



REALISATIEFASE

STAGE REMOTE SUPPORT

VANROEY.BE | 15/04/2021

PHILIPPE BOETS | GIANNI JORDENS



INHOUDSTAFEL

- 1. Governance bestaande resources External services 2
 - 1.1. Security center policies 2
 - 1.1.1. Remediated recomendations..... 3
 - 1.2. PIM..... 5
 - 1.2.1. Usergroepen structuur 5
 - 1.2.2. Instellen van PIM..... 5
 - 1.2.3. PIM gebruiken..... 7
 - 1.3. Policies 8
 - 1.3.1. CAF 8
 - 1.3.2. Custom policies..... 8
 - 1.4. Conditional Access 9
 - 1.4.1. Block legacy authentication.....10
 - 1.4.2. Require MFA.....10
 - 1.5. User RISK policy 11
 - 1.6. Break Glass accounts 11
 - 1.6.1. Sign-in alert..... 11



1. **GOVERNANCE BESTAANDE RESOURCES EXTERNAL SERVICES**

Tijdens het eerste deel van de realisatiefase gaan we de bestaande resources die al in de External Services Tenant stonden op een correcte manier gouverneren en beveiligen. De Azure Security Benchmark (ASB) stond al ingesteld op alle subscriptions maar er was nog niet veel mee gedaan. We gaan dus eerst via het Security Center zo veel mogelijk resources beveiligen en managen. Zo veel mogelijk gaan we zelf doen maar waar nodig zal contact opgenomen worden met de verantwoordelijke van de resource om samen te kijken hoe we de beveiliging kunnen verbeteren en hoe de resources naar de toekomst toe ook veilig kunnen blijven.

1.1. **SECURITY CENTER POLICIES**

Sommige policies van de ASB zijn niet van toepassing op onze omgeving. Policies die niet van toepassing zijn kunnen vrijgesteld worden zodat er geen meldingen meer over komen. Dit kan door per policy op **exempt** te klikken, waarna de subscriptions (of specifieke resources) waarop de policy vrijgesteld moet worden aangeduid kunnen worden alsook de reden waarom deze policy niet nodig is (zie afbeelding).

Voorlopig gaat het om:

- policies omtrent Kubernetes clusters aangezien deze niet gebruikt worden in de omgeving
- External accounts with owner/write permissions should be removed from your subscription. Deze is ook niet van toepassing aangezien we alle gebruikers importeren vanuit de vanroey.be tenant.

Exempt

6 subscriptions

You can exempt a recommendation from any scope so that it doesn't affect your secure score. The resources' status will change to "not applicable". It might take up to 30 min for exemption to take effect
[Learn more](#)

Exemption scope

Scope selection

- ☐ Selected MG 0 selected
- ☒ Selected subscriptions 6 selected
- ☐ Selected resources 0 selected

Exemption details

Exemption name *

ASC-Kubernetes clusters should be accessible only over HTTPS

☐ Set an expiration date

Edited By *

admin.philippe@vanroeyexternal.onmicrosoft.com

Exemption category * ⓘ

- ☐ Mitigated (resolved through a third-party service)
- ☐ Waiver (risk accepted)

Exemption description (optional) ⓘ

We dont use Kubernetes

Create

Cancel



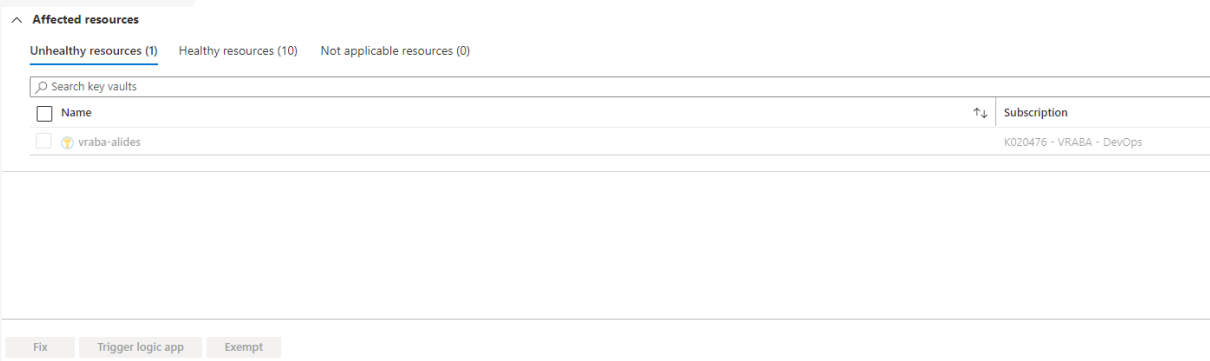
1.1.1. REMEDIATED RECOMENDATIONS

Volgende aanbevelingen zijn door ons manueel opgelost.

Logging and Threat detection

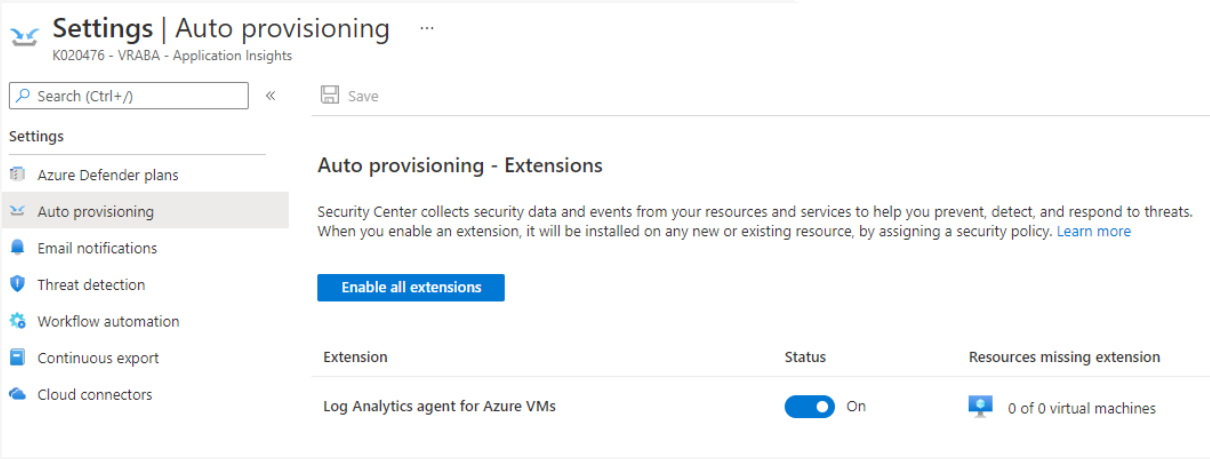
LT.4 Diagnostic logs in Key Vault should be enabled. Deze policy stelt ons in staat om activiteitsporen te reconstrueren voor onderzoeksdoeleinden wanneer zich een beveiligingsincident voordoet of het netwerk gecompromitteerd is.

Deze aanbeveling kan automatisch door Azure opgelost worden, er moet enkel een log analytics workspace meegegeven worden. Om deze op te lossen moeten enkel de gewenste resources aangeduid worden, op fix klikken, workspace meegeven (in dit geval: KeyVaultAnalyticsWS), en Azure doet de rest:



LT.5 Auto provisioning of the Log Analytics agent should be enabled on your subscription. Deze setting zorgt ervoor dat er automatisch een Log Analytics agent op nieuwe vm's geïnstalleerd worden. Deze agents verzamelen beveiligings gerelateerde gegevens zoals configuraties en logon data.

Auto provisioning kan opgezet worden door naar security Center > Pricing & settings > subscription id > auto provisioning te surfen en setting aan te vinken met als log analytics workspace LogAnalyticsAgent:





Incident response
IR.2 Incident notification.

Customer responsibility

Email notification to subscription owner for high severity alerts should be enabled

Subscriptions should have a contact email address for security issues

Email notification for high severity alerts should be enabled

Dit zijn een aantal policies die ervoor zorgen dat de juiste mensen alerts krijgen wanneer er iets mis gaat in de omgeving. Voor deze settings moet er terug naar Pricing & Settings gesurft worden. Daar kunnen bij email notifications de juiste gegevens ingevuld worden. Bij high severity incidenten wordt naar de volgende mensen een email gestuurd: [redacted] en de Owner van de subscription.

Email recipients
Select who'll get the email notifications from Azure Security Center for the [redacted] subscription.
All users with the following roles: Owner
Additional email addresses (separated by commas): [redacted]

Notification types
Use the settings below to select the type of email notifications to be sent by Security Center.
☒ Notify about alerts with the following severity (or higher): High

i You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. [Learn more >](#)

Backup and Recovery

BR.4 Key vaults should have purge protection enabled & Key vaults should have soft delete enabled. Purge protection zorgt ervoor dat Keys en certificates niet, per ongeluk of met slechte intenties, permanent verwijderd kunnen worden. Als secrets verwijderd worden kan dit in sommige gevallen tot permanent dataverlies leiden. Deze setting houdt secrets die verwijderd worden tot 90 dagen bij. De setting kan per keyvault bij properties aan gezet worden:

Soft-delete
Days to retain deleted vaults: 90
Purge protection: ☒ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

i Once enabled, this option cannot be disabled

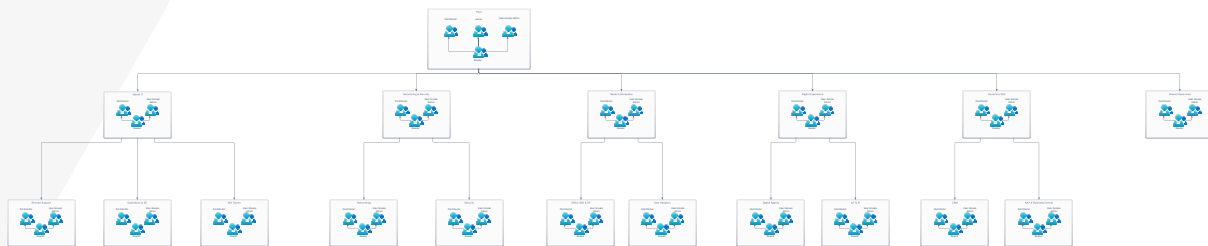
Soft delete has been enabled on this key vault



1.2. PIM

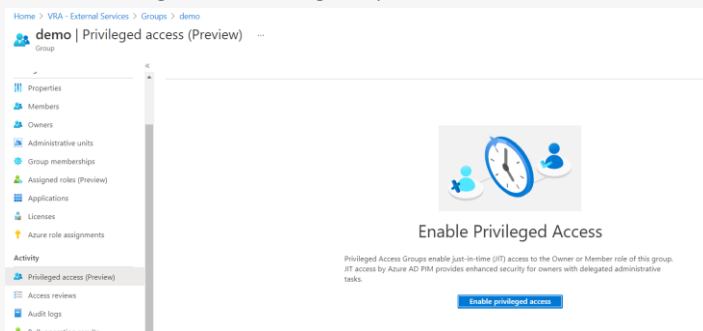
1.2.1. USERGROEPEN STRUCTUUR

Om aan privileged identity management te doen hebben we gekozen om groepen te gebruiken. Deze groepen zijn gemaakt per management group en zijn onderverdeeld in verschillende rechten. Gebruikers kunnen toegevoegd worden tot de reader security groep (SG_VRA_*managementgroup*_Reader), hier na krijgen ze read rechten op de onderliggende subscriptions en resources. Ook kunnen ze dan PIM gebruiken om tijdelijk lid te worden van de contributor (SG_VRA_*managementgroup*_Contributor) of user access admin (SG_VRA_*managementgroup*_User_Access_Admin) security group. Om lid te worden van deze groepen moet er wel een justificatie worden ingevuld en bij elevatie wordt de Admin op de hoogte gesteld via mail.



1.2.2. INSTELLEN VAN PIM

Om groepen in te stellen voor PIM moet je bij de aanmaak van de groep aanvinken om Azure AD rollen toe te kunnen wijzen aan de groep. Hierna kan je privileged access aanzetten in de instellingen van de groep.



Home > VRA - External Services > Groups >

New Group

Group type * ⓘ
Security

Group name * ⓘ
demo ✓

Group description ⓘ
Enter a description for the group

Azure AD roles can be assigned to the group (Preview) ⓘ
☒ Yes ☐ No

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

Roles
No roles selected

Create



Nu kunnen we bepaalde instellingen voor PIM juist zetten volgens de vooropgestelde normen. We kiezen hier de member instellingen want owner gaan we aan niemand toewijzen. Als eerste voor de activatie verplichten we het gebruik van Azure MFA, ook moet je een justificatie ingeven waarom je de elevatie nodig hebt bv welke taak je gaat verrichten. Approval gaan we niet vragen want dit zou te veel werk meebrengen voor de admins, die niet constant bezig gaan zijn met azure.

Activation Assignment Notification

Activation maximum duration (hours)

8

On activation, require

None

Azure MFA

Learn more

Require justification on activation

Require ticket information on activation

Require approval to activate

Select approver(s)

No approver selected

Activation Assignment Notification

Allow permanent eligible assignment

Expire eligible assignments after

1 Year

Allow permanent active assignment

Expire active assignments after

6 Months

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

Voor de toewijzing zelf gaan we dit een permanente verkiesbare toewijzing omdat we deze toewijzing gaan doen aan een hele groep en geen enkele gebruiker en als je dus niet in de juiste groep zit kan je geen PIM elevatie uitvoeren.

Bij de uitvoering van PIM wordt er een mail gestuurd naar de admins en naar jezelf dat je een elevatie gedaan hebt.

Activation Assignment Notification

Send notifications when members are assigned as eligible to this role:			
Type	Default recipients	Additional recipients	Critical emails only ⓘ
Role assignment alert	<input checked="" type="checkbox"/> Admin	Email IDs separated by semicolon(,)	<input type="checkbox"/>
Notification to the assigned user (assignee)	<input checked="" type="checkbox"/> Assignee	Email IDs separated by semicolon(,)	<input type="checkbox"/>
Request to approve a role assignment renewal/extension	<input checked="" type="checkbox"/> Approver	Email IDs separated by semicolon(,)	<input type="checkbox"/>

Send notifications when members are assigned as active to this role:			
Type	Default recipients	Additional recipients	Critical emails only ⓘ
Role assignment alert	<input checked="" type="checkbox"/> Admin	Email IDs separated by semicolon(,)	<input type="checkbox"/>
Notification to the assigned user (assignee)	<input checked="" type="checkbox"/> Assignee	Email IDs separated by semicolon(,)	<input type="checkbox"/>
Request to approve a role assignment renewal/extension	<input checked="" type="checkbox"/> Approver	Email IDs separated by semicolon(,)	<input type="checkbox"/>

Send notifications when eligible members activate this role:			
Type	Default recipients	Additional recipients	Critical emails only ⓘ
Role activation alert	<input checked="" type="checkbox"/> Admin	Email IDs separated by semicolon(,)	<input type="checkbox"/>
Notification to activated user (requestor)	<input checked="" type="checkbox"/> Requestor	Email IDs separated by semicolon(,)	<input type="checkbox"/>
Request to approve an activation	<input checked="" type="checkbox"/> Approver	Only designated approvers can receive this email	<input type="checkbox"/>



Home > VRA - External Services > Groups > demo >

Add assignments

Privileged Identity Management | Privileged access groups (Preview)


Membership Setting

Resource
demo

Resource type
Security

Select role ⓘ
Member

Select member(s) * ⓘ
1 Group(s) selected

Selected member(s) ⓘ
 SG_VRA_MS_Teams_Reader [Remove](#)

Hierna voegen we de reader groep toe aan de juiste PIM groep.

Dit doen we dan voor alle contributor en user access admin groepen en bij de root management groep nog extra voor een owner groep.

1.2.3. PIM GEBRUIKEN

Om PIM te gebruiken ga je in Azure naar Privileged Identity Management, dan navigeer je naar de 'my roles' blade en 'privileged access groups'. Hier zie je onder eligible assignments je rollen waarbij je kunt elevaten via PIM.

Home > Identity Governance > Privileged Identity Management > My roles

My roles | Privileged access groups (Preview)

Privileged Identity Management | My roles

Activate

Refresh | Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role or group

Role	Group	Group type	Membership	End time	Action
Member	SG_VRA_HybridT_Contributor	Security	Group	Permanent	Activate
Member	SG_VRA_HybridT_User_Access_Admin	Security	Group	Permanent	Activate

Activate AD roles
Privileged access groups (Preview)
Azure resources
Troubleshooting + Support
Troubleshoot
New support request

Bij het activeren van PIM moet stel je dan de tijd in hoe lang je je rechten nodig hebt met de nodige justificatie.

Activate - Member

Privileged Identity Management | Privileged access groups (Preview)

Roles **Activate** Status

☐ Custom activation start time

Duration (hours) ⓘ
8

*Reason (max 500 characters) ⓘ



1.3. POLICIES

1.3.1. CAF

Voor de policies die toegepast worden op de management groups kiezen we als starting blueprint voor de CAF Blueprint, hierbij zijn nog enkele extra policies toegevoegd. Dit is nog niet finaal aangezien er nadien nog extra policies toegevoegd kunnen worden als dit nodig is.

Artifact name	Resource type	Parameters
Assigned subscription	Subscription	
Activity log should be retained for at least one year	Policy assignment	0 out of 1 parameters populated
Email notification to subscription owner for high severity alerts should be enabled	Policy assignment	0 out of 1 parameters populated
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	2 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
Azure Security Center template	Azure Resource Manager template	None
Key vaults should have purge protection enabled	Policy assignment	0 out of 1 parameters populated
Managed identity should be used in your Function App	Policy assignment	0 out of 1 parameters populated
Enable Azure Monitor for Virtual Machine Scale Sets	Policy assignment	0 out of 3 parameters populated
Resource Group for Identity Services	Resource group	2 out of 2 parameters populated
Resource Group for First Application	Resource group	2 out of 2 parameters populated

1.3.2. CUSTOM POLICIES

Om een bepaalde naming convention te houden in de resources en resourcegroepen, hebben we voor zowel de meeste gebruikte resources en resourcegroepen een custom naming convention policy aangemaakt.

Deze custom policies zijn aangemaakt via een json file. Zoals deze naming policy waarbij de resource groepen volgens <prd/dev/qa>-<location>-<solution>-<rg> moet benoemd worden.

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "allof": [
        {
          "not": {
            "anyOf": [
              {
                "field": "name",
                "like": "prd-weu-*-rg"
              },
              {
                "field": "name",
                "like": "dev-weu-*-rg"
              },
              {
                "field": "name",
                "like": "qa-weu-*-rg"
              }
            ]
          }
        },
        {
          "field": "type",
          "equals": "Microsoft.Resources/subscriptions/resourceGroups"
        }
      ]
    },
    "then": {
      "effect": "audit"
    }
  }
}
```

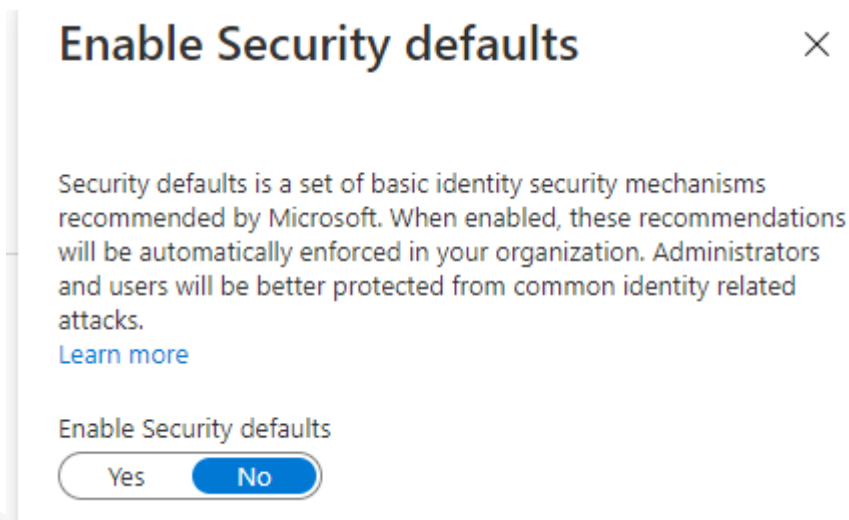


Op deze moment zijn er naming convention policies aangemaakt voor resource groups, vm's, storage accounts, app services en keyvaults aangezien deze het meest gebruikt worden.

Bij het aanmaken van deze policies zal het effect eerst nog een paar weken op audit staan zodat gebruikers tijd hebben om de nodige aanpassingen te maken aan de resources. Nadien worden de policies aangepast naar deny zodat er geen nieuwe resources aangemaakt kunnen worden als ze niet compliant zijn aan de policies.

1.4. **CONDITIONAL ACCESS**

Voor Conditional access in te schakelen moeten we de security defaults van Azure uitzetten. Dit doen we in de Azure active directory blade in de properties tab.



Nu kunnen we in de Security tab bij Conditional access nieuwe policies invoeren. We zorgen in deze policies vooral dat MFA afgedwongen wordt en dat legacy authentication geblokkeerd wordt.



1.4.1. BLOCK LEGACY AUTHENTICATION

Deze legacy authentication zijn requests van verouderde protocollen van office 2010 en ouder. Deze zijn niet veilig omdat je er eerst en vooral geen MFA kan mee afdwingen en worden daardoor vaak gebruikt bij password spray attacks en credential stuffing.

CA_VRA_Block_Legacy

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

CA_VRA_Block_Legacy

Assignments

Users and groups

All users included and specific users excluded

Cloud apps or actions

All cloud apps

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk

Not configured

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps

2 included

Device state (Preview)

Not configured

Enable policy

Report-only

On

Off

Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure

Yes

No

Select the client apps this policy will apply to

Modern authentication clients

Browser

Mobile apps and desktop clients

Legacy authentication clients

Exchange ActiveSync clients

Other clients

1.4.2. REQUIRE MFA

We voegen de policy voor MFA ook in voor alle users zodat ze enkel toegang kunnen krijgen als MFA aangezet is, er is standaard 14dagen tijd om deze MFA te activeren voor de user nadien wordt het verplicht.

De

Grant

Control user access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

Require app protection policy

Require password change

For multiple controls

Require all the selected controls

Require one of the selected controls

CA_VRA_MFA

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

CA_VRA_MFA

Assignments

Users and groups

All users

Cloud apps or actions

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

PHILIPPE BOETS & GIANNI JORDENS | voornaam.achternaam@vanroey.be | 014 470 605

10



1.5. USER RISK POLICY

Aangezien we gaan werken met guest users van de VanRoey AD gaan de user risk reports daar afgehandeld worden, ze gaan dus niet zichtbaar zijn in de reports van de external services tenant. Enkel de break glass accounts zullen hier dus zichtbaar zijn.

1.6. BREAK GLASS ACCOUNTS

Best practises dicteren het gebruik van 2 Break glass accounts, dit zijn accounts die global administrator rechten hebben die enkel in noodzaak dienen gebruikt te worden (bv . Voor deze accounts moeten dan ook extra maatregelen genomen worden. Zo gebruiken ze geen Multi factor authenticatie en is er een alert geplaatst op de sign in van deze break glass accounts. De admins worden zo op de hoogte gebracht bij een login met 1 van de break glass accounts.

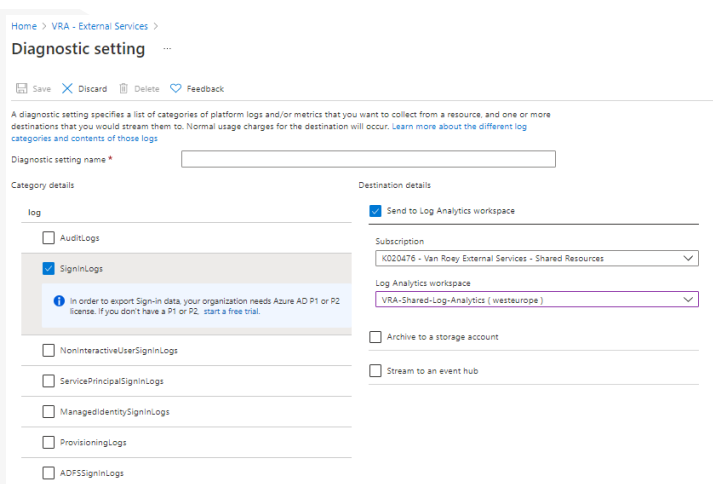
1.6.1. SIGN-IN ALERT

Om een alert aan te maken moeten we eerst zorgen dat de sign-ins van de tenant bijgehouden worden in een logfile. Hiervoor hebben we een log analytics workspace aangemaakt. Op deze workspace kunnen we verschillende logs verzamelen.

Om de sign-in logs in de workspace te krijgen gaan we in **Azure active directory** naar de **Diagnostic settings** blade.



In deze blade kan je data van verschillende logs doorsturen naar bepaalde resources zoals log analytics workspace, storage accounts of event hubs. Wij gaan dan de SignInLogs doorsturen naar de log analytics workspace.





> REALISATIEFASE STAGE REMOTE SUPPORT

Break Glass account Sign-in ✕ ...

Edit alert rule

Save ✕ Discard ☐ Disable ☐ Delete ☐ Properties

Edit the details below to modify the alert rule.
When defining the alert rule, check that your inputs do not contain any sensitive content.

Scope

Select the target resource you wish to monitor.

Resource	Hierarchy
VRA-Shared-Log-Analytics	K020476 - Van Roey External Services - Shared Resources > RG_Shared_Log_Analytics

Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name	Estimated monthly cost (USD) ⓘ
Whenever the average custom log search is greater than 0	\$ 1.50
Add condition	Total \$ 1.50

You can define only one log signal per alert rule. To alert on more signals, create another alert rule.

Search query * ⓘ

SignInLogs
| where AlternateSignInName contains 'VRA_BGAdmin@vanroeyexternal.onmicrosoft.com'
or AlternateSignInName contains 'VRA_BG2admin@vanroeyexternal.onmicrosoft.com'

[View result of query in Azure Monitor - Logs](#) ⓘ

Query to be executed: SignInLogs | where AlternateSignInName contains 'VRA_BGAdmin@vanroeyexternal.onmicrosoft.com' or AlternateSignInName contains 'VRA_BG2admin@vanroeyexternal.onmicrosoft.com' | count
For time window : 5/3/2021, 11:14 AM - 5/3/2021, 11:19 AM

It may take in the range of 6 minutes, to have the logs available for provided query [Learn more](#)

Alert logic

Based on ⓘ Operator ⓘ Threshold value * ⓘ ⓘ

Number of results	Greater than	0
-------------------	--------------	---

Condition preview

Whenever count of results in Custom log search log query for last 5 minutes is greater than 0. Evaluated every 1 minute.

Evaluated based on

Period (in minutes) * ⓘ	Frequency (in minutes) ⓘ
5	1 (preview)

Nu kunnen we een nieuwe alert rule aanmaken bij sign in van de break glass accounts. We selecteren bij de scope de log analytics workspace waar de sign-in logs naar gestuurd worden. Bij de condition geven we een kusto query in waarna gequeryed moet worden.

Bij deze query wordt er gekeken of er sign ins zijn geweest met de AlternateSignInName van de break glass accounts. Als er 1 of meerdere resultaten zijn (dus een sign in met 1 van deze accounts) wordt de conditie voldaan en gaan we over naar de actie.



> REALISATIEFASE STAGE REMOTE SUPPORT

Voor de actie hebben we een actiegroep aangemaakt, hier kunnen we 1 of meerdere acties bepalen. Voor onze alert sturen we een email naar het internalsupport email adres. Maar je kan hier ook nog andere notificaties sturen zoals sms/ push bericht of voice call. Je kan ook bepaalde acties ondernemen via functies, logic apps, webhooks,

Home > Break Glass account Sign-in >

Action-Group-Shared_Resources

Edit action group

Save changes Delete action group

This is a summary of your action group. Please review to ensure the information is correct and consider [Azure Alerts Pricing](#) and the [Azure Privacy Statement](#).

Basics

Subscription: K020476 - Van Roey External Services - Shared Resources

Resource group: RG_Shared_Log_Analytics

Action group name: Action-Group-Shared_Resources

Display name *: Action-Group

Notifications

Notification type	Name	Status	Email
Email/SMS message/Push/Voice	Login-Break-Glass-Account	Subscribed	Email: internalsupport@vanroey.be
			Email

Actions

Action type	Name	Selected

Tags

Name	Value
Owner	Internal Support

Als laatste geven we de alert een naam, descriptie en severity zodat er direct een duidelijk zicht is bij het aankrijgen van een email. Omdat dit gaat om privileged accounts hebben we dit een grote severity grade gegeven.

Alert rule details

Provide details on your alert rule so that you can identify and manage it later.

Alert rule name *: Break Glass account Sign-in

Description: Break Glass Account Sign-in. Possible Breach ✓

Save alert rule to resource group *: RG_Shared_Log_Analytics

Severity *: 0 - Critical