Experts Live Australia

Thank you to our Sponsors

THALES

PATCH MY PC

FUSION5 Business Solutions

digital61

ARINCO

SquaredUp

NiCE IT Management Solutions

PARALLO A Crayon company

Microsoft Community

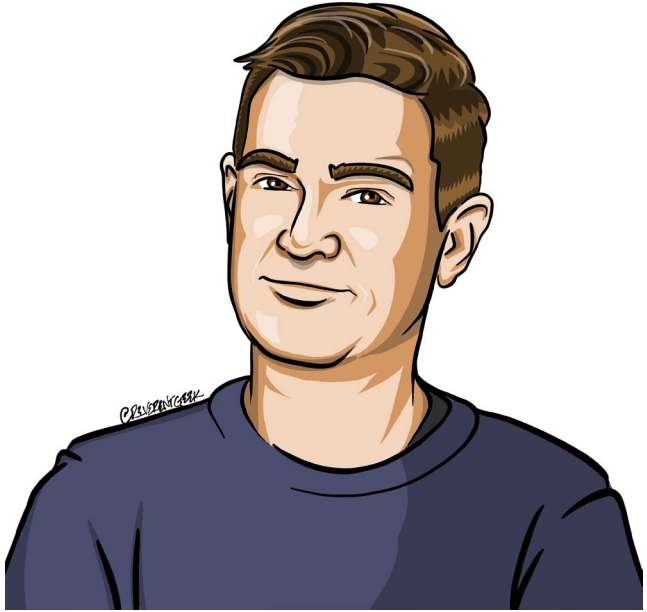
Experts Live Australia 2023

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

SquaredUp

THALES

ARINCO

FUSION5
Business Solutions

NiCE
IT Management Solutions

PARALLO
A Crayon company

Administrator accounts

Question for all:

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

Administrator accounts

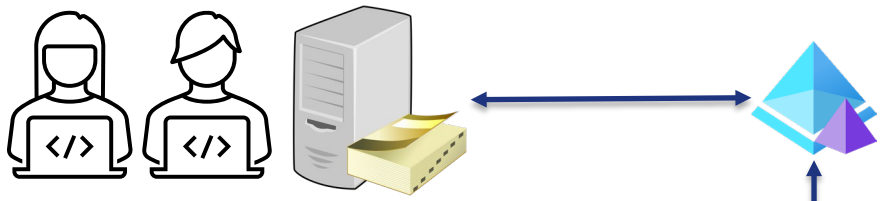
Question for all:

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

Administrator accounts

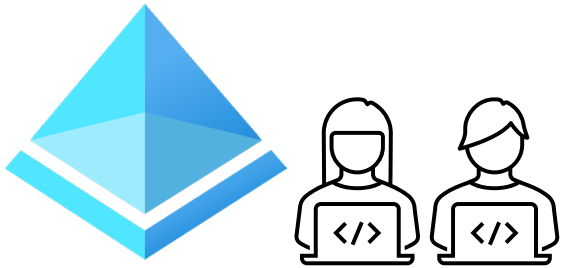
Instead of using everyday user accounts that have been assigned administrator roles, create dedicated administrator accounts that have the admin roles in Microsoft Entra ID.

Separate synced / cloud admin account



Domain administrator
User

jeroen@thepeskyghosts.it
adm-jeroen@thepeskyghosts.it



Global Administrator

adm-jeroen@thepeskyghosts.onmicrosoft.com

2. Emergency accounts

Sponsors

SquaredUp

THALES

ARINCO

FUSION5
Business Solutions

NiCE
IT Management Solutions

PARALLO
A Crayon company

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

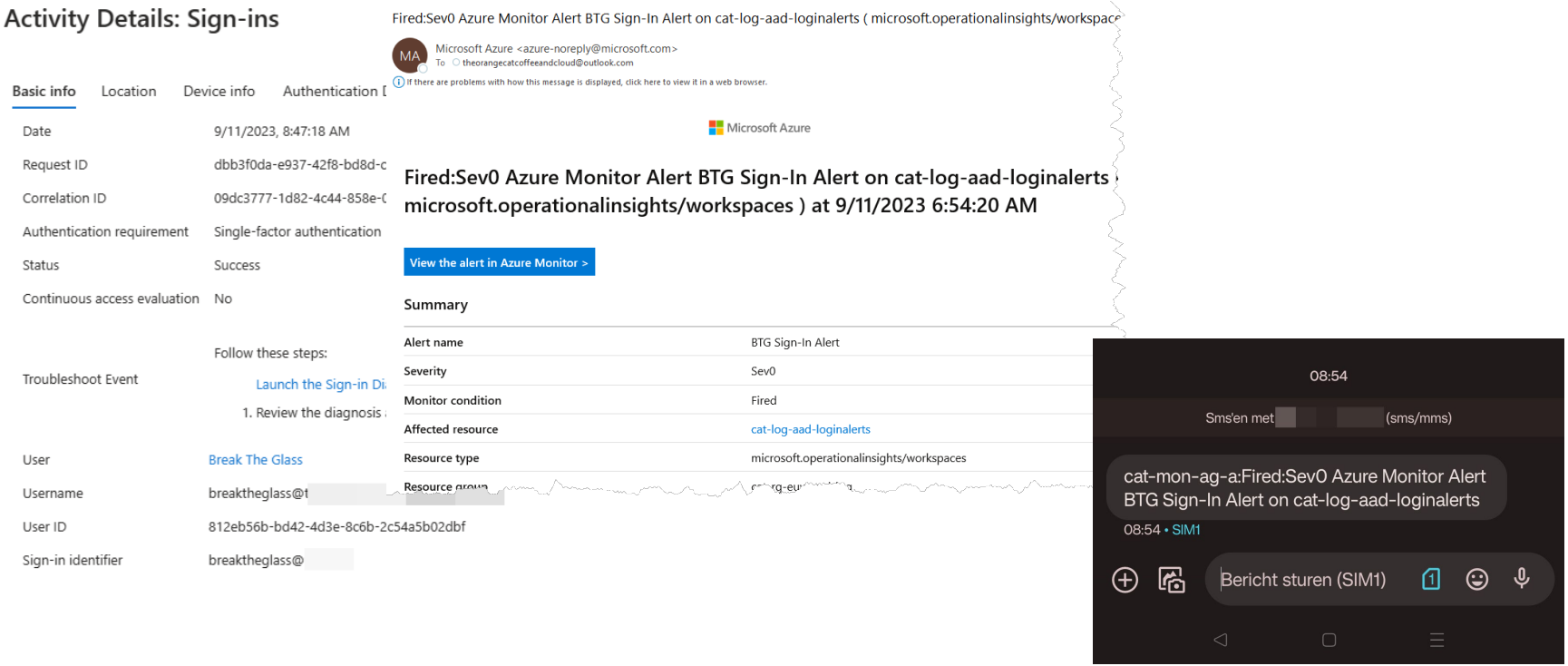
preferable on a FIDO2 key

or

write down the password on a piece of paper

Monitor sign-in logs

Monitor sign-in logs



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

SquaredUp

THALES

ARINCO

FUSION5
Business Solutions

NiCE
IT Management Solutions

PARALLO
A Crayon company


LIVE DEMO

Experts Live Australia

Sponsors

SquaredUp THALES ARINCO FUSION5 NiCE PARALLO


TO DO: Require Multi-factor Authentication
#EXPERTS LIVE