PSCONF.EU

PowerShell Conference Europe

Next Up:

Evgenij Smirnov

Antwerp24

3

2

1

PSCONF.EU

PowerShell Conference Europe

Outfitting WAC with proper RBAC

Evgenij Smirnov

Antwerp24

Many thanks to our sponsors:

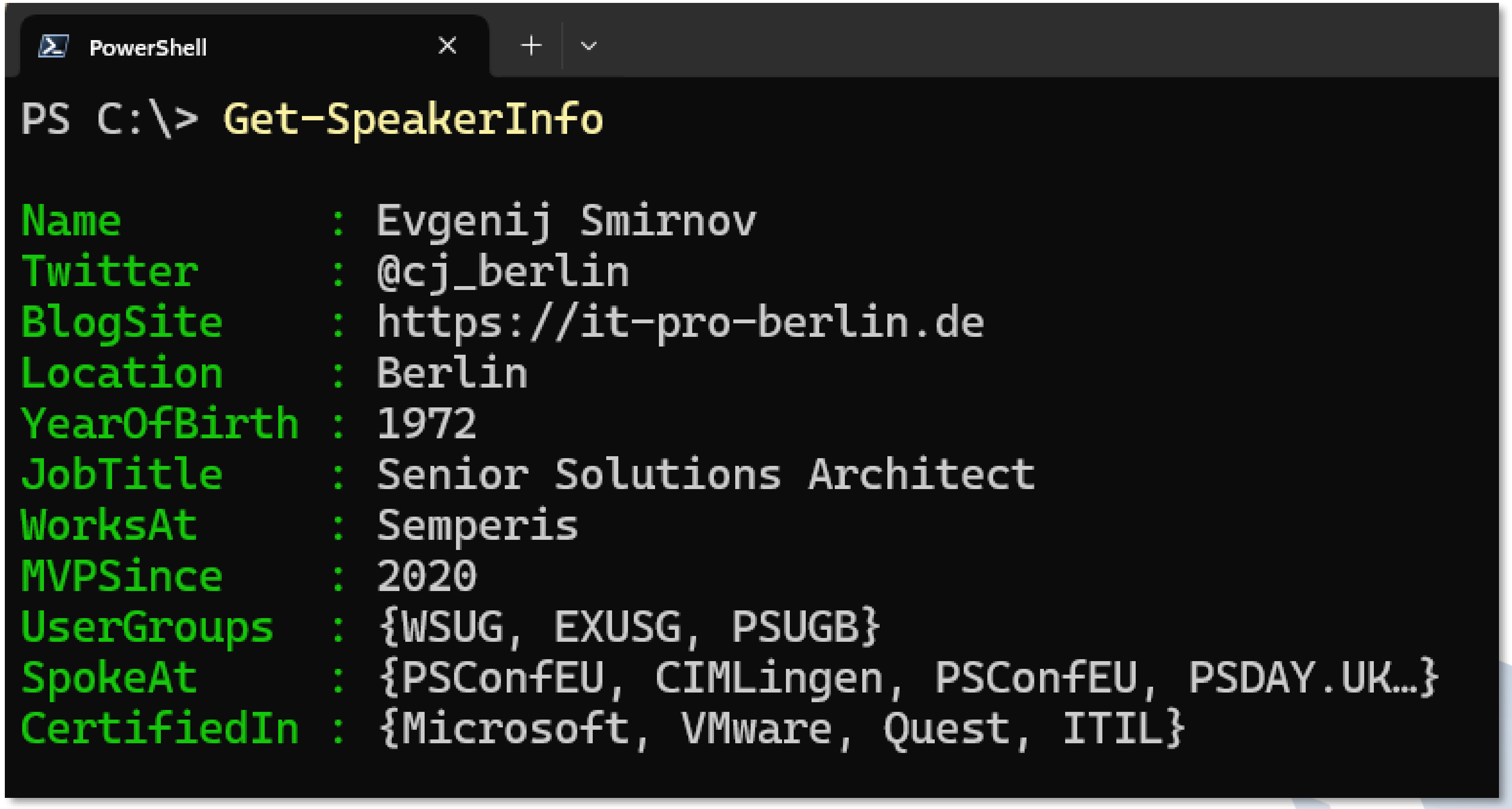
Chocolatey

PATCH MY PC

semperis

ScriptRunner®
Your #1 for PowerShell Automation

Evgenij Smirnov



```
PS C:\> Get-SpeakerInfo

Name        : Evgenij Smirnov
Twitter     : @cj_berlin
BlogSite    : https://it-pro-berlin.de
Location    : Berlin
YearOfBirth : 1972
JobTitle    : Senior Solutions Architect
WorksAt     : Semperis
MVPSince    : 2020
UserGroups  : {WSUG, EXUSG, PSUGB}
SpokeAt     : {PSConfEU, CIMLingen, PSConfEU, PSDAY.UK…}
CertifiedIn : {Microsoft, VMware, Quest, ITIL}
```

MVP Microsoft® Most Valuable Professional

@cj_berlin

In this session…

- a belated declaration of love…
- some wishful thinking…
- a peek under the hood and down a rabbit hole…
- mapping out the way forward!

My little secret

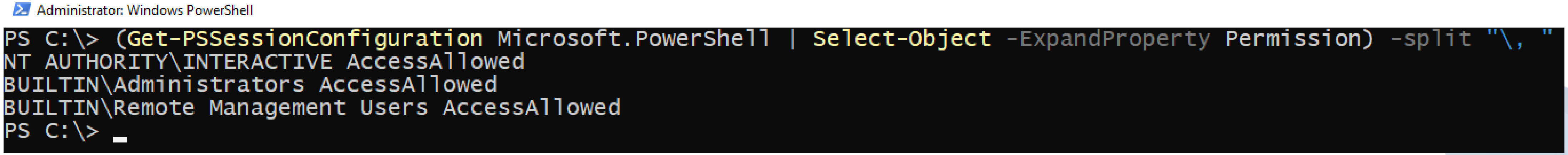
- I fell in love with web-based management in the 90s, once I undserstood how server-side processing works
- It was mostly platonic, since I did not consider programming a career choice for me,
  always thinking I was too far behind the curve…
- …but looking at some of the software that graced the world in the last 30 years,
  I would probably have done just fine.

Enter WAC

- Web-based management portal…
- …in Azure portal design we all (*learned to*) love…
- …can manage servers, clusters and workstations….
- …extensible in functionality…
- …but…

Not all is shiny in WAC

- Central administration is not granular enough
  - Everybody can log on to WAC (**by default**, configurable)
  - All „Shared Connections“ are visible to everybody
- Access to registered targets is not granular enough
  - governed by the default JEA endpoint:



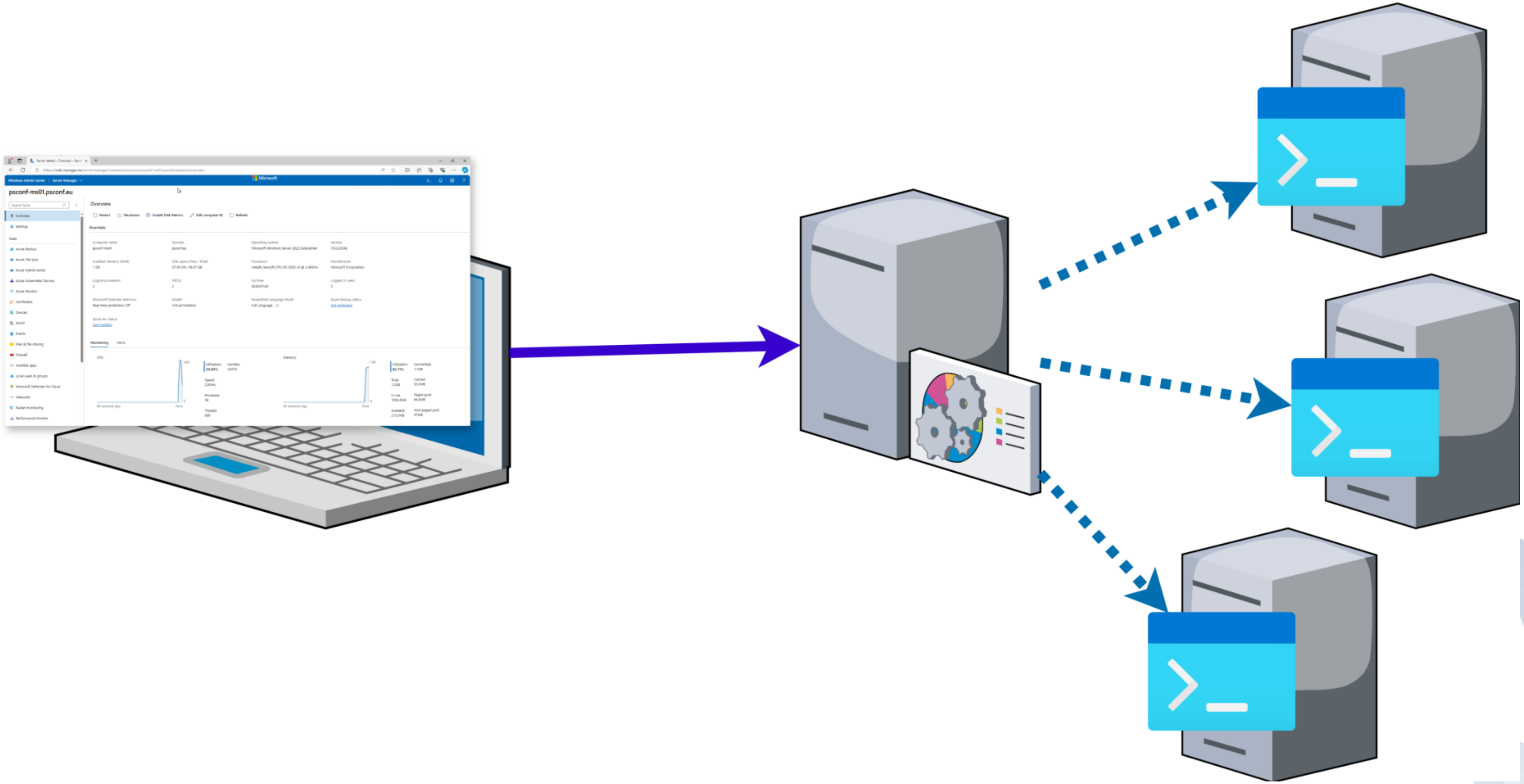
```
PS C:\> (Get-PSSessionConfiguration Microsoft.PowerShell | Select-Object -ExpandProperty Permission) -split "\, "
NT AUTHORITY\INTERACTIVE AccessAllowed
BUILTIN\Administrators AccessAllowed
BUILTIN\Remote Management Users AccessAllowed
PS C:\> _
```

What’s in the Box

What can we work with without it getting hacky and unmanageable?

@cj_berlin

WAC for 3rd-graders



psconf-ms01.psconf.eu

Overview

Essentials

Computer name: psconf-ms01

Domain: psconf.eu

Operating system: Microsoft Windows Server 2022 Datacenter

Version: 10.0.20348

Installed memory (RAM): 1 GB

Disk space (Free / Total): 37.39 GB / 59.37 GB

Processors: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz

Manufacturer: Microsoft Corporation

Logical processors: 2

NIC(s): 2

Up time: 0:0:00:01:43

Logged in users: 0

Microsoft Defender Antivirus: Real-time protection: Off

Model: Virtual Machine

PowerShell Language Mode: Full Language

Azure Backup status: Not protected

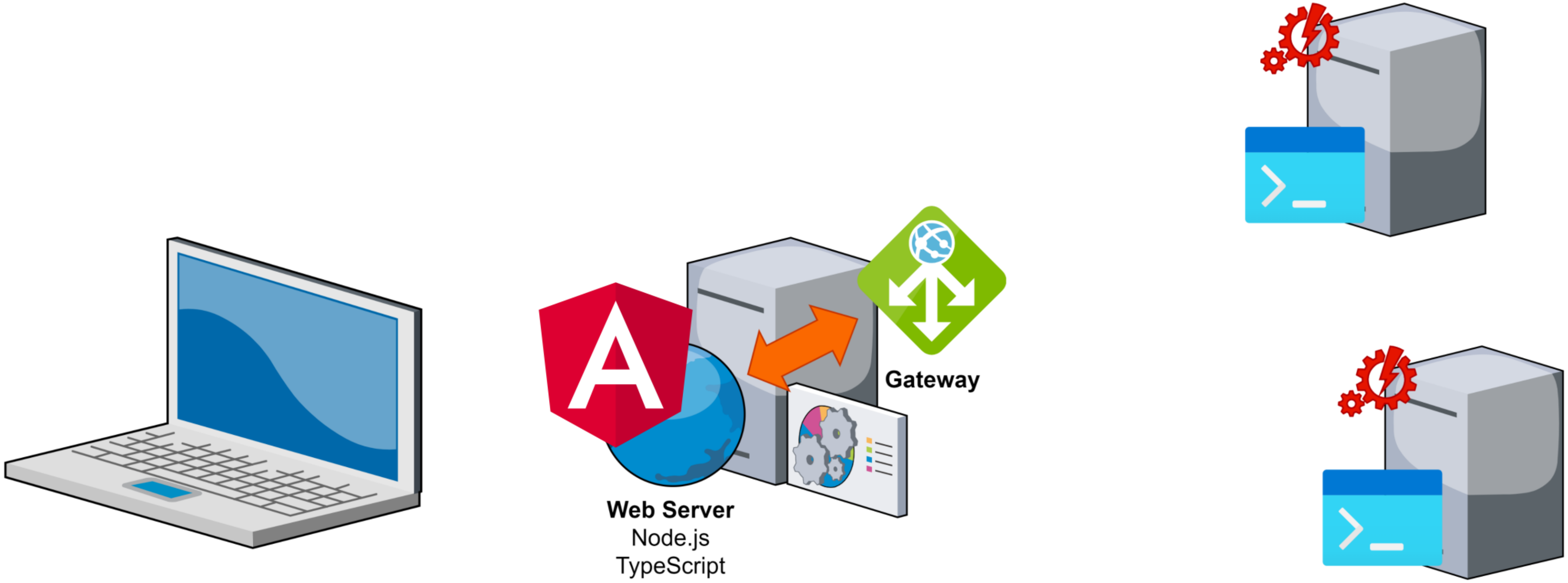
Azure Arc status: Not installed

CPU: Utilization 39.84%, Handles 23276, Speed 2.40GHz, Processes 58, Threads 899

Memory: Utilization 82.71%, Committed 1.1GB, Total 1.2GB, Cached 50.5MB, In use 1006.5MB, Paged pool 56.4MB, Available 210.5MB, Non-paged pool 37MB

@cj_berlin

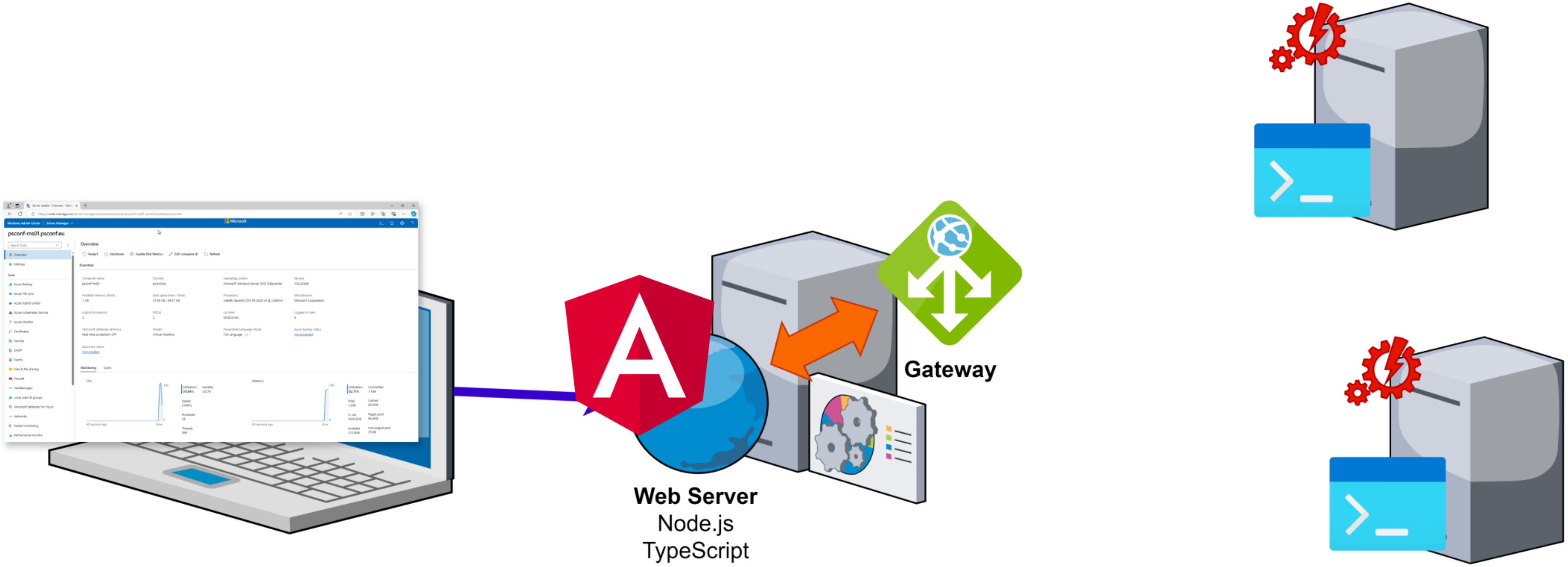
How it *really* works



Web Server
Node.js
TypeScript

Gateway

How it *really* works



Windows Admin Center | Server Manager

psconf-ms01.psconf.eu

Overview

Restart | Shutdown | Enable Disk Metrics | Edit computer ID | Refresh

Essentials

Computer name: psconf-ms01

Operating system: Microsoft Windows Server 2022 Datacenter

Manufacturer: Microsoft Corporation

Logical processors: 2

NIC(s): 2

Logged in users: 0

Microsoft Defender Antivirus: Real-time protection: Off

Model: Virtual Machine

PowerShell Language Mode: Full Language

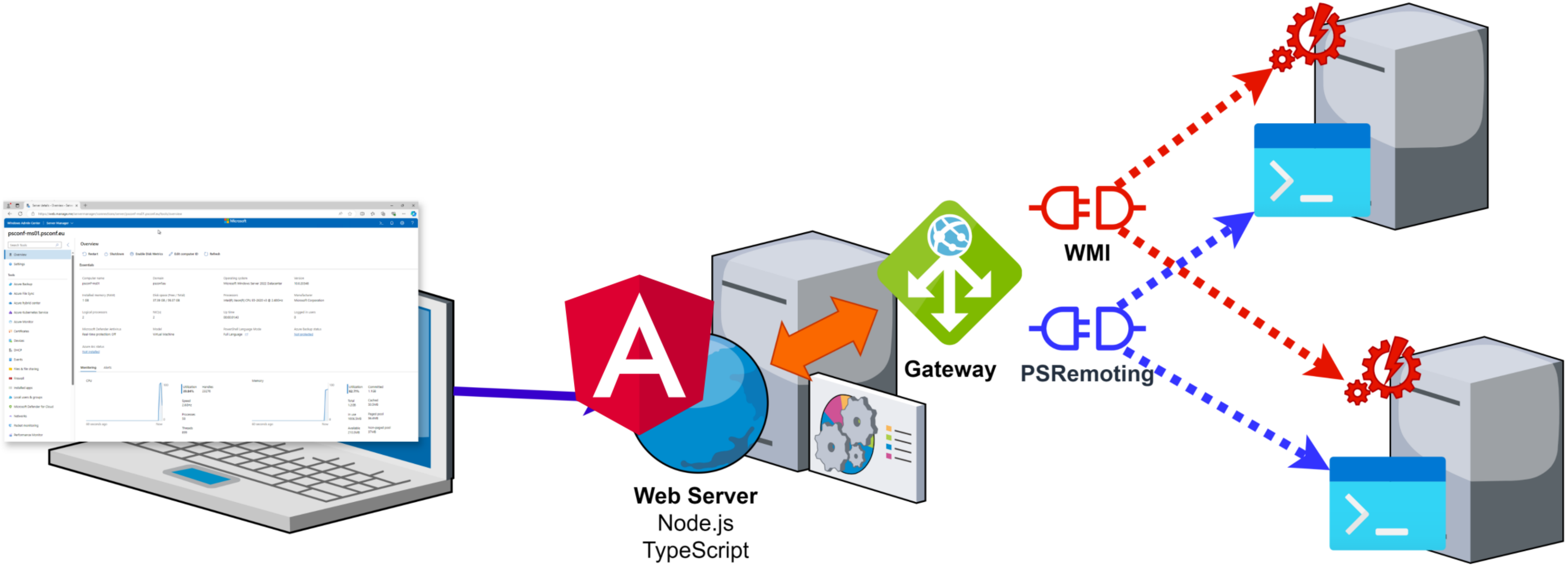
Azure Backup status: Not protected

Azure Arc status: Not installed

Monitoring | Alerts

@cj_berlin

How it *really* works



psconf-ms01.psconf.eu

Overview

Essentials

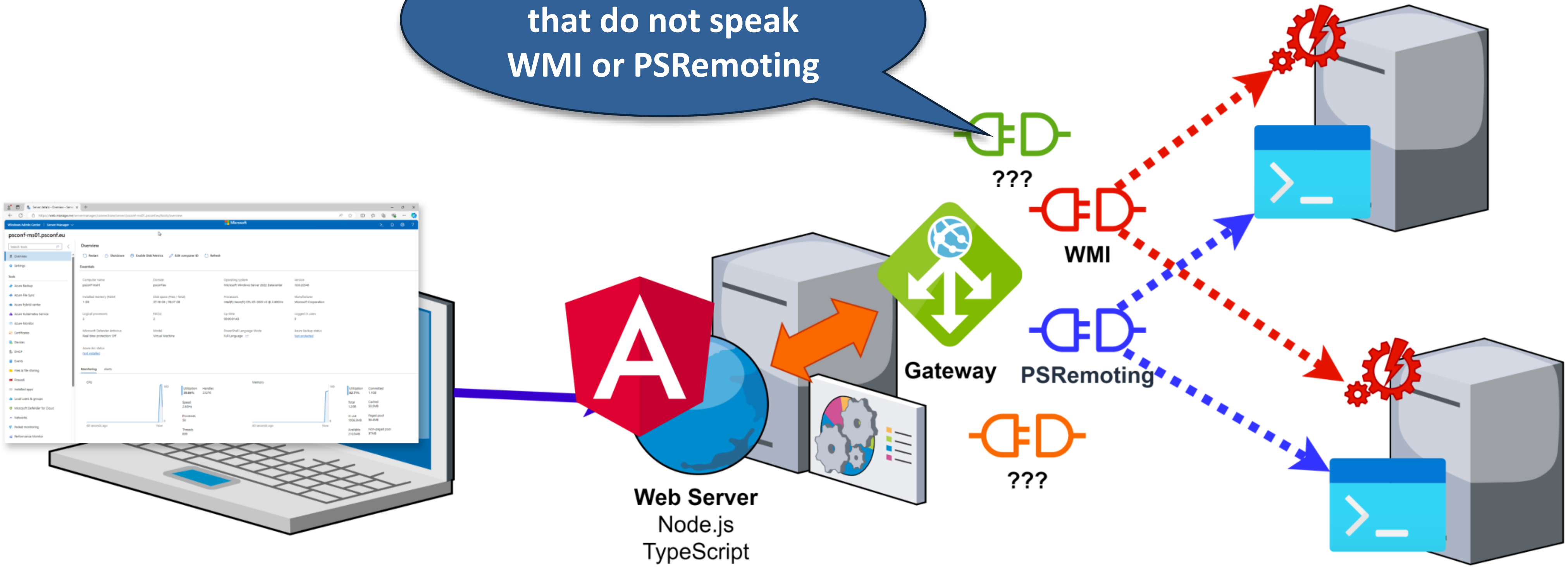
Computer name: psconf-ms01
Domain: psconf.eu
Operating system: Microsoft Windows Server 2022 Datacenter
Installed memory (RAM): 1 GB
Logical processors: 2
NIC(s): 2
Microsoft Defender Antivirus: Real-time protection: Off
Model: Virtual Machine
PowerShell Language Mode: Full Language
Azure Backup status: Not protected
Azure Arc status: Not installed

X @cj_berlin

Extending WAC: Gateway Plugins

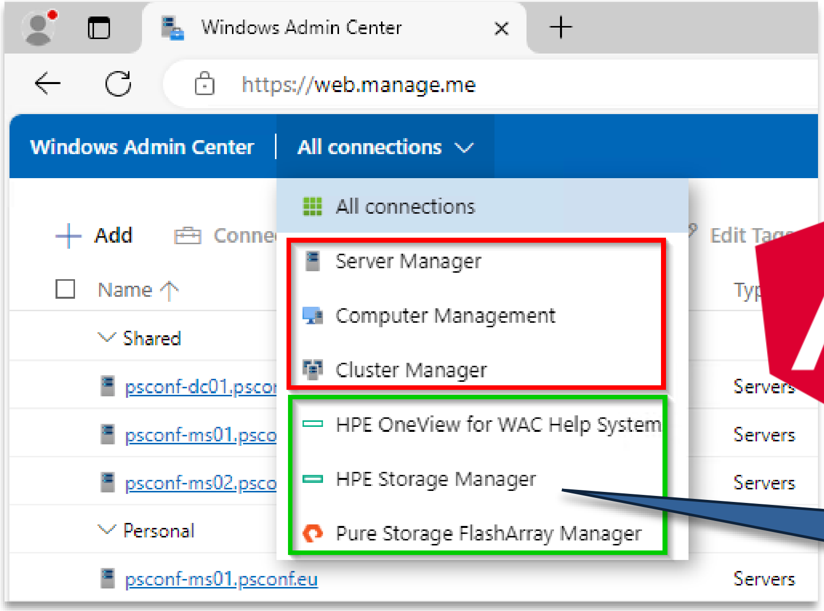
PSCONF.EU Antwerp24

Connect to systems that do not speak WMI or PSRemoting



@cj_berlin

Extending WAC: Solutions



Windows Admin Center × +

https://web.manage.me

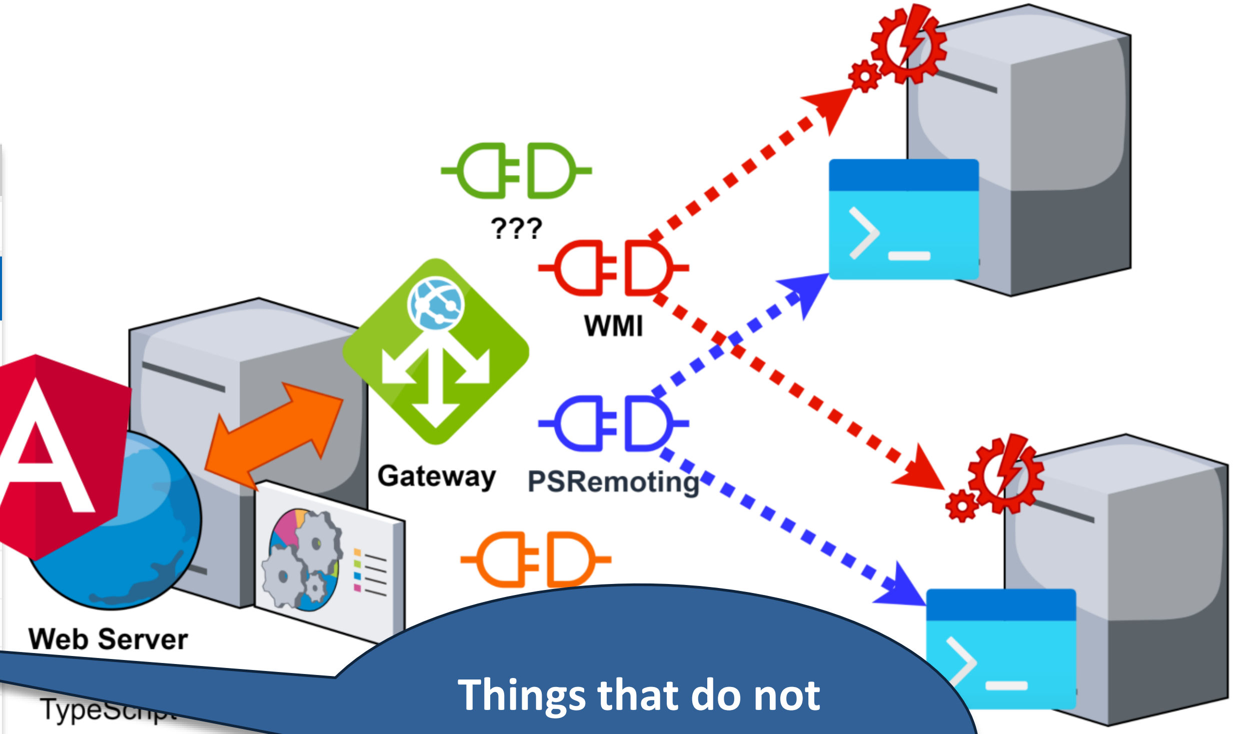
Windows Admin Center | All connections

+ Add   Conne…   Edit Tag…

□ Name ↑   Typ…

- Shared
  - psconf-dc01.psco…   Servers
  - psconf-ms01.psco…   Servers
  - psconf-ms02.psco…   Servers
- Personal
  - psconf-ms01.psconf.eu   Servers

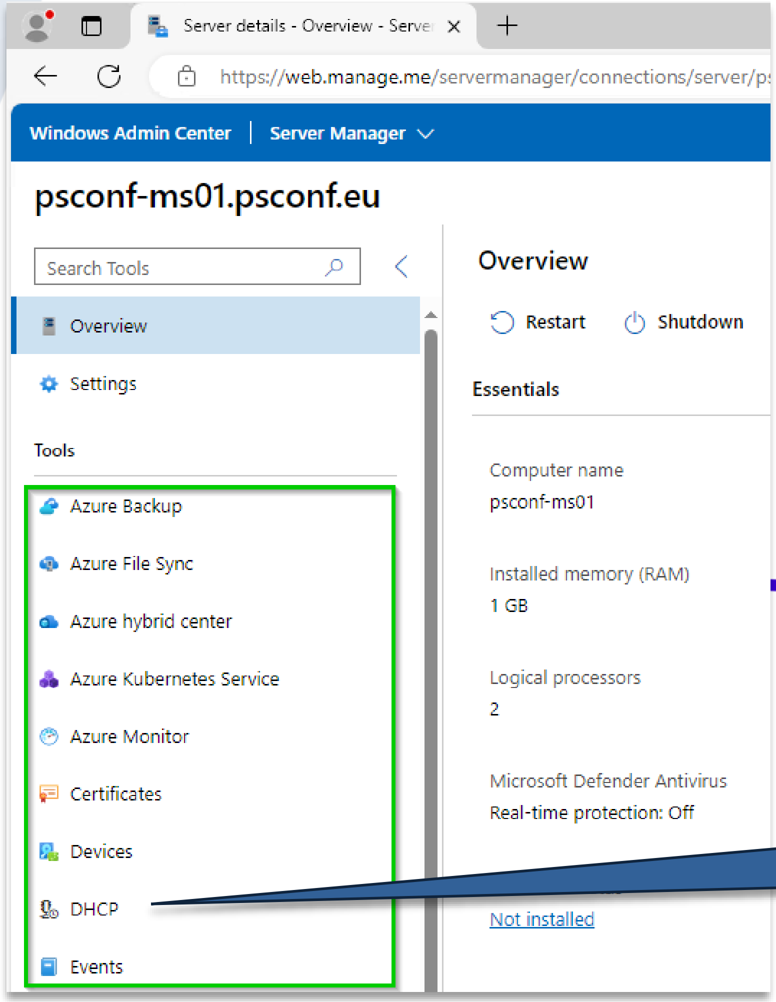
- All connections
- Server Manager
- Computer Management
- Cluster Manager
- HPE OneView for WAC Help System
- HPE Storage Manager
- Pure Storage FlashArray Manager



Things that do not lend themslves well to server-centric view

@cj_berlin

Extending WAC: Tools!



Server details - Overview - Server

https://web.manage.me/servermanager/connections/server/ps

Windows Admin Center | Server Manager

psconf-ms01.psconf.eu

Search Tools

- Overview
- Settings

Tools

- Azure Backup
- Azure File Sync
- Azure hybrid center
- Azure Kubernetes Service
- Azure Monitor
- Certificates
- Devices
- DHCP
- Events

Overview

Restart Shutdown

Essentials

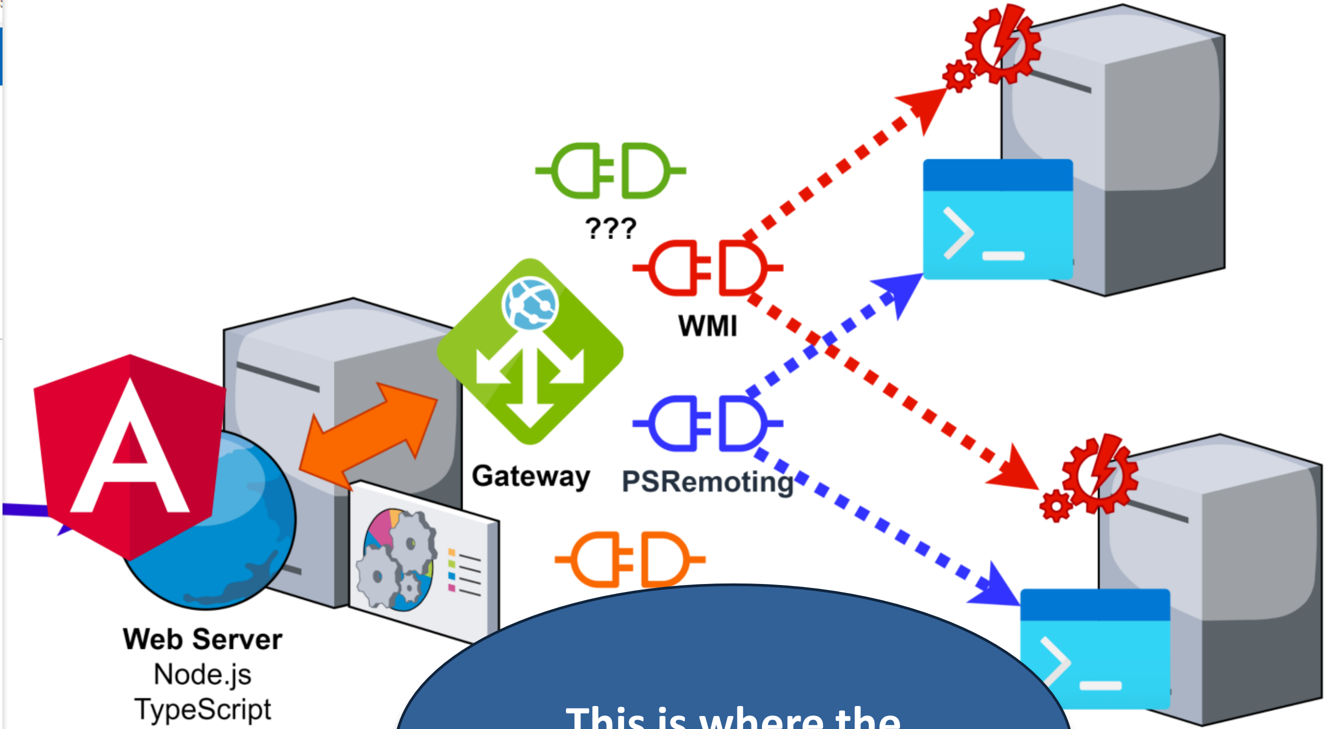
Computer name
psconf-ms01

Installed memory (RAM)
1 GB

Logical processors
2

Microsoft Defender Antivirus
Real-time protection: Off

Not installed



This is where the magic happens ☺

@cj_berlin

How WAC Tools work

…with PowerShell

@cj_berlin

WAC wasn‘t always WAC ☺

- Server Management Gateway
  - That‘s where you find it in the registry and also in %ProgramData%
- SME = Server Management Experience
  - Directly related to PowerShell functionality

When WAC tools run PowerShell

- On connection, to determine own visibility
  - For every installed extension, the entry point is examined
  - Conditions include: localhost, inventory or script result
  - Embedded in manifest (can point to file)
- On tool subpage load, to produce initial inventory
  - Embedded in TypeScript code or loaded from file
- On user actions on tool subpage
  - Embedded in TypeScript code or loaded from file

How WAC tools run PowerShell

- Not at all
  - if WMI or other gateway plug-in is being used
- Against the `Microsoft.PowerShell` endpoint
  - if the connecting user is local administrator, the connection will succeed
  - if the user is just a member of RM Users, the connection will gracefully fail („blocked by RBAC“)
- Against the `Microsoft.SME.PowerShell` endpoint

That‘s how we introduce RBAC!

- Place an RBAC policy file on each managed node
- Use the SME endpoint to allow everybody (entitled) to connect
- Evaluate **`$PSSenderInfo`** against the RBAC policy
- Proceed accordingly

The road ahead

a.k.a. “Wishful Thinking”

@cj_berlin

Making WAC enterprise-ready (i)

- **Delegation** – because no one should have admin rights
  - Achieved by moving all logic to the **SME** endpoint and incorporating RBAC into remote modules
- **Limiting visibility early** – not waste time and screen estate
  - Visibility script runs on the target (managed node) but that has knowledge of RBAC so can provide the answer quickly
- **RBAC** – well, because ☺

Making WAC enterprise-ready (ii)

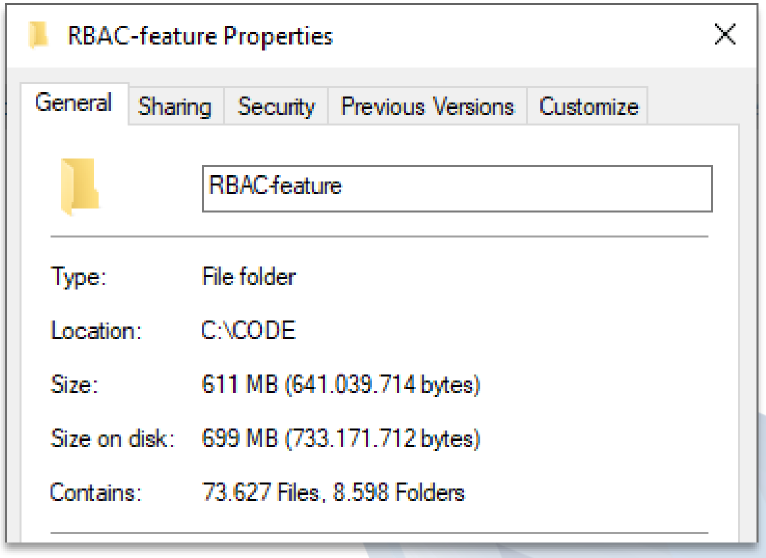
- **Connection management** – because what you don‘t see is what you don‘t get
  - Probably not customizeable in WAC (built-in functionality)
  - Can be worked around by using a user-mode script for injecting personal connections according to RBAC

Short term, long term…

- In the short term, any extensions that are primed for built-in RBAC…
  - Use delegation already
  - Can be RBAC‘d by editing their modules in the node-local package
- In the long term, all other extensions will have to be re-done from scratch…
  - Unfortunately, the source is not available, just the artifacts

Developing your own extensions

- Documentation is… well.. published… and so is an SDK
  https://aka.ms/wacsdkdocs
- Blank tool extension template has 70+ K files and takes up 700+ MB disk space
- Files missing, known vulnerabilities
- Front-End dev kit in PowerPoint ☺
- Trial, error and TypeScript knowledge



RBAC-feature

Type: File folder

Location: C:\CODE

Size: 611 MB (641.039.714 bytes)

Size on disk: 699 MB (733.171.712 bytes)

Contains: 73.627 Files, 8.598 Folders

@cj_berlin

State of the WAC SDK today

- Generally screwed up on all fronts:
- Dependencies
- Package versions
- Example code
- Documentation

Don‘t blame me ☺

wacextensionrequest@microsoft.com

Providing your own extensions

- Just like with PowerShell modules, really ;-)
- A WAC feed is just a NuGet feed…
- …so can be a file share, Azure Artifacts or other stuff: https://learn.microsoft.com/en-us/nuget/hosting-packages/overview
- Can even be a local path on the WAC server!
- Of course, you can try to get Microsoft to publish them for everyone…

Resources

- https://aka.ms/wacsdkdocs
- https://github.com/microsoft/windows-admin-center-sdk
- https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/extend/develop-tool
- https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/extend/guides/powershell

Q&A

15 minutes

PSCONF.EU
Antwerp24

@cj_berlin