www.wpninjas.eu
#WPNinjaS

From Manual to Magical: Automate routine tasks in the cloud

Janic Verboon & Loris Ambrozzo

Workplace Ninja Summit 2025

Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Diamond Sponsor

Microsoft

Platinum Sponsors

2Pint

PATCH MY PC

RECAST SOFTWARE

glueck kanja

Gold Sponsors

nerdio

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

Rimo3

SOFTWARE CENTRAL

eido

EPIC FUSION
BRING IT ALL TOGETHER

Silver Sponsors

APENTO

PROACT

controlUP

UMB creating time®

water
IT Security & Defense

About Loris Ambrozzo

Focus

Security

From

Switzerland

My Blog

lorisambrozzo.medium.com

Certifications

Microsoft / SANS

Hobbies

Running, Hiking

Contact

/lorisambrozzo

About Janic Verboon

www.wpninjas.eu
#WPNinjaS

Focus

Endpoint Management, Entra ID

From

Switzerland

My Blog

-

Certifications

Some Microsoft
Android Enterprise Expert

Hobbies

Concerts, running, football

Contact

/ janic-verboon-04b11b114

/Janic1904

Agenda

www.wpninjas.eu
#WPNinjaS

Key takeaways:

- Gain insight into the various automation solutions available in Microsoft Cloud
- Learn how to apply least privilege principles to secure your automations

Cloud Automation Basics

Learn about authentication and least privilege for Cloud Automation

Logic Apps

Learn about low-code automation

Azure Automation

Learn about the 'Task Scheduler' in the cloud

Real World examples

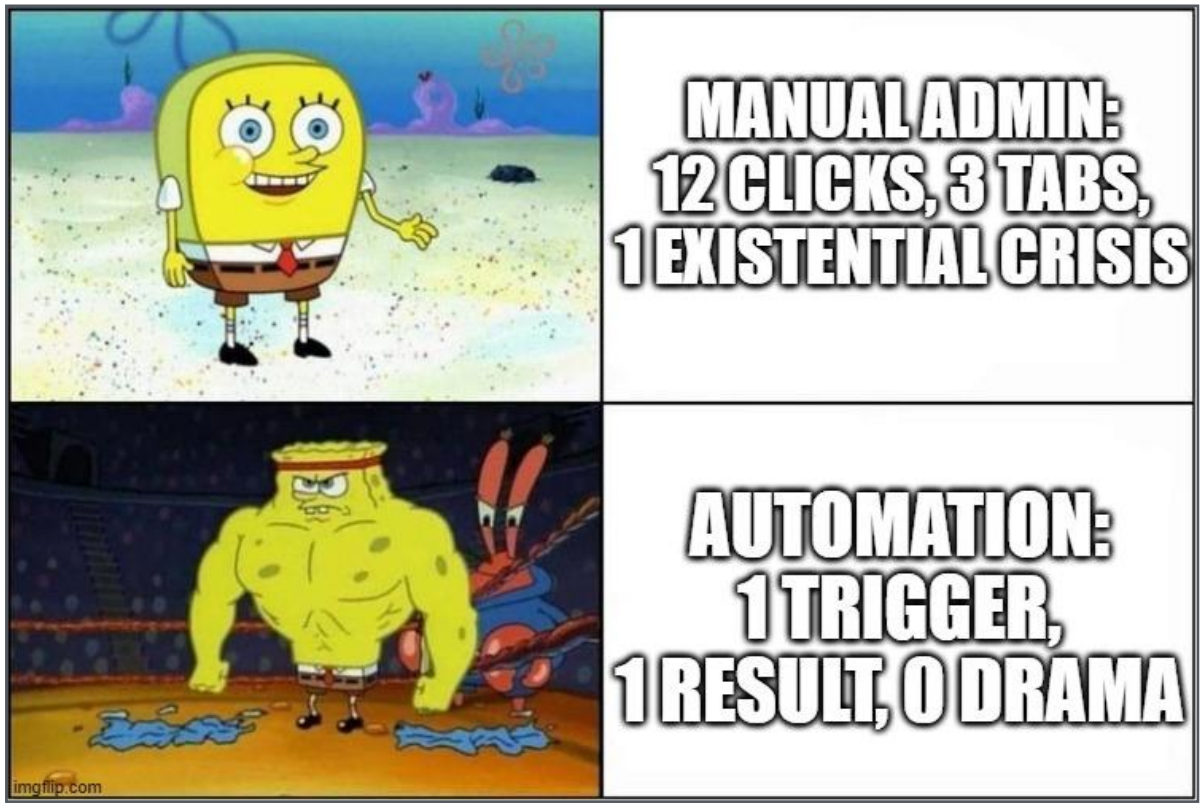
Learn how we use automation solutions in our daily work

Closing

Wrap up

Why automation?

- Eliminates repetitive tasks and frees up time
- Reduces human error in complex or routine processes
- Modern cloud platforms e.g., Microsoft 365, Azure or other 3rd Party Clouds offer API

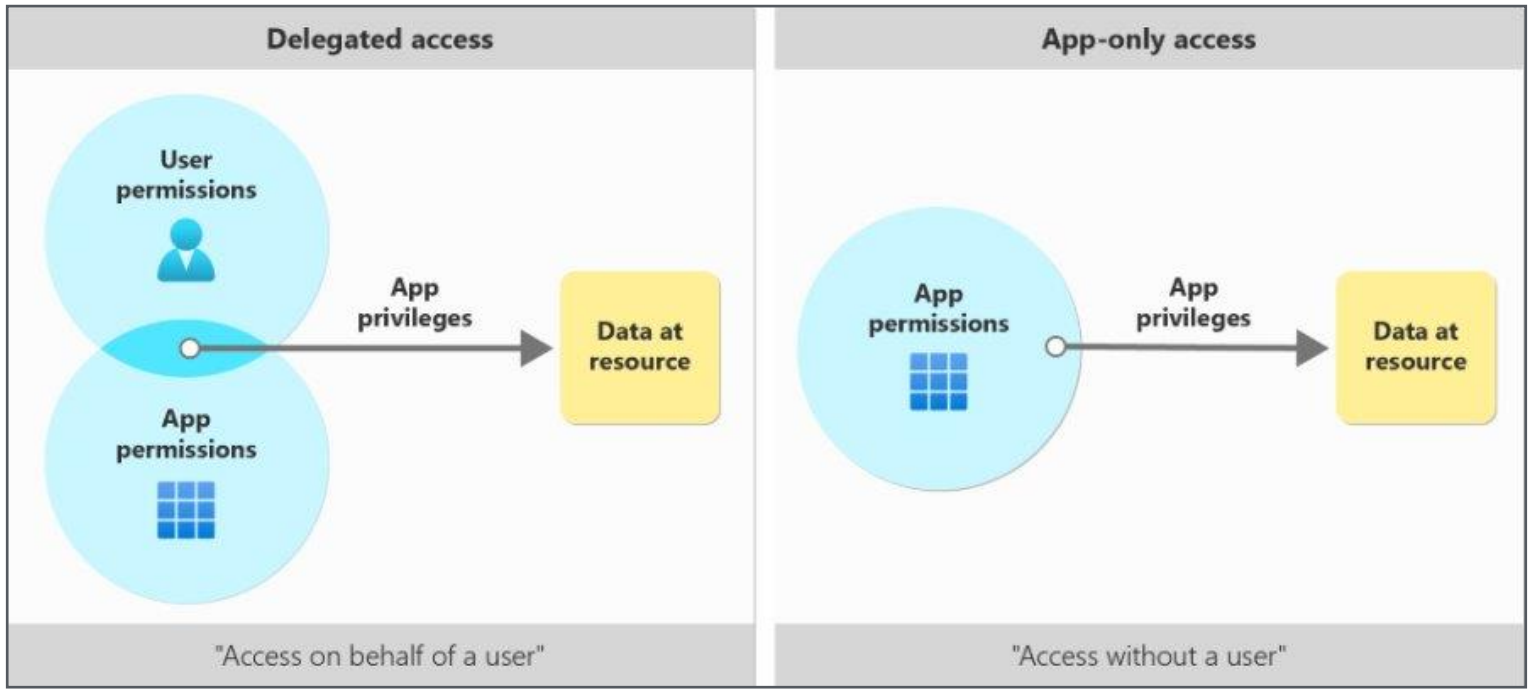


At the end of the session, you will get access to a Github repository which contains some of the scripts we talked about during this session.

Basics

From Manual to Magical:
Automate routine tasks in the cloud

Permission Types



- Delegated access:
  - Both the client and the user must be authorized separately to make the request
- Application access:
  - This scenario includes apps that run as background services or daemons. It's appropriate when it's undesirable to have a specific user signed in, or when the data required can't be scoped to a single user

Consent types

Admin consent | User consent

Search permissions

API name	Claim value	Permission	Type	Grante...	Grante...
Microsoft Graph (43)					
Microsoft Graph	User.Read	Sign in and read us...	Delegated	User co...	1 total ...
Microsoft Graph	openid	Sign users in	Delegated	User co...	2 total ...
Microsoft Graph	profile	View users' basic pr...	Delegated	User co...	2 total ...

- User consent:
  - Are granted for the specific users the consent is granted for
- Admin consent
  - Is granted for all users within the organization
  - Is required for high privileged permissions

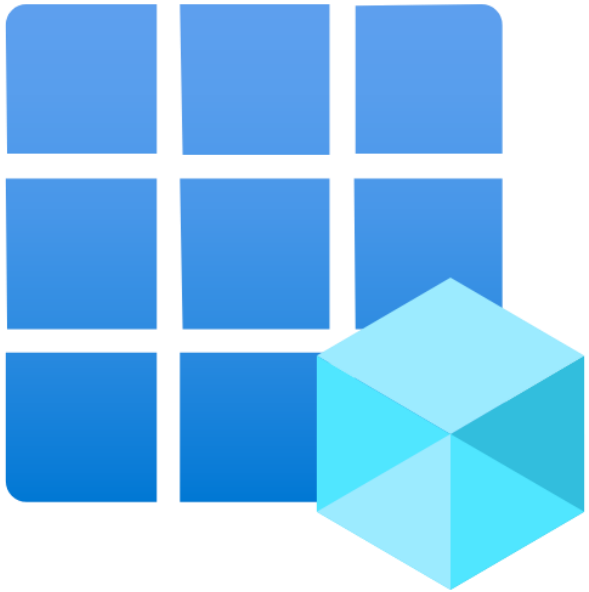
	Delegated	Application
User consent	X	
Admin consent	X	X

Authentication options

How can we authenticate?

User Authentication (Delegated)

App registration (Delegated & Application)



Managed Identity (Application)

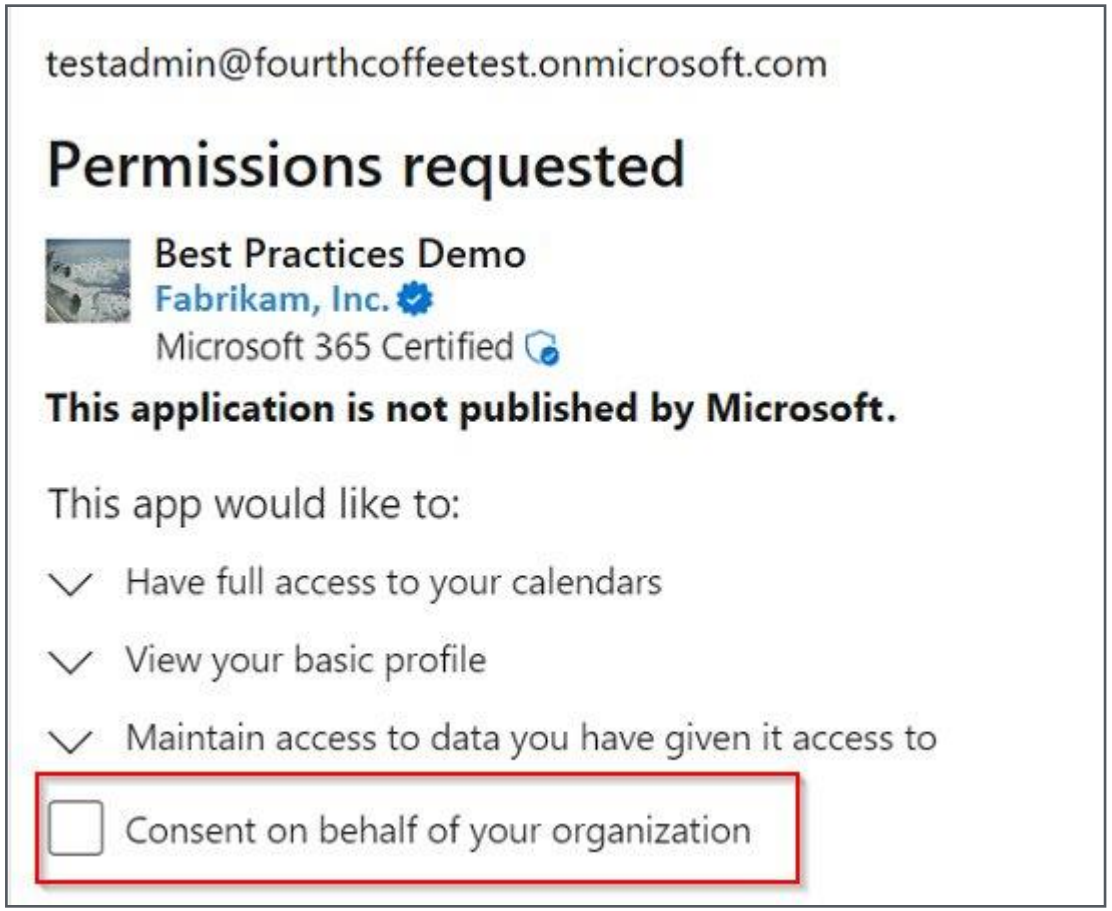
User Authentication

- When user authentication is used, the authentication is happening using the credentials of a user account.
  - Example: Connect-MgGraph

- For this to work the user requires to have:
  - The required permissions in Entra to read that user data
  - The required permissions on the API

User Authentication

- If users access an application / API they where they have no access to, they will get the prompt on the right →
- Admins can grant consent for all users in their org, so that not every user gets these prompts.
  - Especially useful if you want to integrate SaaS apps into your tenant.



User Authentication

- Administrators can configure the user consent options in Entra ID:

Manage

User consent settings

Admin consent settings

Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- Do not allow user consent
  An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps
  All users can consent for any app to access the organization's data.

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

Low | Medium (Preview) | High (Preview)

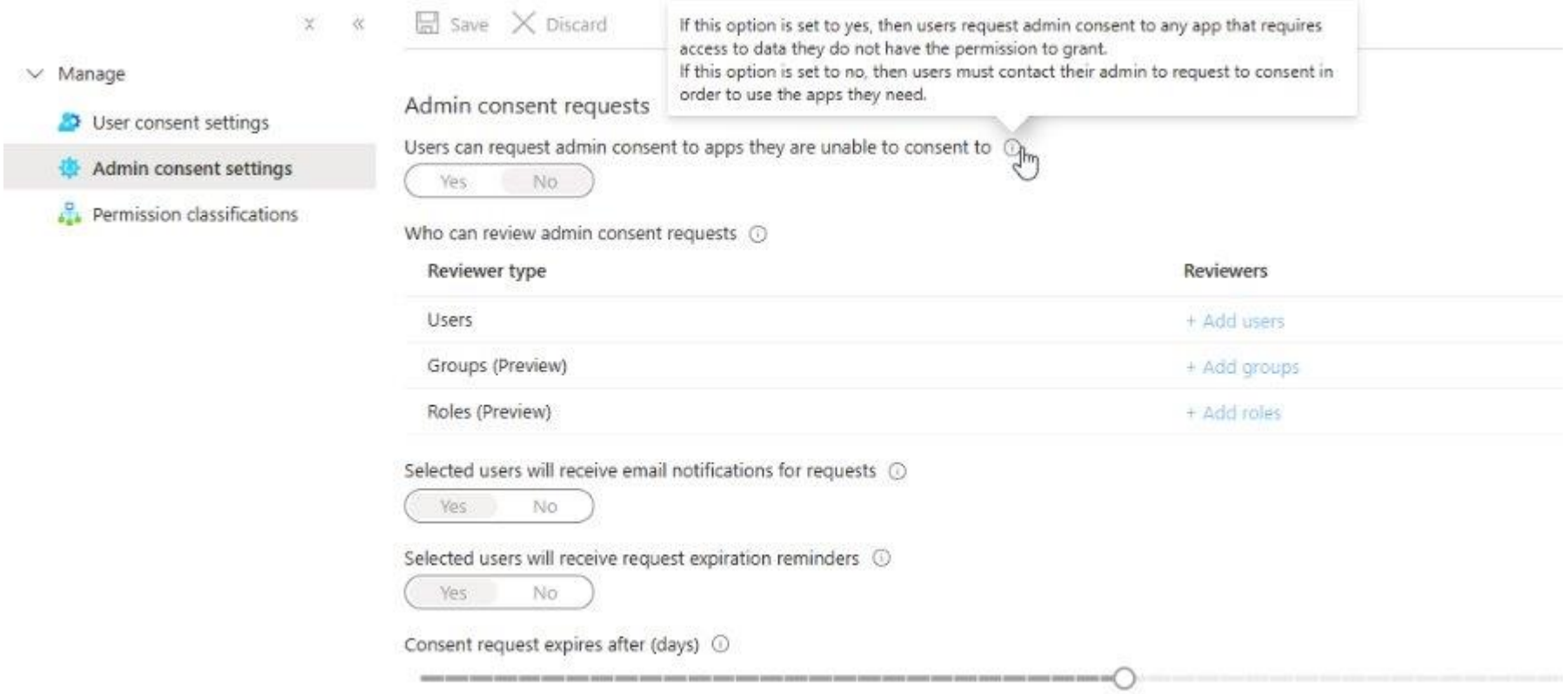
Define low-risk permissions here. Only delegated permissions that don't require admin consent are supported.

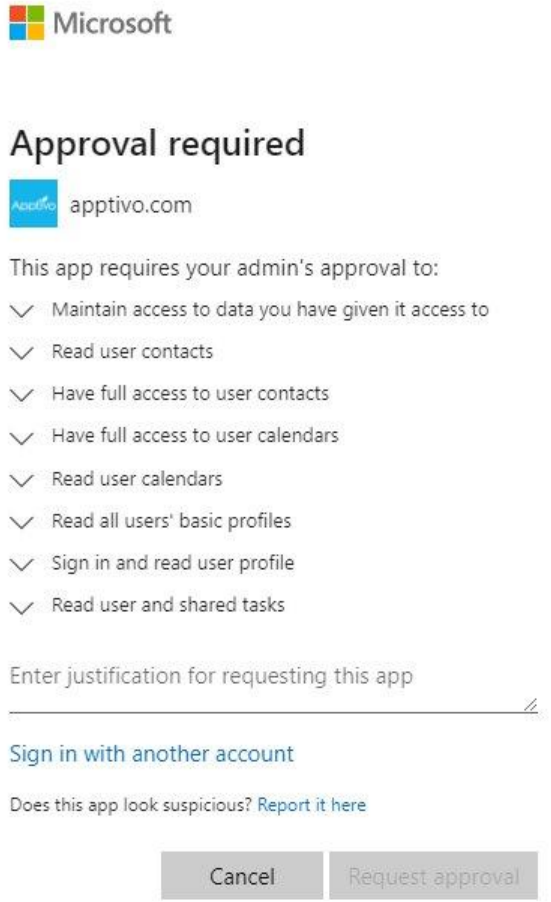
+ Add permissions

API used	Permissions	Description
Microsoft Graph	User.Read	Sign in and read user profile
Microsoft Graph	profile	View users' basic profile
Microsoft Graph	email	View users' email address
Microsoft Graph	openid	Sign users in
Microsoft Graph	offline_access	Maintain access to data you have given it access to

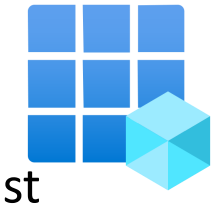
User Authentication

- Administrators can setup consent requests in Entra ID:



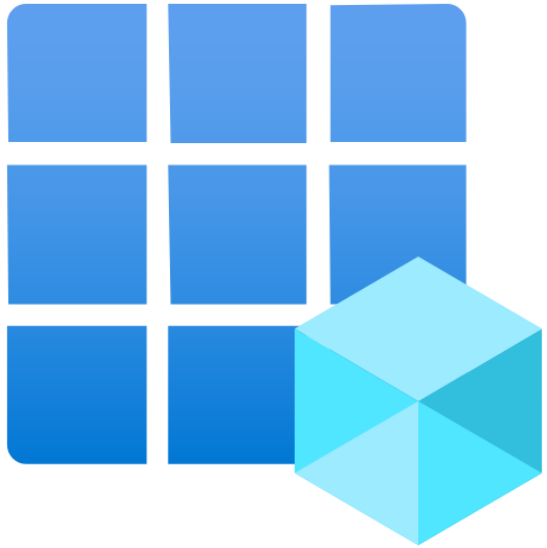


App registrations



- App registrations are application objects inside of Entra ID which can be used to authenticate against other cloud resources.

Application Object



Service Principal

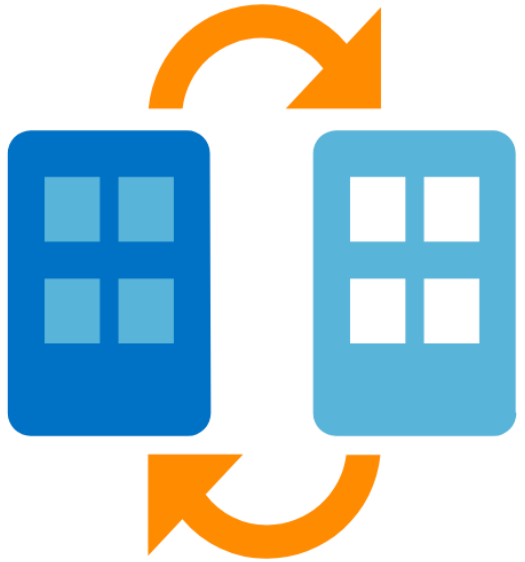
App registrations

www.wpninjas.eu
#WPNinjaS

Secret

Certificate

Federated credentials.



Secrets and certificates always have an expiration date!

App registrations

- Connection to the App registration can be done by knowing the secret:

```
Windows PowerShell
PS C:\Users\JanicVerboon> Connect-MgGraph -ClientId | -TenantId -ClientSecretCredential
```

- Having the certificate and its thumbprint on the local device

```
Windows PowerShell
PS C:\Users\JanicVerboon> Connect-MgGraph -ClientId -TenantId -CertificateThumbprint
```

Authentication using federated credentials can’t be done using PowerShell

App registrations

- Permissions for App registrations can easily be added through the UI on the App registration object:

+ Add a permission ✓ Grant admin consent for JanicVerboon

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (2)				•••
DeviceManagementMar	Application	Read Microsoft Intune devices	Yes	Granted for JanicVerboon •••
User.Read	Delegated	Sign in and read user profile	No	Granted for JanicVerboon •••

After adding a permission, don't forget to add the admin consent.

Managed Identity

Managed Identities are automatically managed credentials provided by Microsoft Entra ID that allow Azure resources to authenticate securely without storing secrets or credentials in code.

They are ideal for enabling secure communication between services that support Entra authentication.

Managed Identity Object types

www.wpninjas.eu
#WPNinjaS

System assigned

Lifecycle

Tied to the lifecycle of an Azure resource

Reusability

Can only be used by the associated Azure Resource

Identity Management

Automatically created and managed when enabled on the Azure resource

Use Case

Single resource scenarios

User assigned

Lifecycle

Standalone Azure resource, has its own lifecycle

Reusability

Can be assigned to multiple Azure resources

Identity Management

Must be manually created and assigned as needed

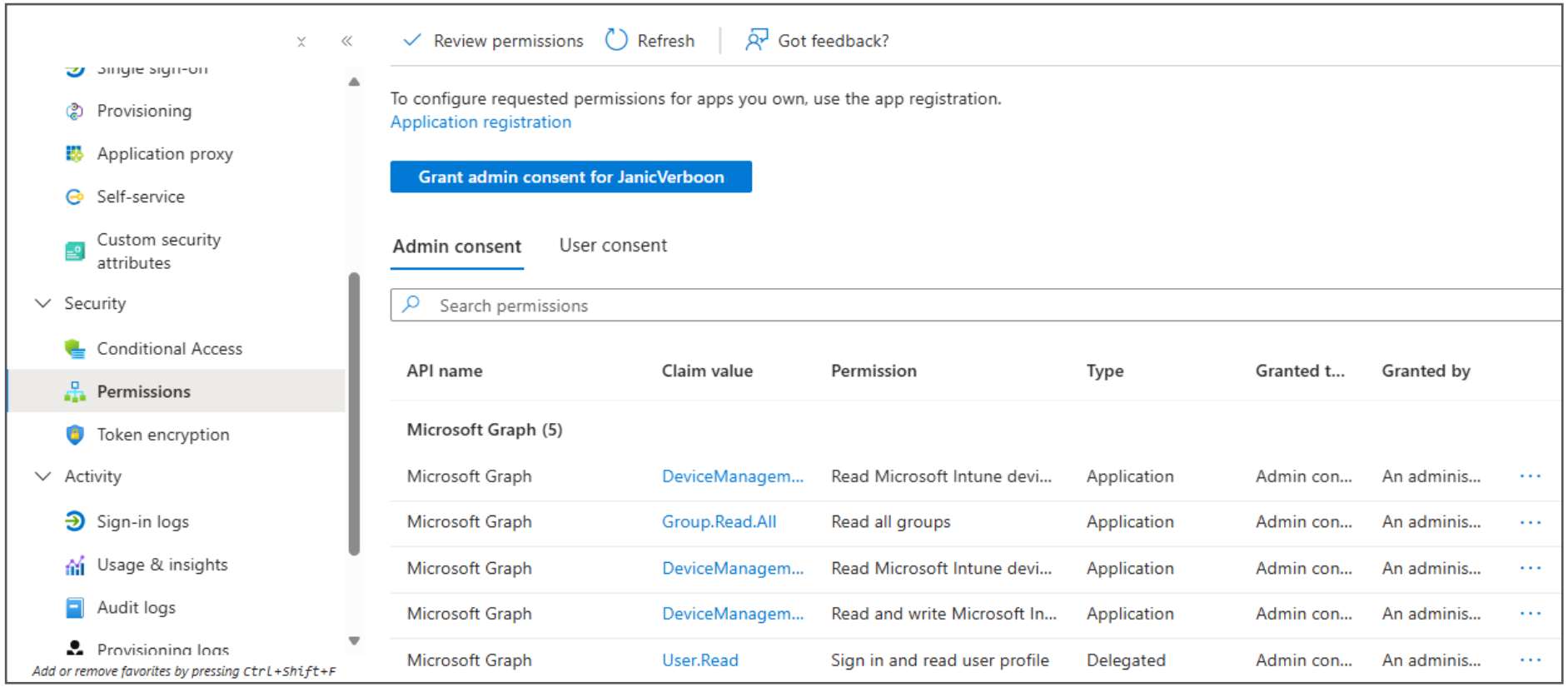
Use Case

Scenarios where multiple resources require the same permissions.

Managed Identities Permissions

www.wpninjas.eu
#WPNinjaS

- Permissions for Managed Identities can’t be added within the Entra ID portal:



Managed Identies


```
#requires -module Microsoft.Graph.Authentication, Microsoft.Graph.Applications

Connect-MgGraph -Scopes "AppRoleAssignment.ReadWrite.All", "Application.Read.All"

$managedIdentityObjectId = "<Managed Identity Object ID>"
$permissions = "DeviceManagementServiceConfig.ReadWrite.All", "Device.Read.All"

$graphApi = Get-MgServicePrincipal -Filter "appId eq '00000003-0000-0000-c000-000000000000'"
$permissions = $graphApi.AppRoles | Where-Object { $_.Value -in $permissions -and $_.AllowedMemberTypes -contains
"Application" }

$permissions | ForEach-Object {

    $appRoleAssignment = @{
        ServicePrincipalId = $managedIdentityObjectId
        PrincipalId        = $managedIdentityObjectId
        ResourceId         = $graphApi.Id
        AppRoleId          = $PSItem.Id
    }

    New-MgServicePrincipalAppRoleAssignment @appRoleAssignment
}
```

Microsoft API's

Microsoft Graph API

Defender API

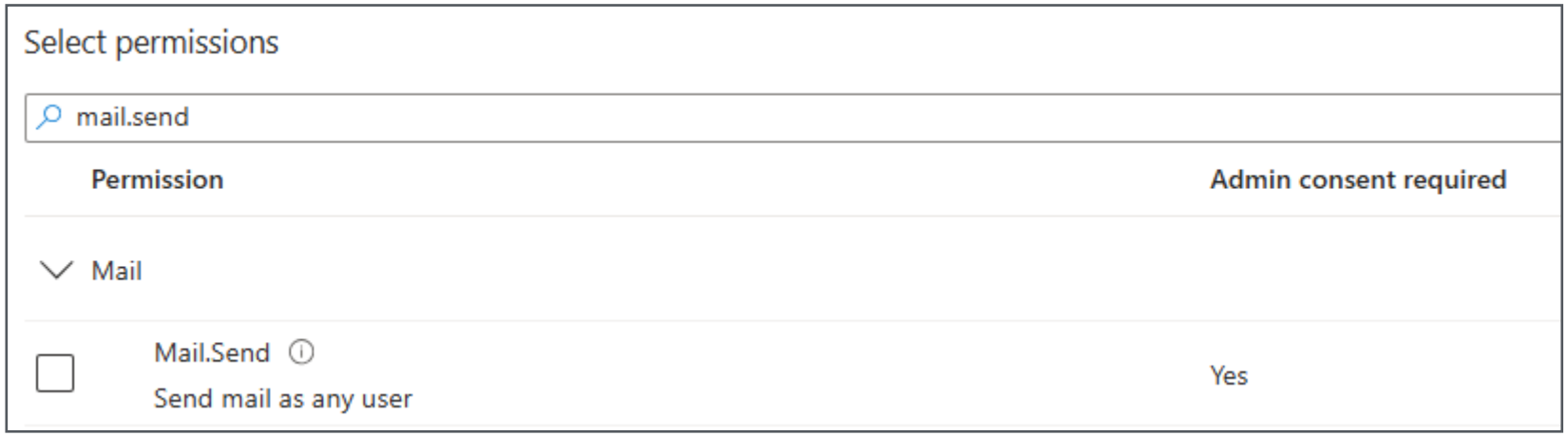
SharePoint

Office 365
Management API's

Azure API

Sending Emails via the Graph API

- The Mail.send permission allows an application to send emails as any user you specify!



- To mitigate this admins had to use Exchange Application Access policies to limit the sending of emails to members of a certain user group

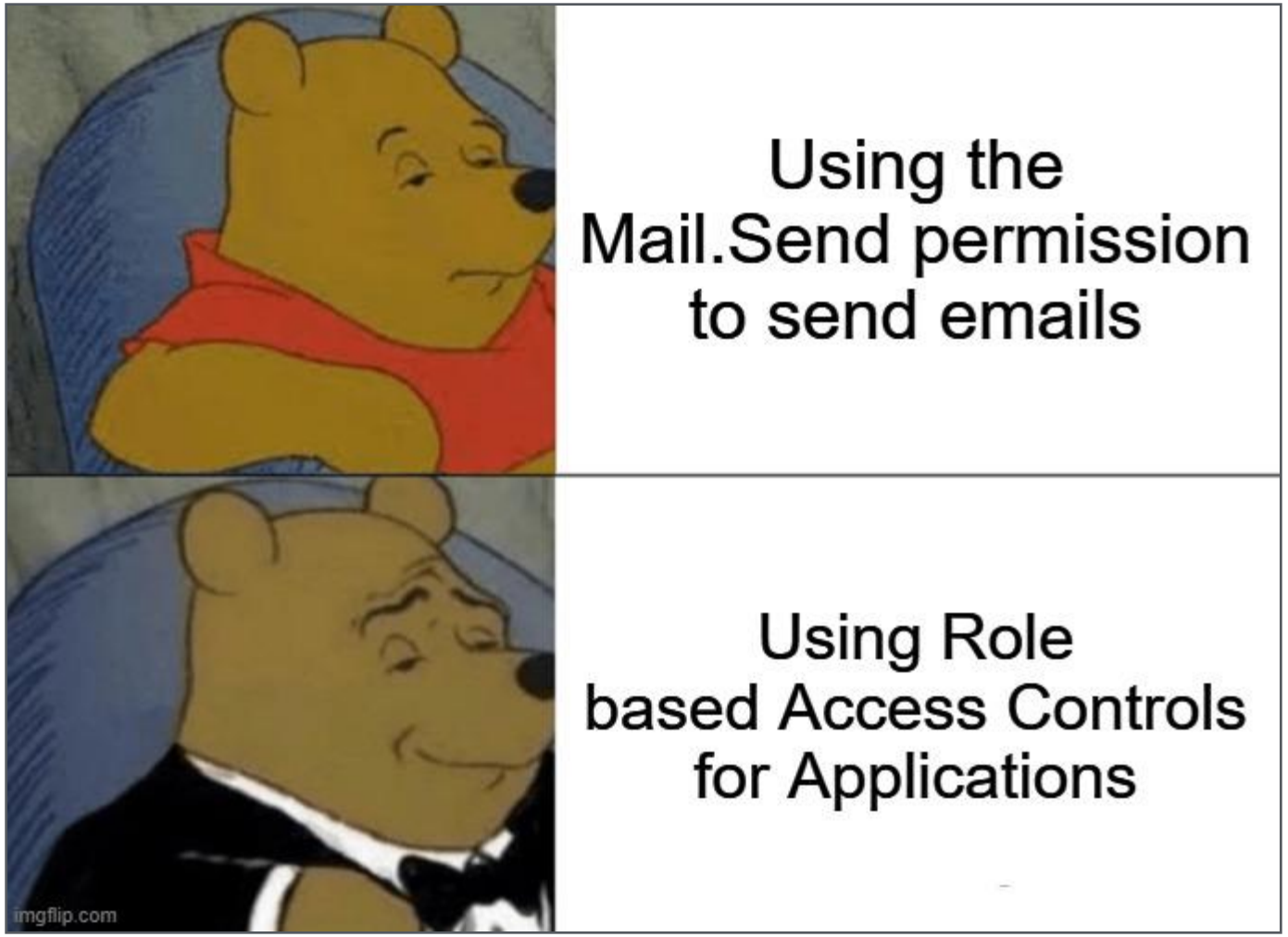
Detailed explanation: Securely sending emails from PowerShell scripts with modern authentication enforced | Nicola Suter

Sending Emails via the Graph API Like a Pro

- We can now leverage a new feature in Exchange Online to granular control who from which mailboxes mails can be sent using modern authentication: **Role Based Access Control for Applications**
- This no longer requires granting the Mail.Send Graph permission.

Awesome Blog by Jan Bakker: A love story about Role Based Access Control for Applications in Exchange Online, Managed Identities, Entra ID Admin Units, and Graph API - JanBakker.tech

Sending Emails via the Graph API



Retrieve SP in your tenant with Mail.Send

Full Script will be in the Github Repository

Output will look like this:

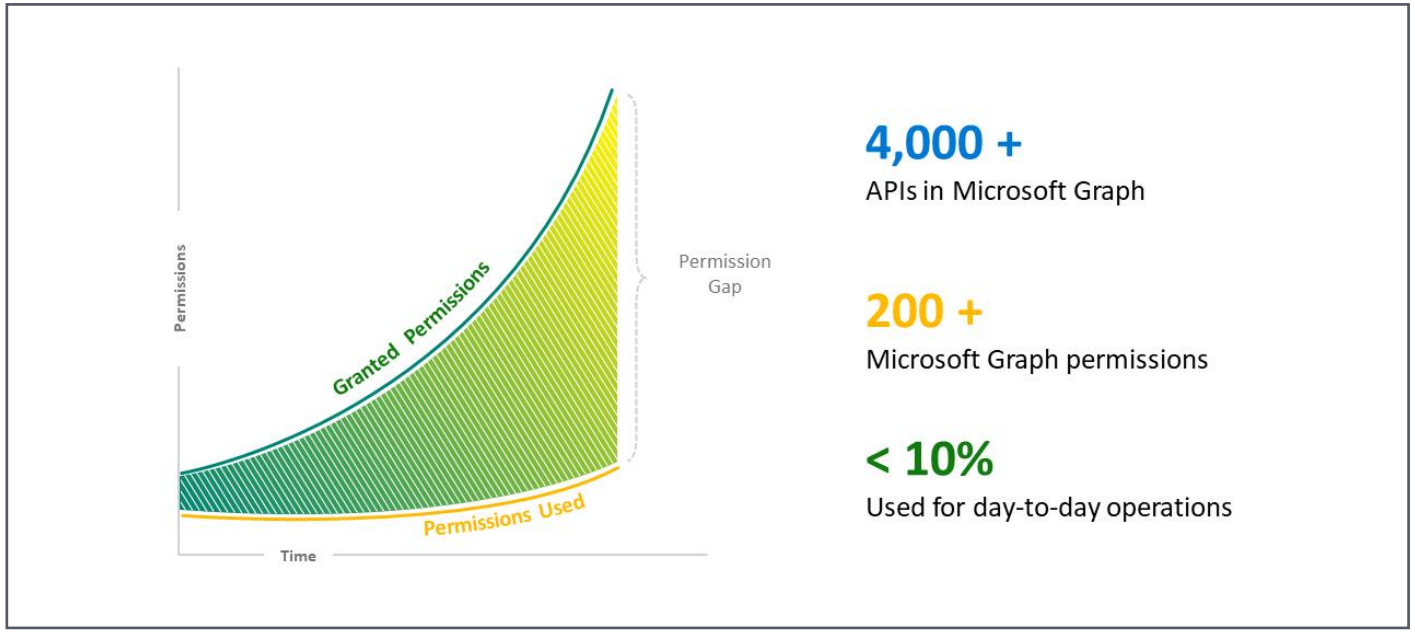
```
AppName                 AppId                                Permission
-------                 -----                                ----------
Intune-AppleMonitoring2 e43e089f-c66f-4bcf-9f27-88c594dae696 Application - Mail.Send
la-socnotebookmail      a2171c36-32b6-4375-8fe9-447631b7822f Application - Mail.Send
```

Demo

- How to use the Browser Tools
- How to use the GraphX Browser Extension
- How you can find out the least needed privileges needed:
    - Graph Explorer
    - Docs
    - Find-MgGraphPermission

Summary

- Cloud automation is powerful but without proper security, it can become an entry point for attackers
- Misconfigured or over-permissioned automation workflows can expose sensitive systems and data
- Enforcing least privilege also to automation (also to access the Azure Resourses) is essential to minimize risk



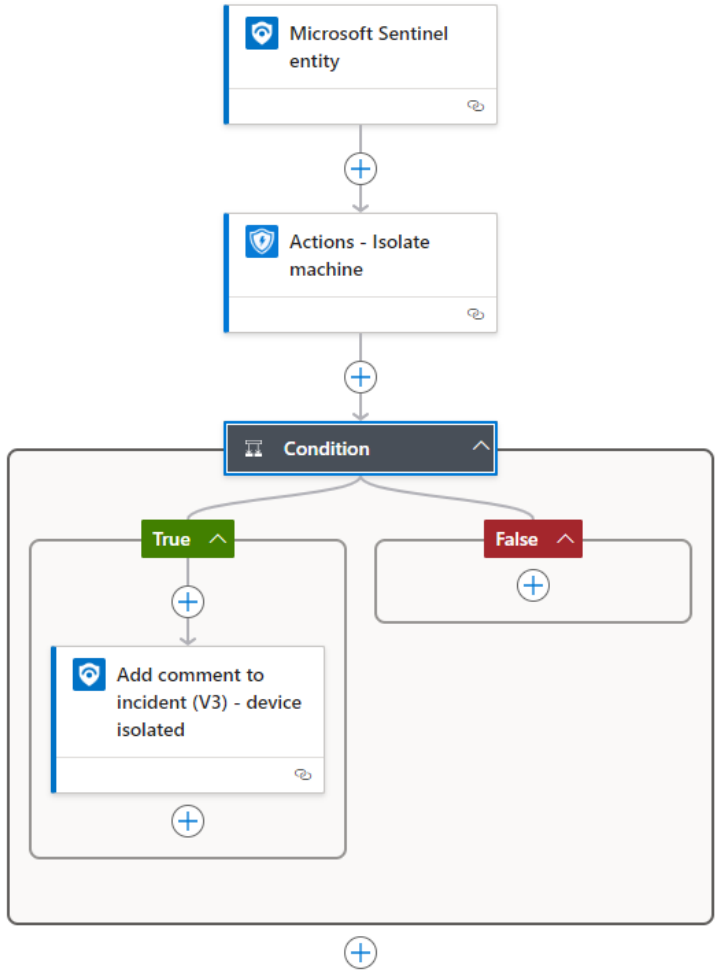
Source: https://learn.microsoft.com/en-us/security/zero-trust/develop/overprivileged-permissions

Logic Apps

From Manual to Magical:
Automate routine tasks in the cloud

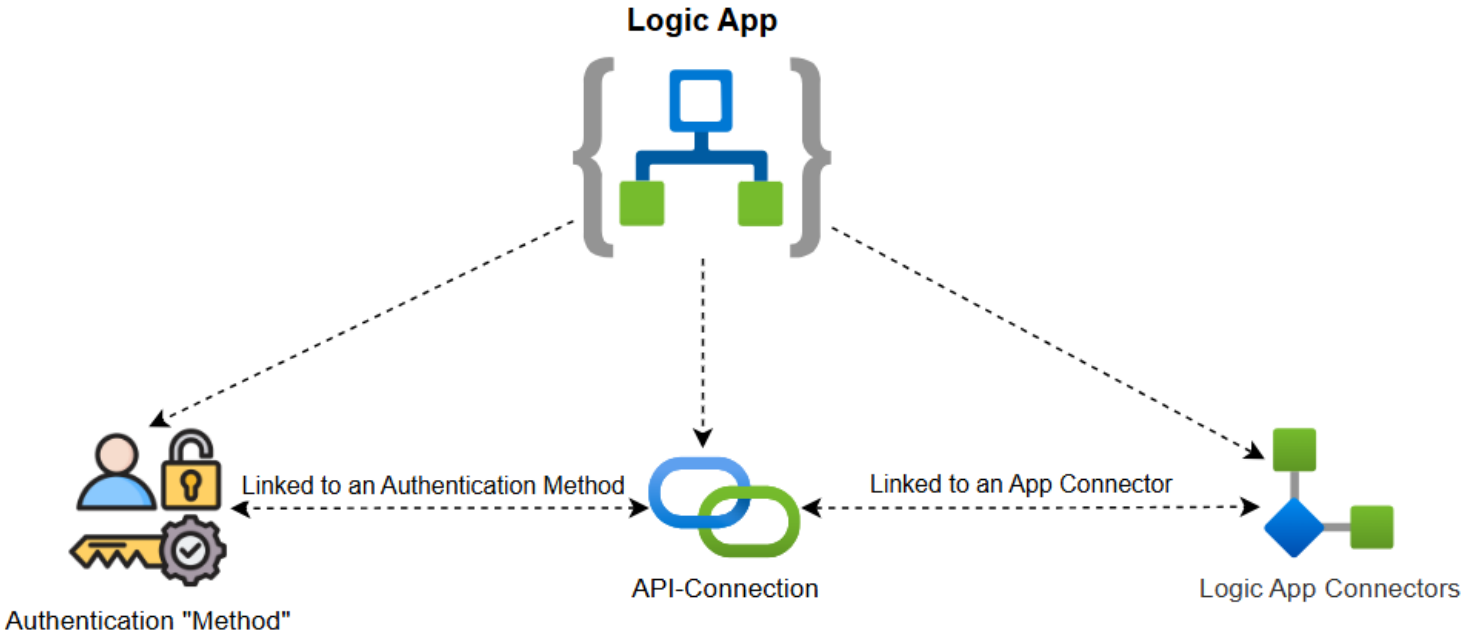
Logic Apps Overview

- Low-Code / No-Code Platform
  - Build code with a designer not “actual” coding
- Serverless
  - Requires no additional infrastructure just the logic app itself
- Many custom connectors available
  - First party (Defender, Microsoft 365, Azure)
  - Third Party (Zendesk, Virus Total)



Logic Apps Parts

- Deployment of Logic app is one single resource in Azure
- But a Logic App has multiple parts which are import to consider

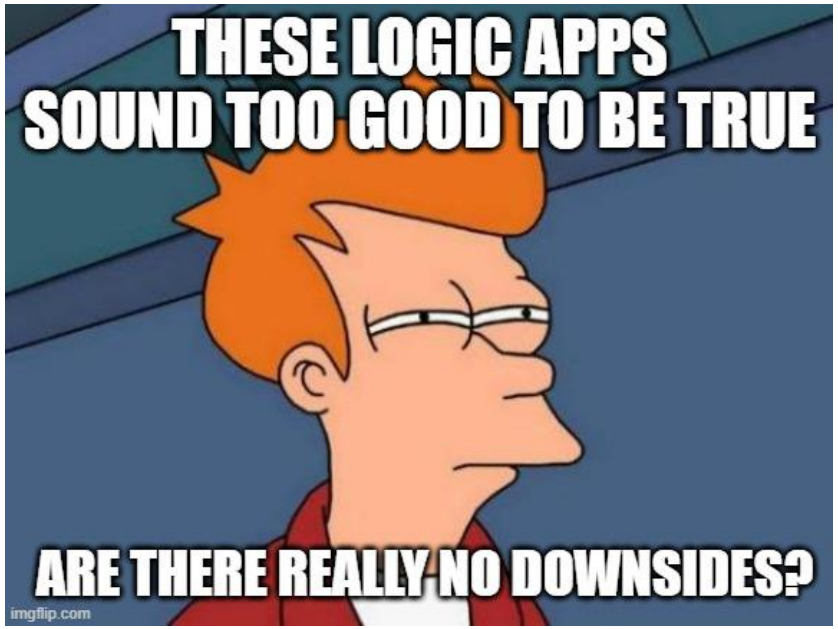


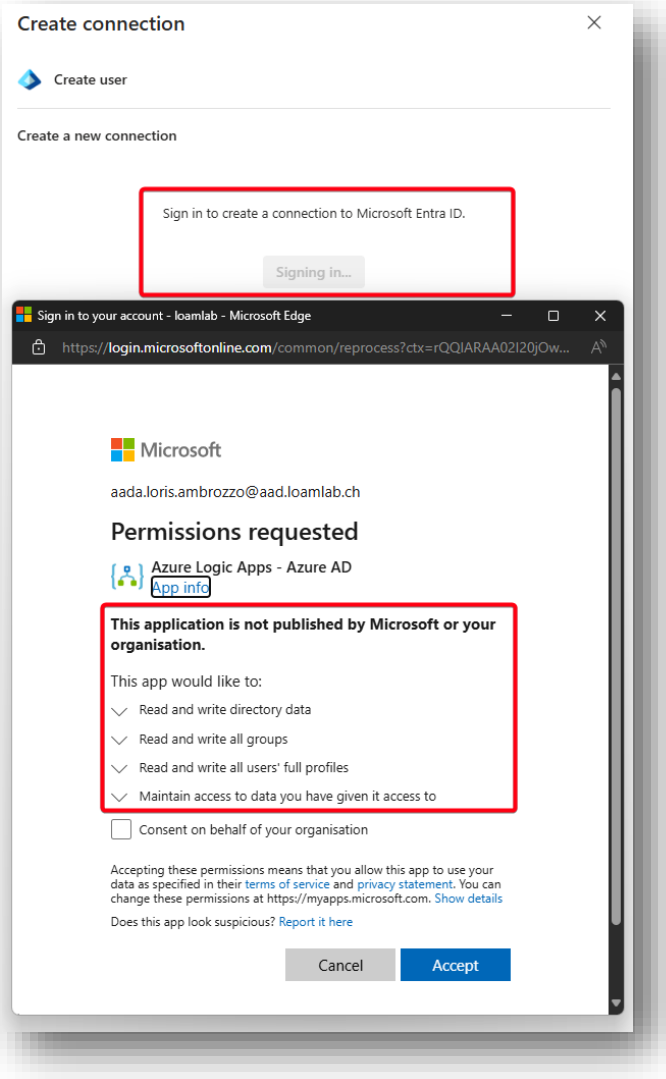
Demo

- Logic App Connectors
- Logic App Authentication
- Logic App API Connections

Logic App – Authentication Challenge

- Not all built in Microsoft Connectors support all authentication methods
- Example Entra ID
  - Only supports OAuth Authentication as the signed-in user



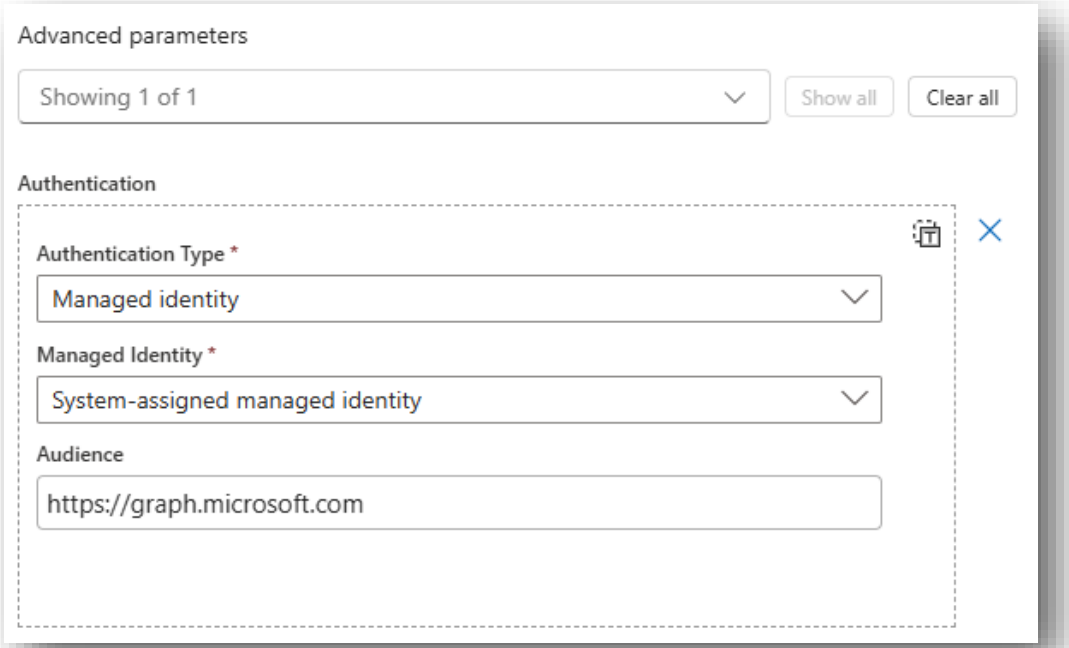


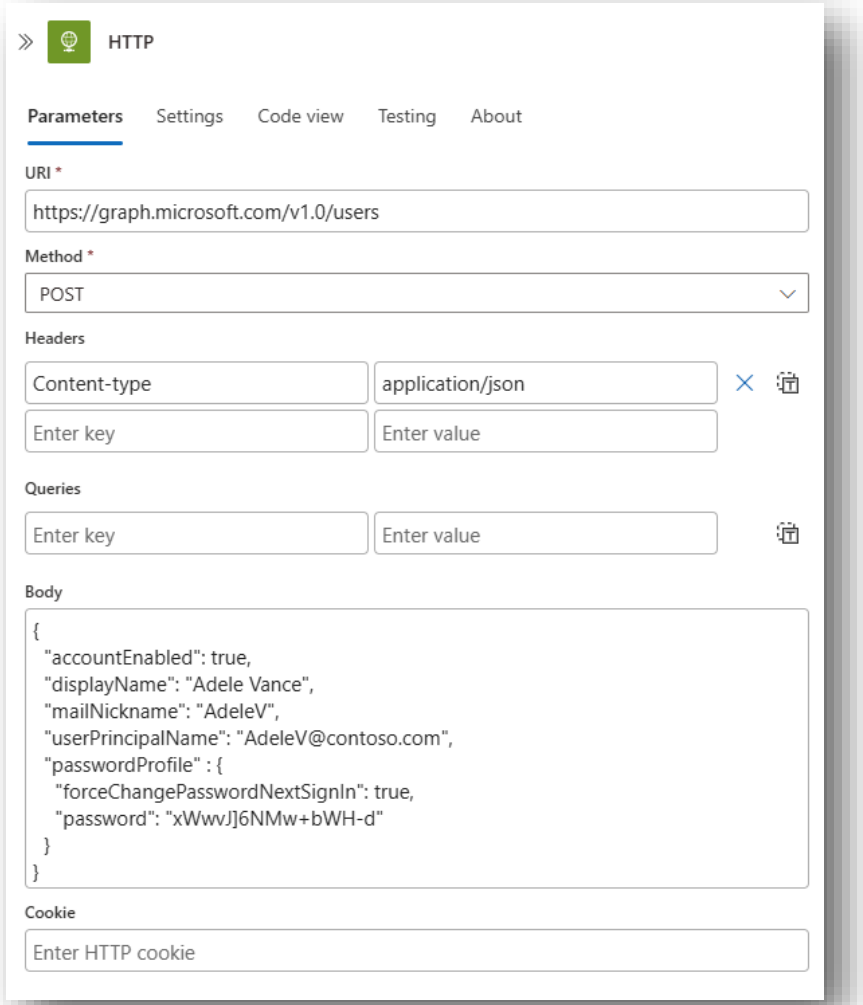
Logic App – Authentication Challenge

www.wpninjas.eu
#WPNinjaS

Solution

- Create API request manual via HTTP connector
- HTTP connector supports Managed Identity Authentication

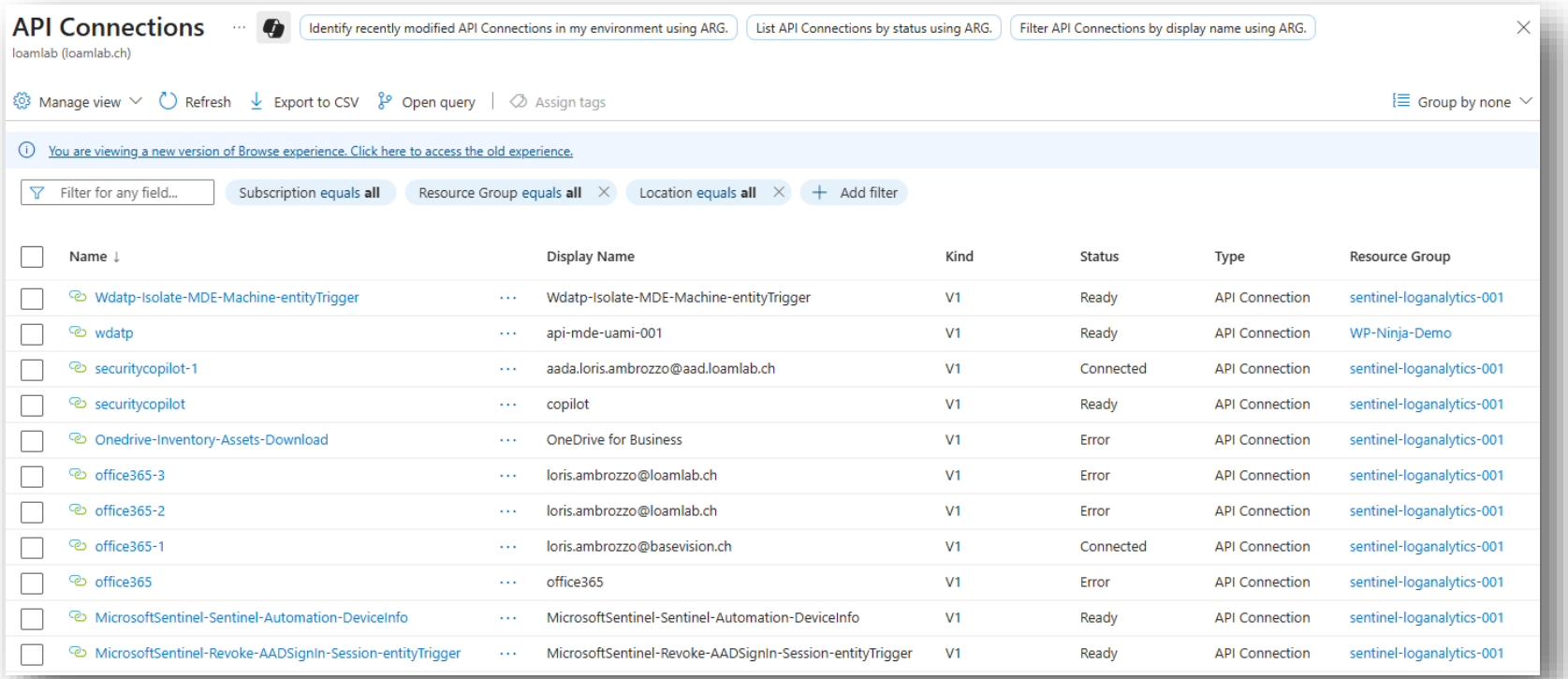




Don’t forget to set the audience in the authentication blade!

Logic Apps – API Connection Challenge

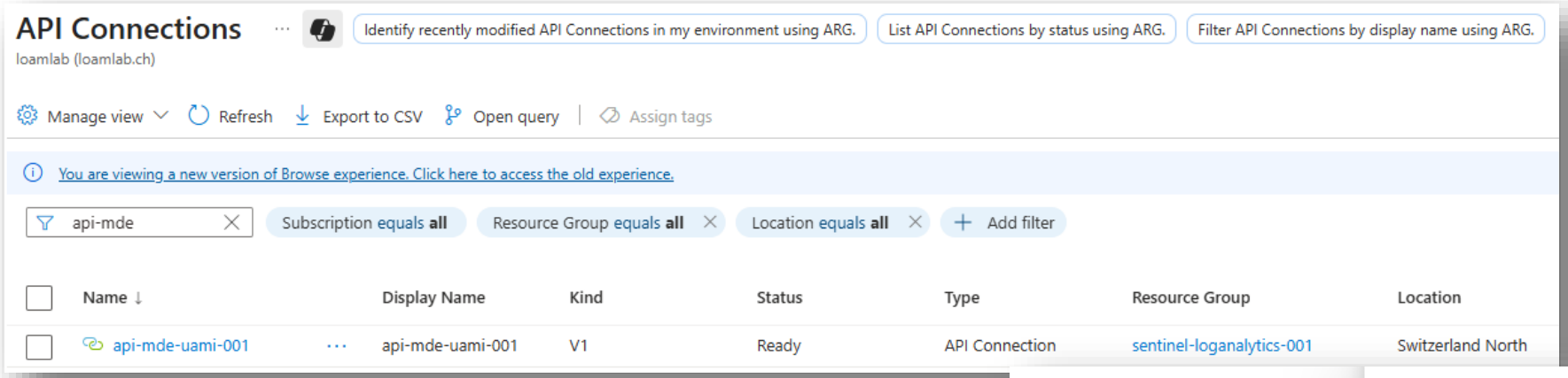
- Logic apps are linked to API connections, but there is no one-to-one relationship between a Logic App and an API connection
- Whenever an Logic App is deleted the API connections will remain active
- This leads to a “chaos” of API Connections

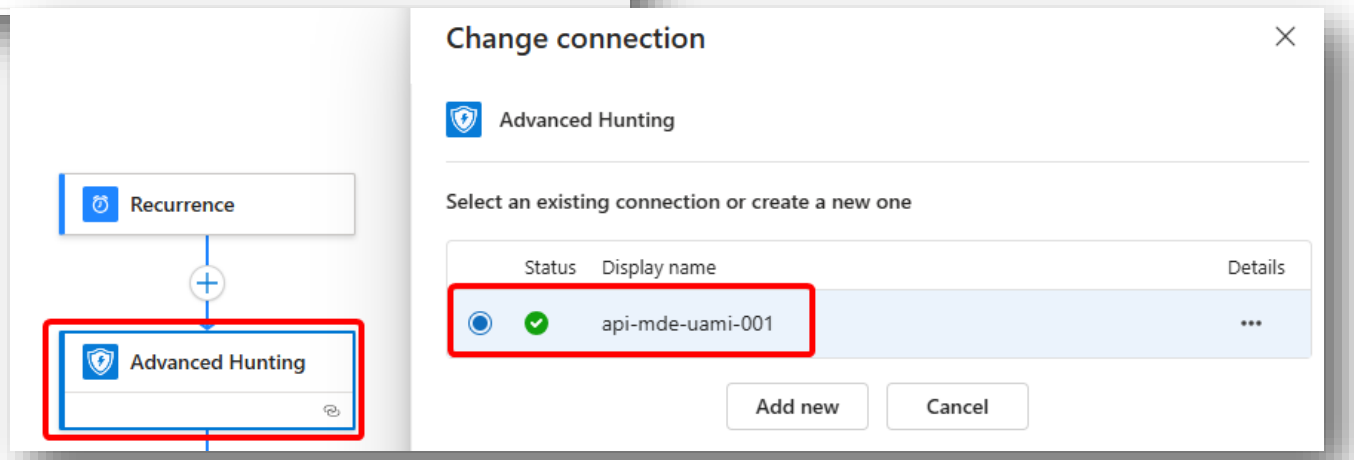


Logic Apps – API Connection Challenge

www.wpninjas.eu
#WPNinjaS

- Solution deploy one API-Connection per service / API and shared managed identity





Logic Apps – API Connection Challenge

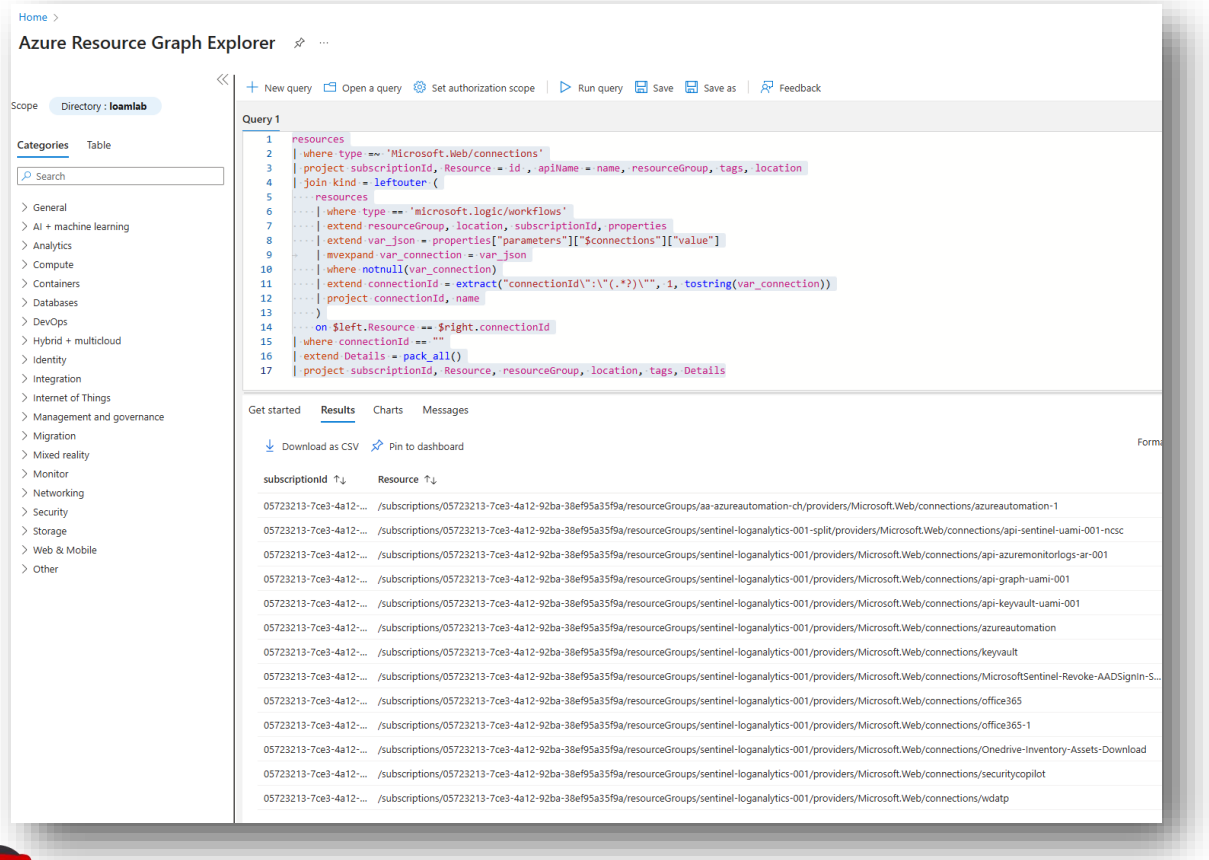

```
param MDEApiConnectionName string = 'api-mde-uami-001'
param resourceGroupLocation string = resourceGroup().location


// describe the mde api connection
resource WdatpConnection 'Microsoft.Web/connections@2016-06-01' = {
  name: MDEApiConnectionName
  location: resourceGroupLocation
  properties: {
    displayName: MDEApiConnectionName
    customParameterValues: {}
    parameterValueType: 'Alternative'
    api: {
      id: subscriptionResourceId('Microsoft.Web/locations/managedApis', resourceGroupLocation, 'Wdatp')
    }
  }
}
```

The name of the API connection can only be configured via the Bicep template. A default value is configured via the GUI, but only the display name can be set.

Logic Apps – API Connection Challenge

www.wpninjas.eu
#WPNinjaS

Find orphan API-Connections



https://github.com/dolevshor/azure-orphan-resources/blob/main/Queries/orphan-resources-queries.md#api-connections

Logic App - Costs

Consumption

	Price Per Execution
Actions	First 4,000 actions free - Included CHF 0.000030

Standard Plan

Workflow Service Plan

	Price
vCPU	CHF 120.127567/month
Memory	CHF 8.605803/month

Based on our experience, Logic Apps are quite cheap unless a lot of loops and actions are required (e.g. looping through all users in the company). In this case, a Standard Plan or another automation solution would be more appropriate.

Automation Account

From Manual to Magical:
Automate routine tasks in the cloud

What is Azure Automation?

www.wpninjas.eu
#WPNinjaS

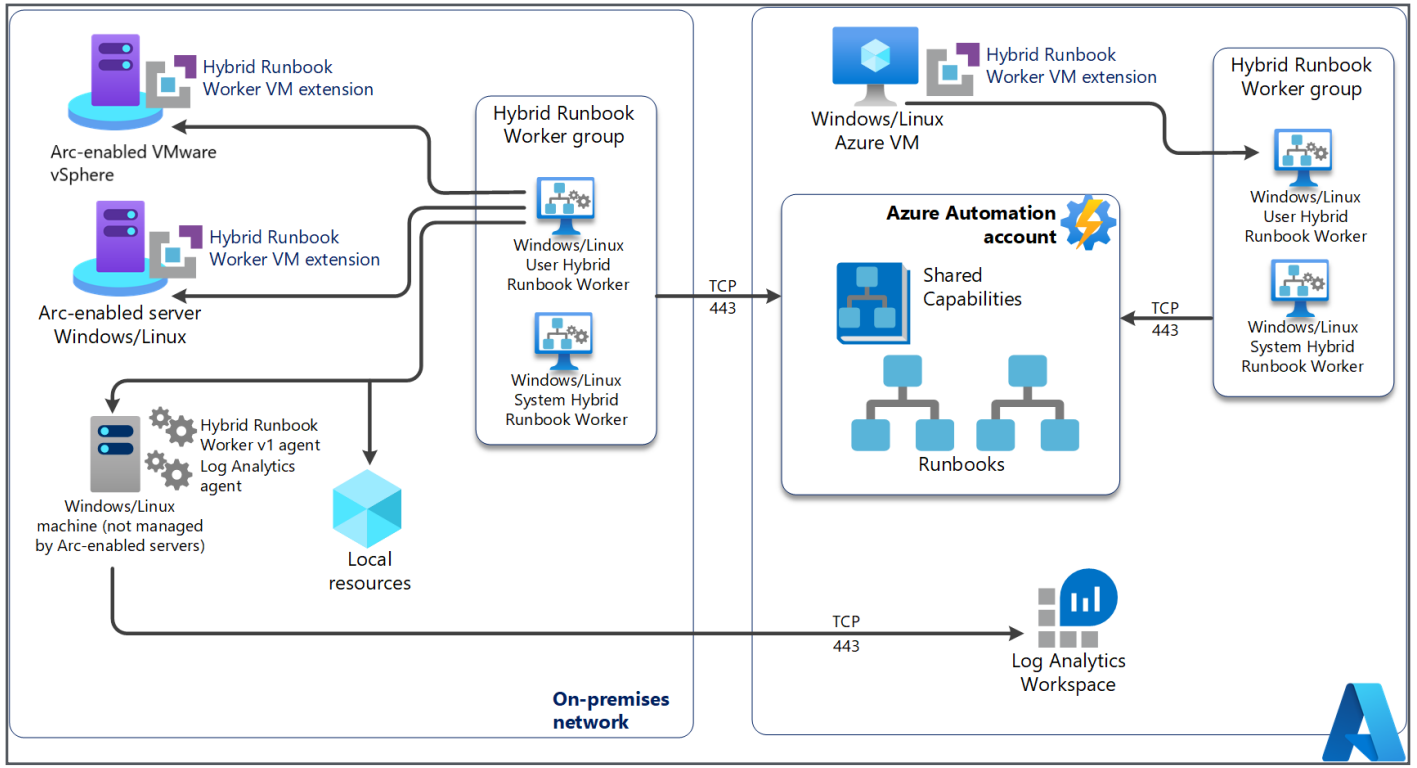
Azure Automation

“Ditch the Task Scheduler—Azure Automation is your cloud-native script whisperer.”

Azure Automation Hybrid Worker

www.wpninjas.eu
#WPNinjaS

- Azure Automation Runbooks can be extended to on-premise resources
- Create and schedule runbooks in the cloud
  - Schedule them to run on-premise
  - Use custom credentials or the computer object of the on-premise computer object for authentication.
  - Install needed PowerShell scripts on the local Server
  - Monitor Runbook results in the Cloud



Demo

- Azure Automation Overview
- Show Runtime environments & Modules
- Show Credentials
- Show Source Controls and runbook state
- Show Webhooks
- Show Schedules
- Show Demos

Costs & Limitations

	Free units included (per month)*	Price
Job run time	500 minutes	**$0.002**/minute

Maximum amount of disk space allowed per sandbox [1]	1 GB	Applies to Azure sandboxes only.
Maximum amount of memory given to a sandbox [1]	400 MB	Applies to Azure sandboxes only.
Maximum number of network sockets allowed per sandbox [1]	1,000	Applies to Azure Sandboxes only
Maximum runtime allowed per runbook [1]	Three hours	Applies to Azure Sandboxes only

Real Word Examples

From Manual to Magical:
Automate routine tasks in the cloud

Real World examples

Problem: Monitoring of Intune Apple environment

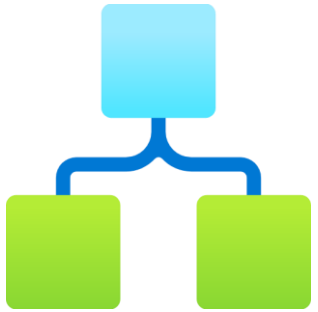
- IT admins may forget to renew expiring Connectors and Tokens in Microsoft Intune which are required for Apple device management (APNS, ADE, VPP
- IT admins may forget to renew LOB app certificates
- Uses might be unable to install new VPP apps, since the license consumption has been exhausted.

Solution: Azure Automation

- Runbook which checks expiring Connectors and LOB Apps
- Checks free VPP licenses
- Informs IT admin per mail if action is required

WPNinja25-FromManualtomagical/Scripts/Intune_Apple_Monitoring at main · JanicVerboon/WPNinja25-FromManualtomagical

Real World examples



Problem: Defender for Endpoint – Settings Management Enablement

- Devices need to have the MDE-Management Tag assigned dynamically based on criteria's (e.g. Naming Convention)
- Dynamic Asset Rule Management in MDE is not supported for Settings Management Tags
- Manual assignment no alternative

Solution: Logic App

- Query for Devices based on naming convention
- Check if MDE-Management Tag is applied
- If not apply the device tag otherwise ignore the host
- Run Logic App on a daily base

WPNinja25-FromManualtomagical/Logic App at main · JanicVerboon/WPNinja25-FromManualtomagical

Real World examples

Problem: MFA Registration Campaign not working

- If a Conditional Access policy blocks MFA registration the registration campaign feature might not work.
- Admins want to migrate users off SMS to MS Authenticator

Solution: Azure Automation

- Queries out users which already have SMS as MFA Method and adds them to a group
- This group can then be excluded from the block MFA registration CA Policy to ensure the Registration campaign feature works.

WPNinja25-FromManualtomagical/Scripts/Invoke-CARegisterSecurityInformationExclusion at main · JanicVerboon/WPNinja25-FromManualtomagical

Real World examples

Problem: Identity Protection policies cannot be enabled because not all users have enrolled for MFA

- To lower the user or sign-in risk in Identity Protection, an additional multi-factor authentication (MFA) prompt or secure password change is required.
- It is not possible to enable Identity Protection alerts for all users, as this would otherwise block all users who are not enrolled in MFA.

Solution: Azure Automation

- Querie users who are already MFA-capable and puts them into one group, while putting the other users into another group.
- The MFA-capable group can then be used to target Identity Protection policies via Conditional Access.

WPNinja25-FromManualtomagical/Scripts/Invoke-UpdateEntraGroupMFACapability at main · JanicVerboon/WPNinja25-FromManualtomagical

Summary

- Familiarity drives efficiency → choose solutions you're comfortable with
- Some solutions simplifies an decision for an automation solutions
  - Microsoft Sentinel Logic App integration with Playbooks (Logic Apps)
  - Microsoft Entra Identity Governance with Custom Extensions (Logic Apps)
- Some decision helpers
  - High-volume workflows with many loops, steps, or tasks may not be cost-effective in Logic Apps
  - If you want to do more than “automation” an Azure Function could a valuable option

Github Repo:
https://github.com/JanicVerboon/WPNinja25-FromManualtomagical

www.wpninjas.eu
#WPNinjaS

We love Feedback

https://wpninjas25.sched.com/

Great Session!

Okay Session!

Not so okay Session!

Workplace Ninja Summit 2025

Have a question but can't get hold of us? Ask for us at the baseVISION booth, our colleagues will be more than happy to connect you with us!

Thank You

Workplace Ninja Summit 2025