groups	Policy assignment	0 out of 1 parameters populated	***
 Deploy network watcher when virtual networks are created	Policy assignment	None	***
 Resource Types that you do not want to allow in your environment	Policy assignment	0 out of 1 parameters populated	***
 Secure transfer to storage accounts should be enabled	Policy assignment	None	***
 Allowed storage account SKUs	Policy assignment	0 out of 1 parameters populated	***
 Allowed virtual machine SKUs	Policy assignment	0 out of 1 parameters populated	***


- De eerste twee policies dienen om een tag toe te voegen aan resource groups. Deze tag is bedoeld om cost monitoring in te stellen, alle resources in deze resource groups krijgen dezelfde tag. De exacte naam van de tag is nog af te spreken.
- Enable Monitoring in Azure Security Center
- Allowed locations beperkt het aantal locations waar resources aangemaakt kunnen worden, bijvoorbeeld: resources mogen alleen in de West Europa regio aangemaakt worden. Hetzelfde geldt voor resource groups.
- Network watcher wordt automatisch aangezet in elk vnet dat aangemaakt wordt voor monitoring.



> PLAN VAN AANPAK STAGE

- De volgende policy zorgt ervoor dat bepaalde soorten resources niet aangemaakt kunnen worden. Bvb: resources van het type Azure Classic Storage mogen niet aangemaakt worden omdat dit een oude manier is van werken.
- De Secure transfer to storage accounts should be enabled policy zorgt ervoor dat storage accounts enkel via een beveiligde verbinding data kunnen doorgeven. Dus als via een REST API call data opgevraagd wordt moet deze request over HTTPS lopen, alle HTTP requests worden tegen gehouden.
- De laatste twee policies bepalen welke vm en storage account SKUs gebruikt kunnen worden, dit om te vermijden dat te dure vm's aangemaakt worden.

Daarnaast worden er ook enkele resources en resource groups aangemaakt via een Azure Resource Manager (ARM) template:

 Azure Security Center template	Azure Resource Manager ...	None
+ Add artifact...		
 Resource Group for Shared Services	Resource group	2 out of 2 parameters populated
 Deploy Key Vault	Azure Resource Manager ...	0 out of 2 parameters populated
 Deploy Log Analytics	Azure Resource Manager ...	0 out of 3 parameters populated
+ Add artifact...		

Eerst wordt de Azure Security Center tier naar standard gezet, dit is best practice omdat de standard tier veel betere monitoring en beveiliging biedt. Hier hangt wel een bepaalde kost aan vast naargelang de grootte van de omgeving, dit wordt later nog besproken met de stakeholders.

Daarna wordt er een resource group aangemaakt voor alle gedeelde services. Hierin wordt een key vault aangemaakt, tijdens de blueprint assignment moet er een object ID meegegeven van de gebruiker(s) of groep die rechten heeft om de key vault aan te passen.

Als laatste wordt er nog een log analytics workspace aangemaakt voor het monitoren van de omgeving. Hier moet meegegeven worden in welke Azure locatie de resource aangemaakt moet worden en ook het aantal dagen dat de logs bijgehouden moeten worden (tussen 30 en 365 dagen). Alle resources die aangemaakt worden hebben ineens ook een resource lock opstaan zodat ze niet per ongeluk verwijderd kunnen worden.

Na onze analyse zullen er waarschijnlijk nog enkele policies toegevoegd moeten worden om aan de eisen van VanRoey te voldoen.

De CAF foundation blueprint vormt samen met de extra afgesproken policies een governance-baseline blueprint. Deze blueprint gaan we aanmaken in de root management group zodat alle onderliggende management groups (en dus ook de subscriptions die hier in zitten) via inheritance ook aan de policies moeten voldoen.



2.2.2. **RBAC**

Aangezien de RBAC rollen niet mee overgezet kunnen worden is het belangrijk dat we goed bijhouden welke rollen van toepassing zijn op welke resources. Het is de bedoeling dat we in de nieuwe tenant met user groepen gaan werken voor role assignments. Het doel is zo weinig mogelijk (liefst geen) roles toe te kennen aan individuele gebruikers. Dit helpt ons een overzicht te behouden over alle role assignments die er zijn en zorgt er ook voor dat er een minimum aan assignments gedaan moet worden. Dit kan ook helpen bij grote organisaties aangezien er een limiet is van 2000 role assignments per subscription, dit lijkt veel maar het aantal assignments kan snel oplopen als die niet goed gemanaged wordt. Het is dus best practice om rechten aan groepen toe te kennen en dan gebruikers in deze groepen toe te voegen om ze de rechten te geven.



We gaan per tenant een overzicht maken wie welke rechten nodig heeft, dit gaan we in samenwerking met de nodige mensen moeten doen aangezien wij niet weten wie waar aan moet kunnen. Dan kunnen we ineens kijken of alle rechten nog up to date zijn en of er eventuele custom roles gebruikt worden. We gaan ook het principe of least privilege toepassen, dit principe zegt dat gebruikers zo weinig mogelijk privileges krijgen om hun job ongehinderd uit te kunnen voeren. Dit zorgt ervoor dat gebruikers enkel aan de resources kunnen die ze nodig hebben en niets meer. Hierdoor zal de omgeving veiliger worden omdat niemand aan alle resources kan.

Privileged Identity Management (PIM) is binnen het RBAC gebeuren ook een belangrijke service. PIM kan helpen bij het managen, controleren en monitoren van toegang tot belangrijke resources en data. Deze service werkt met een aantal concepten die we gaan toepassen om de omgeving veiliger te maken.

Pim staat ons toe om just-in-time privileged acces te geven aan gebruikers.

Dit betekent dat admin gebruikers niet altijd geprivilegieerde rechten (dit zijn rechten die toe staan belangrijke resources zoals subscriptions aan te passen) hebben, maar enkel wanneer ze die nodig hebben. Een gebruiker die geprivilegieerde rechten wilt om bepaalde acties uit te voeren moet deze dan aanvragen en ook verantwoorden. Zo krijgt een administrator een overzicht van wie wanneer welke rechten aangevraagd heeft en waarom. We gaan ook Multi Factor Authentication (MFA) instellen, zodat een gebruiker die rechten aanvraagt zich moet authenticeren via bvb. de Microsoft Authenticator app op zijn/haar smartphone. Door MFA in te stellen zijn we zeker van de identiteit van de persoon die de rechten aanvraagt, en is de omgeving dus beter beveiligd.





3. **READY**

In de ready fase gaan we zorgen voor een correcte setup van de tenant waarop alles geconsolideerd wordt. We gaan ons hier aan de best practices van het CAF houden.

Tijdens het opzetten van de nieuwe tenant (en ook tijdens de adopt fase) gaan we rekening houden met de best practices voor de volgende concepten:

- Security:
 - o Azure Security Center (ASC)
- Identity en access control:
 - o RBAC
 - o PIM
- Cost management:
 - o Kosten bijhouden en monitoren via policies/tagging
 - o Budgets
 - o Cost alerts
 - o Cost reduction

3.1. **IDENTITY EN ACCESS CONTROL SECURITY**

We gaan uiteindelijk werken met guest users die vanuit de VanRoey.be AD geïnviteerd worden. In de VanRoey.be tenant. Ondanks dat daar ook al aan MFA gedaan wordt gaan wij de de nieuwe tenant ook voorzien van privileged identity management (PIM) met MFA en de nodige RBAC rechten op de managementgroepen en resources.

3.1.1. **RBAC BEST PRACTICES**

Het principle of least privilege zegt dat users zo weinig mogelijke rechten krijgen zoals eerder vermeld. We moeten er dus voor zorgen dat rollen op de juiste scope worden toegepast, zodat gebruikers bvb. niet toegang hebben tot een hele resource group maar enkel de resources die ze nodig hebben. Als dus 1 gebruiker gebreached is, zijn enkel de resources waar deze gebruiker toegang toe heeft in gevaar.

Limiteer het aantal subscription owners. Microsoft raadt aan maximum 3 owners per subscription te hebben. Dit verkleint ook het risico op een breach.

PIM wordt ook ten zeerste aangeraden om geprivilegieerde rollen te beschermen.

Ken rollen toe aan groepen, niet individuele gebruikers. Dit houdt alles overzichtelijk en maakt het ook gemakkelijker gebruikers rollen toe te kennen of af te nemen.



3.1.2. **PIM BEST PRACTICES**

Voor privileged identity management (PIM) zijn er ook een paar best practices die je helpen om een beter management te bekomen:

- Voor global administrators zoek je best uit waarom ze die rol nodig hebben, als ze niet het alle aspecten van global administrator gebruiken maak je best een **custom role** aan met de nodige privileges.
- Microsoft raadt aan dat er **geen enkele permanente global administrator** toegekend is in de tenant buiten 2 “in case of emergency” accounts.
- Rollen die toegekend zijn aan groepen kunnen via PIM individueel opgenomen worden door leden van die groep. Hierdoor wordt het management van RBAC via groepen versterkt.
- Gebruik users die verantwoordelijk zijn voor resources, subscriptions als **goedkeurder voor PIM** rollen in plaats van een global administrator.
- Stel al de **Global Administrators en Security Administrators eerst** in via PIM omdat zij het meeste schade kunnen aanrichten als ze gecompromitteerd worden.
- Volgende **rollen moeten zeker via PIM** ingesteld worden (niet permanent dus): User administrator, Exchange administrator, SharePoint administrator, Intune administrator, Security reader, Service administrator, Billing administrator, Skype for Business administrator

3.2. **COST MANAGEMENT**

Om een goede, transparante kostenstructuur te verkrijgen is het noodzakelijk om vanaf stap 1 een goede organisatie te behouden. Om een transparant kostenbeleid te bekomen passen we een aantal best practices toe:



Ten eerste is **een duidelijke hiërarchische structuur nodig** binnen de organisatie (resource groups, management groups, ...). Subscriptions indelen volgens afdeling of omgeving zorgt voor meer duidelijkheid

Classificeer resources aan de hand van tags. Door tags te gebruiken kan er in het Cost Management portaal een beter overzicht gegeven worden. Best practice is minstens de volgende drie tags toe te voegen: Cost Center, departement/afdeling, resource owner. Zo kan er gesorteerd worden op deze criteria en kan er bvb. een overzicht van de kosten per afdeling gegeven worden. Dit kan gemakkelijk aan de hand van policies afgedwongen worden.

Zorg dat er per team of afdeling minstens 1 persoon is met de **Cost Management Contributor rol**. Deze rol staat toe om budgetten te stellen en om kosten te monitoren.

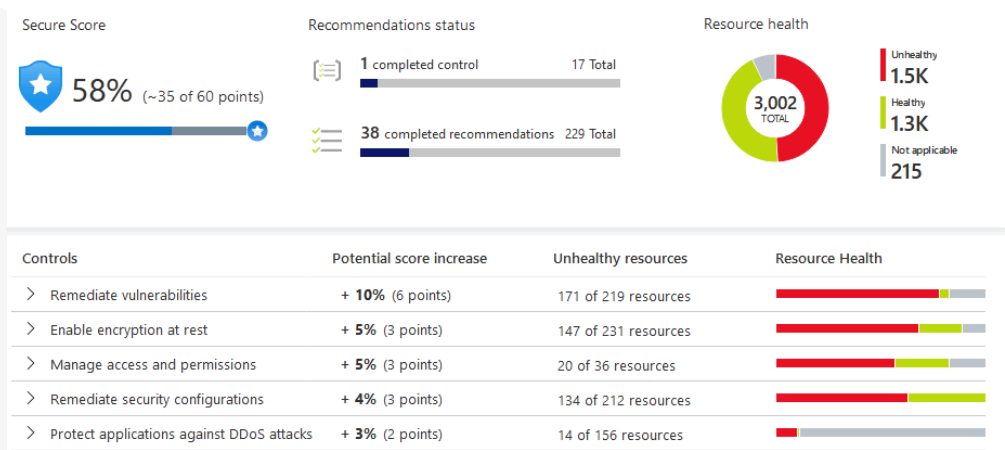


3.3. SECURITY EN MONITORING

Voor monitoring en security gaan we gebruik maken van **Log Analytics** en **Azure Security Center**. Deze tools centraliseren alle data die in de logs verzameld wordt.

Security Center is een centraal dashboard die het beveiligen van een cloud omgeving vergemakkelijkt. Het helpt om ons de omgeving te beveiligen tegen aanvallen, snel en efficiënt resources beveiligen en geeft een overzicht van de algemene beveiliging aan de hand van Secure Score.

Security Center ontdekt voortdurend nieuwe resources en beoordeelt of ze zijn geconfigureerd volgens de best practices voor beveiliging. Zo niet, dan worden ze in een geprioriteerde lijst gegoten , in de lijst staan ook aanbevelingen (security controls) voor hoe deze resources veiliger gemaakt kunnen worden. Deze lijst met aanbevelingen wordt mogelijk gemaakt en ondersteund door **Azure Security Benchmark**, de door Microsoft geautoriseerde, Azure-specifieke set richtlijnen voor best practices op het gebied van beveiliging en compliance. Deze benchmark bouwt voort op de controles van het Center for Internet Security (CIS) en het National Institute of Standards and Technology (NIST) met een focus op cloud-centrische beveiliging.



Figuur 2 Secure Score dashboard met security controls

De Azure Security Benchmark bestaat dus uit een set policies en best practices voor een veilige omgeving. In totaal zijn er ongeveer een 100-tal policies die uitgerold zullen worden, het gaat hier over enkel audits dus deze policies gaan geen tags toevoegen of dergelijke. Deze policies lopen van disk encryption moet ingesteld zijn op vm's tot web apps should only be accessible over HTTPS. (voor een gedetailleerde lijst kijk: <https://docs.microsoft.com/en-us/azure/security/benchmarks/overview>)

Er zijn ook nog andere ingebouwde benchmarks zoals ISO 27001, als vanuit VanRoey deze policies nodig zijn kunnen we die ook implementeren.



4. **ADOPT**

In deze fase beginnen we met de uitvoering van onze migratie van de tenants. We starten met de minst kritische tenant zodat we geen kritieke business infrastructuur onomkeerbaar aanpassen.

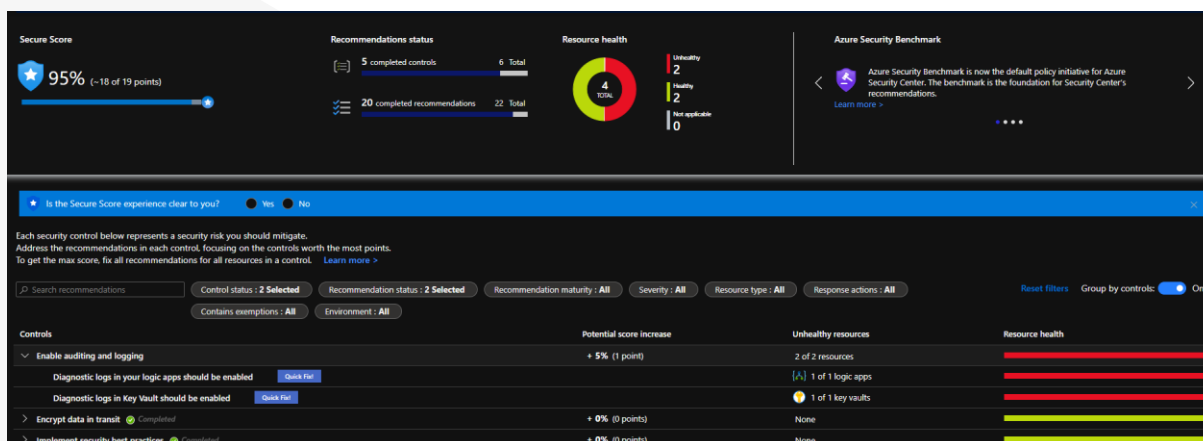
Het is van groot belang dat we per tenant een plan opstellen zodat we duidelijk weten wat we hoe gaan doen, en hoe we dit kunnen doen zonder dingen “kapot” te maken. Daarom gaan we per tenant een document opstellen met een gedetailleerd plan. Bij sommige tenants gaat dit minder belangrijk zijn omdat het over weinig (of minder belangrijke) resources gaat. Omdat we al een goede gedetailleerde samenvatting hebben van alle resources en rollen binnen een tenant moeten we nu alleen nog kijken naar dependencies of custom applicaties/policies die gebruikt worden.

Daarna gaan we over naar de eigenlijke migratie van workloads, rekening houdend met volgende aspecten:

4.1. **SECURITY POLICIES TOEPASSEN**

Zoals in de Ready fase beschreven geeft Azure Security Center(ASC) via de ingestelde policies aanbevelingen om de omgeving veiliger te maken. We gaan per tenant die we overzetten naar deze aanbevelingen kijken en waar mogelijk direct toepassen.

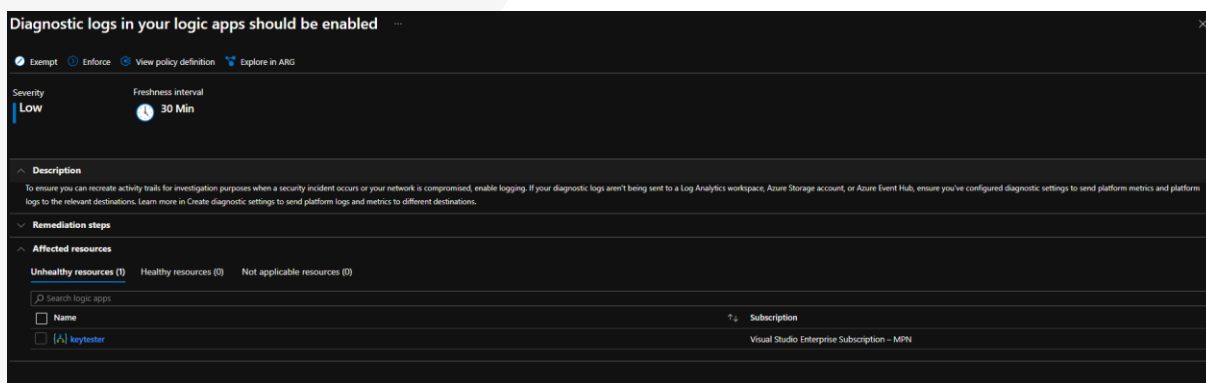
ASC geeft namelijk ook “quick fixes” voor de meest voor de hand liggende problemen:



Per probleem kan doorgeklikt worden naar een overzicht van het probleem:



> PLAN VAN AANPAK STAGE



Per probleem krijgen we een korte beschrijving, een severity en ook een stappenplan om het probleem te verhelpen:

Manual remediation:

To enable diagnostics for a logic app:

1. Open Azure Logic Apps and select the logic app.
2. From the menu, select Diagnostic settings.
3. Select Edit setting if you have an existing setting or select Add diagnostic setting to create a new configuration.
4. Select the options to define what to log and where to store it.
5. Save your settings.

4.2. RBAC

We gaan gebruik maken van onze inventaris om ervoor te zorgen dat alle gebruikers alle rechten die ze nodig hebben toegewezen krijgen. Hier is het belangrijk om te kijken of mensen niet te veel rechten hebben, deze moeten we dan af nemen zodat we via het principe of least privilege blijven werken. We gaan ook zorgen dat PIM overal waar nodig toegepast wordt, want dit wordt nu nog niet overal goed toegepast. Daarnaast zal MFA verplicht zijn voor alle users.

4.3. POLICIES

Net zoals bij security policies geeft Azure ook aanbevelingen om resources compliant te houden aan de policies die wij hun opleggen. We gaan kijken of alle resources die van de andere tenants komen ook compliant zijn aan de standaarden die wij opleggen. Waar nodig gaan we de resources moeten aanpassen zodat ze wel compliant worden. Er gaan waarschijnlijk heel wat resources niet compliant zijn, we hebben namelijk gezien dat de compliance in de verschillende tenants niet altijd even goed is.





4.4. **TESTEN**

Als we dit allemaal gedaan hebben moeten we testen of alles nog werkt hoe het hoort. Als we ons aan het plan houden en de inventaris goed opvolgen zouden er weinig problemen mogen opduiken. Moest er toch iets zijn dat niet meer juist zit, gaan we kijken hoe we dit kunnen oplossen.

Als alles van een bepaalde workload/tenant werkt moeten we dit plan opnieuw overlopen met de volgende tenant, en zo verder tot alles dat gemigreerd moet worden overgezet is.

5. **BESLUIT**

Voor deze opdracht hebben we gemerkt dat **planning** heel belangrijk gaat zijn. We moeten eerst goed weten waar we mee bezig zijn zodat we vlot en zonder fouten ons plan kunnen uitvoeren. Als we niet goed nadenken over wat we gaan doen kunnen bepaalde resources misschien onomkeerbaar aangepast worden.

Omdat we hier met veel aspecten van Azure in contact komen, vooral Governance, gaan we wel veel moeten bijleren. De eerste weken bestonden vooral uit veel lezen en te weten komen over Azure en Azure Governance.

Ook samen werken met de andere afdelingen van VanRoey.be is hier heel belangrijk. Iedereen moet ten eerste al weten waar wij mee bezig zijn, maar het is ook van belang dat wij weten waar iedereen mee bezig is en in welke tenant. Afstemmen met de afdelingshoofden gaat ook cruciaal zijn voor een vlotte overgang.

We zijn ervan overtuigd dat, als we de migratie goed plannen en in kaart brengen, we de opdracht naar behoren gaan kunnen uitvoeren. We gaan er alleszins sowieso heel veel van bijleren.