METSYS

Comment garder la configuration de votre tenant M365 au carré avec DSC et Maester ?

Qui suis-je ?

Léo BOUARD

- Ingénieur systèmes chez METSYS depuis 7 ans
- www.labouabouate.fr
- 14 titres de MVP partagés entre Laurent, Yoann et moi

METSYS

Disclaimer

- J'ai pas eu le mémo sur la ligne édito
- J'ai menti sur le nom de la présentation

METSYS

Comment garder la configuration de votre tenant M365 au carré avec ~~*DSC et Maester*~~ UTCM ?

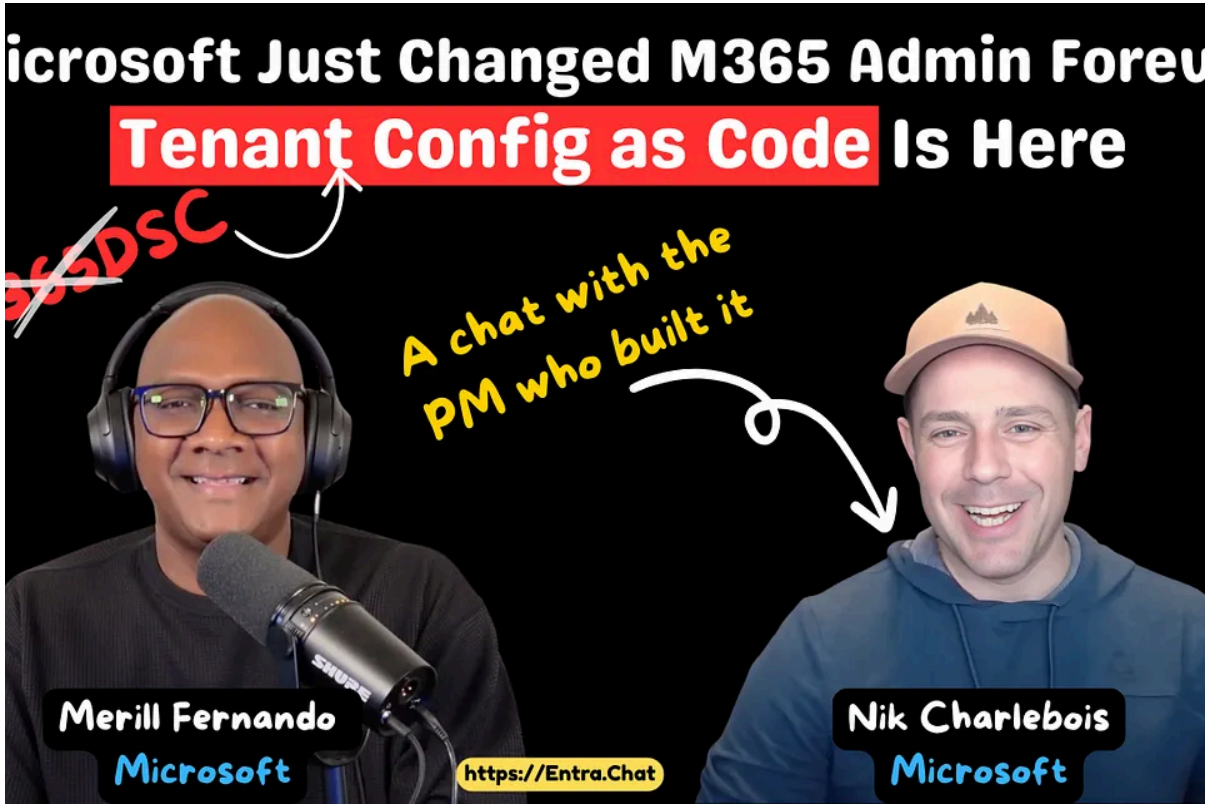
METSYS

UTCM c'est quoi ?

- Universal Tenant Configuration Management
- Projet officiel de Microsoft, en succession de M365DSC
- Public Preview depuis janvier 2026
- La pierre angulaire d'un nouveau module de M365

METSYS

Source principale



Historique

METSYS

M365DSC

Module PowerShell open-source créé en 2018 par Nik Charlebois (PFE Microsoft et MVP) pour répliquer des configurations clients à distance.

S'appuie sur la technologie DSC (*Desired State Configuration*) et les APIs des différents produits

METSYS

Les limites de M365DSC

- Projet mené par Microsoft, mais supporté par la communauté donc en "best effort"
- Peu de contributeurs et beaucoup de travail de maintenance

METSYS

Vous êtes une licorne ! 

METSYS

Début du projet UTCM

2024 : début du projet UTCM côté Microsoft avec pour objectif :

- Répliquer les fonctionnalités de M365DSC
- Offrir un support client
- Suivre plus facilement des évolution de M365
- Plus simple d'utilisation

METSYS

Fonctionnalités prises en charge

M365DSC pouvait gérer la configuration de nombreux produits comme Microsoft 365. Pour UTCM, dans la public preview sortie en janvier 2026, n'est supporté pour le moment uniquement :

- Defender (limited coverage)
- Entra ID
- Exchange Online
- Intune
- Purview
- Teams

METSYS

Périmètre d'action

UTCM ne gère que la partie configuration, donc pas de sauvegarde de données sauf si celles-ci sont directement liées à la configuration du tenant.

Disponible à partir de Entra ID P1

METSYS

Mise en place de UTCM

Création de l'application

Avec les modules PowerShell Microsoft Graph :

```
Install-Module Microsoft.Graph.Authentication, Microsoft.Graph.Applications
Connect-MgGraph -Scopes @('Application.ReadWrite.All', 'AppRoleAssignment.ReadWrite.All')
New-MgServicePrincipal -AppId '03b07b79-c5bc-4b5e-9bfa-13acf4a99998'
```

METSYS

Ajout de permissions

Code PowerShell :

```powershell
$permissions = 'User.ReadWrite.All', 'Group.ReadWrite.All', 'Directory.Read.All', 'Policy.ReadWrite.ConditionalAccess'
$Graph = Get-MgServicePrincipal -Filter "AppId eq '00000003-0000-0000-c000-000000000000'"
$TCM = Get-MgServicePrincipal -Filter "AppId eq '03b07b79-c5bc-4b5e-9bfa-13acf4a99998'"

foreach ($requestedPermission in $permissions) {
    $AppRole = $Graph.AppRoles | Where-Object { $_.Value -eq $requestedPermission }
    $body = @{
        AppRoleId = $AppRole.Id
        ResourceId = $Graph.Id
        PrincipalId = $TCM.Id
    }
    New-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $TCM.Id -BodyParameter $body
}
```

Mais beaucoup plus simple depuis l'interface graphique : Gouvernance des locataires - Centre d’administration Microsoft Entra

METSYS

Les ressources vont vous permettre de cibler la configuration à sauvegarder/auditer.

Quelques exemples :

- `deviceCleanupRule` pour obtenir le paramétrage du nettoyage automatique des périphériques dans Intune
- `transportRule` pour les règles de flux dans Exchange
- `conditionalaccesspolicy` pour les stratégies d'accès conditionnels

METSYS

Utilisation de UTCM

Méthodologie :

1. **Faire un snapshot**
2. Créer une baseline à partir du snapshot
3. Créer un monitor à partir de la baseline
4. Surveiller vos dérives de configuration

METSYS

Création d'un snapshot

Instantané de votre configuration actuelle, sur les ressources ciblées (ici les accès conditionnels) :

```
$uri = '/beta/admin/configurationManagement/configurationSnapshots/createSnapshot'
$body = @"
{
    "displayName": "Snapshot CA $(Get-Date -Format 'yyyyMMddHHmmss')",
    "resources": ["microsoft.entra.conditionalaccesspolicy"]
}
"@
$responsePOST = Invoke-MgGraphRequest -Method POST -Uri $uri -Body $body
```

METSYS

Suivre l'avancement du snapshot

```
$uri = "/beta/admin/configurationManagement/configurationSnapshotJobs/$($responsePOST.id)"
$responseGET = Invoke-MgGraphRequest -Method "GET" -Uri $uri
```

Exemple de retour :

Name	Value
status	succeeded
id	fc7e6096-e324-469e-aba9-ab00aac45b2b
displayName	Snapshot CA 20260331115104
resources	{microsoft.entra.conditionalaccesspolicy}

METSYS

Télécharger le snapshot

Une fois que le snapshot est terminé :

```
$splat = @{
    Method = 'GET'
    Uri = $responseGET.resourceLocation
    OutputFilePath = "C:\temp\snapshot_$(Get-Date -Format 'yyyy-MM-dd_HHmmss').json"
}
Invoke-MgGraphRequest @splat
```

On télécharge le fichier JSON pour pouvoir le transformer en baseline.

Utilisation - Création d'un snapshot

METSYS


```
{
  "displayName": "AADConditionalAccessPolicy-Multifactor authentication for Microsoft partners and vendors",
  "resourceType": "microsoft.entra.conditionalaccesspolicy",
  "properties": {
    "ApplicationEnforcedRestrictionsIsEnabled": false,
    "SecureSignInSessionIsEnabled": false,
    "Ensure": "Present",
    "SignInFrequencyIsEnabled": false,
    "GrantControlOperator": "OR",
    "CloudAppSecurityIsEnabled": false,
    "Id": "00565114-097a-4357-854b-e3687a4d74ef",
    "PersistentBrowserIsEnabled": false,
    "DisplayName": "Multifactor authentication for Microsoft partners and vendors",
    "State": "enabled",
    "IncludeApplications": [ "All" ],
    "IncludeUsers": [ "All" ],
    "ExcludeRoles": [ "Directory Synchronization Accounts" ],
    "ClientAppTypes": [ "all" ],
    "BuiltInControls": [ "mfa" ],
    "ExcludeUsers": [ "admin@M365x32408877.onmicrosoft.com" ]
  }
}
```

METSYS

Utilisation de UTCM

Méthodologie :

1. Faire un snapshot
2. **Créer une baseline à partir du snapshot**
3. Créer un monitor à partir de la baseline
4. Surveiller vos dérives de configuration

Qu'est-ce qu'une baseline ?

La baseline va représenter la configuration souhaitée de votre tenant, c'est-à-dire l'état de référence. Toutes les différences entre la baseline et l'état actuel seront soulignés.

Vous ne pouvez pas utiliser votre snapshot directement comme baseline, il y a une légère adaptation à faire.

METSYS

Format d'une baseline

Voici la structure attendue :

```
{
  "displayName": "Le nom de votre baseline",
  "baseline": {
    "displayName": "Le nom de votre snapshot",
    "resources": [ { ... } ]
  }
}
```

METSYS

Utilisation de UTCM

Méthodologie :

1. Faire un snapshot
2. Créer une baseline à partir du snapshot
3. **Créer un monitor à partir de la baseline**
4. Surveiller vos dérives de configuration

Qu'est-ce qu'un monitor ?

Evaluation de la configuration du tenant par rapport à la baseline pour souligner les différences ou la conformité.

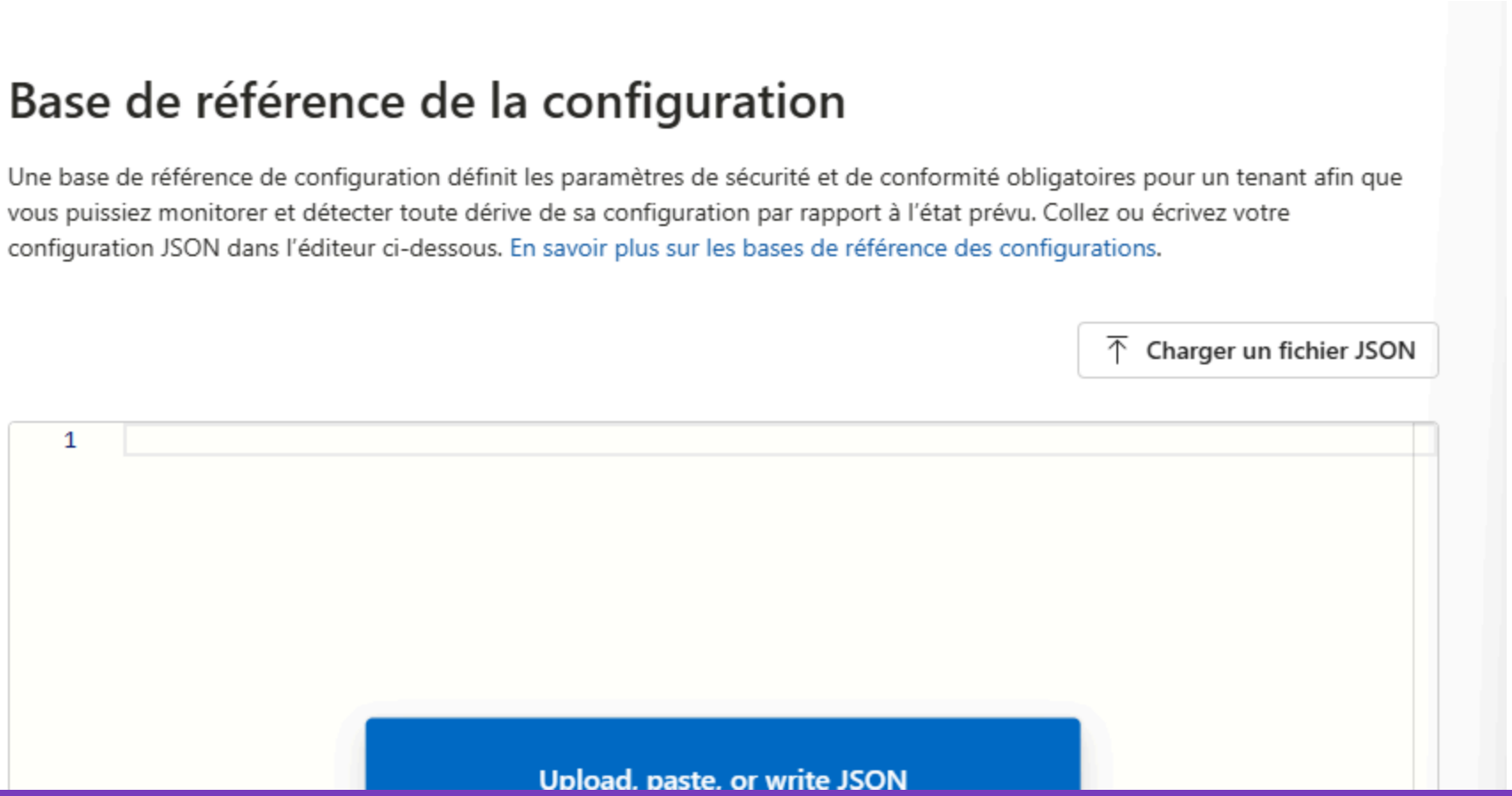
Passage toutes les 6 heures pour le moment

Possibilité d'auditer jusqu'à 800 objets par jour

METSYS

Création d'un monitor

Possible de le faire en PowerShell / Graph API, mais beaucoup plus simple en interface graphique :



METSYS

Utilisation de UTCM

Méthodologie :

1. Faire un snapshot
2. Créer une baseline à partir du snapshot
3. Créer un monitor à partir de la baseline
4. **Surveiller vos dérives de configuration**

Dérives de configuration

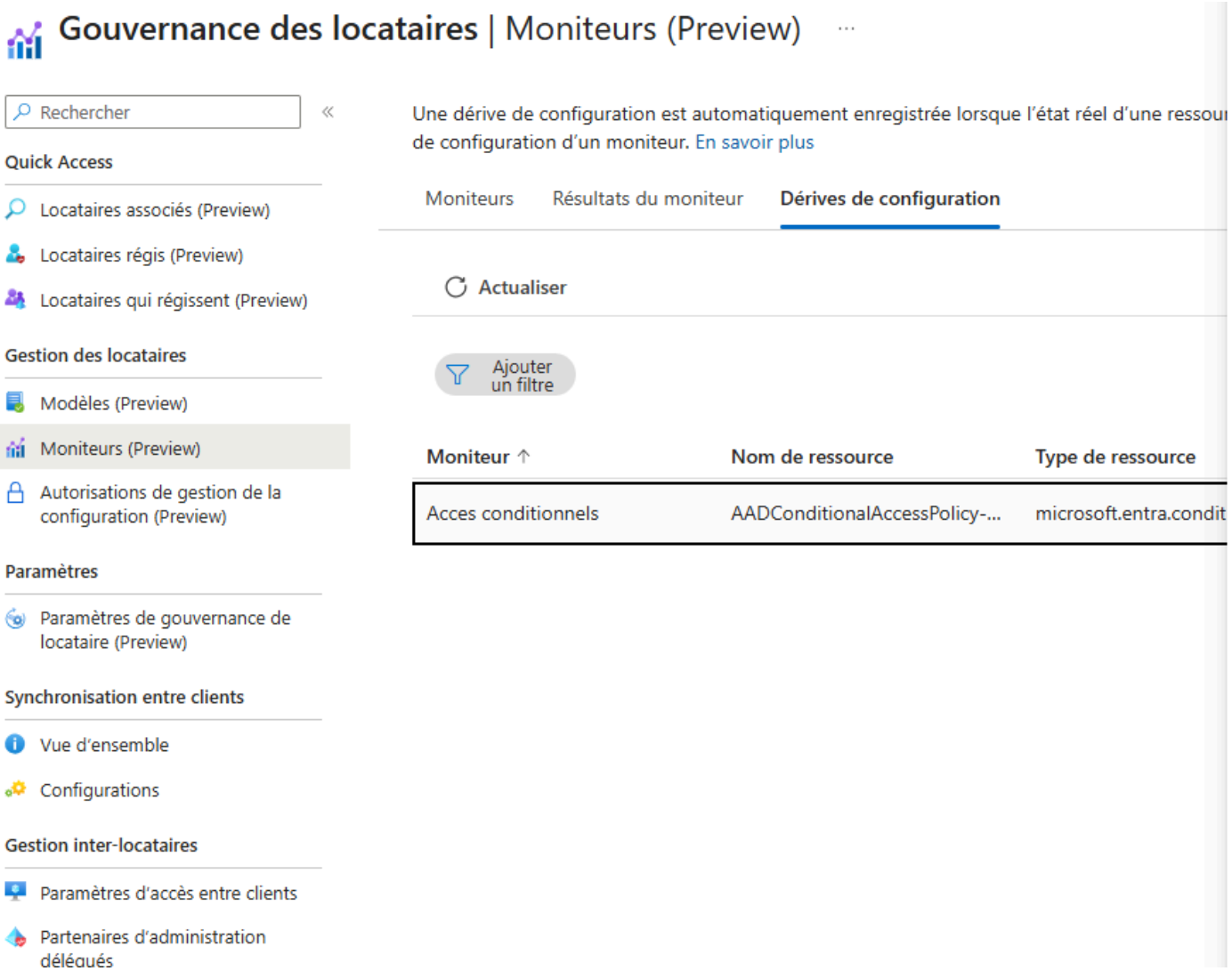
Si une différence est trouvée par le monitor entre la baseline et l'état actuel du tenant, une derive de configuration sera levée.

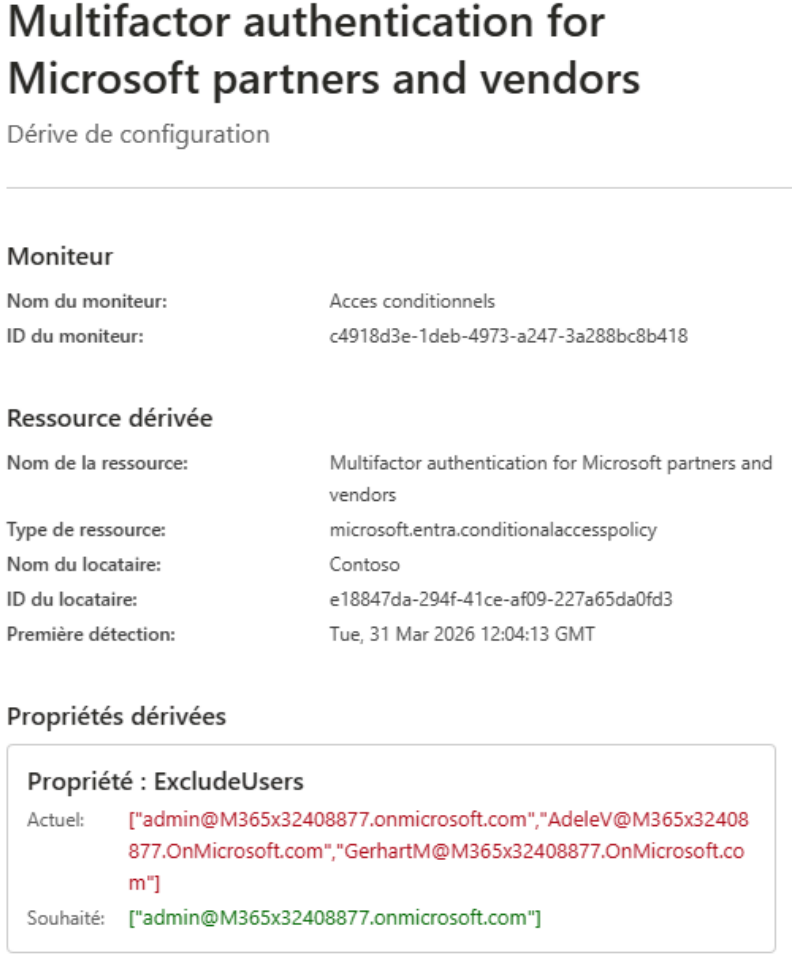
```
$uri = 'beta/admin/configurationManagement/configurationDrifts'
$drifts = Invoke-MgGraphRequest -Method GET -Uri $uri -OutputType PSObject
```

METSYS

property	value
monitorId	c4918d3e-1deb-4973-a247-3a288bc8b418
tenantId	e18847da-294f-41ce-af09-227a65da0fd3
resourceType	microsoft.entra.conditionalaccesspolicy
baselineResourceDisplayName	AADConditionalAccessPolicy-Multifactor authentication for Microsoft partners and vendors
firstReportedDateTime	31/03/2026 12:04:13
status	active
resourceInstanceIdentifier	@{DisplayName=Multifactor authentication for Microsoft partners and vendors}
driftedProperties	{@{propertyName=ExcludeUsers; currentValue=System.Object[]; desiredValue=System.Object[]}}

Utilisation - Surveillance des dérives





METSYS

Exemples d'utilisation d'UTCM

Il manque encore un élément de UTCM : **le rollback**.

Pour l'instant il n'est pas encore possible d'appliquer une baseline sauvegardée sur la configuration du tenant. Une fois que cette fonction sera disponible :

- Audit quotidien de la configuration
- Garantir un environnement de DEV & PREPROD iso à la PROD
- ... ou simplement un garde-fou pour vos configurations sensibles

METSYS

Conclusion

UTCM a fortement évolué depuis sa sortie en janvier 2026 et va continuer d'évoluer (*nombres de ressources, possibilité de rollback, gestion d'autres tenants...*)

Aujourd'hui il permet simplement d'exporter et surveiller la configuration de votre tenant, mais très prochainement il devrait être en mesure de déployer une baseline sur un tenant vierge ou d'administrer plusieurs tenants de manière centralisée et programmatique (moyennant finances évidemment).

A terme, UTCM (et au général le module **Tenant Governance**) pourrait venir challenger des produits comme CoreView

METSYS

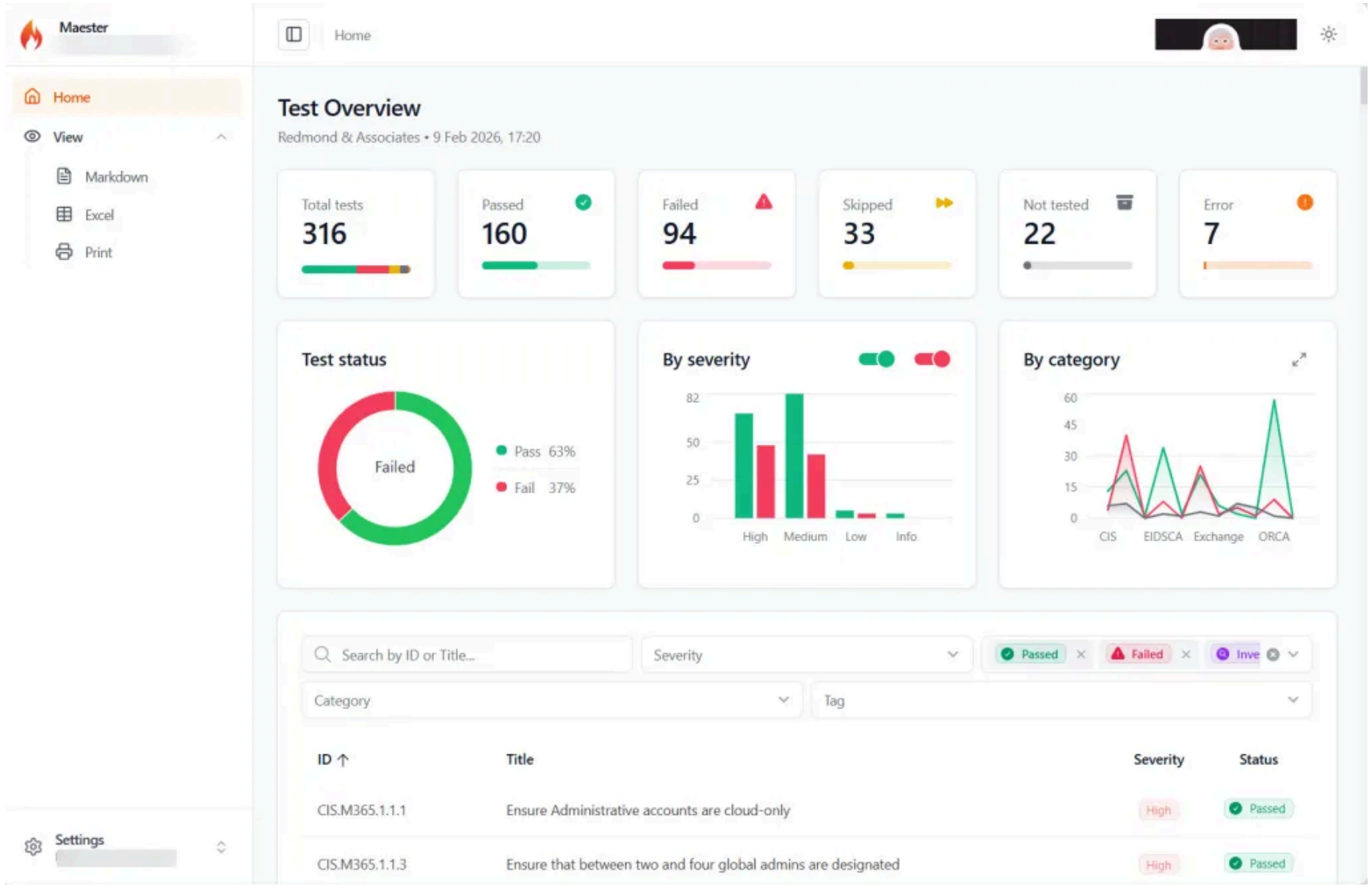
Quelques mots sur Maester

Module PowerShell pour faire une analyse des bonnes pratiques de votre tenant. Il permet également de faire des tests personnalisés sur vos propres indicateurs (via Pester).

UTCM et Maester sont complémentaires

maester.dev

Conclusion


Maester
Home
Home
View
Markdown
Excel
Print
Settings
Test Overview
Redmond & Associates • 9 Feb 2026, 17:20
Total tests
316
Passed
160
Failed
94
Skipped
33
Not tested
22
Error
7
Test status
Failed
Pass 63%
Fail 37%
By severity
82
50
25
0
High
Medium
Low
Info
By category
60
45
30
15
0
CIS
EIDSCA
Exchange
ORCA
Search by ID or Title...
Severity
Passed
Failed
Inve
Category
Tag
ID
Title
Severity
Status
CIS.M365.1.1.1
Ensure Administrative accounts are cloud-only
High
Passed
CIS.M365.1.1.3
Ensure that between two and four global admins are designated
High
Passed

Merci à tous pour votre attention !