SCRIPT #03 · AUTOMAZIONE E REPORTISTICA GENERALE

Logging centralizzato multi-server

Raccoglie eventi specifici da piu server in un unico file di log centralizzato.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Connettivita CIM/WMI verso i server target

Cosa fa questo script

Lo script si collega a un elenco di server e raccoglie da ciascuno gli eventi di un log e tipo specifico (es. errori applicativi delle ultime ore), consolidandoli in un unico file centralizzato con l'indicazione del server di provenienza.

Come si usa

Prepara un file di testo con un server per riga, poi esegui lo script indicando log da monitorare e finestra temporale.

```
.\Logging-CentralizzatoMultiServer.ps1 -ListaServer "C:\Dati\server.txt" -NomeLog "Application" -OreInd
```

In quale contesto usarlo

Una soluzione minimale di log centralizzato per chi non dispone (ancora) di un vero SIEM: schedulato ogni ora, costruisce nel tempo un archivio consultabile centralmente, molto piu comodo che dover collegarsi manualmente a ogni singolo server per cercare un evento specifico.

Codice completo

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

```
<#
.SYNOPSIS
    Raccoglie eventi specifici da più server in un unico file di log centralizzato.
#>
param(
    [Parameter(Mandatory=$true)]
    [string]$ListaServer,
    [string]$NomeLog = "Application",
    [int]$OreIndietro = 1,
    [string]$LogCentralizzato = "C:\Report\LogCentralizzato.csv"
)

$server = Get-Content -Path $ListaServer
$dataLimite = (Get-Date).AddHours(-$OreIndietro)

$eventi = foreach ($srv in $server) {
    try {
        Get-WinEvent -ComputerName $srv -FilterHashtable @{LogName=$NomeLog; Level=(1,2); StartTime=$dataLimite} `
            -ErrorAction Stop |
            Select-Object @{N="Server";E={$srv}}, TimeCreated, Id, LevelDisplayName,
```

```
                @{N="Messaggio";E={$_.Message.Split("`n")[0]}}
    }
    catch {
        Write-Host "Impossibile leggere il log da $srv : $_" -ForegroundColor Yellow
    }
}

$eventi | Export-Csv -Path $LogCentralizzato -NoTypeInformation -Encoding UTF8 -Delimiter ";" -Append
Write-Host "Raccolti $($eventi.Count) eventi da $($server.Count) server in: $LogCentralizzato" -ForegroundColor Green
```