LIVE! 360
TECH EVENTS WITH PERSPECTIVE

Visual Studio LIVE! · SQL Server LIVE! · TECHMENTOR · Office & SharePoint LIVE! · Artificial Intelligence LIVE! · Cloud & Containers LIVE!

Secure Remote Management with Just Enough Administration (JEA)

Jeff Hicks
PSSensei
@jeffhicks

Level:
Intro/Intermediate

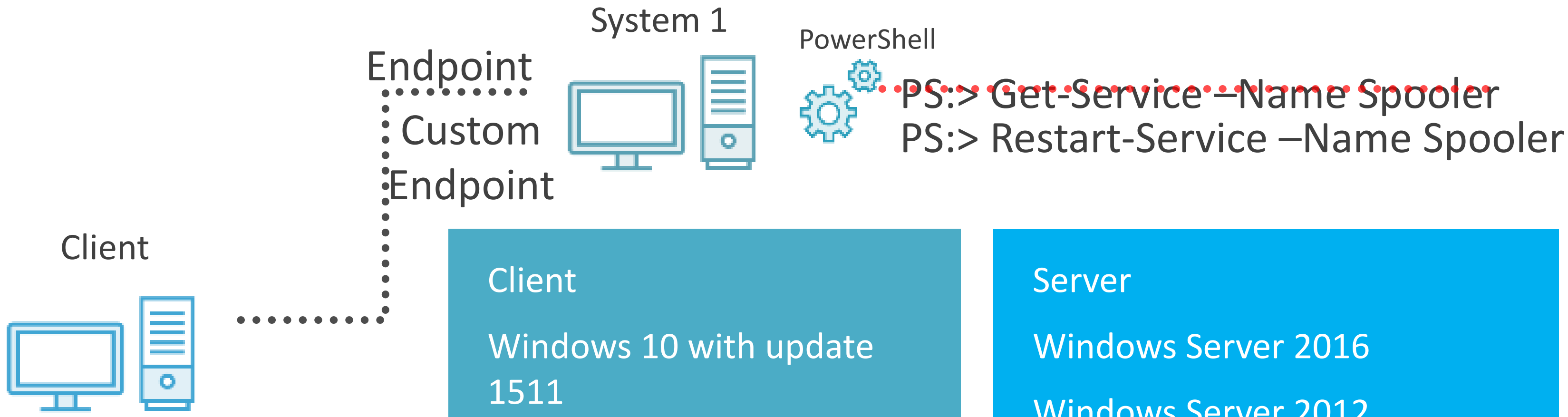
The Ultimate Education Destination
ORLANDO 2019

What Is this About?

- Remote PowerShelll management requires full administrator access
- You may need to provide more limited or constrained access
- We’ve been able to do this all along…
- JEA makes it easier

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

Requirements for JEA



```
PS:> Get-Service –Name Spooler
PS:> Restart-Service –Name Spooler
```

Client

Windows 10 with update 1511

Windows 8, 8.1

Windows 7*

Server

Windows Server 2016

Windows Server 2012,

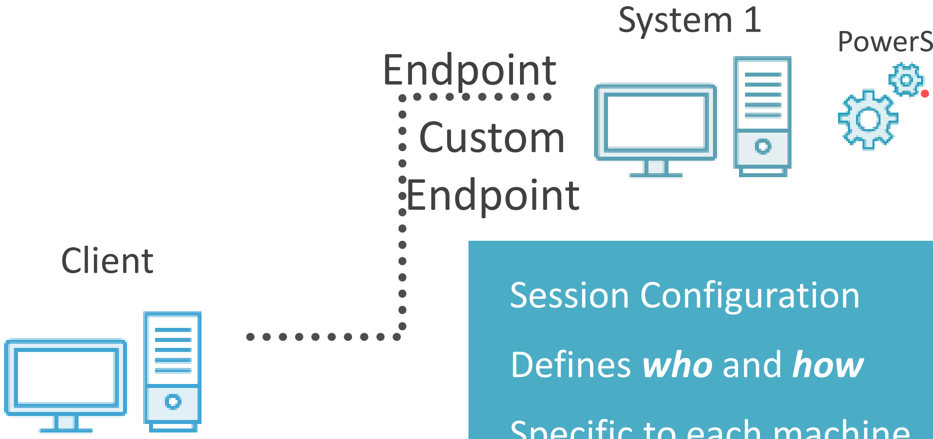
2012 R2

Windows Server 2008R2*

Windows Management Framework 5 or above

* Support for virtual account not currently available

PS Remoting with JEA



```
PS:> Get-Service –Name Spooler
PS:> Restart-Service –Name Spooler
```

Session Configuration

Defines ***who*** and ***how***

Specific to each machine

(.pssc) file

Role Capability

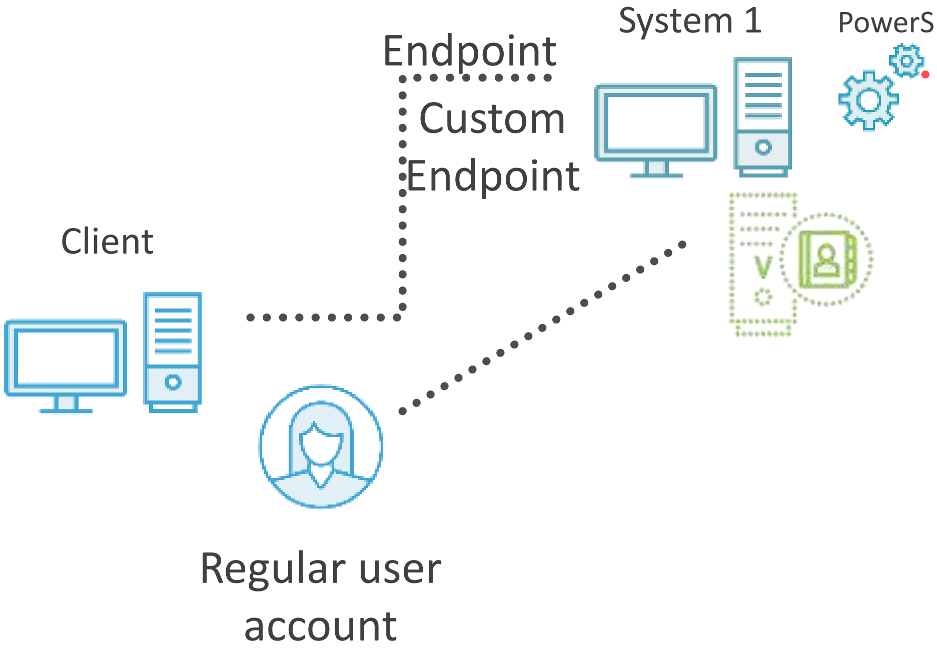
Defines *what* users can do

Can be shared across environment

(.psrc) file

JEA and Virtual Accounts

Currently does not work for Windows 7 or Windows Server 2008R2



```
PS:> Get-Service –Name Spooler
PS:> Restart-Service –Name Spooler
```

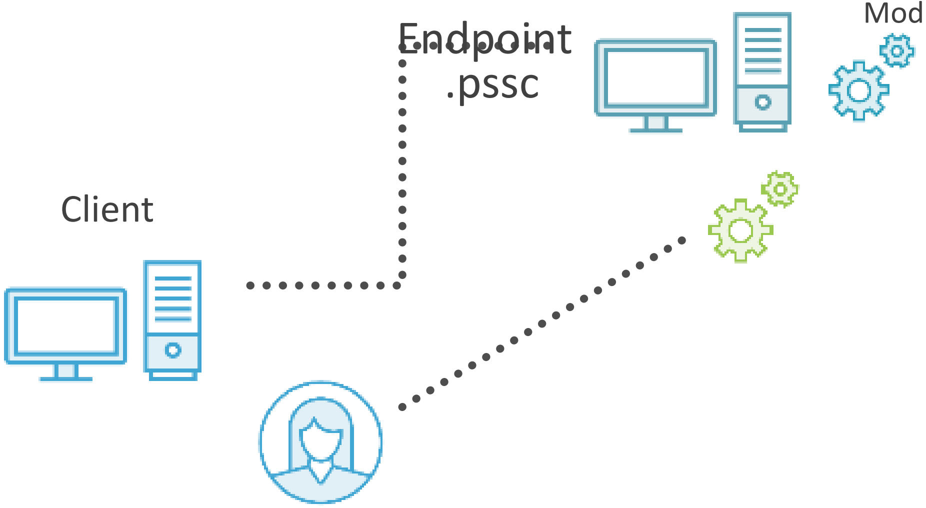
Virtual Accounts

One time privileged account

Runs under local Administrator

Can be configured for other accounts

Automated Deployment



Custom Endpoint .pssc

System 1

Module with Role capability file

```
PS:> Get-Service –Name Spooler
PS:> Restart-Service –Name Spooler
```

Client

Run Registration Script

Deployment

Copy module to target

Copy session config to target

Register Endpoint

Benefits

- Reduce the number of excessive privileged accounts
- Easy to create and manage endpoints
- Decide exactly what an administrator can do
- See what administrators are doing

Challenges

- Many administrators still use older GUI based applications
- PowerShell proficiency is mandatory
- Understanding the exact needs of an administrative role
- Handling emergencies (“Break the glass”)
- Rolling out with educated administrators

Process

1. Identify the Role and the tasks that need to be enabled
2. Restrict those tasks as needed
3. Put them in a Role Capability file
4. Register the Session Configuration through automation or DSC
5. Test and correct as needed

Pilot to Production

Work with administrators that have the required PowerShell skills

Define and create roles

Create a “BreakTheGlass” endpoint for emergencies

Test and correct on a few ”Pilot” servers

Begin roll-out to other servers

SHOW ME

Stay in Touch

- @jeffhicks
- https://jdhitsolutions.com
- https://github.com/jdhitsolutions
- https://www.pluralsight.com/authors/jeff-hicks
- https://leanpub.com/u/jeffhicks

MVP Microsoft® Most Valuable Professional

LIVE! 360
TECH EVENTS WITH PERSPECTIVE