Secure Emergency Access Strategies: Zero Trust Break the Glass Solutions

Start 10:10

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

?

Break the glass

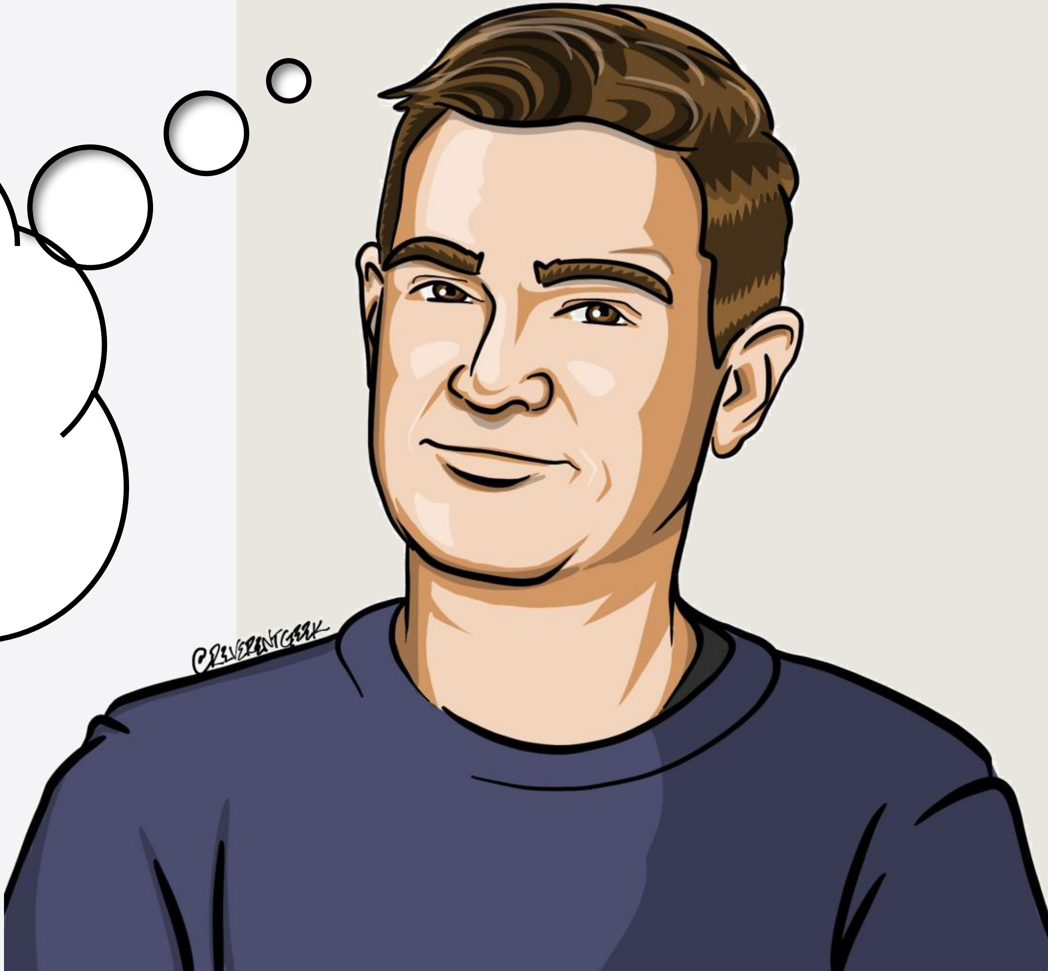
Jeroen Burgerhout

🍺 Modern Workplace Brewer

🧑‍🏫 Microsoft Certified Trainer

📰 burgerhout.org

🔗 burgerhou.tj/connect



Who is Sander

Creative Cloud Developer

Hobbies
- Play around with technology
- Blog @ rozemuller.com
- Athletics
- Gardening, brewing and BBQ

Microsoft® Most Valuable Professional MVP

Enterprise Mobility & Security

Stands for Automation first & everything

RAW
LINSEED
OIL
NAILS
WATTYL

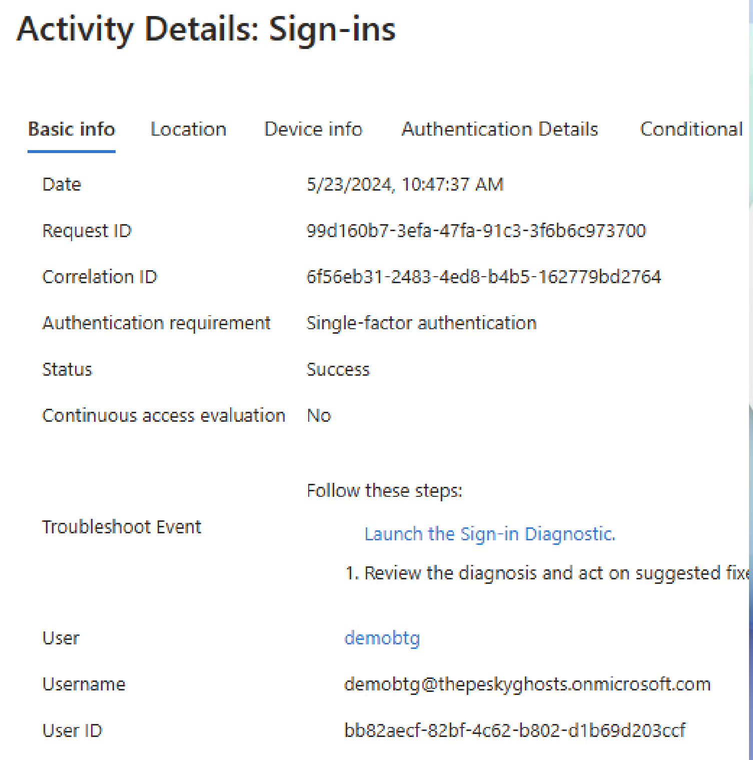
dm

What do we need?

- Object ID from the emergency account
- A custom logs alert rule

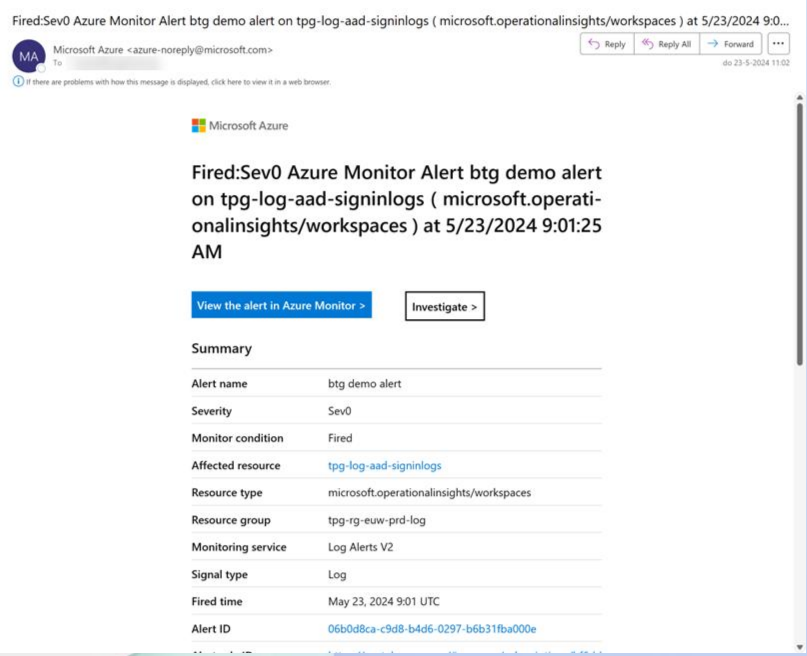
```
SigninLogs
| where UserId contains “object-id“
```

- Action Group
- Logic App that monitors the certificate



Activity Details: Sign-ins

Date	5/23/2024, 10:47:37 AM
Request ID	99d160b7-3efa-47fa-91c3-3f6b6c973700
Correlation ID	6f56eb31-2483-4ed8-b4b5-162779bd2764
Authentication requirement	Single-factor authentication
Status	Success
Continuous access evaluation	No
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixe
User	demobtg
Username	demobtg@thepeskyghosts.onmicrosoft.com
User ID	bb82aecf-82bf-4c62-b802-d1b69d203ccf



Fired:Sev0 Azure Monitor Alert btg demo alert on tpg-log-aad-signinlogs (microsoft.operationalinsights/workspaces) at 5/23/2024 9:0...

MA Microsoft Azure <azure-noreply@microsoft.com>

To [redacted]

do 23-5-2024 11:02

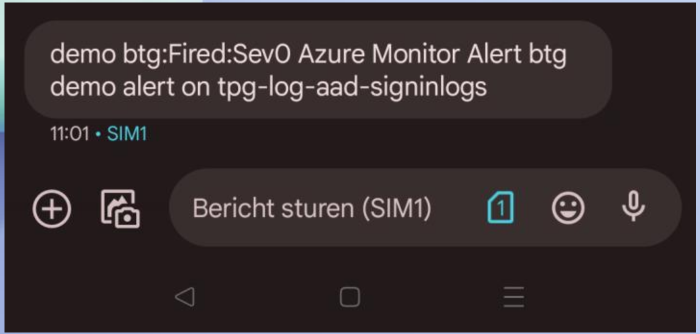
If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft Azure

Fired:Sev0 Azure Monitor Alert btg demo alert on tpg-log-aad-signinlogs (microsoft.operationalinsights/workspaces) at 5/23/2024 9:01:25 AM

Summary

Alert name	btg demo alert
Severity	Sev0
Monitor condition	Fired
Affected resource	tpg-log-aad-signinlogs
Resource type	microsoft.operationalinsights/workspaces
Resource group	tpg-rg-euw-prd-log
Monitoring service	Log Alerts V2
Signal type	Log
Fired time	May 23, 2024 9:01 UTC
Alert ID	06b0d8ca-c9d8-b4d6-0297-b6b31fba000e



demo btg:Fired:Sev0 Azure Monitor Alert btg demo alert on tpg-log-aad-signinlogs

11:01 • SIM1

Why?

In case of:

- Natural disaster, like earthquake, flooding
- network issues
- Identity providers outage, like MFA services

Create

- At least, create 2 break the glass accounts
- Cloud-only (*.onmicrosoft.com)
- Global Administrator role

Store it

- In a vault
- Internal and external from office
- Preferable FIDO2 key
- Write it down and keep the u/p separate from each other

Attention

- Exclude from MFA, CA and SSPR
- Exclude from Entra ID Protection

- GA behind PIM activation with auto approval

Monitoring

- Log Analytics Workspace
- Change the Diagnostic settings to forward the Entra ID loggings
- Action Group (SMS/Email)
- Alert Rule KQL query

Test / validate it

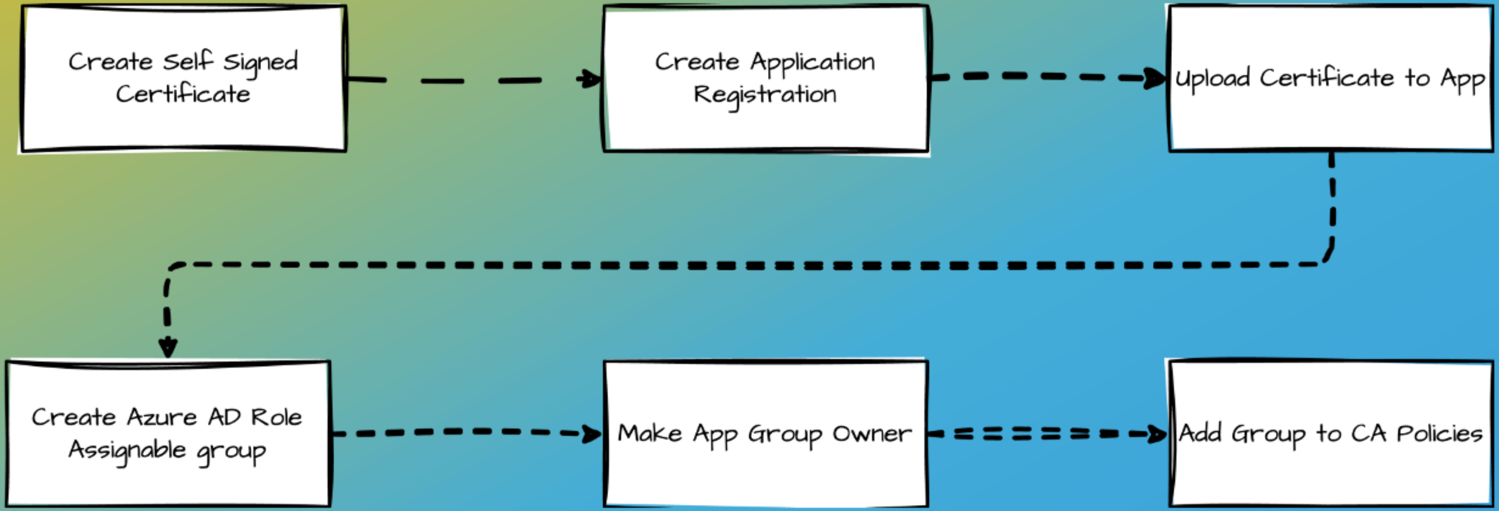
- at least every 90 days
- Recent change in IT staff
- process to use these accounts is documented and current

And now, from a different angle

I also did break a glass, but then with a football

What differs this break glass approach?

Deployment process



Create Self Signed Certificate

Create Application Registration

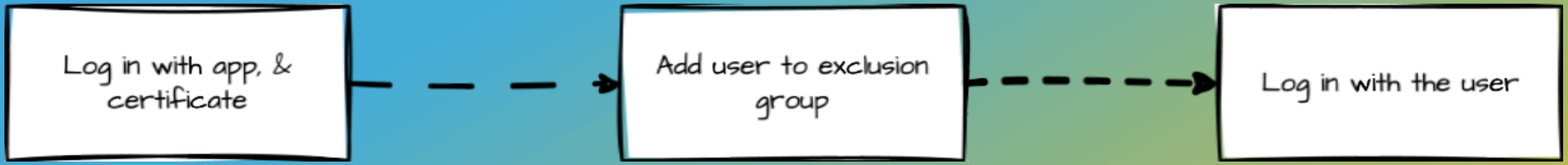
Upload Certificate to App

Create Azure AD Role Assignable group

Make App Group Owner

Add Group to CA Policies

Login process



Log in with app, & certificate

Add user to exclusion group

Log in with the user

CONSIDERATIONS

Emergency account has ONLY GroupMember.ReadWrite.All permissions;

When logged in, The userId as the groupId CAN NOT be craweled by the app;

Add the user to the exclusion group based on user ID and Group ID

The exclusion group is an Azure Role Assignable group

ONLY a Global Admin, Privileged Role Admin or owner can add users

Wrap up

Please evaluate this session in the App.

THANK YOU

Are there any questions?

Next session 11:10 – 12:00

Azure Firewall: The Legacy Firewall Killer