SCRIPT #12 · MICROSOFT 365

Attivita amministrative recenti

Estrae dal registro di controllo unificato le operazioni amministrative piu recenti.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Modulo ExchangeOnlineManagement, ruolo di audit

Cosa fa questo script

Lo script interroga il registro di controllo unificato di Microsoft 365 (Unified Audit Log) filtrando sulle operazioni amministrative piu comuni (creazione utenti, modifica ruoli, modifiche a policy) nelle ultime N ore.

Come si usa

Esegui lo script indicando quante ore indietro analizzare. Il registro di controllo deve essere abilitato per il tenant (verificalo con Get-AdminAuditLogConfig se il report risulta sempre vuoto).

```
.\Report-AuditAmministrativo.ps1 -OreIndietro 24
```

In quale contesto usarlo

Da eseguire come controllo di routine per chi gestisce un tenant con piu amministratori: permette di individuare rapidamente modifiche non pianificate o non comunicate a livello di configurazione del tenant, prima che i loro effetti si manifestino come problemi apparentemente slegati.

Codice completo

Il codice è lo stesso del file Report-AuditAmministrativo.ps1: per usarlo scarica il file dalla pagina invece di copiarlo da questo PDF.

```
<#
.SYNOPSIS
    Estrae dal registro di controllo unificato le operazioni amministrative più recenti.
#>
param(
    [int]$OreIndietro = 24,
    [string]$PercorsoCSV = "C:\Report\AuditAmministrativo.csv"
)

Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -ShowBanner:$false

$dataInizio = (Get-Date).AddHours(-$OreIndietro)
$dataFine = Get-Date

$operazioni = @("Add-MailboxPermission","Add member to group","Add member to role",
    "Set-Mailbox","Update user","Add user")

$risultati = Search-UnifiedAuditLog -StartDate $dataInizio -EndDate $dataFine -Operations $operazioni -ResultSize 500 |
```

```
    Select-Object CreationDate, UserIds, Operations, ResultIndex

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Trovate $($risultati.Count) operazioni amministrative nelle ultime $OreIndietro ore." -ForegroundColor Cyan
Disconnect-ExchangeOnline -Confirm:$false
```