

Thank you to our Sponsors

THALES



FUSION5
Business Solutions



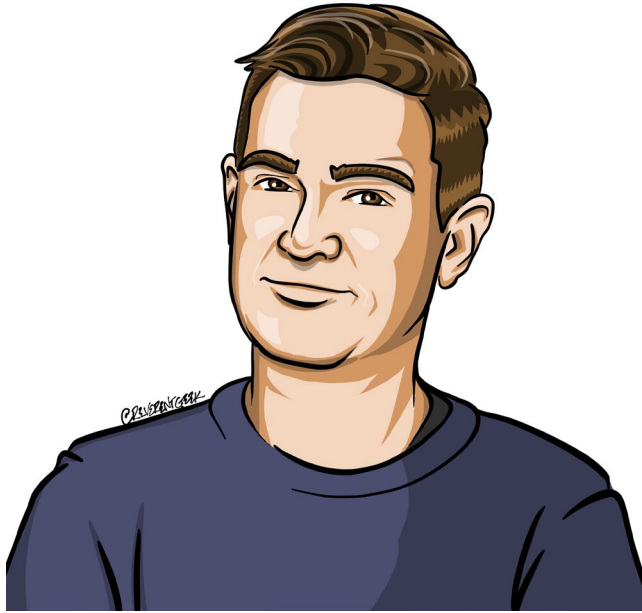
Follow us: @ExpertsLiveAUS

Manage your environment when MFA fails, a break the glass saga.....

Jeroen Burgerhout

Follow us: @ExpertsLiveAUS

Jeroen Burgerhout



- Microsoft 365 Consultant
- Microsoft Certified Trainer
- Netherlands
- WorkplaceDudes
- Microsoft 365 Modern Management Meetup
- Experts Live NL Team







1. Administrator accounts



Sponsors





Administrator accounts

Question for all:

Who is using a synced user/admin account for Azure management?





Administrator accounts

Question for all:

Who is using a cloud-only admin account for Azure management?



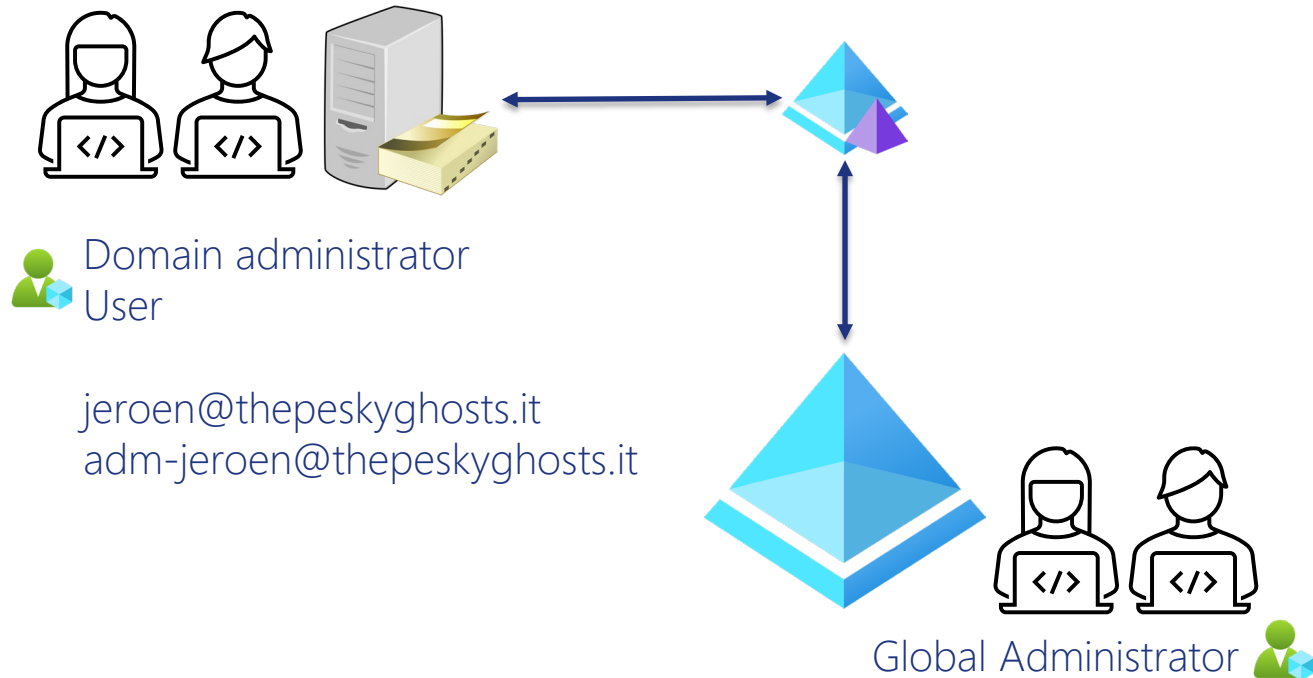


Administrator accounts

Instead of using everyday user accounts that have been assigned administrator roles, create dedicated administrator accounts that have the admin roles in Microsoft Entra ID.



Separate synced / cloud admin account



adm-jeroen@thepeskyghosts.onmicrosoft.com

2. Emergency accounts



Sponsors





Emergency accounts

Question for all:

Who is using an emergency account for Azure management?





Why use an emergency access account

An organization might need to use an emergency access account in the following situations:

- ❖ The user accounts are federated, and federation is currently unavailable because of a cell-network break or an identity-provider outage.
- ❖ The administrators are registered through Azure AD Multi-Factor Authentication, and all their individual devices are unavailable, or the service is unavailable. Users might be unable to complete Multi-Factor Authentication to activate a role.
- ❖ The person with the most recent Global Administrator access has left the organization. Azure AD prevents the last Global Administrator account from being deleted, but it does not prevent the account from being deleted or disabled on-premises. Either situation might make the organization unable to recover the account.
- ❖ Unforeseen circumstances such as a natural disaster emergency, during which a mobile phone or other networks might be unavailable.





Create emergency access accounts

Create two or more emergency access accounts. These accounts should be cloud-only accounts that use the *.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment.



Store the credentials safely





Store the credentials safely

preferable on a FIDO2 key

or

write down the password on a piece of paper





Monitor sign-in logs





Monitor sign-in logs

Activity Details: Sign-ins

Basic info Location Device info Authentication

Date	9/11/2023, 8:47:18 AM
Request ID	dbb3f0da-e937-42f8-bd8d-c
Correlation ID	09dc3777-1d82-4c44-858e-c
Authentication requirement	Single-factor authentication
Status	Success
Continuous access evaluation	No

Troubleshoot Event

Follow these steps:
[Launch the Sign-in Di...](#)
1. Review the diagnosis :

User	Break The Glass
Username	breaktheglass@t
User ID	812eb56b-bd42-4d3e-8c6b-2c54a5b02dbf
Sign-in identifier	breaktheglass@

Fired:Sev0 Azure Monitor Alert BTG Sign-In Alert on cat-log-aad-loginalerts (microsoft.operationalinsights/workspaces



Microsoft Azure <azure-noreply@microsoft.com>
To: theorangecatcoffeeandcloud@outlook.com

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

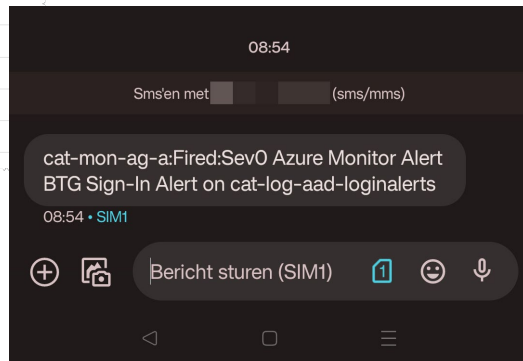


Fired:Sev0 Azure Monitor Alert BTG Sign-In Alert on cat-log-aad-loginalerts (microsoft.operationalinsights/workspaces) at 9/11/2023 6:54:20 AM

[View the alert in Azure Monitor >](#)

Summary

Alert name	BTG Sign-In Alert
Severity	Sev0
Monitor condition	Fired
Affected resource	cat-log-aad-loginalerts
Resource type	microsoft.operationalinsights/workspaces
Resource group	rg-eu





Monitor sign-in logs

What do we need?

- Object ID from the emergency account
- An alert rule

`SigninLogs`

| where UserId contains "object-id"

- Action Group



3. Setting it up



Sponsors





Experts Live Australia



