

Microsoft 365 Infrastructure-as-Code

@thomasvochten

About me



Thomas Vochten

Technology Evangelist     
#Microsoft365 #Azure #CommunityRocks

@thomasvochten

<https://thomasvochten.com>

mail@thomasvochten.com



Microsoft®
Most Valuable
Professional

BIWUG



Managing Microsoft 365

- Admin Center
- PowerShell



It's your responsibility to know

- Where to go
- How to do it



Two approaches

Imperative

- Procedural
- Describes the How
- You describe the order of commands

Declarative

- Functional
- Describes the What
- You describe the desired outcome

Two approaches

Imperative

```
Set-SPOTenant -OneDriveStorageQuota 1048576
```

Declarative

```
ODSettings "ODSettings"  
{  
    ... OneDriveStorageQuota = 1048576;  
}
```

Benefits of a declarative approach



- Repeatability
- Consistency
- Efficiency
- Testability
- Stability

Buzzword bingo



ARM



Bicep



Terraform

- Infrastructure-as-Code
- Configuration-as-Code

Extend your toolbox: Source Control

- Version history
- Collaboration
- Branches
- Releases
- Automation



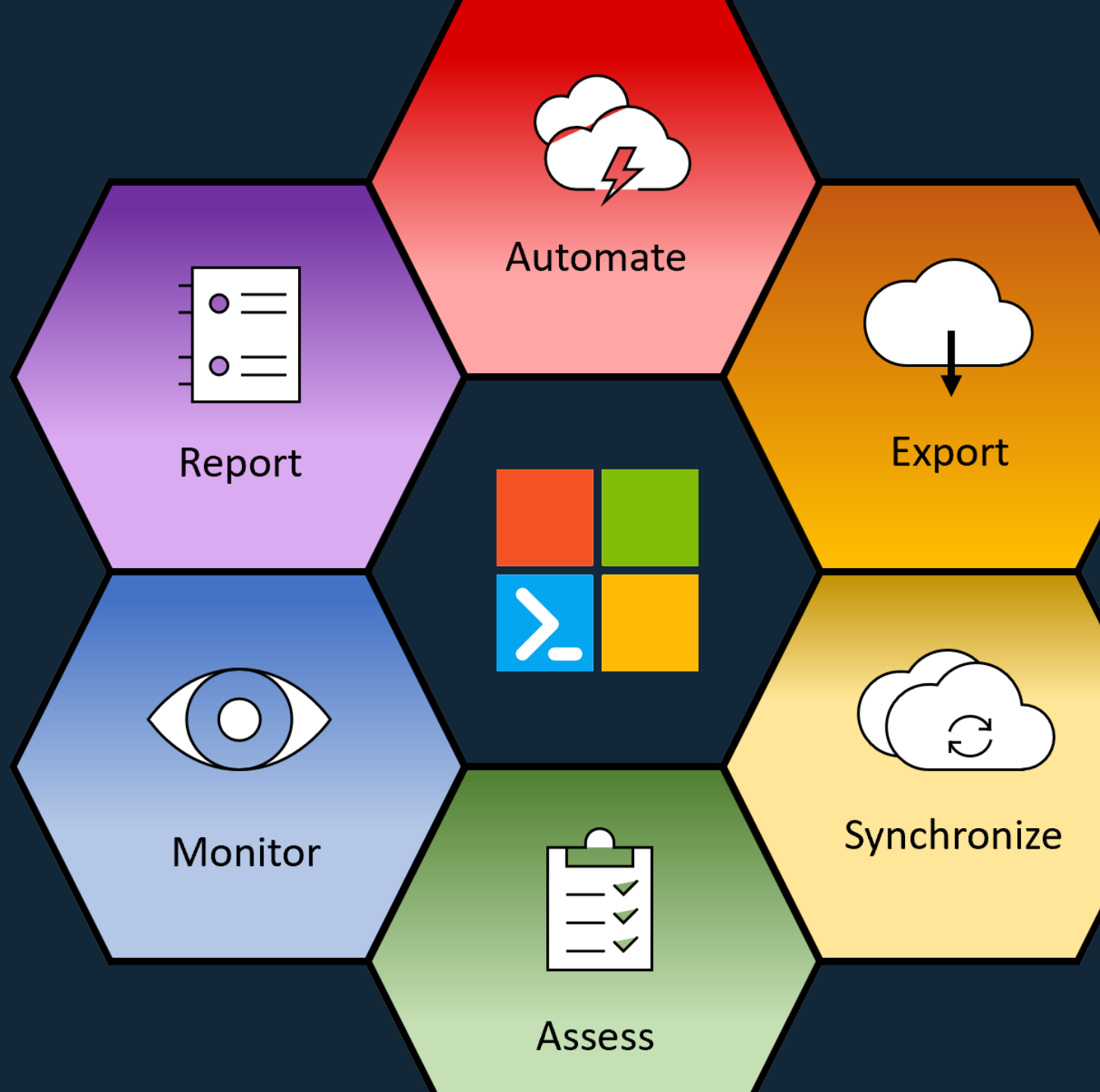
What about Microsoft 365?

- Not built with Configuration-as-Code in mind
- Community or third-party solutions needed
- Always at the mercy of Microsoft API's
- Limited to Configuration-as-Code



Microsoft 365 DSC

- Open source
- PowerShell module



Desired State Configuration?

- PowerShell-based
- The “make it so” engine
- Simple & scalable
- Build + Push or Pull (MOF files)

```
FirewallRule Rule1
{
    Name = "Rule1"
    Port = 80;
    Direction = "Inbound"
}
FirewallRule Rule2
{
    Name = "Rule2"
    Port = 90;
    Direction = "Inbound"
}
```

Automate / Apply

Start-DSCConfiguration

```
ODSettings "ODSettings"  
{  
    . . . . OneDriveStorageQuota = 1048576;  
}
```

Example of repeatable configurations

Conditional Access baseline rules to be applied across tenants:

- CA Groups
- CA Policies using those groups



AADConditionalAccessPolicy bf8ea9dd-154c-4fec-87a0-183bfe577248

```
{
  ApplicationEnforcedRestrictionsIsEnabled = $False;
  BuiltInControls = @"mfa","compliantDevice";
  ClientAppTypes = @"all";
  CloudAppSecurityIsEnabled = $False;
  CloudAppSecurityType = "";
  Credential = $Credscredential;
  DisplayName = "CA100-Admins-BaseProtection-AllApps-AnyPlatform-CompliantorAADHJ";
  Ensure = "Present";
  ExcludeApplications = @"d4ebce55-015a-49b5-a083-c84d1797ae8c";
  ExcludeDevices = @();
  ExcludeGroups = @"CA-BreakGlassAccounts","CA-Persona-Admins-BaseProtection-Exclusions","CA-Persona-Microsoft365ServiceAccounts","CA-
  ExcludeLocations = @();
  ExcludePlatforms = @();
  ExcludeRoles = @();
  ExcludeUsers = @();
  GrantControlOperator = "OR";
  Id = "99b56601-10cc-4706-8b5b-3479ef3b0f4f";
  IncludeApplications = @"All";
  IncludeDevices = @();
  IncludeGroups = @"CA-Persona-Admins";
  IncludeLocations = @();
  IncludePlatforms = @"all";
  IncludeRoles = @();
  IncludeUserActions = @();
  IncludeUsers = @();
  PersistentBrowserIsEnabled = $False;
  PersistentBrowserMode = "";
  SignInFrequencyIsEnabled = $False;
  SignInFrequencyType = "";
  SignInRiskLevels = @();
  State = "disabled";
  UserRiskLevels = @();
}
```



Export-M365DSCConfiguration -LaunchWebUI

Microsoft365DSC | Configuration-as-Code for the Cloud Generate

Home

- Azure AD
- Exchange
- Intune
- Office 365
- OneDrive
- Planner
- Power Platform
- Security & Compliance
- SharePoint
- Teams

Selection mode: Default


Authentication: Credentials

Azure AD 31 selected

<input checked="" type="checkbox"/> AADAdministrativeUnit	<input checked="" type="checkbox"/> AADApplication	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicy	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicyAuthenticator
<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicyEmail	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicyFido2	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicySms	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicySoftware
<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicyTemporary	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicyVoice	<input checked="" type="checkbox"/> AADAAuthenticationMethodPolicyX509	<input checked="" type="checkbox"/> AADAAuthenticationStrengthPolicy
<input checked="" type="checkbox"/> AADAuthorizationPolicy	<input checked="" type="checkbox"/> AADConditionalAccessPolicy	<input checked="" type="checkbox"/> AADCrossTenantAccessPolicy	<input checked="" type="checkbox"/> AADCrossTenantAccessPolicyConfigurationDefault

Export

ation-as-Code for the Cloud

 **Intune**

☐ IntuneAntivirusPo
Catalog

☐ IntuneAppProtect

☒ IntuneDeviceCate

Export

```
1 # Generated by Microsoft365DSC from https://export.microsoft365dsc.com on 19/5/2023, 14:35:49
2 # Visit https://microsoft365dsc.com for more information
3
4 # Getting client credential
5 $Credential = Get-Credential
6
7 # Exporting resources using credentials
8 Export-M365DSCConfiguration -Components @("IntuneDeviceCategory") -Credential $Credential
```

Export

```
Administrator: PowerShell
Connecting to {SecurityComplianceCenter}...✓
[1/217] Extracting [AADAdministrativeUnit] using {Credentials}...✓
[2/217] Extracting [AADApplication] using {Credentials}...
|---[1/6] EXO_App2✓
|---[2/6] Salesforce✓
|---[3/6] LinkedIn✓
|---[4/6] Microsoft365DSC✓
|---[5/6] Box✓
|---[6/6] BrowserStack✓
[3/217] Extracting [AADAuthorizationPolicy] using {Credentials}...
|---[1/1] Authorization Policy✓
[4/217] Extracting [AADConditionalAccessPolicy] using {Credentials}...
|---[1/2] Exchange Online Requires Compliant Device✓
|---[2/2] Office 365 App Control✓
[5/217] Extracting [AADEntitlementManagementAccessPackage] using {Credentials}...
|---[1/1] Sales and Marketing✓
[6/217] Extracting [AADEntitlementManagementAccessPackageAssignmentPolicy] using {Credentials}...✓
[7/217] Extracting [AADEntitlementManagementAccessPackageCatalog] using {Credentials}...
|---[1/1] General✓
[8/217] Extracting [AADEntitlementManagementAccessPackageCatalogResource] using {Credentials}...
|---[1/1] General
|---[1/1] sg-Sales and Marketing✓
[9/217] Extracting [AADEntitlementManagementConnectedOrganization] using {Credentials}...✓
[10/217] Extracting [AADGroupLifecyclePolicy] using {Credentials}...✓
[11/217] Extracting [AADGroupsNamingPolicy] using {Credentials}...✓
[12/217] Extracting [AADGroupsSettings] using {Credentials}...✓
[13/217] Extracting [AADNamedLocationPolicy] using {Credentials}...✓
[14/217] Extracting [AADRoleDefinition] using {Credentials}...
|---[1/101] Global Administrator✓
|---[2/101] Guest User✓
```

Export



@thomasvochten

```
> TeamsMessagingPolicy·ebef2ec9-f207-4a9d-b98b-37965c3dc6fd
{
  ····AllowGiphy·····=$False;
  ····AllowImmersiveReader·····=$True;
  ····AllowMemes·····=$True;
  ····AllowOwnerDeleteMessage·····=$False;
  ····AllowPriorityMessages·····=$True;
  ····AllowRemoveUser·····=$True;
  ····AllowStickers·····=$True;
  ····AllowUrlPreviews·····=$True;
  ····AllowUserChat·····=$True;
  ····AllowUserDeleteMessage·····=$True;
  ····AllowUserEditMessage·····=$True;
  ····AllowUserTranslation·····=$True;
  ····AudioMessageEnabledType·····="ChatsAndChannels";
  ····ChannelsInChatListEnabledType·····="DisabledUserOverride"
  ····Credential·····=$Credscredential;
  ····Ensure·····="Present";
  ····GiphyRatingType·····="Strict";
  ····Identity·····="EduStudent";
  ····ReadReceiptsEnabledType·····="UserPreference";
}
> TeamsMobilityPolicy·575d6b1f-93c7-46da-b745-814c70d6c96f
{
  ····Credential·····=$Credscredential;
  ····Ensure·····="Present";
  ····Identity·····="Global";
  ····IPAudioMobileMode·····="AllNetworks";
  ····IPVideoMobileMode·····="AllNetworks";
  ····MobileDialerPreference·····="Teams";
}
> TeamsMobilityPolicy·f70c61b2-4787-4901-b0e9-c065d1359428
{
```

Report

New-M365DSCReportFromConfiguration



Tenant



Report

Synchronize

Export-M365DSCConfiguration
Start-DSCConfiguration



Tenant A



Tenant B

Assess / Assert

Assert-M365DSCBlueprint



Tenant



Blueprint



Report

Assess / Assert




Microsoft365DSC

Configuration-as-Code for the Cloud

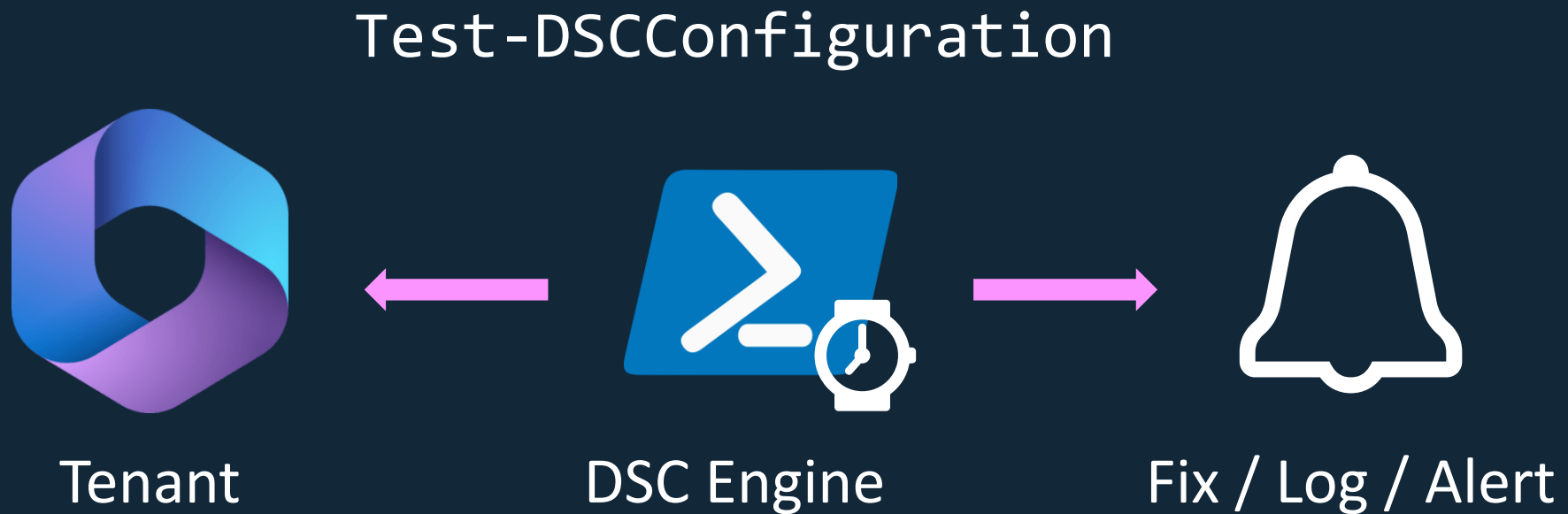
Delta Report

Comparing C:\Users\nicharl\AppData\Local\Temp\55abac50-9bdb-4e81-b42c-724ae765bdea.ps1 to C:\Users\nicharl\AppData\Local\Temp\bed99890-bc4f-43e3-9690-f17262040213.M365

Resources that are Configured Differently

 Teams	TeamsMeetingPolicy - Identity = Global		
	Property	Source Value	Destination Value
	We don't recommend you allowing external Participant to give request control because that exposes your organization to threats.		
	AllowExternalParticipantGiveRequestControl	\$False	\$True
	We recommending allowing your recordings to be saved to the cloud. Set this value to true .		
	AllowCloudRecording	\$True	\$False
	TeamsMessagingPolicy - Identity = Global		

Monitor



Monitor

Three configuration modes:

- ApplyOnly
- ApplyAndMonitor
- ApplyAndAutoCorrect

The Challenge: Configuration Drift

- Uncontrolled changes
- Unclear processes

Authentication & Authorization

- AAD Service Principals are preferred
- Regular credentials also work
- Does not support MFA

Workload	PowerShell Module	Credential	Service Principal			Managed Identity
			Certificate Thumbprint	Certificate Path	Application Secret	
AzureAD*	Microsoft.Graph.Authentication (Connect-MgGraph)	✓	✓	✗	✓	✓
Exchange Online	ExchangeOnlineManagement (Connect-ExchangeOnline)	✓	✓	✓	✗	✓
Intune*	Microsoft.Graph.Authentication (Connect-MgGraph)	✓	✓	✗	✓	✓
Office 365*	Microsoft.Graph.Authentication (Connect-MgGraph)	✓	✓	✗	✓	✓
OneDrive	PnP.PowerShell (Connect-PnPOnline)	✓	✓	✓	✓	✓
Power Apps	Microsoft.PowerApps.Administration.PowerShell	✓	✓	✗	✓	✗
Planner*	Microsoft.Graph.Authentication (Connect-MgGraph)	✓	✓	✗	✓	✓
Security & Compliance Center	ExchangeOnlineManagement (Connect-IPPSession)	✓	✓	✓	✗	✗
SharePoint Online	PnP.PowerShell (Connect-PnPOnline)	✓	✓	✓	✓	✓
Teams	MicrosoftTeams (Connect-MicrosoftTeams)	✓	✓	✗	✗	✗

Installation & Prerequisites

`Install-Module Microsoft365DSC`

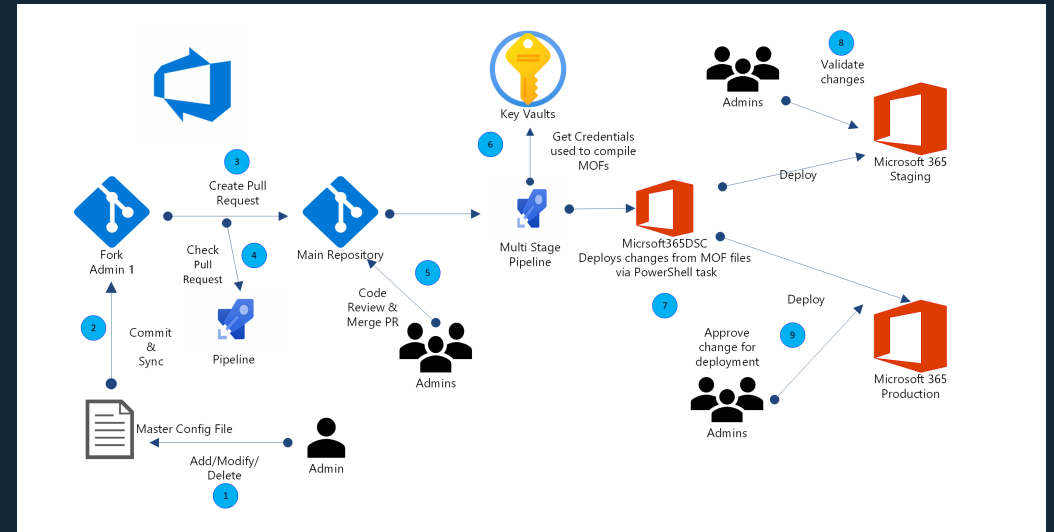
`Update-M365DSCDependencies`

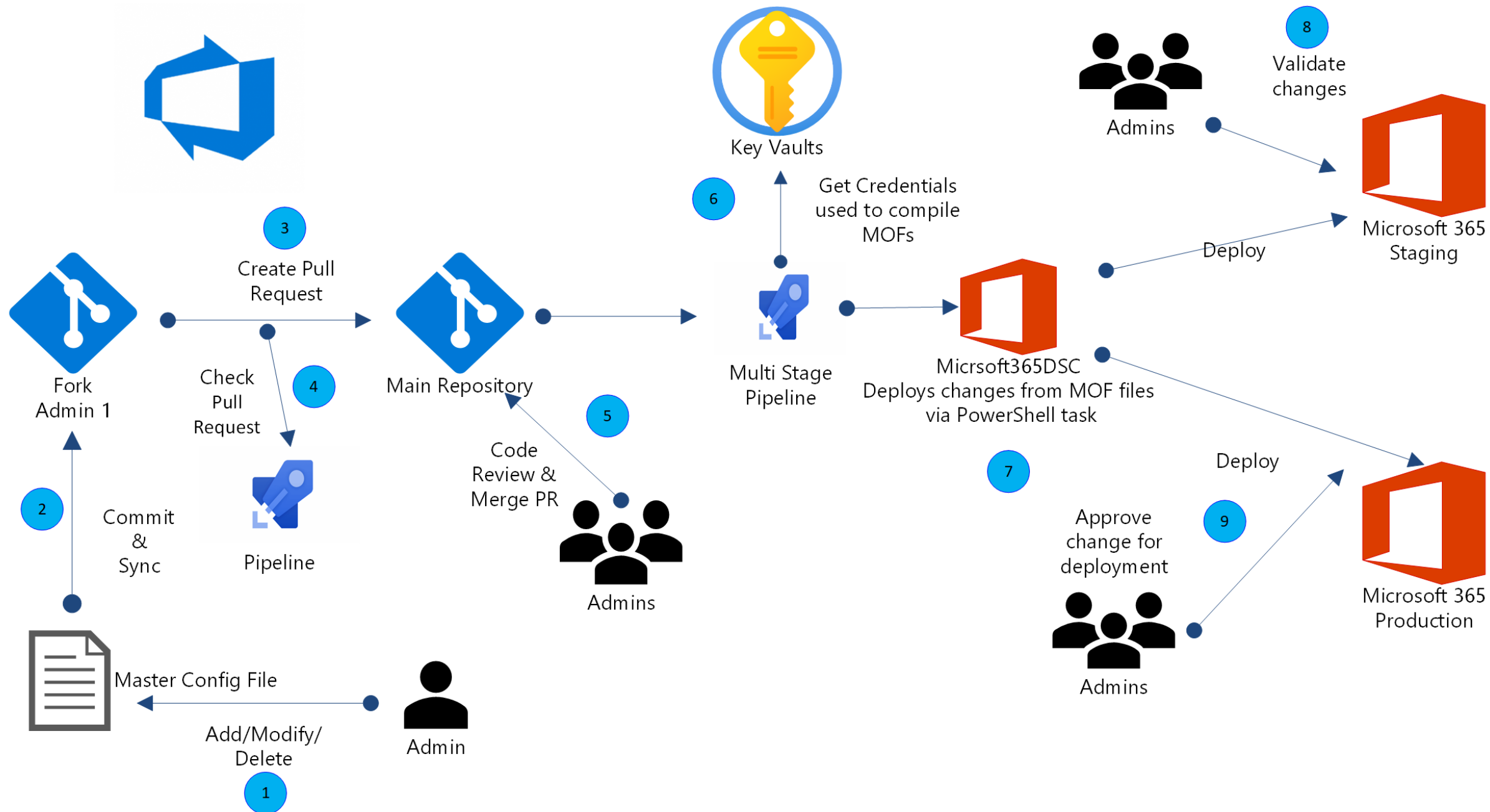
The holy grail: Automation

- Consistency is key
- Controllable process (approvals & quality gates)
- More deliberate change management
- Helps with configuration drift

Using Azure DevOps to manage your M365 config

- Maintain your config in git
- Create a Pull Request to integrate your changes
- Config gets deployed to one or more tenants





Settings

The screenshot shows a PowerShell DSC configuration editor with a file explorer on the left and a code editor on the right. The file explorer shows the path: M365-IaC > M365Config > 0.0.1 > DscResources > Teams > Teams.schema.psm1. The code editor displays the content of Teams.schema.psm1, which defines a TeamsClientConfiguration and a TeamsEmergencyCallingPolicy. A yellow box highlights the TeamsClientConfiguration block.

File Explorer Path: M365-IaC > M365Config > 0.0.1 > DscResources > Teams > Teams.schema.psm1

Teams.schema.psm1 Content:

```
29  
30 TeamsClientConfiguration 'ClientConfiguration_Global'  
31 {  
32     Identity           = "Global"  
33     AllowBox           = $False  
34     AllowDropBox       = $False  
35     AllowEgnyte        = $False  
36     AllowEmailIntoChannel = $True  
37     AllowGoogleDrive    = $False  
38     AllowGuestUser      = $True  
39     AllowOrganizationTab = $True  
40     AllowResourceAccountSendMessage = $True  
41     AllowScopedPeopleSearchandAccess = $False  
42     AllowShareFile      = $False  
43     AllowSkypeBusinessInterop = $True  
44     ContentPin          = "RequiredOutsideScheduleMeeting"  
45     ResourceAccountContentAccess = "NoAccess"  
46     Credential          = $Credential  
47 }  
48  
49 #region Emergency Policies  
50 TeamsEmergencyCallingPolicy 'EmergencyCallingPolicy_Global'  
51 {  
52     Identity = "Global"  
53     Ensure   = "Present"  
54     Credential = $Credential  
55 }
```


Configuration

PowerShell to configure

- Environments/tenants
- Pipeline execution scripts
- Configuration scripts

@thomasvochten

The screenshot displays a PowerShell DSC configuration environment. On the left, a file explorer shows the project structure for 'M365-IaC'. The 'Datafiles' folder is expanded, showing 'Production.psd1' (highlighted with a yellow box). Below it, the 'M365Config' folder is expanded, showing 'build.ps1', 'checkdsccompliance.ps1', and 'deploy.ps1' (all highlighted with yellow boxes). Other files in the project include '.gitattributes', '.gitignore', 'DSCCertificate.cer', 'DscResources.psd1', 'M365Configuration.ps1' (highlighted with a yellow box), and 'ReadMe.md'.

On the right, the 'Production.psd1' file is open, showing its contents. The file is a PowerShell script that defines the configuration for the 'Production' environment. It includes settings for 'AllNodes', 'NonNodeData', 'Environment', 'Accounts', and 'Workload'.

```
1 @{
2     AllNodes = @(
3         @{
4             NodeName = 'localhost'
5             CertificateFile = '.\DSCCertificate.cer'
6             PsDscAllowPlainTextPassword = $true
7             PsDscAllowDomainUser = $true
8         }
9     )
10    NonNodeData = @{
11        Environment = @{
12            Name = 'Production'
13            ShortName = 'PRD'
14            TenantId = 'M365x48213529.onmicrosoft.com'
15            OrganizationName = 'M365x48213529.onmicrosoft.com'
16        }
17        Accounts = @(
18            @{
19                Workload = 'Exchange'
20                Account = 'DscAdmin@M365x48213529.onmicrosoft.com'
21            }
22            @{
23                Workload = 'Office365'
24                Account = 'DscAdmin@M365x48213529.onmicrosoft.com'
25            }
26            @{
27                Workload = 'PowerPlatform'
28                Account = 'DscAdmin@M365x48213529.onmicrosoft.com'
29            }
30            @{
31                Workload = 'SecurityCompliance'
32                Account = 'DscAdmin@M365x48213529.onmicrosoft.com'
33            }
34            @{
35                Workload = 'SharePoint'
36                Account = 'DscAdmin@M365x48213529.onmicrosoft.com'
37            }
38        )
39    }
```

Applying

Before

Apps that don't use modern authentication

Some third-party apps and previous versions of Office can't enforce device-based restrictions. Use this setting to block all access from these apps.

☒ Allow access

☐ Block access

Save

Cancel

Applying

No legacy auth for SharePoint please

f7590b10 Thomas Vochten committed Just now main in progress

Files Details

Parent 1 → This commit Filter 1 changed file

M365-IaC

M365Config/0.0.1/DscResources/Sh...

SharePoint.schema.psm1

SharePoint.schema.psm1 -1+1

/M365Config/0.0.1/DscResources/SharePoint/SharePoint.schema.psm1

```
.....
34 34      ConditionalAccessPolicy                = "AllowFullAccess"
35 35      FilePickerExternalImageSearchEnabled    = $true
36 36      HideDefaultThemes                      = $false
37 37      - LegacyAuthProtocolsEnabled            = $true
38 37      + LegacyAuthProtocolsEnabled            = $false
39 38      MarkNewFilesSensitiveByDefault          = "AllowExternalSharing"
40 39      MaxCompatibilityLevel                  = 15
40 40      MinCompatibilityLevel                   = 15
.....
```



Applying

Change has been detected and build pipeline starts

Pipelines

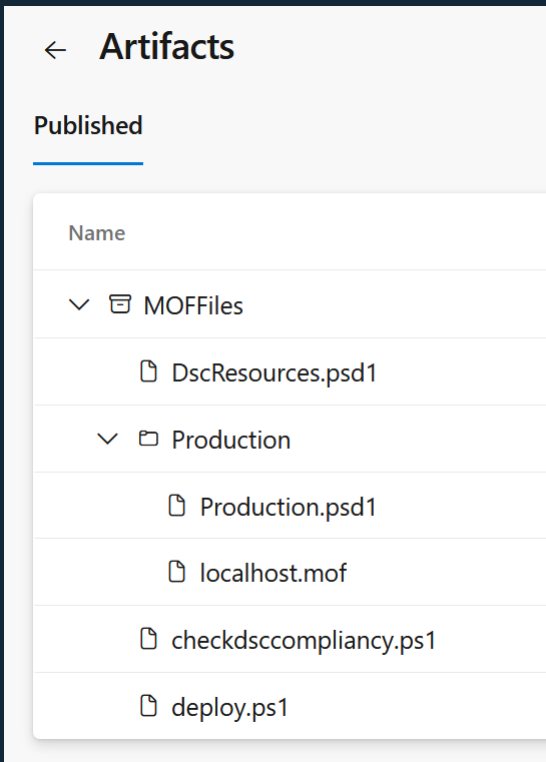
Recent All Runs

Recently run pipelines

Pipeline	Last run
 M365-IaC	#20230520.1 • No legacy auth for SharePoint please 🔗 Individual CI for  main

Applying

Build generates the DSC MOF files



Applying

Release pipeline kicks off and applies the change

The screenshot displays the 'Release-7' configuration page in Azure DevOps. The 'Pipeline' tab is active, showing a 'Continuous deployment' for 'Thomas Vochten' initiated on 20/5/2023 at 09:22. The pipeline includes an artifact named '_M365-lac' with version '20230520.1' from the 'main' branch. A 'Deploy Configuration' box indicates the deployment 'Succeeded' on 20/5/2023 at 09:25. The interface also features tabs for 'Variables' and 'History', and buttons for 'Deploy', 'Cancel', 'Refresh', and 'Edit'.

@thomasvochten

Applying

After

Apps that don't use modern authentication ×

Some third-party apps and previous versions of Office can't enforce device-based restrictions. Use this setting to block all access from these apps.

☐ Allow access

☒ Block access

Save Cancel

Auditing

Wait a minute...

Apps that don't use modern authentication

Some third-party apps and previous versions of Office can't enforce device-based restrictions. Use this setting to block all access from these apps.

☒ Allow access

☐ Block access

Save

Cancel

Auditing

Compliance job is running (scheduled)

The screenshot displays the Azure DevOps interface for a release named 'Test DSC Compliance' under the 'Release-7' branch. The interface is divided into two main sections: 'Release' and 'Stages'.

Release Section:

- Manually triggered:** Indicated by a blue icon and text.
- by:** Thomas Vochten (profile icon).
- 20/5/2023, 09:29:** The time the release was triggered.
- Artifacts:** A section showing the artifacts generated by the release.
- _M365-IaC_20230520.1:** The name of the artifact, with a download icon and a link to the artifact.
- main:** The branch name.

Stages Section:

- Test Compliance:** The name of the stage.
- In progress:** Indicated by a blue circle and text.
- 2/3 tasks:** A progress indicator showing that 2 out of 3 tasks are completed.
- Download artifact -:** The name of the task.
- 00:01:** The duration of the task.

@thomasvochten

Auditing



Microsoft365DSC 9:31 AM

DSC Compliance Report (2023-05-20)



Check(s) failed!

Generated at: Sat 20-05-2023 07:31

Number of noncompliant environments: 1


Details

Environment	In Desired State	Error Count	Details
-------------	------------------	-------------	---------

Production	False	1	[SPOTenantSettings]TenantSettings::[SharePoint]SharePoint_Configuration
------------	-------	---	---


↩ Reply

Auditing



Microsoft365DSC 10:01 AM

DSC Compliance Report (2023-05-20)



All checks passed!
Generated at: Sat 20-05-2023 08:01
Number of noncompliant environments: 0

Details

Environment	In Desired State	Error Count	Details
Production	True	0	-

↩ Reply

Solution Components

- Git repository
- Azure KeyVault
- Azure DevOps Build & Release Pipelines
- Azure DevOps (Self) Hosted Agents
- PowerShell
- Microsoft 365 DSC

But... why?

- Enforce governance policies & avoiding configuration drift
- When you need strict change management
- If you want to maintain the same baseline across tenants
- Development / Test / Acceptance / Production
- ...

Key takeaways & advice

- Just because you can, doesn't mean you should
- Get familiar with PowerShell DSC if you aren't already
- Testing is key. Be careful with (auto)applying changes
- Using proper source control is a must
- Automation is cool, but optional (and complicated)

Key resources

- <https://microsoft365dsc.com>
- <https://github.com/microsoft/microsoft365DSC>
- <https://microsoft365dsc.com/about/community-resources>
- <https://github.com/microsoft/ConditionalAccessforZeroTrustResources>

Thank you

@thomasvochten

<https://thomasvochten.com>

mail@thomasvochten.com

Get the slides

