What's in my AD – Active Directory Health Check package.

azureblog.pl/2021/11/01/adaudit-1

Robert Przybylski

Hello Dear Reader,

Recently I was thinking about creating small repo of the scripts that will perform AD Health Check.

To be honest from thinking to doing it went very fast and today I'd like to share with you my latest idea.

Repo is available on my GitHub, and below you can see how it is working.

Get-ADAudit

The idea is to make it simpler as possible – I don't want to update the 'master' script in order to run new features. This is why I have decided to create one main file that will trigger all scripts that are placed under the **Scripts** folder with the exception of **Scripts\Excluded** location which is something like a playground with unfinished scripts. In order to run the master script run the following line

```
.\Get-ADAudit.ps1 -AuditPath C:\Audit
```

As you can see there is only one parameter **AuditPath** which is the location for output files.

Scripts

So what are the magical scripts that I have created? Some of them are just log files with raw output of the commands, some of them are CSV files with custom columns – just run it and discover *(if you trust me)*

At the moment of writing this article there are the following scripts:

- Get-ADAuditSettings – Checks auditing settings configuration
- Get-ADDetails – Gets basic ADDS details
- Get-ADTrusts – Checks if there are any trusts
- Get-BackupInfo – Information about backups
- Get-ComputerDetails – Information about computer objects
- Get-ComputerMachineQuota – Checks what are the settings about 'domain join'
- Get-DCDiag – Self explanatory
- Get-DCFeatures – List of the features installed on the DC
- Get-DCUACIssues – List of the DCs with wrong UAC settings

- Get-DCwithSpooler – List of the DCs with print spooler service
- Get-DefaultContainers – What are the default containers for users and computers
- Get-DNSAdmins – List of the DNS admins
- Get-GMSADetails – Checks if there are and how are configured GMSA accounts
- Get-InactiveDCs – Checks if there are any inactive DCs
- Get-KrbtgtPwdLastSet – LAst password changefor KRBTGT
- Get-LAPSDetails – checks if LAPS is configured under the domain
- Get-NTPDetails – RAW NTPoutput
- Get-PrivilegedGroupsDetails – Checks membership under the privileged groups
- Get-Repadim – Self explanatory
- Get-SchemaAdmins – Self explanatory
- Get-ServicesOnDC – What services are running on DCs
- Get-SysvolDetail – Self explanatory
- Get-UserDetails – Information about computer objects

I can imagine what you are thinking – *Those are basic scripts … what is the innovation here?*

And the answer is simple – **There is no innovation** – these are the scripts that should be created by every admin but sometimes we don't have time, PowerShell skills, etc. to create such.
This is why I have decided to create this repo to help others not only me.

Run

So how do those scripts work? The picture below depicts the script run.

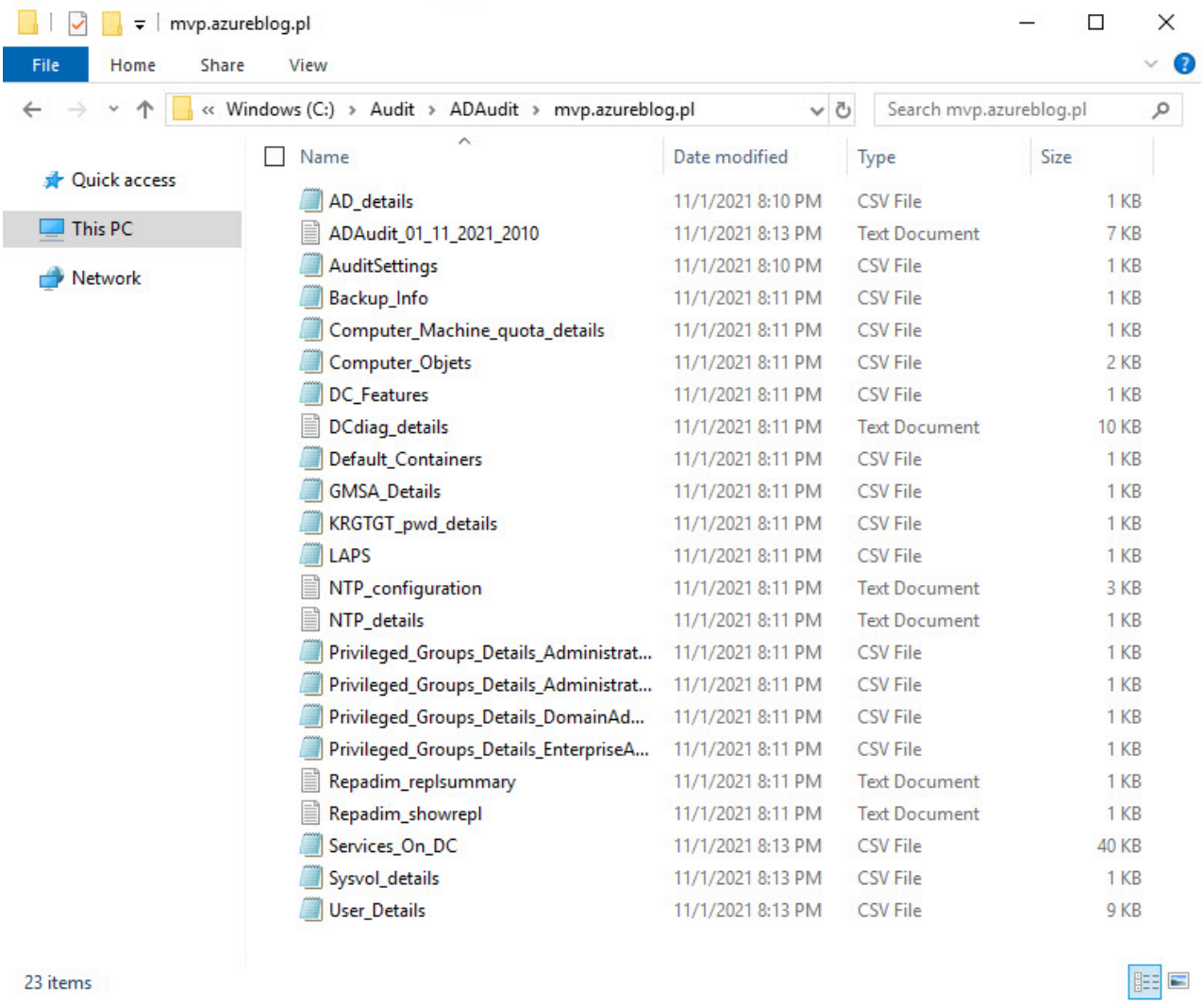
```
PS C:\tools\ADHealthCheck> .\Get-ADAudit.ps1 -AuditPath C:\Audit
Transcript started, output file is C:\Audit\ADAudit\mvp.azureblog.pl\ADAudit_01_11_2021_2010.log
----> Running Get-ADAuditSettings script  <-----
Checking DC 'vm-dc-neu'
Building Results string for for category 'Authentication Policy Change'
Building Results string for for category 'Computer Account Management'
Building Results string for for category 'DPAPI Activity'
Building Results string for for category 'Kerberos Authentication Service'
Building Results string for for category 'Kerberos Service Ticket Operations'
Building Results string for for category 'Logoff'
Building Results string for for category 'Logon'
Building Results string for for category 'Process Creation'
Building Results string for for category 'Security Group Management'
Building Results string for for category 'Security System Extension'
Building Results string for for category 'Sensitive Privilege Use'
Building Results string for for category 'Special Logon'
Building Results string for for category 'User Account Management'
AuditSettings.csv file updated and temporary file removed
----> Running Get-ADDetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Forest Info check...
----> Running Get-ADTrusts script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running AD Trusts check...
Found '0' ADTrust(s)
INFO: There are no trusts configured
----> Running Get-BackupInfo script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Backup Info check...
----> Running Get-ComputerDetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Computer Objects check...
Found '8' Computer Accounts
----> Running Get-ComputerMachineQuota script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Machine Account Quota check...
----> Running Get-DCDiag script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running DCDIAG check...
----> Running Get-DCFeatures script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Installed DC Features check...
Processing vm-dc-neu (Windows Server 2019 Datacenter)...

----> Running Get-DCUACIssues script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running DC UAC Settings check...
INFO: There are DC's with UAC issues
----> Running Get-DCwithSpooler script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Spooler Service check...
INFO: There are DC's with print spooler service running
----> Running Get-DefaultContainers script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Default Containers check...
----> Running Get-DNSAdmins script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running DNS Admins check...
INFO: DNS Admins group is empty
----> Running Get-GMSADetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running GMSA check...
Found '2' GMSA Accounts
----> Running Get-InactiveDCs script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Inactive DCs check...
INFO: There are no inactive DCs'
----> Running Get-KrbtgtPwdLastSet script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running KRBTGT Password Last Set check...
----> Running Get-LAPSDetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running LAPS check...
----> Running Get-NTPDetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running NTP Configurtion check...
----> Running Get-PrivilegedGroupsDetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Privileged Groups check...
####################   Creating 'Administrators' 'Group' members report
Found '2' 'Group' entries
####################   Creating 'Administrators' 'User' members report
Found '1' 'User' entries
####################   Creating 'DomainAdmins' 'Group' members report
Found '0' 'Group' entries
INFO: Group 'DomainAdmins' does not have any 'Group' objects'
####################   Creating 'DomainAdmins' 'User' members report
Found '3' 'User' entries
####################   Creating 'ProtectedUsers' 'Group' members report
Found '0' 'Group' entries
INFO: Group 'ProtectedUsers' does not have any 'Group' objects'
####################   Creating 'ProtectedUsers' 'User' members report
Found '0' 'User' entries
INFO: Group 'ProtectedUsers' does not have any 'User' objects'
####################   Creating 'SchemaAdmins' 'Group' members report
Found '0' 'Group' entries
INFO: Group 'SchemaAdmins' does not have any 'Group' objects'
####################   Creating 'SchemaAdmins' 'User' members report
Found '0' 'User' entries
INFO: Group 'SchemaAdmins' does not have any 'User' objects'
####################   Creating 'EnterpriseAdmins' 'Group' members report
Found '0' 'Group' entries
INFO: Group 'EnterpriseAdmins' does not have any 'Group' objects'
####################   Creating 'EnterpriseAdmins' 'User' members report
Found '1' 'User' entries
----> Running Get-Repadm script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Replication check...
----> Running Get-SchemaAdmins script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Schema Admins check...
INFO: There are no members of Shema Admins group
----> Running Get-ServicesOnDC script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running DC Services check...
Found '226' entries
----> Running Get-SysvolDetails script  <-----
----> Running Get-UserDetails script  <-----
[C:\tools\ADHealthCheck\Get-ADAudit.ps1] Running Users Objects check...
Found '30' User Accounts
Transcript stopped, output file is C:\Audit\ADAudit\mvp.azureblog.pl\ADAudit_01_11_2021_2010.log
```

Script run

Output

As I mentioned before – you will get some output from the script, even the whole transcript of the script run. All files will be available based on the location that was provided for the **AuditPath** parameter under the ADAudit\<YourDomainName> folder



Script output

There are 3 types of files available:

- CSV – tabular report
- LOG – RAW output of the command run
- LOG **(ADAudit_<CurrentDate>.log)** – transcript from the **Get-ADAudit.ps1** script run

Sumamry

As you can this article wasn’t so long, but the value of the scripts should be much bigger for everyday usage under your AD DS environment.
There will be more articles regarding this repo when new features will be developed by me.

Stay tuned and see you soon…