PowerShell Conference Europe

Putting JEA to Good Use on Hyper-V Clusters

Evgenij Smirnov

PRAGUE23

Many thanks to our sponsors:

Centino systems

PATCH MY PC

ScriptRunner®
The #1 for PowerShell Management

MVP Microsoft® Most Valuable Professional

@cj_berlin

Evgenij Smirnov

- Born in Riga 1972, lives in Berlin since 1994
- 25+ years of infrastructure consulting
- Senior Solutions Architect @ **Semperis**
- User Group Lead: WSUGB, PSUGB, EXUSG
- MVP Cloud & Datacentre Management
- Blog: it-pro-berlin.de
- Speaker: PSConfEU, CIM, PSDAY.UK, SS2022

Microsoft® Most Valuable Professional

@cj_berlin

In this session

- The Objective
- The Problem | Solution architectures
- Level 200
- Level 300
- Level 400 | and above
- Things still left to do ☺

Not in this session

- AI
- PowerShell 7
  - although parts will absolutely work in 7
- Windows Terminal
  - see above
- Cloud
  - Azure Arc edition coming at a future time

The Objective

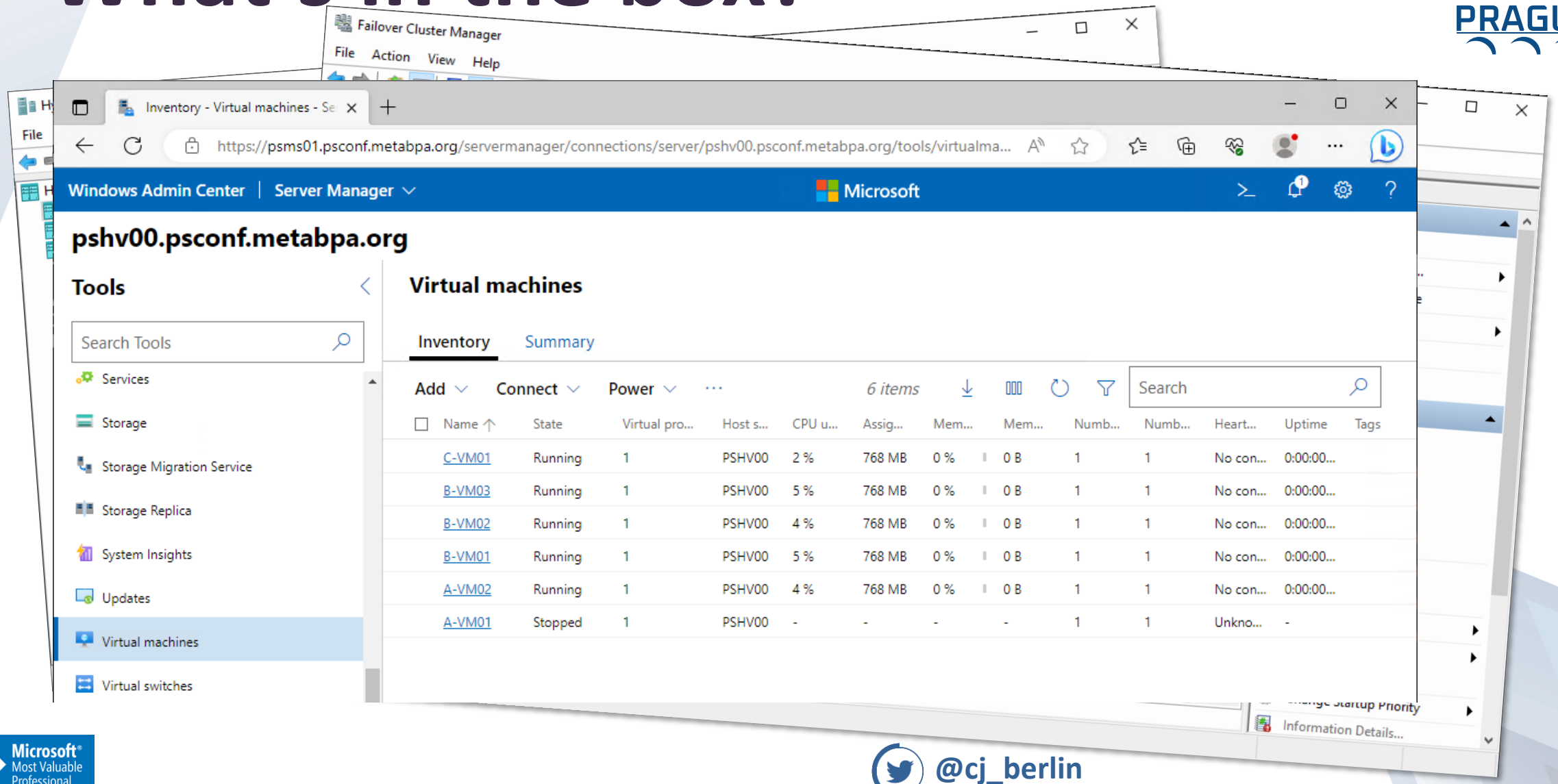
NIST 800-125A | HY-SR-18

"The access control solution for **VM administration** *should have a* **granular capability**, *both at the* **permission assignment level** *and the* **object level** *(i.e., the specification of the target of the permission can be a single VM or any logical grouping of VMs based on function or location).*

In addition, the ability to deny permission to some specific objects within a VM group (e.g., VMs running workloads of a particular sensitivity level) in spite of having access permission to the VM group should exist."


@cj_berlin

What's in the box?



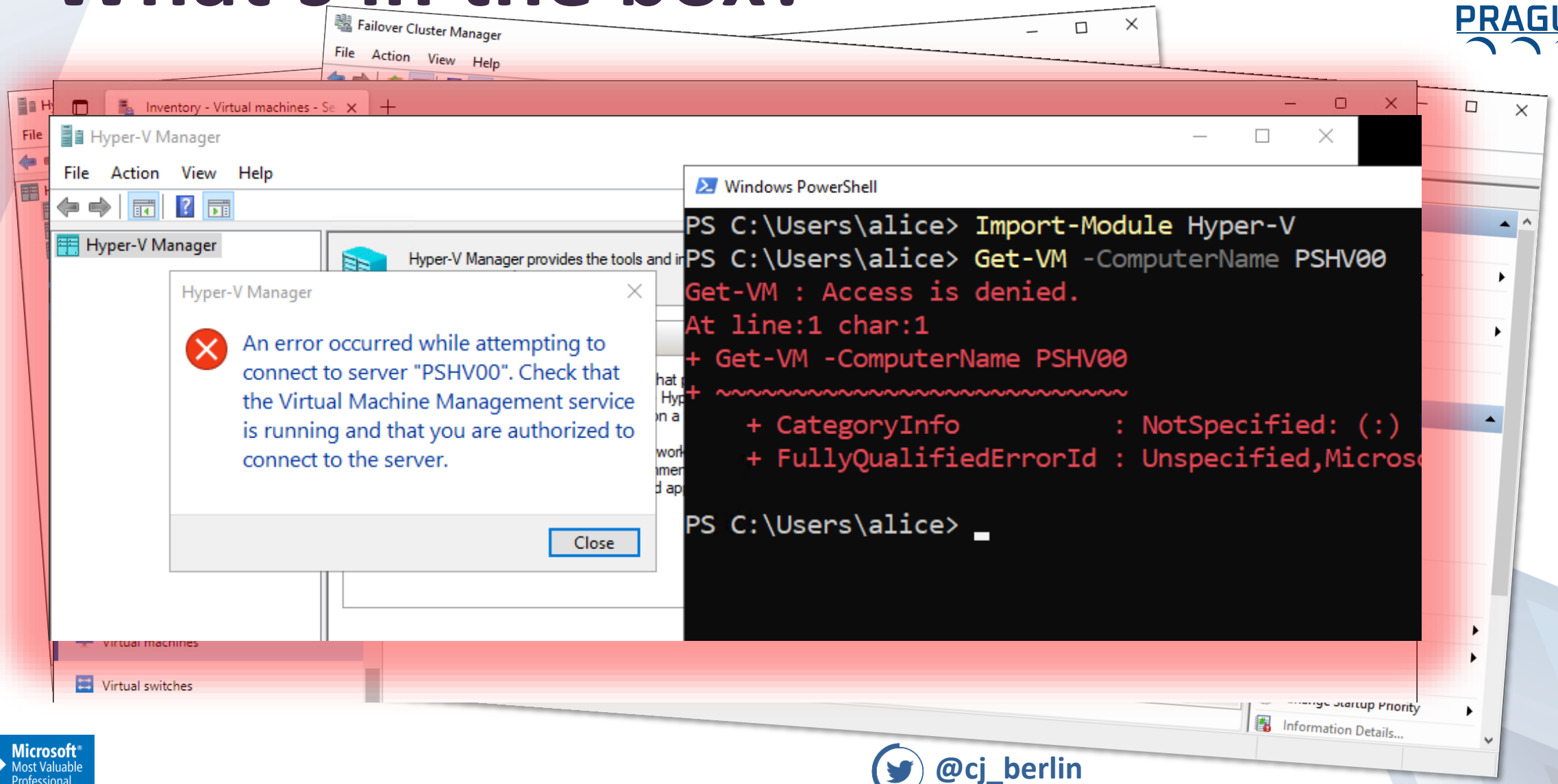
@cj_berlin

Microsoft® Most Valuable Professional

The Problem

@cj_berlin

What's in the box?



@cj_berlin

Solution approaches

- Have an agent installed on every host and RBAC within the server side of the solution → SCVMM
- Use a God-level account for remote administration and RBAC within the solution → HVManager 
- JEA?

JEA TLDR;

PSCONF.EU PRAGUE23

- By having users connect to a certain **WinRM** endpoint
- We can ~~severely restrict~~ precisely describe what they are allowed to do...
  - modules, cmdlets, parameter of cmdlets, values of parms
- ...but the allowed actions will be carried out under a different security context
  - hopefully permitted to perform the requested operation
  - by default → virtul local account with local admin rights

Level 200

Bits & Pieces

@cj_berlin

The „classic“ JEA approach…

```
Get-VM -Name <VM01 | VM02 | …>
Stop-VM -Name <VM01 | VM02 | …>
Get-VM -Name <VM01 | VM02 | …> | Stop-VM
```

If we impose restrictions on the values for -Name,

`Get-VM`

without parameters **will not work anymore**!

The „classic“ JEA approach…

- We could achieve granularity in VMs…
- …and/or in possible actions…
- …but not in a convenient, PowerShell-y manner!

- Besides, the role capabilities are static
  so any change in permissions (or VM grouping)
  would result in recreation of the endpoint!

The intelligent JEA approach

- For the more dynamic approach, we need following information within the remote session:
  - VM and permissions topology *at execution time*
  - Identity or, better still, role affiliation of the caller (*since the JEA session is running as an Admin, $env:USERNAME cannot be processed directly*)
- Topology → needs some kind of data store
- Identity → `$PSSenderInfo.UserInfo.WindowsIdentity.Groups`

Demo (Level 200)

Basic dynamic administration – restricted VMs, restricted actions

PSCONF.EU
PRAGUE23

MVP Microsoft® Most Valuable Professional

@cj_berlin

Level 300

Catering to more demanding clients

@cj_berlin

Named endpoints are Bah!

- Users will keep forgetting to use
  `-ConfigurationName AwesomeHyperVManagement`
  and will get frustrated → request admin rights
- You can redefine the default endpoint
  but have to add an „Allow All“ role capability for:
  - NT AUTHORITY\INTERACTIVE
  - BUILTIN\Administrators
  - BUILTIN\Remote Management Users

DO NOT DO IT!

PSCONF.EU PRAGUE23

Microsoft MVP Most Valuable Professional

@cj_berlin

If you do: Recreating the defaults


```
PS> Unregister-PSSessionConfiguration
    -Name Microsoft.PowerShell
    -Force
PS> Enable-PSRemoting -Force
```

@cj_berlin

Custom cmdlet names are Bah!

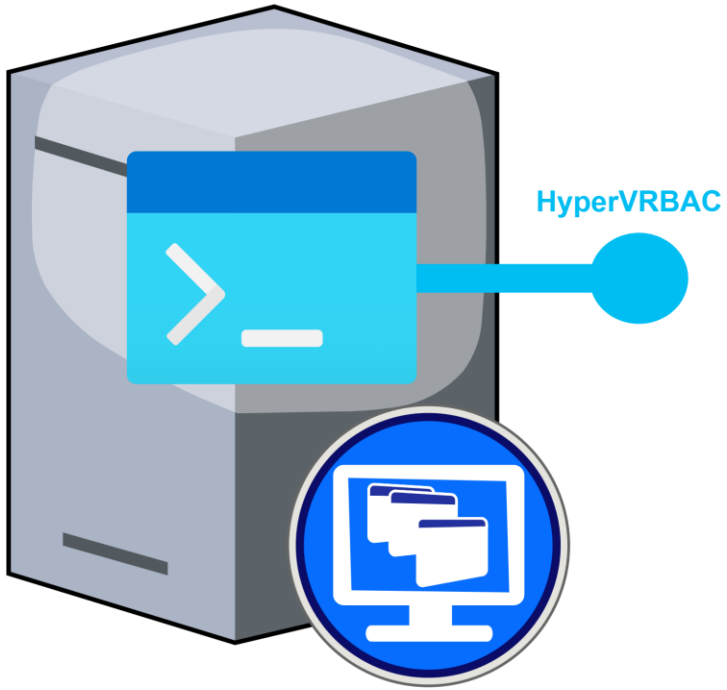
PSCONF.EU
PRAGUE23

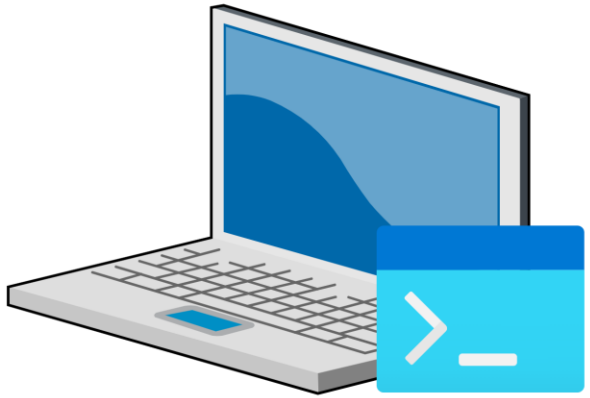
- Users will keep forgetting to use `Get-MyAllowedVM | Start-MyAllowedVM` and will get frustrated
- By using „proxy functions“ (i.e. overwriting cmdlet names with your function names) you can provide them with the commands they know… but ~~may~~ will behave differently!
- This can be both a **curse** and a **blessing**!

A slightly different approach…

- Even full Hyper-V Admins would rather use
  ```
  Get-VM -ComputerName HOST007
  ```
  than
  ```
  Invoke-Command { Get-VM } -ComputerName HOST007
  ```
  or
  ```
  Enter-PSSession -ComputerName HOST007
  Get-VM
  ```
- …which gives us a good way to hide the **Bah** stuff ☺

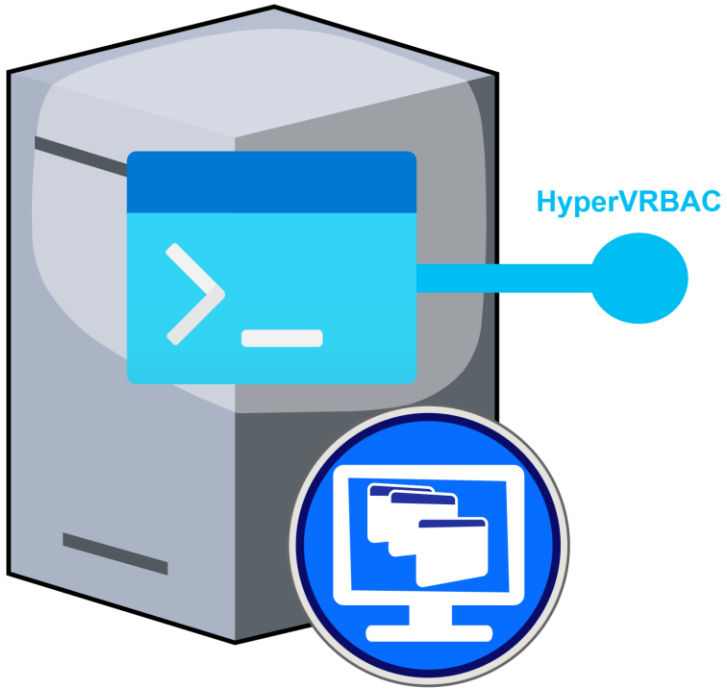
A slightly different approach…

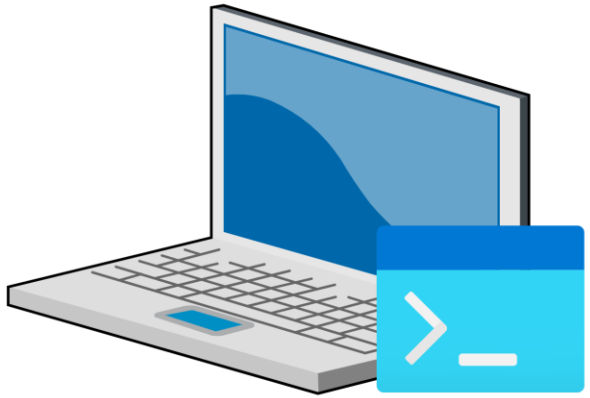




```
PS> Import-Module HyperVManagement
PS> Get-VM -ComputerName HOST007
```

A slightly different approach…

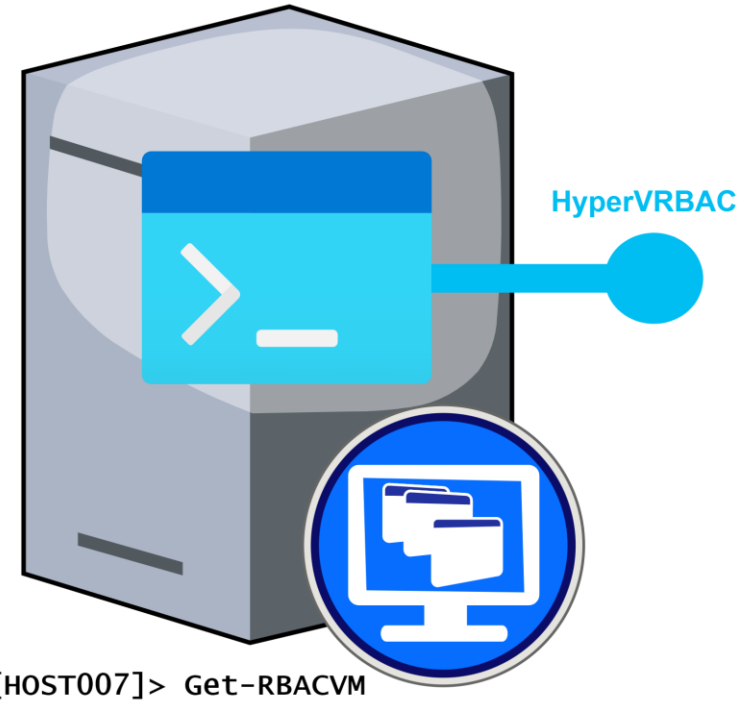




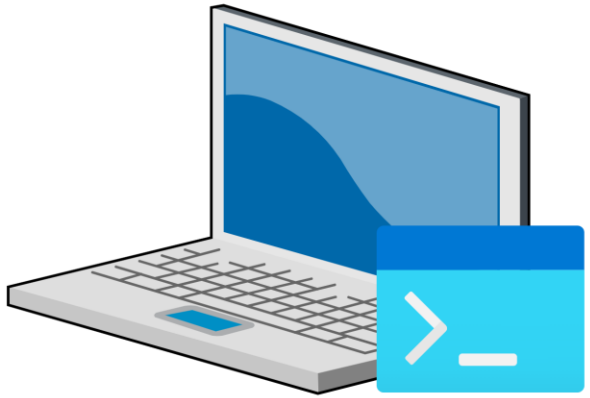
```
PS> Import-Module HyperVManagement
PS> Get-VM -ComputerName HOST007
{
    Invoke-Command
        -ComputerName HOST007
        -ConfigurationName HyperVRBAC
        -ScriptBlock {
                Get-RBACVM
            }
}
```

@cj_berlin

A slightly different approach…




```
PS[HOST007]> Get-RBACVM
{
    <determine user connecting from client>
    <determine VMs user is entitled to see>
    Hyper-V\Get-VM -Name $VMList
}
```



```
PS> Import-Module HyperVManagement
PS> Get-VM -ComputerName HOST007
{
    Invoke-Command
        -ComputerName HOST007
        -ConfigurationName HyperVRBAC
        -ScriptBlock {
                Get-RBACVM
            }
}
```

Demo (Level 300)

Faking the default administration

PSCONF.EU

PRAGUE23

MVP Microsoft® Most Valuable Professional

@cj_berlin

Things to consider

- Data is being passed between host and client
  - Might want to select a limited set of properties
- Raw Deserialized.* types are returned
  - Format definitions can be stolen from the official module

Level 400

Working with Clusters | Added Functionality

@cj_berlin

Working with Clusters

- Additional functionality:
  - Move VM from one node to another
- Additional hurdles:
  - Shared configuration store (*SQL?*)
  - Locating VM:
    PSSession connected to one node, VM is on another node
  - Moving VM is a WSFC operation, not a Hyper-V operation
  - Creating VM is both a WSFC and a Hyper-V operation

Authorization in Clusters

Use gMSA:

- gMSA must have admin permissions on cluster and all nodes
- gMSA could, in theory, get pwned independently of the cluster
- some orgs still do not like using gMSA

Use VA:

- every cluster node must have admin permissions on cluster and the other nodes
- this sort of configuration is potentially easier to maintain

Demo (Level 400)

Simple RBAC in Clusters

PSCONF.EU
PRAGUE23

MVP Microsoft® Most Valuable Professional

@cj_berlin

Adding Functionality (i)

Hiding the business logic behind a JEA endpoint allows you to offer VM admins additional functionality:

- Datastores → offering logical storage locations without disclosing physical paths behind them
  - Requires modification of VM objects before returning
- Cloning of template VMs
  - IMPORTANT → disclosure of VM names otherwise hidden
  - IMPORTANT → initial permissioning of new VMs

Adding Functionality (ii)

Hiding the business logic behind a JEA endpoint allows you to offer VM admins additional functionality:

- Tab completion for names of VMs available via RBAC

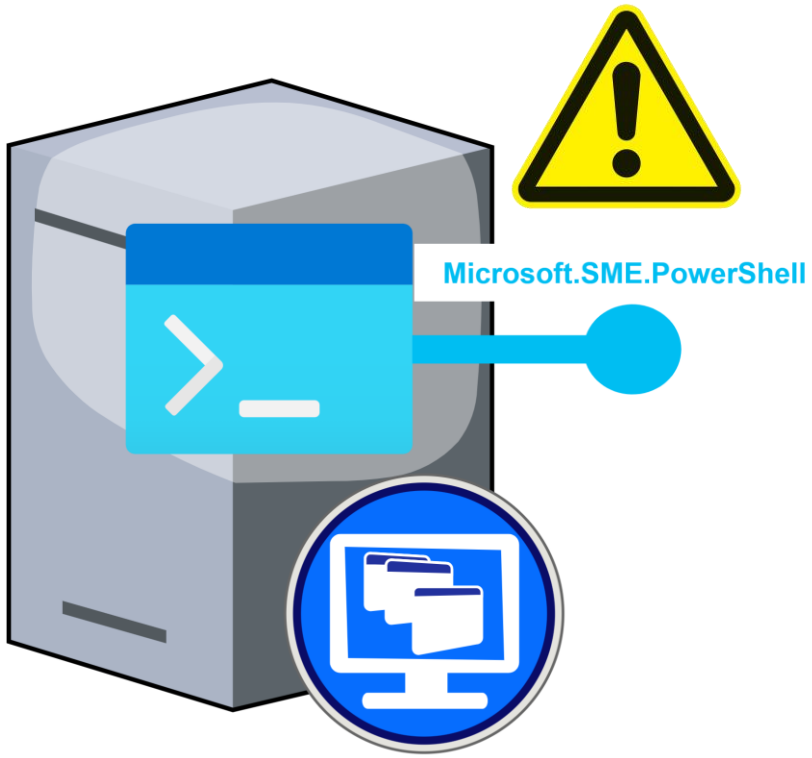
- Weird and exciting stuff ☺
  - Integrating other virtualization platforms
  - Approval workflows
  - Audit logging

Level 500

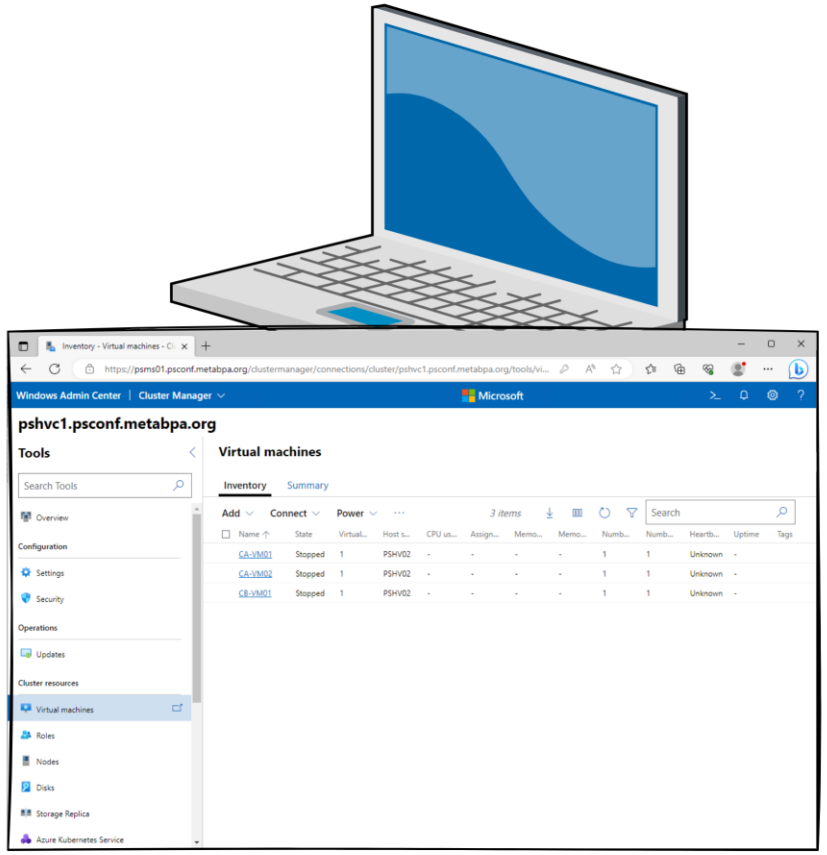
Cheating on WAC

@cj_berlin

WAC and RBAC




```
PS[HOST007]> function main([string]$vmId)
{
    $vm = Get-VM -Id $vmId
    ...
}
```



@cj_berlin

Demo (Level 500)

Wacky WAC

PSCONF.EU
PRAGUE23

Microsoft MVP Most Valuable Professional

@cj_berlin

Things still left to do…

@cj_berlin

Things left to do (i)

- Decide upon architecture(s)
- Implement all the things ☺
- Central config store with local caching
- Human-friendly management interface
  - For WAC: a WAC extension would be great

Things left to do (ii)

- Console connections
  - WAC uses RDP+CredSSP to provide credentials (but the user must be authorized for it to work)
  - JEA endpoint (running on host) does not help much, unless we implement our own video transport for this
  - VMConnect.exe permissions must be figured out
  - Endpoint initialization must perform `Grant-VMConnectAccess` / `Revoke-VMConnectAccess`

Q&A

15 minutes, they said…

PSCONF.EU
PRAGUE23

MVP Microsoft® Most Valuable Professional

@cj_berlin

Thank you!

Code mentioned and shown in this session:

https://github.com/metabpa/hyper-v-rbac

will go public on 2023-06-26!

Blog post series on RBAC-enabling WAC coming: https://it-pro-berlin.de

Demo code & Slides: https://github.com/psconfeu/2023

Microsoft MVP Most Valuable Professional

@cj_berlin