



AZURE POLICY COMPLIANCE HANDLEIDING

PHILIPPE BOETS | 12/05/2021

PHILIPPE BOETS | STAGAIR REMOTE SUPPORT
Philippe.boets@vanroey.be |



INLEIDING

Om onze cloud omgeving veilig en overzichtelijk te houden maken we in onze Azure omgeving gebruik van policies. Deze policies zijn een aantal richtlijnen die ons helpen met het beveiligen en managen van de omgeving. Een aantal van deze policies lopen op de achtergrond en zorgen ervoor dat bepaalde zaken niet uitgevoerd kunnen worden, een groter deel van de policies staat echter op 'audit'. Dit wil zeggen dat alle resources die op onze omgeving gebruikt worden automatisch gemonitord worden. Als een bepaalde resource zich niet voldoet aan de voorwaarden van een bepaalde policy, komt er een melding die uitlegt wat er moet gebeuren. Als gebruiker van de cloud omgeving van VanRoey.be is het ook uw verantwoordelijkheid ervoor te zorgen dat alle resources, die door u of uw team gebruikt worden, voldoen aan deze opgelegde richtlijnen.

In deze handleiding wordt uitgelegd waar je deze audits kan vinden, en hoe je ervoor kan zorgen dat alle resources veilig en overzichtelijk blijven.

KORT OVERZICHT

Policies zijn op twee plaatsten te vinden: Security Center en de Policy pagina op het Azure portaal.

Security center:

-Azure portal > Security Center

- Secure Score > doorklikken naar juiste subscription
- Regulatory compliance > Door scrollen tot Azure security Benchmark:

Policy pagina:

-Azure portal > Policy > links boven bij scope juiste subscription aanduiden:

The screenshot shows the Azure Policy page for the scope 'Van Roey Digital Experience'. The overall resource compliance is 100%. The resources by compliance state are: 0 - Compliant, 0 - Exempt, and 0 - Non-compliant. There are 0 non-compliant initiatives and 0 non-compliant policies. The table below lists the policies and their compliance status.

Name	Scope	Compliance state	Resource compliance	Non-Compliant Resources
Storage accounts should restrict network access	Tenant Root Group	Compliant	100% (0 out of 0)	0
Require the 'Owner' tag on resource groups	Tenant Root Group	Compliant	100% (0 out of 0)	0
resource group naming policy	Tenant Root Group	Compliant	100% (0 out of 0)	0

Azure Security Benchmark

Under each applicable compliance control is the set of all controls for any particular regulation are covered by S

[Azure Security Benchmark is applied to 6 subscriptions](#)

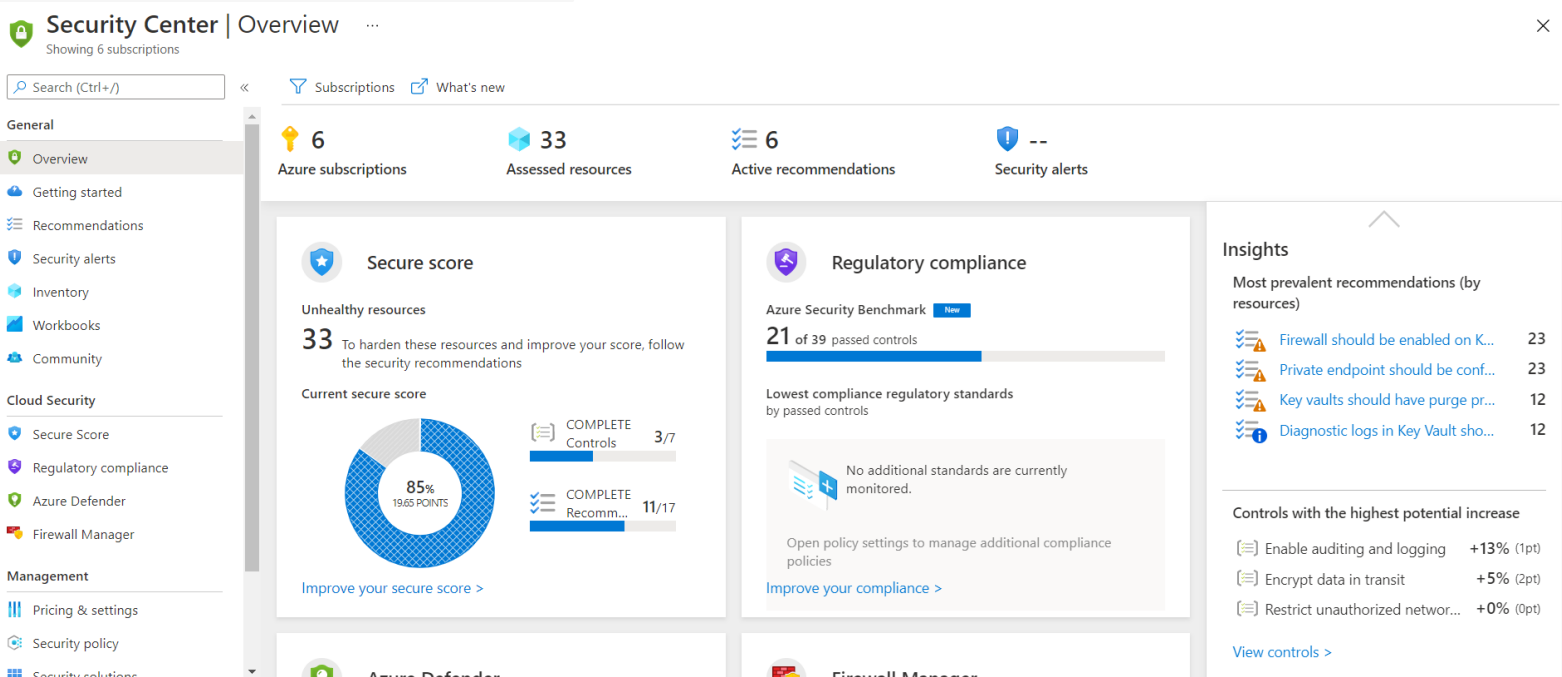
☐ Expand all compliance controls

- ✓ ✗ **NS. Network Security**
- ✓ ✗ **IM. Identity Management**
- ✓ ✗ **PA. Privileged Access**
- ✓ ✗ **DP. Data Protection**
- ✓ ✓ **AM. Asset Management**



1. **AZURE SECURITY CENTER**

Voorlopig zijn zo goed als alle policies terug te vinden in het Azure Security center. Om hier te geraken kan je gewoon zoeken naar Security Center op het Azure portaal:

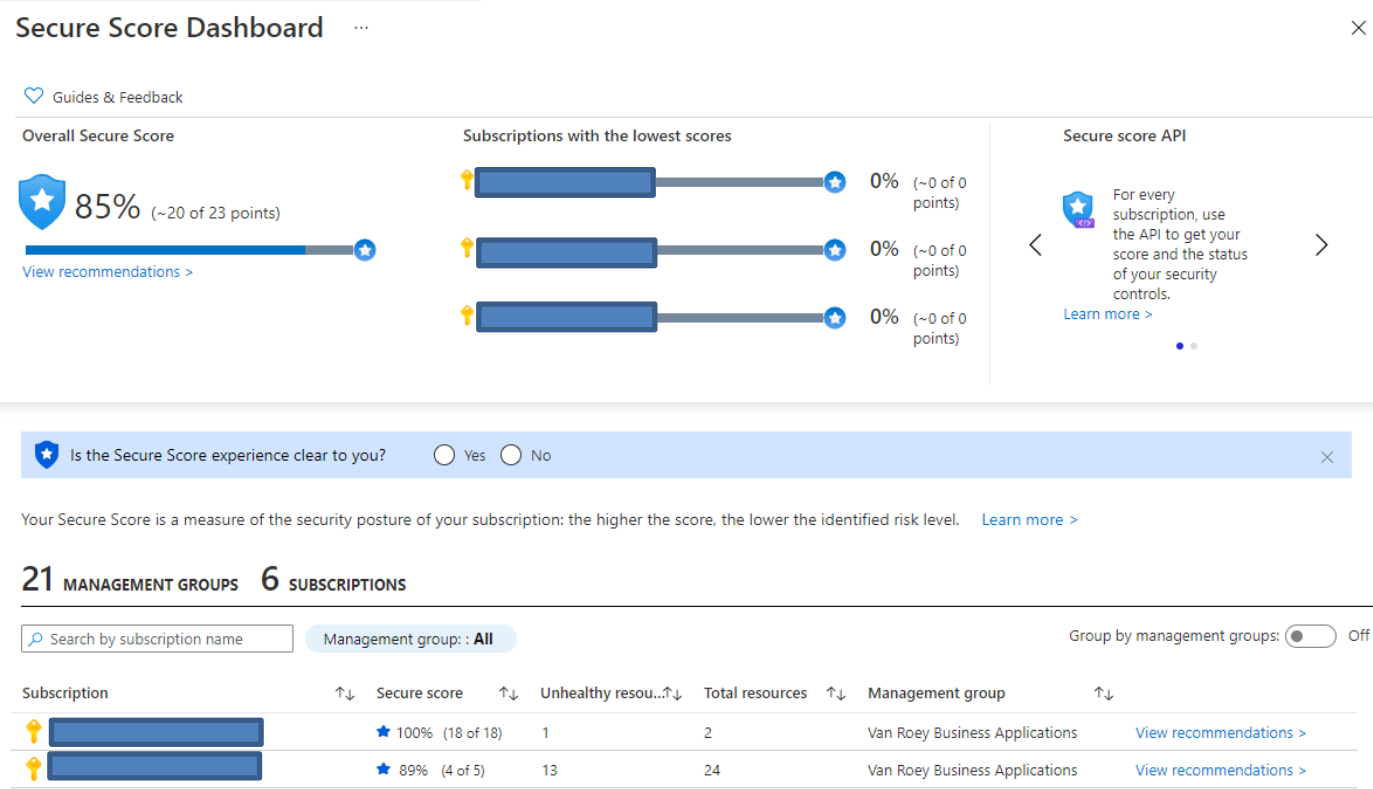


Op deze beginpagina is een overzicht te zien over de compliancy van uw resources. Deze is onderverdeeld in 2 scores: de Secure Score en Regulatory compliance. Deze geven allebei weer hoe goed uw resources voldoen aan de opgelegde policies. Via deze pagina kan doorgeklikt worden naar secure Score en naar Regulatory Compliance. Deze twee Dashboards werken op dezelfde manier.



1.1. SECURE SCORE DASHBOARD

Doorgeklikt op Secure Score krijg je een dashboard te zien met een overzicht van alle subscriptions waar u toegang toe hebt.





> AZURE POLICY COMPLIANCE HANDLEIDING

Om de resources compliant te maken kan er per policy doorgeklikt worden naar een detail pagina (in dit geval doorgeklikt op Diagnostic logs in Key Vault should be enabled):

Diagnostic logs in Key Vault should be enabled ...

Exempt Enforce View policy definition Open query

Severity: Low Freshness interval: 30 Min

1

2

3

Description
Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised.

Remediation steps

Affected resources
Unhealthy resources (12) Healthy resources (10) Not applicable resources (0)

Search key vaults

<input type="checkbox"/> Name	Subscription
<input type="checkbox"/> [Redacted]	K020476 - VRABA - DevOps
<input type="checkbox"/> [Redacted]	K020476 - VRABA - DevOps

Voor elke policy is er zo een pagina te zien. Deze pagina is heel belangrijk en geeft per policy het volgende weer:

1. een beschrijving van wat de policy doet
2. te ondernemen stappen om resources compliant te maken
3. non-compliant resources

Remediation steps kan nog verder open geklikt worden:

Remediation steps

Quick fix:
Select the unhealthy resources and click "Fix" to launch "Quick fix" remediation. [Learn more >](#)
Note: After the process completes, it may take several minutes until your resources move to the 'healthy resources' tab.

Quick fix logic

Manual remediation:
To enable Key Vault diagnostics:
1. Go to Key Vault and click on your subscription.
2. Click **Diagnostic settings** and then click **Turn on diagnostics**.
3. Select one of the options to store the diagnostics logs and follow the instructions.
Note: We recommend setting a retention for the logs. If you select the storage account option, make sure to set the retention to 1 year.

Hier komen dan de stappen te staan die per resource ondernomen moeten worden om deze te laten voldoen aan de policy. Bij bepaalde resources zijn er "quick fixes" mogelijk, deze staan on toe om in een paar klikken alle resources compliant te maken.



> AZURE POLICY COMPLIANCE HANDLEIDING

Quick Fix:

Voor de bovenstaande policy is het mogelijk een quick fix toe te passen. Om deze toe te passen moeten gewoon al de gewenste resources aangeduid worden, en daarna op fix klikken:

Unhealthy resources (12) Healthy resources (10) Not applicable resources (0)

Search key vaults

<input checked="" type="checkbox"/> Name	Subscription
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps
<input checked="" type="checkbox"/>	K020476 - VRABA - DevOps

Fix

Trigger logic app

Exempt

Na op fix te klikken komt er een extra wizard open die gewoon gevolgd moet worden om te resources compliant te maken. **Let op** na een resource compliant maken kan het 30 minuten tot een uur duren voordat deze resources als Healthy of 'compliant' aangeduid worden!

Zonder quick fix:

Bij sommige policies zal het jammer genoeg niet gaan om een quick fix uit te voeren. Bij volgend voorbeeld is een quick fix niet mogelijk (Firewall should be enabled on Key Vault). In dat geval kan u remediation steps openklikken om een stappenplan (en evt. extra documentatie) dat uitlegt wat er gedaan moet worden te verkrijgen:

Remediation steps

Manual remediation:

To enable the key vault firewall:

1. In the Azure portal, open your key vault.
2. From the left sidebar, select Networking (located under the "Settings" section).
3. Set the radio button to Private endpoint and selected networks and select Save.

Daarna de stappen volgen en als nodig extra documentatie van microsoft raadplegen: <https://docs.microsoft.com/> en dan search.

Bij sommige policies, zoals bvb. Firewall should be enabled on Key Vault, is het na verloop van tijd best practice om bij het aanmaken van de resource direct de stappen uit te voeren. Dus bvb firewall voor Key Vaults direct op te zetten.



1.2. REGULATORY COMPLIANCE

Regulatory compliance werkt hetzelfde als het Secure Score dashboard maar ziet er een beetje anders uit. De controls worden op een beetje een andere manier weergegeven, het zijn hier ook meer policies dan bij regulatory compliance. Eerst zijn controls nog onderverdeeld in groepen, onder deze groepen zitten de controls en onder elke control zitten de specifieke policies. (groene controls zijn volledig in orde):

^

NS. Network Security

^

NS.1. Implement security for internal traffic

Control details

C

Customer responsibility	Resource type	Failed resources	Resource compliance status
Firewall should be enabled on Key Vault	Key vaults	23 of 23	
Storage accounts should restrict network access using virtual network rules	Storage accounts	3 of 3	
Adaptive network hardening recommendations should be applied on internet f	Virtual machines	0 of 0	
Cognitive Services accounts should restrict network access	Azure resources	0 of 0	
Virtual networks should be protected by Azure Firewall	Virtual networks	0 of 0	

1 2 3 4 5 < >

^

NS.2. Connect private networks together

Control details

C

^

NS.3. Establish private network access to Azure services

Control details

C

^

NS.4. Protect applications and services from external network attacks

Control details

C

^

NS.5. Deploy intrusion detection/intrusion prevention systems (IDS/IPS)

Control details

C

^

NS.6. Simplify network security rules

Control details

C

^

NS.7. Secure Domain Name Service (DNS)

Control details

C

^

IM. Identity Management

^

PA. Privileged Access

Per policy kan er hier weer doorgeklikt worden naar de detailpagina van de policy zelf. Vanaf hier kan verdergewerkt worden zoals beschreven op pagina 4-5:

Storage accounts should restrict network access using virtual network rules

Azure Security Benchmark

Exempt

Deny

View policy definition

Open query

Severity

Medium

Freshness interval

30 Min

^

Description

Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.

^

Remediation steps

^

Affected resources

Unhealthy resources (3)

Healthy resources (0)

Not applicable resources (0)

Search storage accounts

Name

Subscription

Trigger logic app

Exempt

PHILIPPE BOETS | Philippe.boets@vanroey.be | 6



2. BELANGRIJK

Voor alle policies die met **logging of diagnostics gewerkt wordt** zijn er log analytics workspaces aangemaakt (deze workspaces verzamelen logs op een centrale plaats, deze staan in de Shared Resources subscription). Er is per categorie een workspace aangemaakt. Dat wil zeggen dat als er logging aangezet wordt dat het belangrijk is dat de logs naar de juiste workspace doorgestuurd worden! Logs voor Key vaults moeten dus doorgestuurd worden naar KeyVaultAnalyticsWS, agents voor vm's naar LogAnalyticAgent etc.


Voorbeeld ter verduidelijking:

Diagnostic logs in Key Vault should be enabled.

Voor deze policy is een quick fix mogelijk, er moet alleen een workspace doorgegeven worden. Aangezien het hier over logs omtrent Key Vaults gaan moet dus de KeyVaultAnalyticsWS aangeduid worden.

Als er nog geen workspace aanwezig is voor de resources waar u mee aan het werken bent kan u mailen naar internalsupport@vanroey.be om er één te laten aanmaken. De logs zullen door internal support gebruikt worden als er ergens iets misgelopen is. Dus u moet ze gewoon aanzetten, niet gebruiken.

Voorlopig staan er ook nog heel wat policies op die te maken hebben met **Azure defender**. Deze policies mogen voorlopig genegeerd worden, we zijn bezig om te bekijken wat er mogelijk is voor het aanzetten van Azure Defender.

Als er iets niet duidelijk is of het lukt niet bepaalde policies toe te passen, neem dan contact op met 

Fixing resources

Fix 12 resources

This action will enable diagnostic logs on key vault

Parameters

[Create new workspace](#)

Workspace ID *

