



13 februari 2025 – APE Meetup

Automate your way into a  
compliant Azure DevOps platform

Onno Hettema – Principal Consultant Cloud & Security

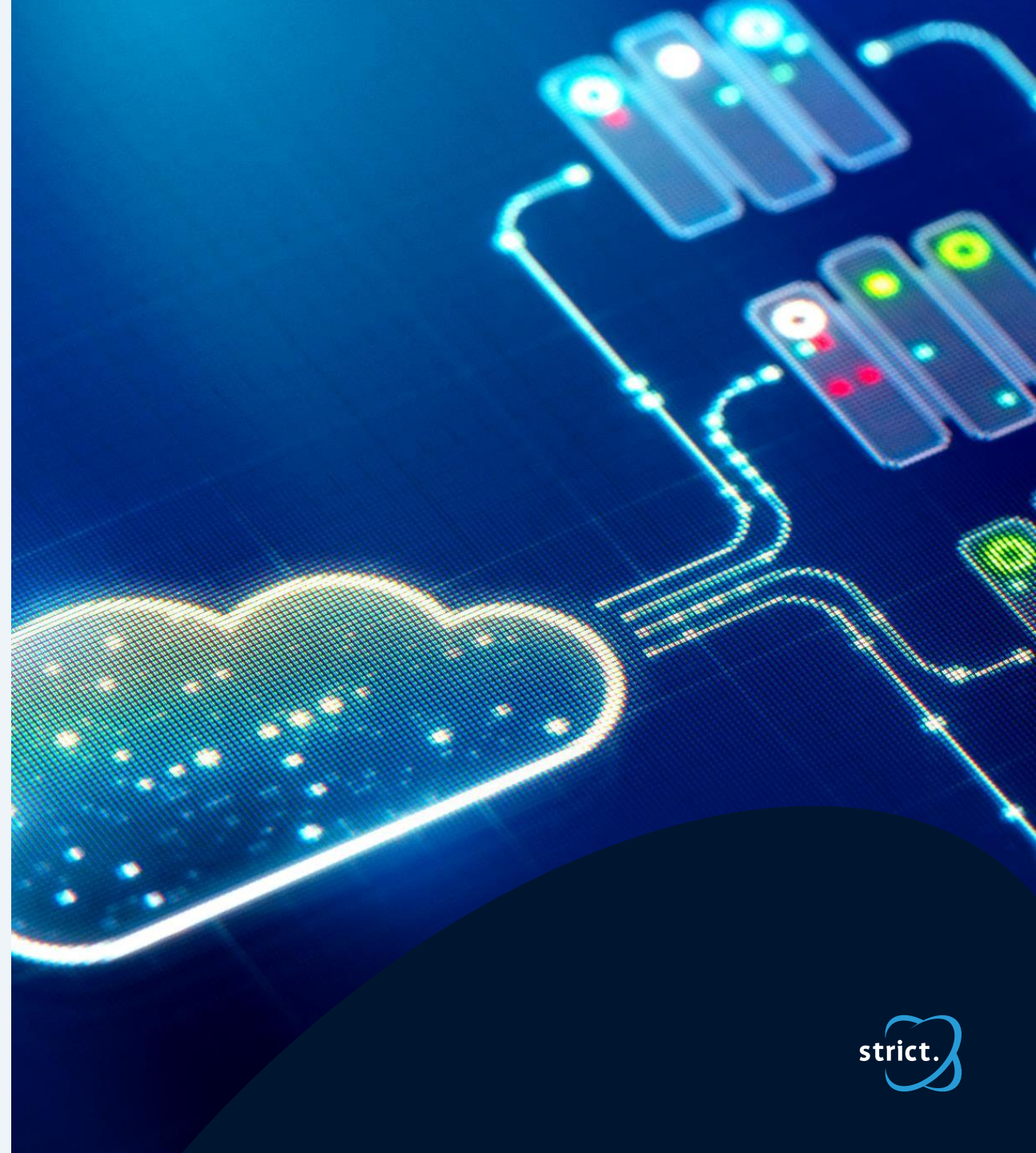
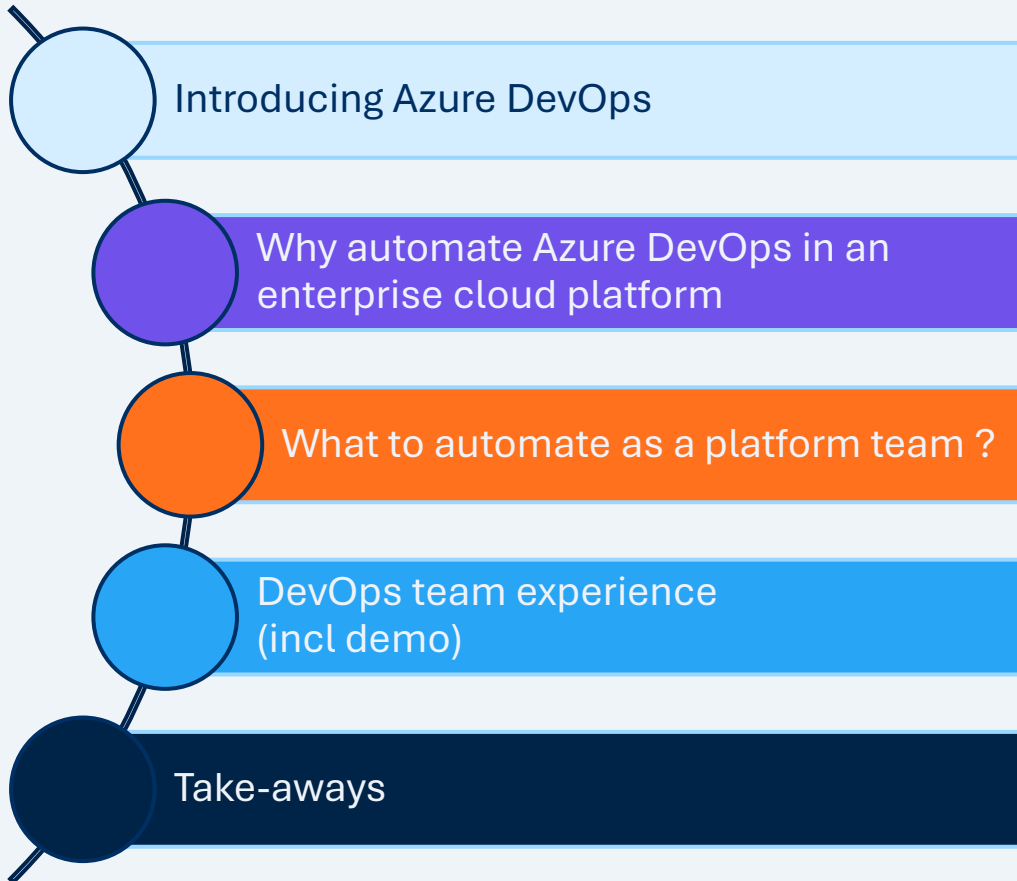
# Introduction



- [Connect: Onno Hettema | LinkedIn](#)



# Agenda



# Introducing Azure DevOps



Azure  
Boards

Plan, track, and discuss work across teams, deliver value to your users faster.



Azure  
Repos

Unlimited cloud-hosted private Git repos. Collaborative pull requests, advanced file management, and more.



Azure  
Pipelines

CI/CD that works with any language, platform, and cloud. Connect to GitHub or any Git provider and deploy continuously to any cloud.



Azure  
Test Plans

The test management and exploratory testing toolkit that lets you ship with confidence.



Azure  
Artifacts

Create, host, and share packages. Easily add artifacts to CI/CD pipelines.

Why automate Azure DevOps  
in an enterprise cloud  
platform?

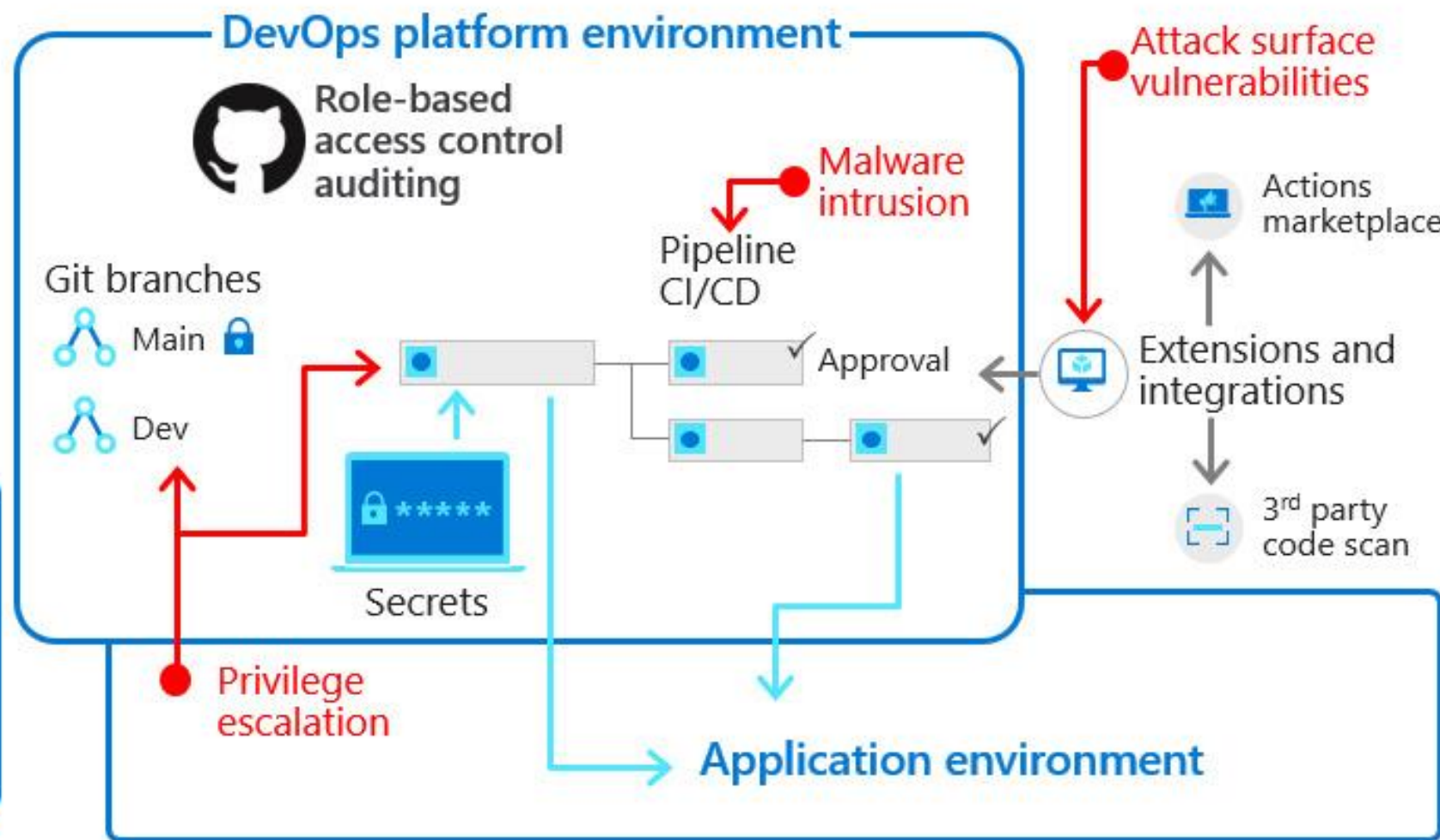
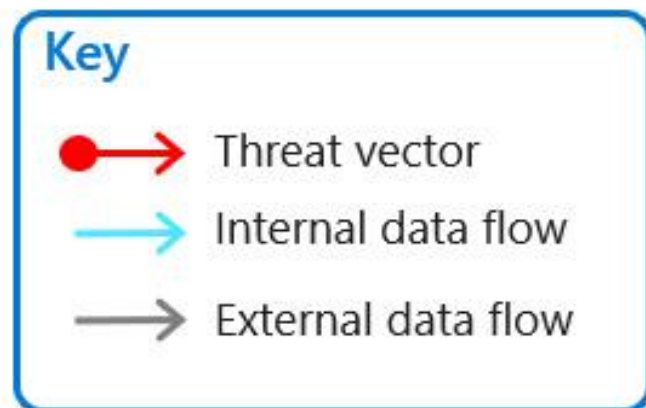


# Why automate?

- Improved security and compliance
- Consistency and repeatability
- Scalable to large number of Azure DevOps projects/teams
- Help DevOps teams with a valuable, secure and compliant platform



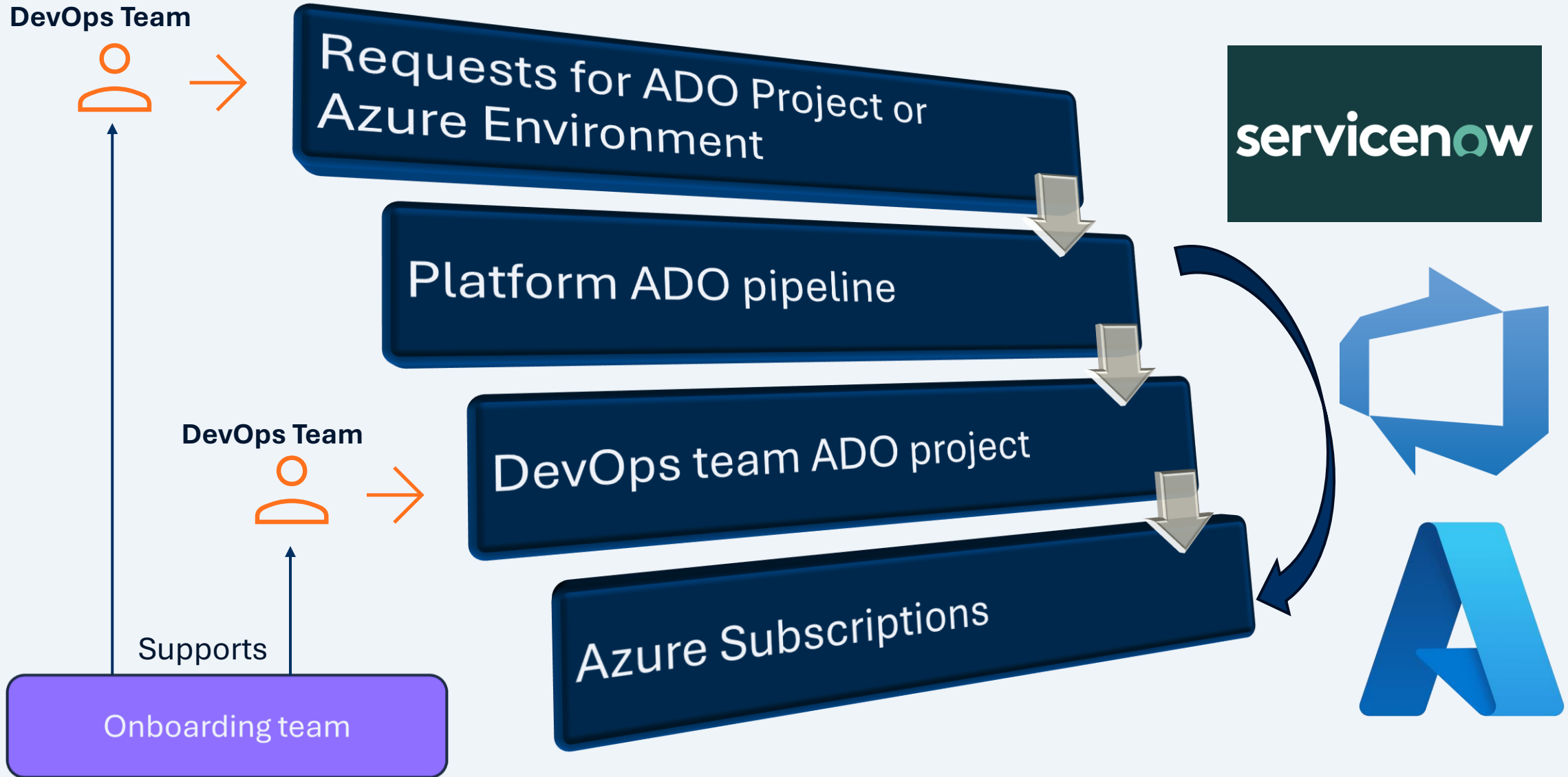
# DevOps platform environment Overview



What should a platform  
team automate and how?



# Platform overview



# What to automate

Project:

- Policies
- Identities
- Integrations



# Create application system (project)

← Jobs in run #CHG1962...  
Create-ApplicationSystem

Jobs

✓	✓	Creating Applicati...	3m 26s
	✓	Initialize job	3s
	✓	Checkout DRCP@ma...	2s
	✓	Create custome...	1m 51s
	✓	Checkout ado-author...	1s
	✓	Create ADO proj...	1m 4s
	✓	Create DRCP variabl...	16s
	✓	Install internal root c...	2s
	✓	Create SonarQube E...	3s
	⌚	Create Mule Applic...	<1s
	✓	Post-job: Checkout ...	<1s
	✓	Post-job: Checkout ...	<1s
	✓	Finalize Job	<1s

✓ Create customer Application system Microsoft Entra ID groups

View raw log

```
66 Connecting to Microsoft Graph with modern token retrieval method (using Get-AzAccessToken).
67 WARNING: Upcoming breaking changes in the cmdlet 'Get-AzAccessToken' :
68 The Token property of the output type will be changed from String to SecureString. Add the [-AsSecureString] switch to avoid the imp
69 - The change is expected to take effect in Az version : '14.0.0'
70 - The change is expected to take effect in Az.Accounts version : '4.0.0'
71 Note : Go to https://aka.ms/azps-changewarnings for steps to suppress this breaking change warning, and other information on breakin
72 Successfully connected to Microsoft Graph.
73 Microsoft Entra ID group [REDACTED] found.
74 Microsoft Entra ID group [REDACTED] is already configure
75 Connecting to Microsoft Graph with modern token retrieval method (using Get-AzAccessToken).
76 WARNING: Upcoming breaking changes in the cmdlet 'Get-AzAccessToken' :
77 The Token property of the output type will be changed from String to SecureString. Add the [-AsSecureString] switch to avoid the imp
78 - The change is expected to take effect in Az version : '14.0.0'
79 - The change is expected to take effect in Az.Accounts version : '4.0.0'
80 Note : Go to https://aka.ms/azps-changewarnings for steps to suppress this breaking change warning, and other information on breakin
81 Successfully connected to Microsoft Graph.
82 Microsoft Entra ID group [REDACTED] found.
83 Microsoft Entra ID group [REDACTED] is alr
84 Connecting to Microsoft Graph with modern token retrieval method (using Get-AzAccessToken).
85 WARNING: Upcoming breaking changes in the cmdlet 'Get-AzAccessToken' :
86 The Token property of the output type will be changed from String to SecureString. Add the [-AsSecureString] switch to avoid the imp
87 - The change is expected to take effect in Az version : '14.0.0'
88 - The change is expected to take effect in Az.Accounts version : '4.0.0'
89 Note : Go to https://aka.ms/azps-changewarnings for steps to suppress this breaking change warning, and other information on breakin
90 Successfully connected to Microsoft Graph.
91 Microsoft Entra ID group [REDACTED] found.
92 Microsoft Entra ID group [REDACTED] is alr
```



# Create application system (project)

← Jobs in run #CHG1962...  
Create-ApplicationSystem

Jobs

✓ Creating Applicati... 3m 26s

✓ Initialize job 3s

✓ Checkout DRCP@ma... 2s

✓ Create custome... 1m 51s

✓ Checkout ado-author... 1s

✓ Create ADO proj... 1m 4s

✓ Create DRCP variabl... 16s

✓ Install internal root c... 2s

✓ Create SonarQube E... 3s

▶ Create Mule Applic... <1s

✓ Post-job: Checkout ... <1s

✓ Post-job: Checkout ... <1s

✓ Finalize Job <1s

✓ Create ADO project

```
22 ---- Check of all AAD groups in authorization model are registered in AAD -----
23 waiting for AAD groups to be synchronized in Azure
24 ----- Check Basic access level on AAD groups -----
25 Create endpoint teams if not existing
26 ----- Check team membership and correct differences -----
27 ----- Check team permissions and correct differences -----
28 ----- Check repository permissions and correct differences -----
29 ----- Check pipeline permissions and correct differences -----
30 ----- Check authorization for DRCP-Templates and correct differences -----
31 --- Check authorization for S01-App-MULE-Templates and correct differences ----
32 Check authorization on agent pool 'Azure Pipelines' and correct differences ---
33 =====
34 ===== Authorization report for S01-App-DRCP-TEST-PRD in CPP =====
35 Apply permissions to Azure DevOps project using version v1.7 of the authorization model
36 ---- Check of all AAD groups in authorization model are registered in AAD -----
37 No differences found
38 ----- Check Basic access level on AAD groups -----
39 No differences found
40 ----- Check team membership and correct differences -----
41 No differences found
42 ----- Check team permissions and correct differences -----
43 No differences found
44 ----- Check repository permissions and correct differences -----
45 No differences found
46 ----- Check pipeline permissions and correct differences -----
47 No differences found
48 ----- Check authorization for DRCP-Templates and correct differences -----
49 No differences found
```

# Create application system (project)

← Jobs in run #CHG1962...  
Create-ApplicationSystem

Jobs

✓ Creating Applicati... 3m 26s

✓ Initialize job 3s

✓ Checkout DRCP@ma... 2s

✓ Create custome... 1m 51s

✓ Checkout ado-author... 1s

✓ Create ADO proj... 1m 4s

✓ Create [redacted] variabl... 16s

✓ Install internal root c... 2s

✓ Create SonarQube E... 3s

▶ Create Mule Applic... <1s

✓ Post-job: Checkout ... <1s

✓ Post-job: Checkout ... <1s

✓ Finalize Job <1s

✓ Create [redacted] variable group in customer project

View raw log

```
1 Starting: Create [redacted] variable group in customer project
2 =====
3 Task      : PowerShell
4 Description : Run a PowerShell script on Linux, macOS, or Windows
5 Version   : 2.247.1
6 Author    : Microsoft Corporation
7 Help      : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/powershell
8 =====
9 Generating script.
10 ===== Starting Command Output =====
11 /usr/bin/pwsh -NoLogo -NoProfile -NonInteractive -Command . '/agent/_work/_temp/be9195db-e94b-4f50-ad2f-6a263191f2de.ps1'
12 Successfully updated variable 'serviceNowChangeUri' in variable group 'DRCPVariables' from ADO project [redacted] of AD
13 Successfully updated variable group '[redacted]Variables' in ADO project [redacted] of ADO organization [redacted] wit
14 Successfully updated variable 'serviceNowCustomerApiUsername' in variable group [redacted] from ADO pro
15 Successfully updated variable 'serviceNowCustomerApiSecret' in variable group [redacted] from ADO proje
16 Successfully updated variable 'serviceNowOAuthClientId' in variable group [redacted] from ADO project '[redacted]'
17 Successfully updated variable 'serviceNowOAuthClientSecret' in variable group [redacted] from ADO proje
18 Successfully updated variable 'serviceNowOAuthTokenUri' in variable group [redacted] from ADO project '[redacted]'
19 Successfully created variable group '[redacted]' for DevOps project [redacted] of ADO organiz
20
21 Finishing: Create [redacted] variable group in customer project
```

# Create application system (project)

The screenshot displays an Azure DevOps pipeline interface. On the left, a list of jobs is shown, with 'Create SonarQube E...' highlighted. The main panel shows the execution details for this job, which is a PowerShell task. The task description indicates it runs a PowerShell script on Linux, macOS, or Windows. The log output shows the script generating a request to the SonarQube Enterprise API to create an application. A warning message at the bottom states: '##[warning] SonarQube Enterprise API message: The SonarQube Enterprise application with application key, [redacted] already exist'.

**Jobs in run #CHG1962180 S01-A...**

- ✓ Create [redacted] variabl... 16s
- ✓ Install internal root c... 2s
- ✓ Create SonarQube E... 3s
- ⌚ Create Mule Applic... <1s
- ✓ Post-job: Checkout ... <1s
- ✓ Post-job: Checkout ... <1s
- ✓ Finalize Job <1s
- ✓ Reporting the pipeline... 10s
- ✓ Initialize job <1s
- ✓ Checkout [redacted] @ma... 2s
- ✓ Report to ServiceNow 6s
- ✓ Post-job: Checkout ... <1s
- ✓ Finalize Job <1s

**Finalize build**

- ✓ Report build status <1s

**Create SonarQube Enterprise application and service connection**

1 Starting: Create SonarQube Enterprise application and service connection  
2 =====  
3 Task : PowerShell  
4 Description : Run a PowerShell script on Linux, macOS, or Windows  
5 Version : 2.247.1  
6 Author : Microsoft Corporation  
7 Help : <https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/powershell>  
8 =====  
9 Generating script.  
10 ===== Starting Command Prompt =====  
11 /usr/bin/pwsh -NoLogo -NoProfile -NonInteractive -Command . '/agent/\_work/\_temp/2a46316e-57ad-44c7-b9a6-6425e2bbb616.ps1'  
12 Reading service connection template at FilePath: /agent/\_work/1/s/Ado/ServiceConnections/ServiceConnectionSonarQubeEnterprise.json  
13 Az devops CLI working. ADO project [redacted] can be reached.  
14 Creating SQE API request.  
15 Calling SQE API with request: {  
16 "ContentType": "application/json",  
17 "Method": "POST",  
18 "Body": "{\n \"name\": \"[redacted]\", \n \"description\": \"SonarQube Enterprise application generat  
19 \"Headers\": {  
20 \"client\_secret\": \"\*\*\*\*\",  
21 \"client\_id\": [redacted]  
22 },  
23 \"Uri\": \"[redacted]443/api/[redacted]-sonarqube-papi/v1/applications\"  
24 }  
25 ##[warning] SonarQube Enterprise API message: The SonarQube Enterprise application with application key, [redacted] already exist  
26 SonarQube Enterprise API response.  
27 Response status code: 500  
28 Scriptname: /agent/\_work/1/s/Scripts/Create-ADOServiceConnectionSonarQubeEnterprise.ps1



# Create application system (project)

← Jobs in run #CHG1962180 S01-A...

✓ Create DRCP variabl... 16s

✓ Install internal root c... 2s

✓ Create SonarQube E... 3s

▶ Create Mule Applic... <1s

✓ Post-job: Checkout ... <1s

✓ Post-job: Checkout ... <1s

✓ Finalize Job <1s

✓ Reporting the pipeline... 10s

✓ Initialize job <1s

✓ Checkout DRCP@ma... 2s

✓ Report to ServiceNow 6s

✓ Post-job: Checkout ... <1s

✓ Finalize Job <1s

Finalize build

✓ Report build status <1s

✓ Report to ServiceNow

```
76     u_usage : development ,
77     "unverified": "false",
78     "metadata": {
79       "security": 0,
80       "operations": 0
81     },
82     "config_variables": {
83       "beta_resource_providers": [
84         ""
85       ],
86       "allowed_PEPL_Service_Connections": [
87         ""
88       ]
89     }
90   },
91   "buildId": "38380",
92   "changeNumber": "CHG1962180",
93   "pipelineStatus": "Succeeded"
94 }
95
96 Succeeded
97 result
98 -----
99 @{message=Event created for orchestration.waitFor.azure.38380 for change CHG19...
100
101
102 Finishing: Report to ServiceNow
```

# What to automate

Environment/subscription:

- Service Connection



# Create environment (Azure subscription)

Jobs in run #CHG1

Virtual network state 10s

Virtual network <1s

Entra ID groups 16s

Setting routing vers... <1s

Peeringstate Hub 9s

Peeringstate Spoke 8s

Peering Spoke to H... <1s

Peering Hub to Spo... <1s

Checkout Policy@hot... 1s

Policies 2m 43s

Setting Environment ... 9s

Delete global locatio... 8s

App registration 19s

ADO service connecti... 1s

Environment principa... 7s

App registration

View raw log

```
20 Directory: /usr/share/az_12.4.0
21
22 ModuleType Version PreRelease Name PSEdition
23 -----
24 Script 12.4.0 Az Core,Desk
25 Script 7.5.0 Az.Resources Core,Desk
26 Connecting to Microsoft Graph with modern token retrieval method (using Get-AzAccessToken).
27 WARNING: Upcoming breaking changes in the cmdlet 'Get-AzAccessToken' :
28 The Token property of the output type will be changed from String to SecureString. Add the [-AsSecureString] switch to avoid the in
29 - The change is expected to take effect in Az version : '14.0.0'
30 - The change is expected to take effect in Az Az.Accounts version : '4.0.0'
31 Note : Go to https://aka.ms/azps-changewarnings for steps to suppress this breaking change warning, and other information on break
32 Successfully connected to Microsoft Graph.
33 Skipped creation of app registration with displayname [REDACTED] because it already exists.
34 Skipped creation of service principal for app registration with displayname [REDACTED] it already exist
35 Removed secret with key id [REDACTED] from app registration [REDACTED]
36 Added secret with key id [REDACTED] to app registration [REDACTED]
37 Successfully created or processed app registration with displayname [REDACTED]
38
39
40 /usr/bin/pwsh -NoLogo -NoProfile -NonInteractive -ExecutionPolicy Unrestricted -Command . '/agent/_work/_tasks/AzurePowerShell_72a
41 Disconnect-AzAccount -Scope CurrentUser -ErrorAction Stop
42 Disconnect-AzAccount -Scope Process -ErrorAction Stop
43 Clear-AzContext -Scope Process -ErrorAction Stop
44
45 Finishing: App registration
```



# Create environment (Azure subscription)

← Jobs in run #CHG

✓	Virtual network state	10s
🔄	Virtual network	<1s
✓	Entra ID groups	16s
✓	Setting routing vers...	<1s
✓	Peeringstate Hub	9s
✓	Peeringstate Spoke	8s
🔄	Peering Spoke to H...	<1s
🔄	Peering Hub to Spo...	<1s
✓	Checkout Policy@hot...	1s
✓	Policies	2m 43s
✓	Setting Environment ...	9s
✓	Delete global locatio...	8s
✓	App registration	19s
✓	ADO service connecti...	1s
✓	Environment principa...	7s

✓ ADO service connection

View raw log

```
12 Loading FilePath: /agent/_work/1/s/Ado/ServiceConnections/ServiceConnectionAzureRM.json.
13 Updating service connection
14 Updated service connection.
15 Loading FilePath: /agent/_work/1/s/Ado/ServiceConnections/Checks/ExtendsDefinition.json.
16
17 settings : @({extendsChecks=System.Object[]})
18 createdBy :
19
20 iptor=aad.0WZmNGM1NWEtZjBjMy03MzcxLTk5YzItMmZjMzc3NmM2OWU4}
21 createdOn : 06/06/2023 09:51:56
22 modifiedBy : @({displayName:
23 c69e8;
24 iptor=a
25 modifiedOn : 12/16/2024 11:07:37
26 timeout : 43200
27 _links : @({self=})
28 id : 84
29 version : 1
30 type : @({id=4020e66e-b0f3-47e1-bc88-48f3cc59b5f3; name=ExtendsCheck})
31 url :
32 2565d98a/_apis/pipelines/checks/configurations/84
33 resource : @({type=endpoint; id=2d4ed90d-0dbf-4837-8d2d-b17d2de690ae; name=SC-
34
35
36 Extends template updated on service connection.
37 Successfully handled service connection in project for service principal
38
39 Finishing: ADO service connection
```

# DevOps team experience

# DevOps team experience

Onboarding team supports the teams in their maturity and shares templates

- Policies (Demo)
- Identities (Demo)
- Integrations (Demo)
- Service Connection (Demo)
  - Approval
  - Branch evaluation
  - Extends template





# Key take-aways

1. Understanding how to translate company policies to Azure DevOps policies is crucial for compliancy and security automation.
2. Integrating with central managed security and compliance systems helps with a secure and compliant Azure DevOps platform.
3. Streamlined processes enhance compliance and efficiency for DevOps teams.



# Questions?



# Thanks!

Lange Dreef 11-F  
4131 NJ Vianen  
Nederland  
T: 088 55 55 800