
Introducing
Get-WindowsTroubleShootingReportCommunity
Petri Paavola
Microsoft MVP - Windows and Intune

Petri Paavola

Microsoft MVP – Windows and Intune

Senior Modern Management Principal

Petri.Paavola@yodamiitti.fi

@petripaavola

@intune.ninja

https://github.com/petripaavola

Intune.ninja

Powershell.ninja

Skills

- **Powershell / Graph API**
- **AI**
- **Windows Autopilot + Intune + Intune for Education**
- **Windows 10&11 Deployment and Management**
- **Traditional on-prem deployment and management**
- **Consulting &Training**

Over 24 years of work experience

Current (10+ years):

- **Yodamiitti Oy / Owner**
  Consulting / Training

Past:

- **Aalto university / IT-services**
  Responsible for Workstation service

Agenda

World Premiere! Introducing Get-WindowsTroubleShootingReportCommunity

The Ultimate Intune and Windows Troubleshooting Tool
Something new, something unique(?), something for and from community

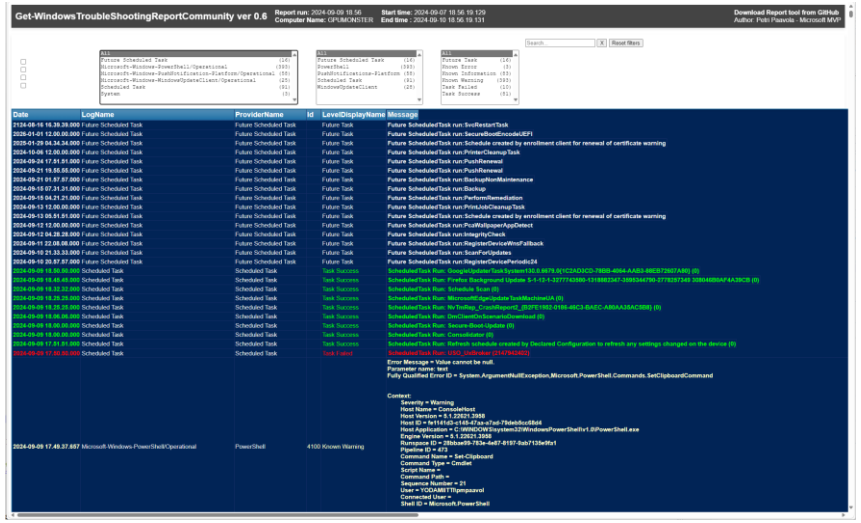
You can help making tools better! ☺

Key takeaways:

- **World "premiere" - Introducing**

  Get-WindowsTroubleShootingReportCommunity

www.wpninjas.fi



Introducing -

Get-WindowsTroubleShootingReportCommunity

The Ultimate Windows and Intune Troubleshooting Tool to troubleshoot anything and you can be part of the Contributing Community!

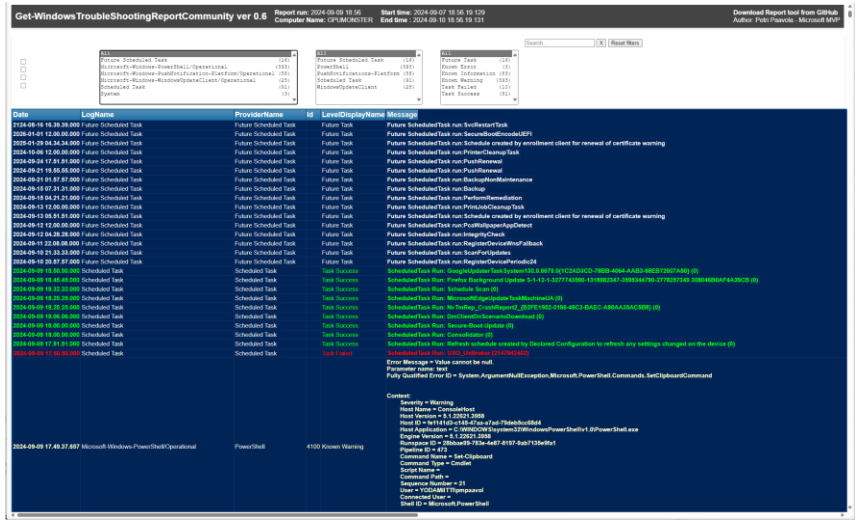
- With PowerShell we can
  - get information very easily from Windows Events and from any log file
  - **objectify** data
  - sort and filter data(=objects) really easily
  - And we can show information in human readable format
- It all started with 2 commands (maybe don't run these commands ☺)
  - **Get-WinEvent * | Out-GridView**
  - **Get-Content -Path C:\Programdata\Microsoft\IntuneManagementExtension\logs*.log | Out-GridView**

- That got me thinking about creating something new and unique
- Something where anyone can contribute the troubleshooting features

- Is this **THE** Troubleshooting Tool to analyze and report any events and log files?

Get-WindowsTroubleShootingReportCommunity

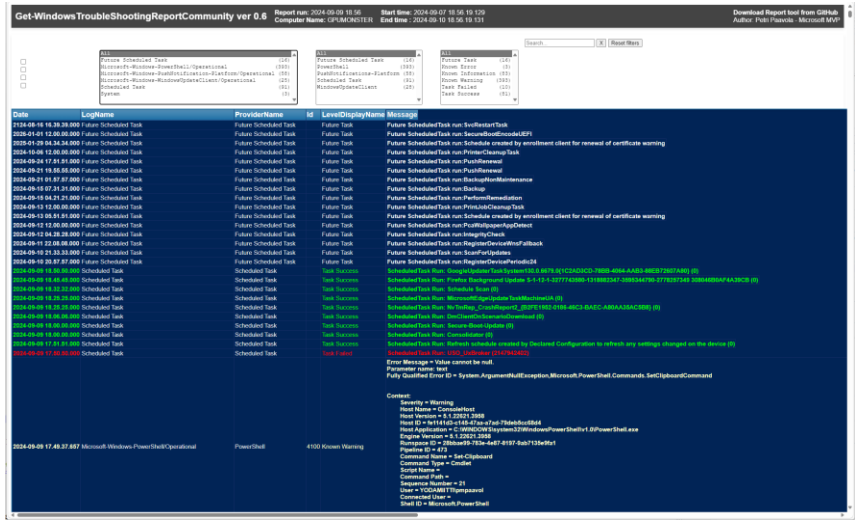
www.wpninjas.fi



- **Read Windows Event logs**
  - Online or from saved files (downloaded Diagnostics package)
- **Read any .log file format**
  - No restrictions for log file format as long as there is dateTime and message information in structured format
  - Intune/ConfigMgr CMTrace the most important ones but others too
- **Show events and logs sorted by dateTime**
  - This gives **timeline** what happened
  - For troubleshooting specific case you can show **ALL** events and logs
- **Detect Known Events and log messages**
  - Create easy to read report with only Known Events and log entries
  - Run report for extended long period (easily 30-365 days)
- **Realtime filtering and search by many ways in HTML report**
  - Scenario-based troubleshooting, for example Updates troubleshooting
- **Create your own Event Rules easily for detection**
- **Share you Event Rules to the rest of the world! ☺**

Get-WindowsTroubleShootingReportCommunity

www.wpninjas.fi



- **Scenario based views. For example do you really know exactly**
  - When Windows Updates installed in last 30 days, or not installed
    - When updates where actually installed after restart
    - What Firmware updates have been installed during last 365 days
  - Has Defender for Endpoint updated AV signatures and how often it runs
  - When computer restarted and changed to different power modes
  - What and when MSI applications installed and if they succeeded
  - When Store apps updated or failed
  - What PowerShell scripts ran in computer
  - Intune related events (enrollment, sync, MDM setting, app and scripts run)
  - ConfigMgr related events
  - What Errors there are in Event logs for last x minutes/hours/days
  - Did your Intune MDM policies succeeded or failed
  - and much more …
- **This list is just the beginning**
- **You can help by creating and sharing more Known Event rules!**

Showcase and DEMO
of the new
troubleshoot anything in the world -tool

Get-WindowsTroubleShootingReportCommunity

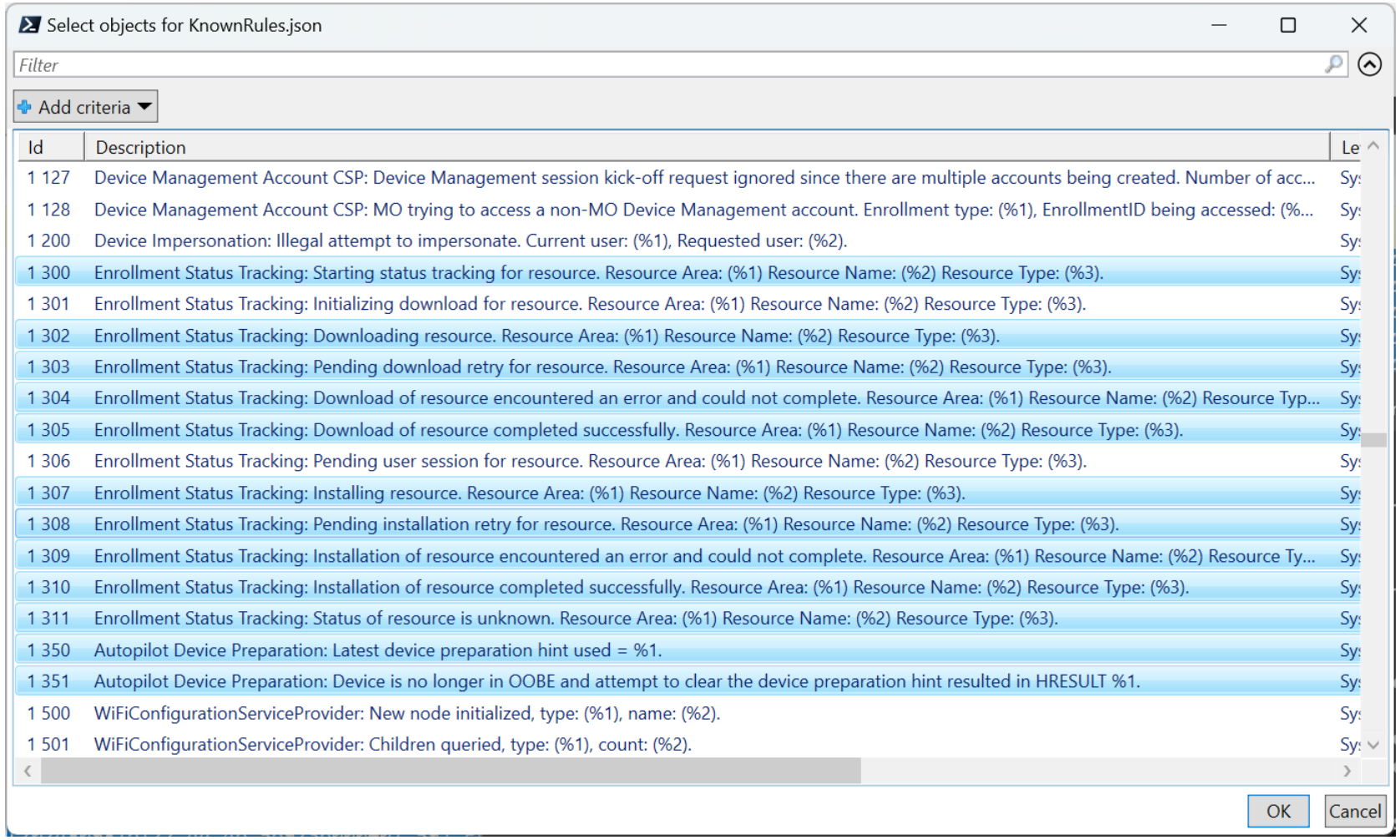
Create Known Events rules easily

www.wpninjas.fi

- I created a helper tool which helps you to create Scenarios from Event log events

.\Create-EventRules-GUI-HelperTool.ps1

- Hard part is to figure out Categories and what events we are interested on
- Something completed -> Green
- Something failed -> Red
- Do not add everything?
- Or create 2 sets?
  - Limited (success and fails)
  - Full (all events)




```
[
    {
        "CategoryName": "Intune MDM",
        "KnownEventRules": [
            {
                "CategoryName": "Intune MDM",
                "LogType": ".evtx",
                "Channel": "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin",
                "Id": 404,
                "ProviderName": "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider",
                "ToolTipText": "Error with Intune MDM policies!",
                "Color": "Red",
                "DeveloperNotes": "Error: MDM ConfigurationManager: Command failure status. "
                "Author": "Petri.Paavola@yodamiitti.fi / Microsoft MVP - Windows and Intune",
                "LinkToBlogArticle": null
            }
        ]
    },
    {
        "CategoryName": "Application installation",
        "KnownEventRules": [
            {
                "CategoryName": "Application installation",
                "LogType": ".evtx",
                "Channel": "Application",
                "Id": 1033,
                "ProviderName": "MsiInstaller",
                "ToolTipText": "Windows Installer installed the product.",
                "Color": "Green",
                "DeveloperNotes": "Windows Installer installed the product. Product Name: Mozilla Firefo
                130.0.0.0. Product Language: 0. Manufacturer: Mozilla. Installation success or error sta
                "Author": "Petri.Paavola@yodamiitti.fi / Microsoft MVP - Windows and Intune",
                "LinkToBlogArticle": null
            },
```


Create and Share your Known Event Rules

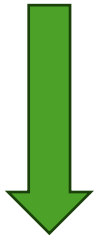
Download tools from GitHub and Powershell Gallery

Työkalu vielä "hiljaisessa" jakelussa, joten se on saatavilla,
mutta sitä ei ole julkisesti julkaistu vielä.
Kokeile ja laita palautetta miltä näyttää.

https://github.com/petripaavola/Get-WindowsTroubleshootingReportCommunity

Check out my GitHub for Community Tools downloads and documentation

Powershell.ninja



https://github.com/petripaavola

Thank You