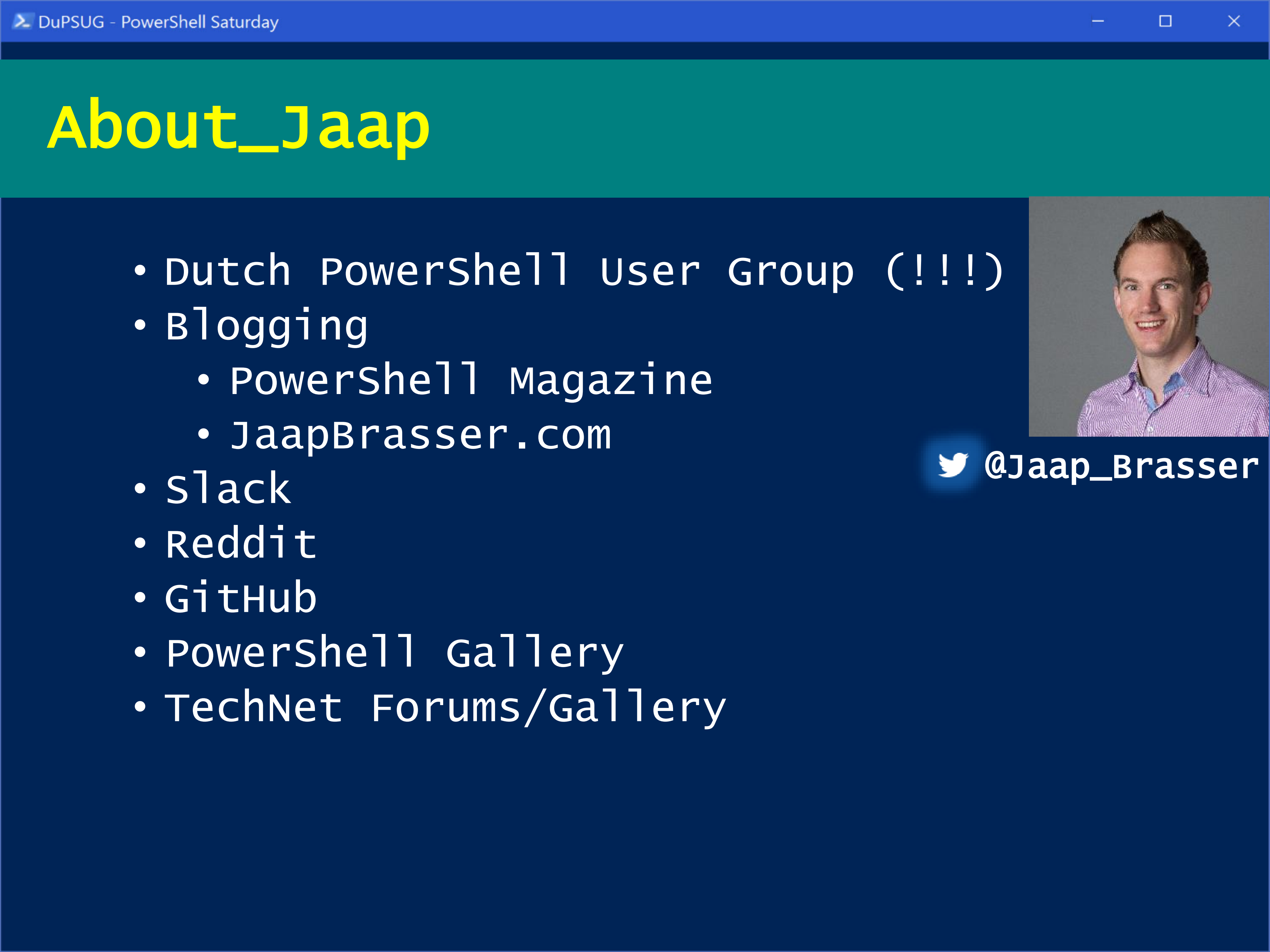
No more admins

Using delegated rights and JEA

Jaap Brasser

@Jaap_Brasser



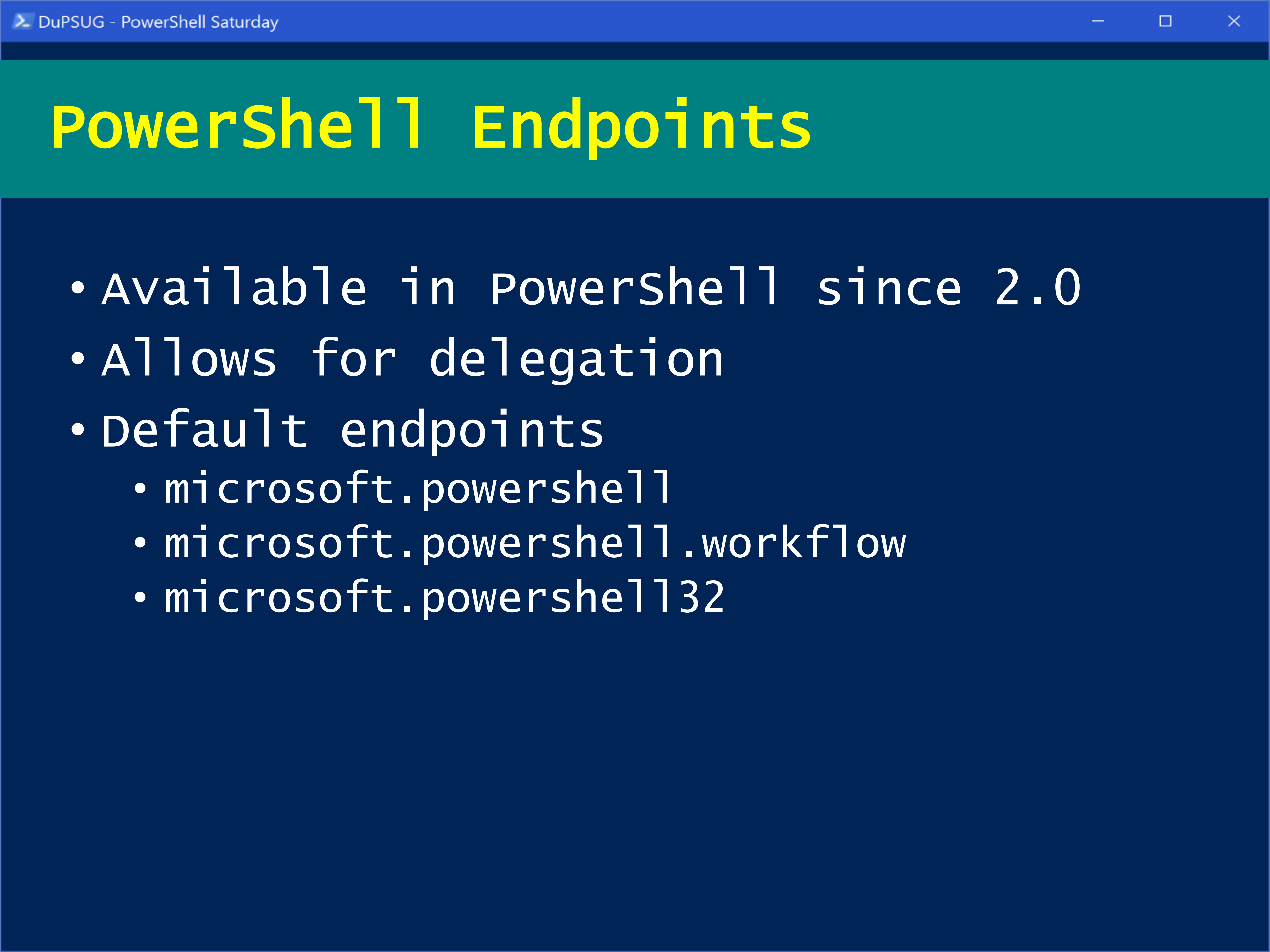
About_Jaap

- Dutch PowerShell User Group (!!!)
- Blogging
  - PowerShell Magazine
  - JaapBrasser.com
- Slack
- Reddit
- GitHub
- PowerShell Gallery
- TechNet Forums/Gallery

@Jaap_Brasser

Agenda

- Download and install JEA module
- Explain different components of JEA
- Setup JEA endpoints
- Set permissions on session endpoints

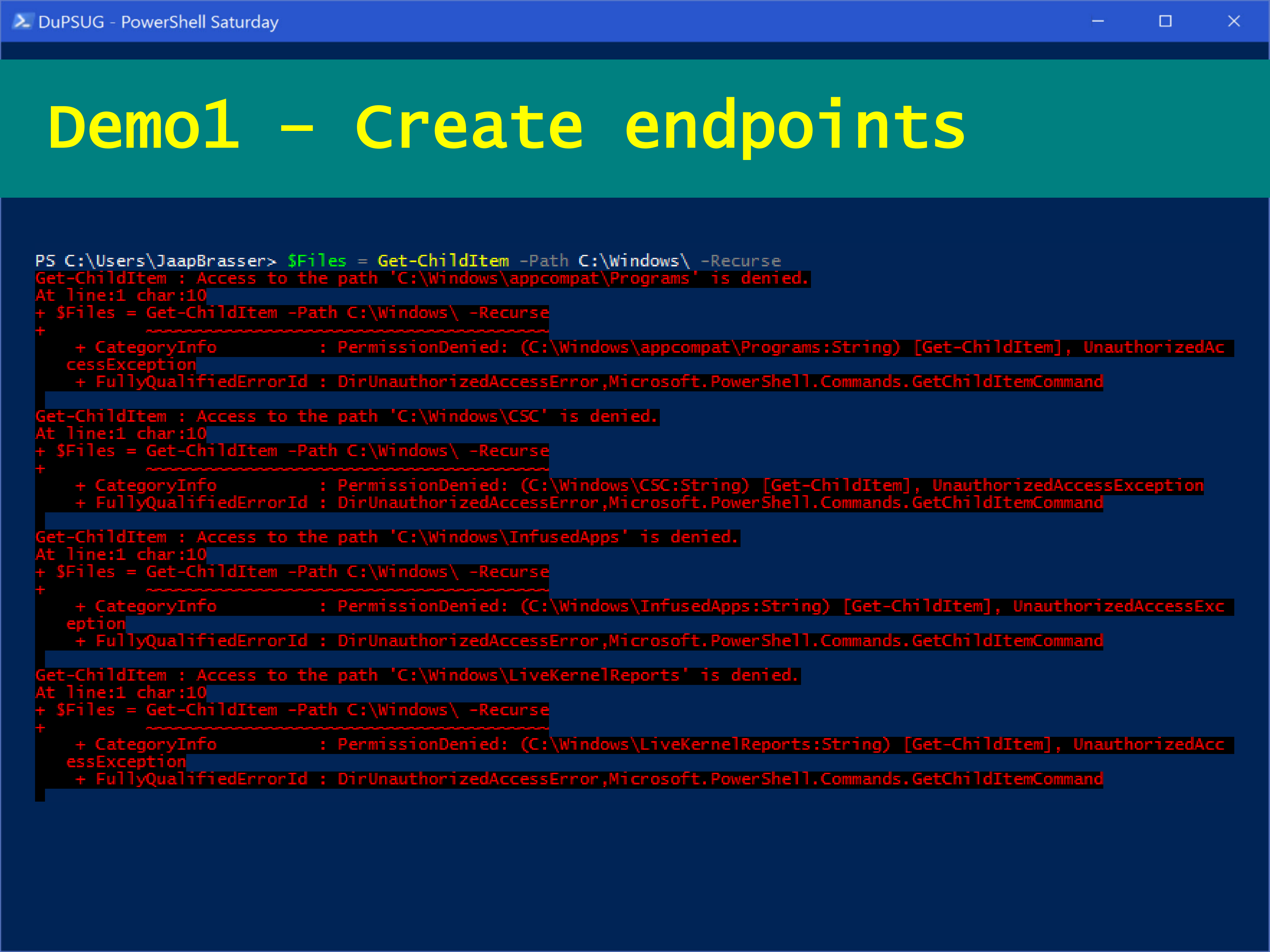


PowerShell Endpoints

- Available in PowerShell since 2.0
- Allows for delegation
- Default endpoints
  - microsoft.powershell
  - microsoft.powershell.workflow
  - microsoft.powershell32

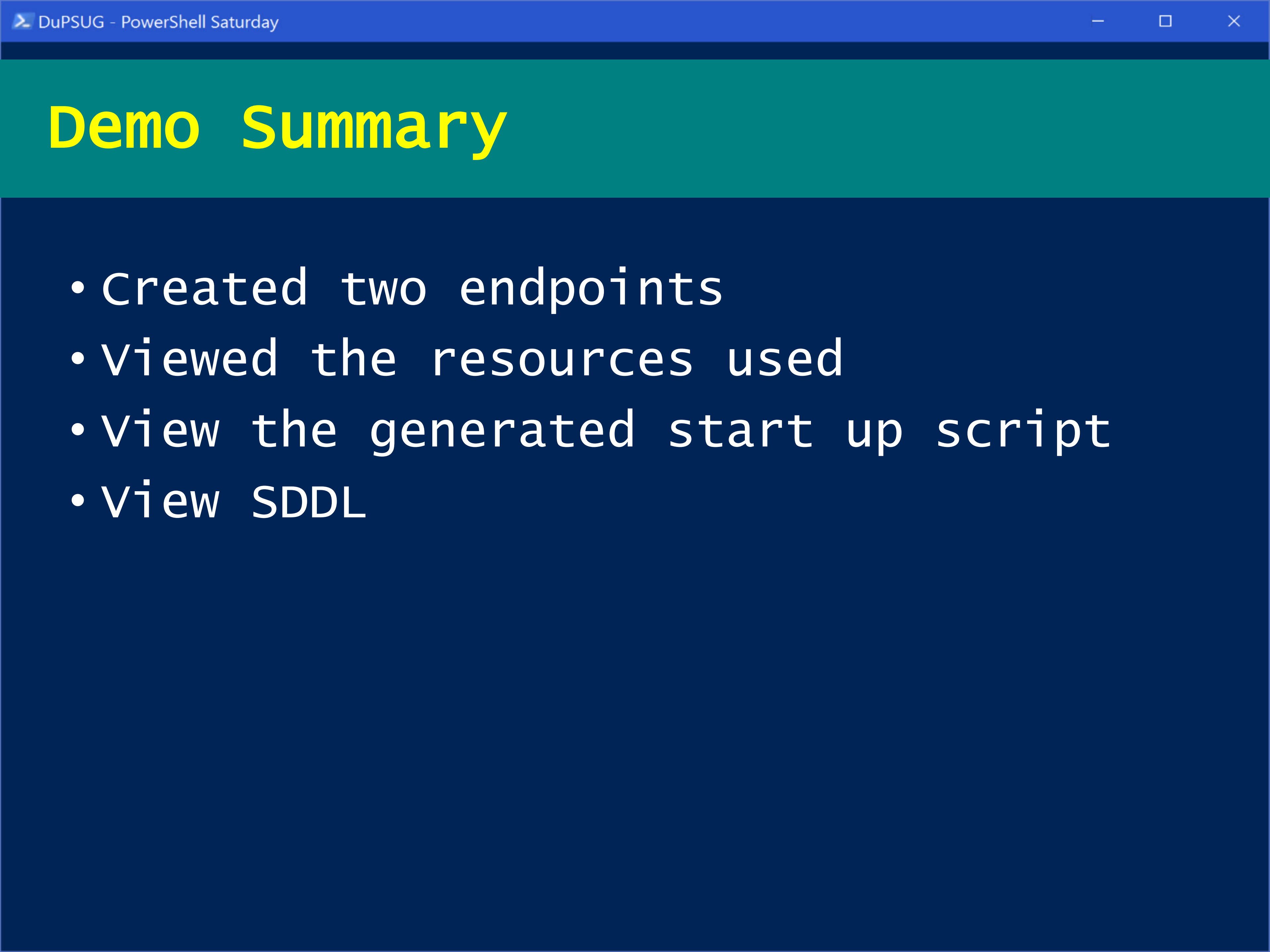
PowerShell Language Modes

- Different language modes
  - FullLanguage
  - ConstrainedLanguage
  - RestrictedLanguage
  - NoLanguage
- Determines what the console can do



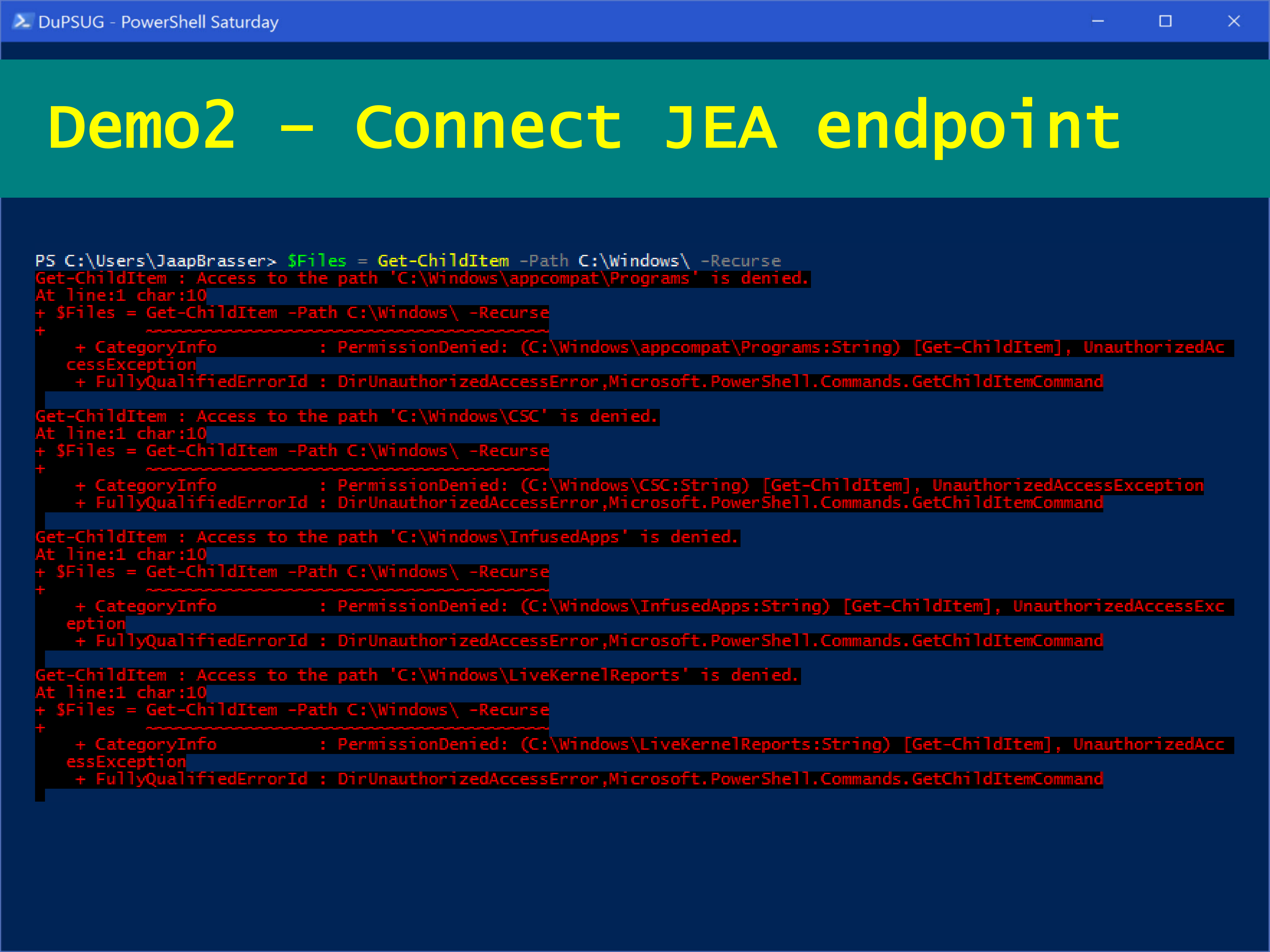
Demo1 – Create endpoints

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```



Demo Summary

- Created two endpoints
- Viewed the resources used
- View the generated start up script
- View SDDL

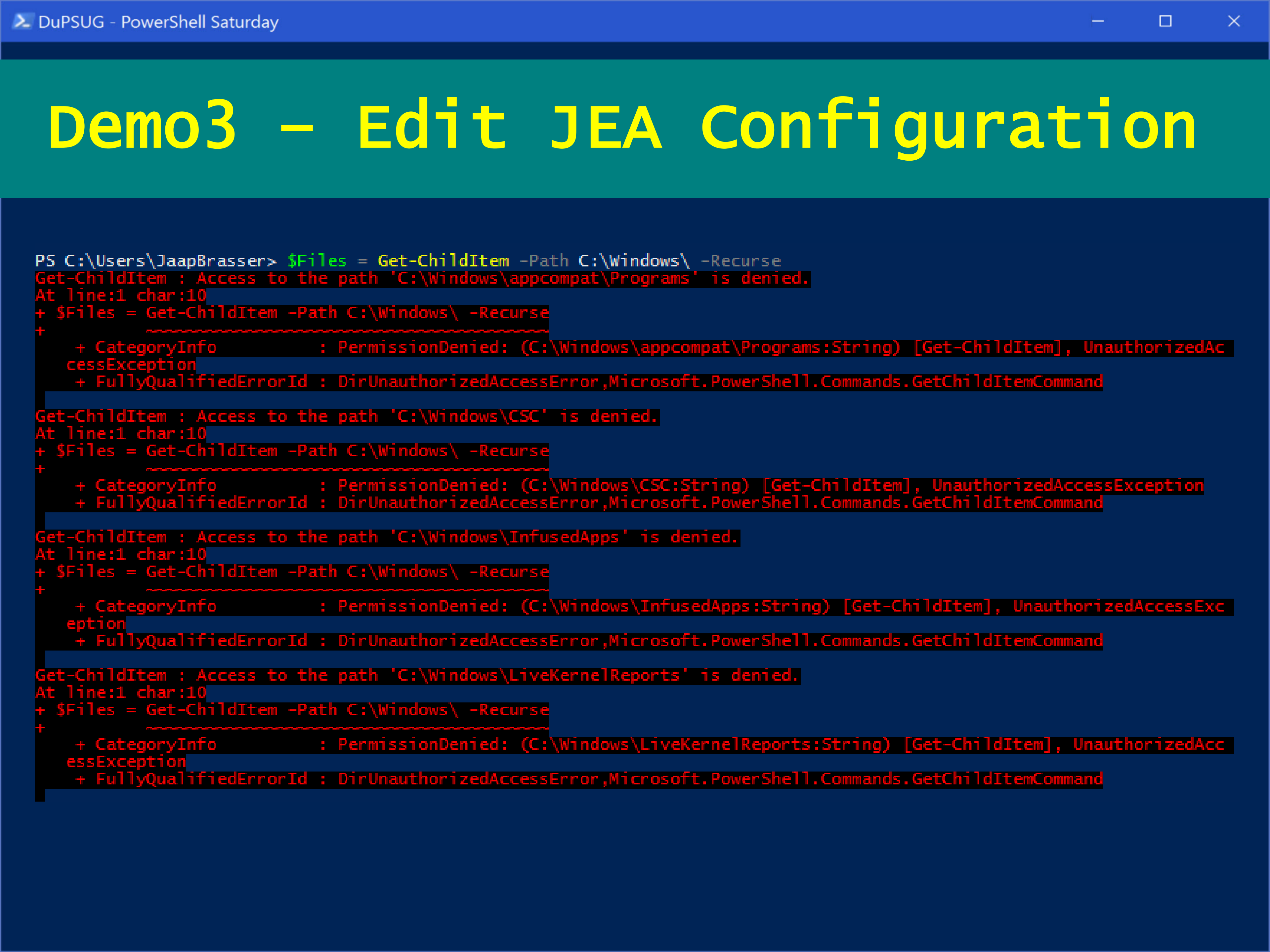


Demo2 – Connect JEA endpoint

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

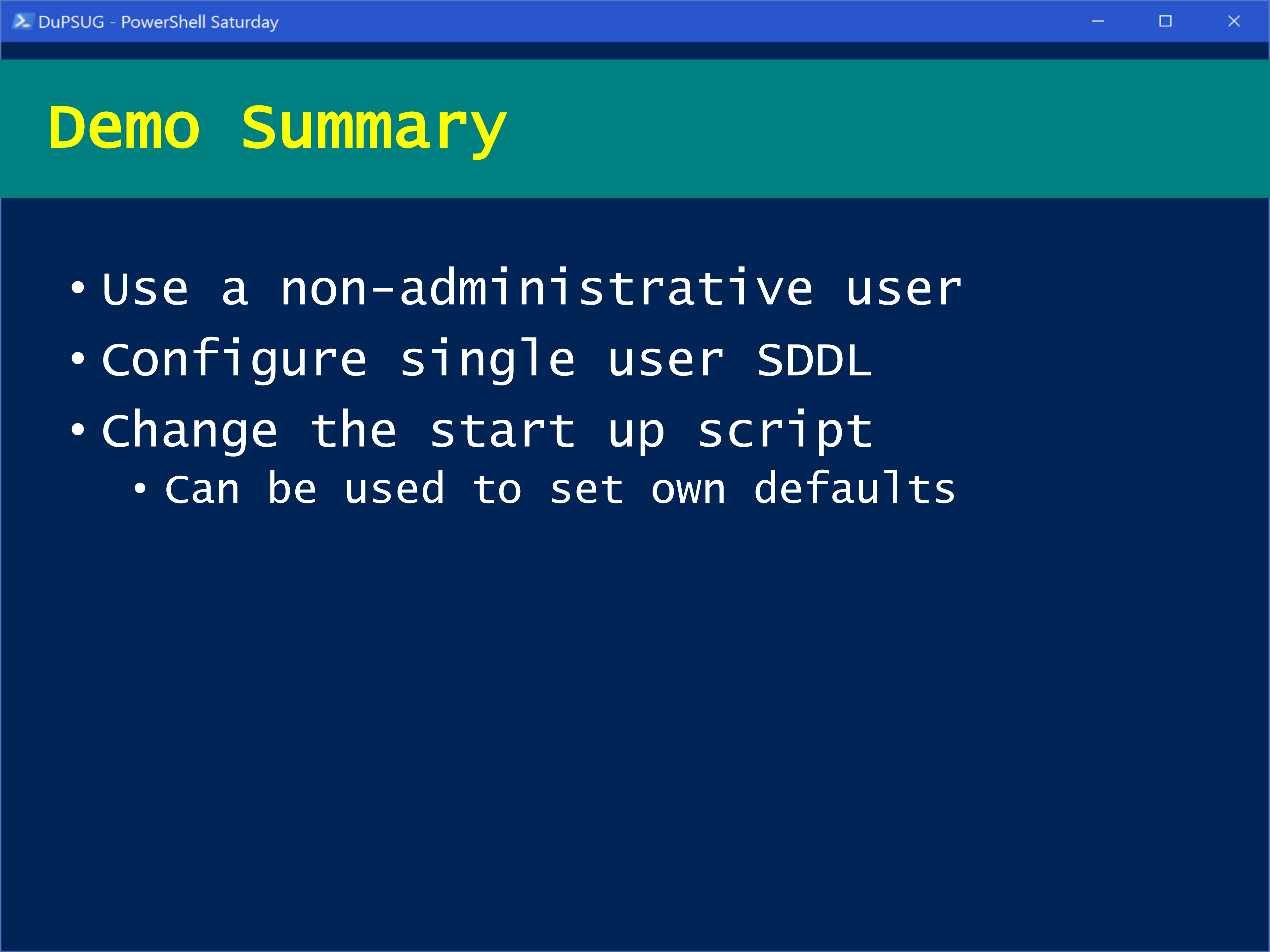
Demo Summary

- Connect to a JEA endpoint
- View the output
- What is retricted in the languagemode



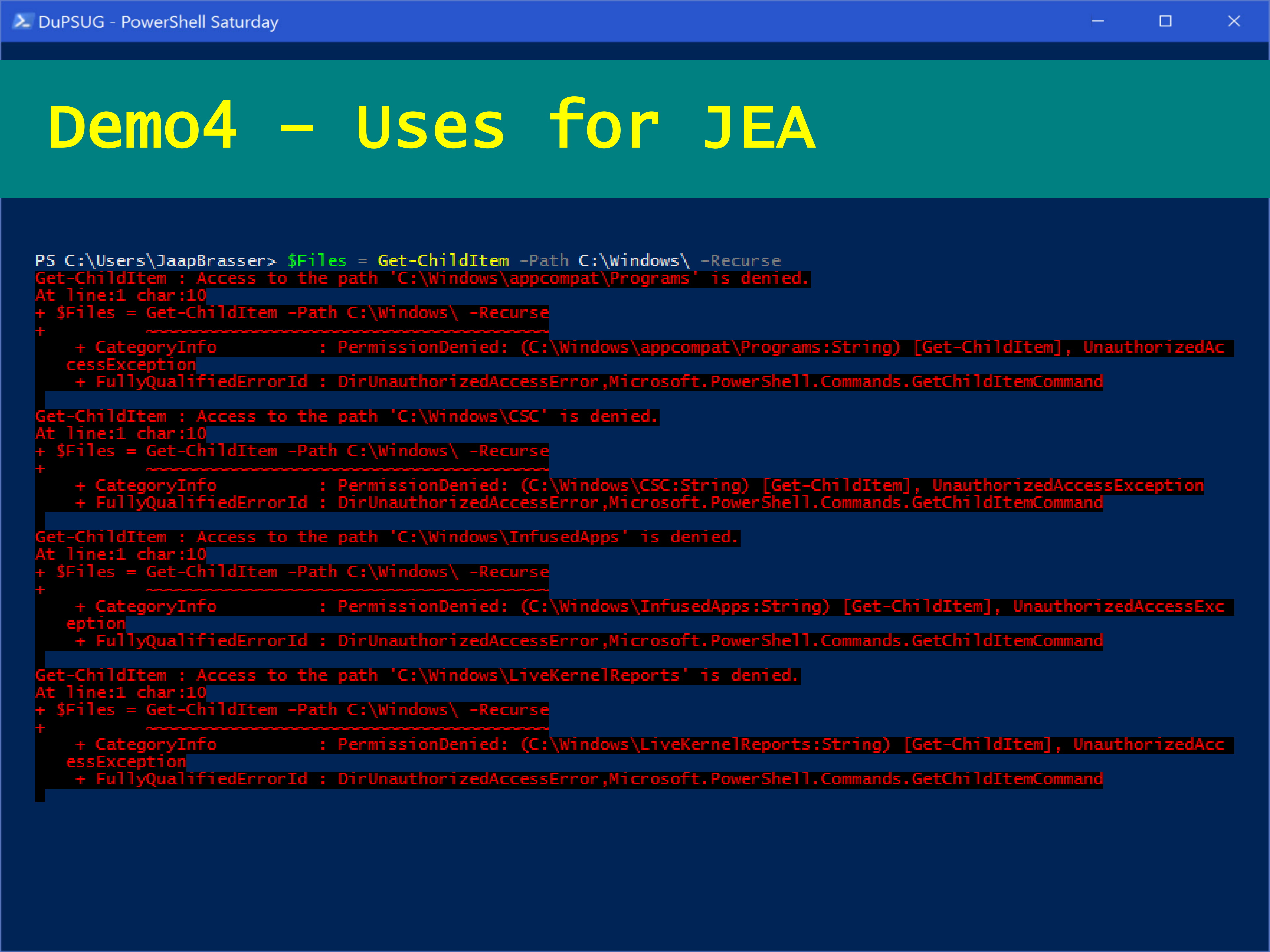
Demo3 – Edit JEA Configuration

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```



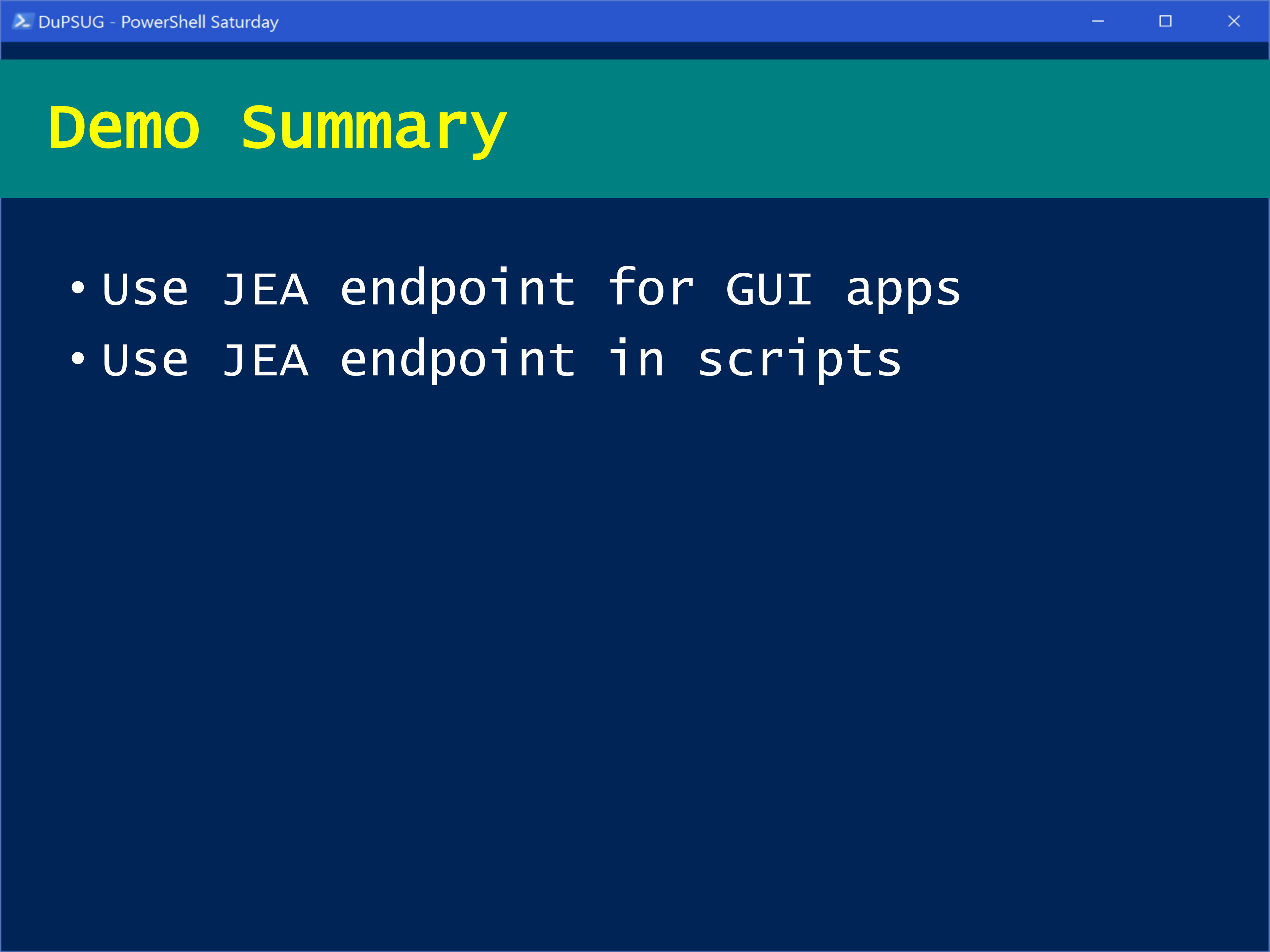
Demo Summary

- Use a non-administrative user
- Configure single user SDDL
- Change the start up script
  - Can be used to set own defaults



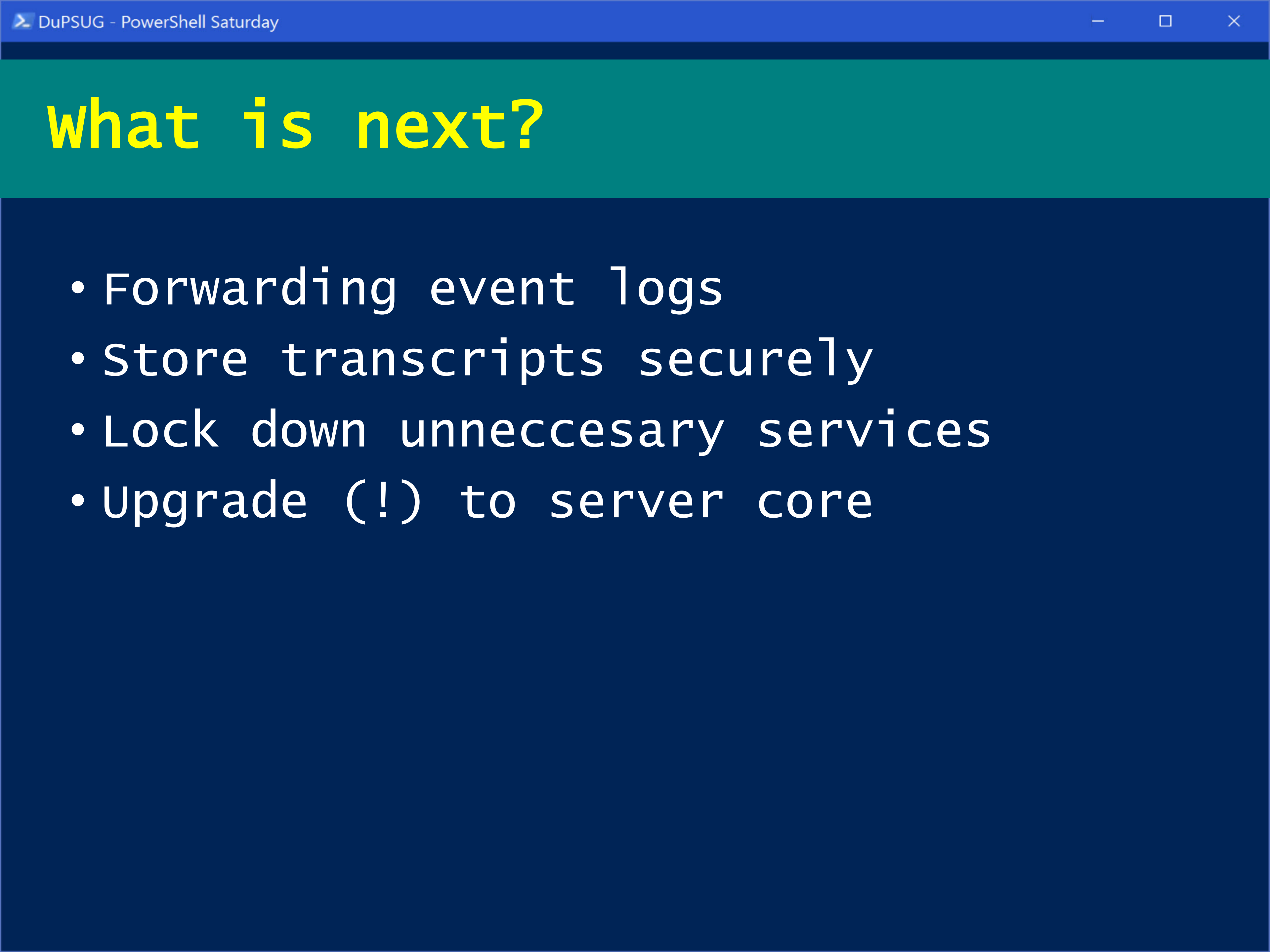
Demo4 – Uses for JEA

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```



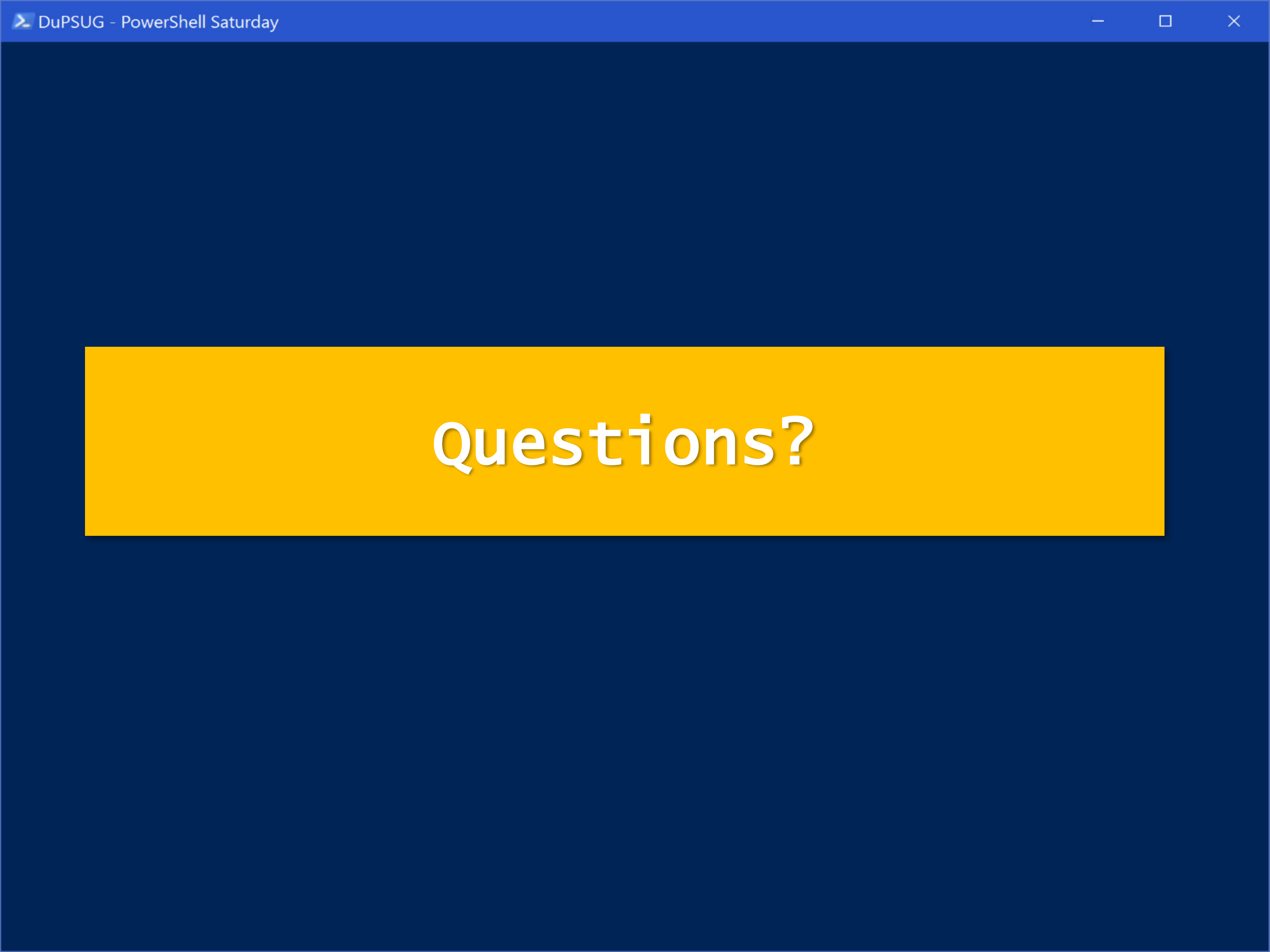
Demo Summary

- Use JEA endpoint for GUI apps
- Use JEA endpoint in scripts



What is next?

- Forwarding event logs
- Store transcripts securely
- Lock down unneccesary services
- Upgrade (!) to server core



DuPSUG - PowerShell Saturday

Questions?