PowerShell

- Active Directory

Active Directory

Get BitLocker recovery key of an defined OU

```
# Définition de la OU
param(
    [Parameter(Mandatory)] [string]$ou
)

# Récupération de tous les ordinateurs du domaine Active Directory
$computers = Get-ADComputer -Filter * -Property Name -SearchBase $ou

# Boucle pour interroger les clés de récupération BitLocker pour chaque machine
$result = foreach ($computer in $computers) {
    # Les informations BitLocker sont stockées dans des objets enfants "msFVE-
RecoveryInformation"
    $bitlockerObjects = Get-ADObject -Filter {objectclass -eq "msFVE-RecoveryInformation"} -
SearchBase $computer.DistinguishedName -Properties "msFVE-RecoveryPassword", "whenCreated"

    if ($bitlockerObjects) {
        foreach ($obj in $bitlockerObjects) {
            # Extraction de l'identifiant unique (GUID) de la clé à partir du nom de l'objet
            $recoveryId = if ($obj.Name -match '\{(.+?)\}') { $Matches[1] } else { $obj.Name }
            $recoveryKey = $obj."msFVE-RecoveryPassword"

            [PSCustomObject]@{
                "Nom du PC"             = $computer.Name
                "Identifiant BitLocker" = $recoveryId
                "Clé de récupération"    = $recoveryKey
            }
        }
    } else {
        [PSCustomObject]@{
            "Nom du PC"             = $computer.Name
            "Identifiant BitLocker" = "N/A"
            "Clé de récupération"    = "Aucune clé trouvée dans AD"
        }
    }
```

```
}

# Affichage des résultats sous forme de tableau formaté dans la console
$result | Format-Table -AutoSize

# Optionnel : Pour exporter les résultats dans un fichier CSV (décommenter la ligne ci-dessous)
# $result | Export-Csv -Path "C:\temp\BitLocker_Keys_Report.csv" -NoTypeInformation -Encoding utf8
```