

# Conference Notes

## Fall 2018

Microsoft  
Ignite



<https://myignite.techcommunity.microsoft.com/videos?p=3&t=%257B%2522from%2522%253A%25222018-09-23T08%253A00%253A00-04%253A00%2522%252C%2522to%2522%253A%25222018-09-28T19%253A00%253A00-04%253A00%2522%257D>

 Dog Food

The logo for Dog Food, featuring a stylized 'D' composed of four colored quadrants (red, green, blue, yellow) followed by the words 'Dog Food' in a white, sans-serif font on a grey background.

<https://dogfoodcon.com/>

## Upgrade Paradigm:

FAQ on Windows Server, version 1709 and Semi-Annual Channel

<https://cloudblogs.microsoft.com/windowsserver/2017/10/26/faq-on-windows-server-version-1709-and-semi-annual-channel/>

Say No to Long Term Servicing Channel (LTSC)

<https://blogs.technet.microsoft.com/ukplatforms/2018/06/11/say-no-to-long-term-servicing-channel-ltsc/>

### **LTSC (Long-Term Servicing Channel) formerly known as LTSB (Long-Term Servicing Branch):**

Long-Term Servicing Channel (LTSC) continues to have 5 years of mainstream support and 5 years of extended support, with a new release planned for every 2-3 years. Windows Server 2019 is the latest LTSC release.

LTSC recent:

- 2016 - 10/12/2016
- 2019 - 10/2/2018

### **SAC (semi-annual channel), formerly known as CBB (Current Branch for Business):**

The Semi-Annual Channel releases are supported for 18 months and a new release will be out twice a year. 1709 is the first release in the SAC.

1709 is not an update to Windows Server 2016. Instead, it is a new release in a different channel with a different support model. To move from Windows Server 2016 (or previous versions) to Windows Server, version 1709 you'll need to run a clean install. In-place upgrades are not supported as Windows Server 2016 is a LTSC release and version 1709 is a Semi-Annual Channel release and they have different support models.

1803 is the 2nd Semi-Annual Channel release

SAC offers no GUI. Windows Admin Center (code named Project Honolulu) was unveiled by Microsoft on September 14th, 2017 as the necessary evolution of the Windows Server GUI.

[https://en.wikipedia.org/wiki/Windows\\_Admin\\_Center](https://en.wikipedia.org/wiki/Windows_Admin_Center)

SAC (spring and fall release schedule) recent:

- 1709 - 10/17/2017
- 1803 - 5/7/2018

Build your Own Test Lab in Azure:

# Using Microsoft Azure

to build your own **Test Lab**



<https://daniellbenway.net/use-azure-to-build-your-test-lab/>

## Table of Contents:

Abstract: .....	2
Intended Audience: .....	2
Document Revision and History: .....	2
Freeware License and Disclaimer: .....	3
About the Author: .....	3
Special Thanks: .....	3
Table of Contents: .....	4
General Information: .....	5
Your Azure Bill: .....	6
Create Your Resource Groups: .....	10
Set Up Azure PowerShell: .....	11
Create Your Virtual Network: .....	13
Create Your VMs: .....	16
Create Your Test VMs (not the RDP Jump Box): .....	17
Create Your RDP Jump Box: .....	22
Create Automation Account and Runbook for Automatic Deallocation: .....	27
Security Center: .....	33
VM Update Management: .....	40
Azure Advisor: .....	42
Snapshotting Your VMs: .....	43
ARM Templates: .....	44

## Admin Center and Server Core

### **Admin Center and Server Core - presenter Jeff Woolsey**

- MMC paradigm is at end of useful life
- AC is agentless - is uses WinRM (ports 5985, 5986), WMI, PSh, JEA, etc..
- AC installs on 10, 16, or 19 and manages fully back to 12, and partially back to 08R2
- AC makes using Server Core a lot more appealing
  - what if NIC drivers are bad on a Core system? Install FOD (features on demand) on that system from KVM, FOD will give you a limited shell from which to repair the NIC
- AC is browser-based: it can be used on Windows, Mac, iOS, Android, etc..
- AC can be clustered to provide high-availability
- AC has a PSh plugin
- AC has an RDP plugin
- <http://aka.ms/WindowsAdminCenter>

Spin up your own Azure test lab and start learning Admin Center and Server Core!

# Azure Security Center:

Azure Security Center is offered in two tiers: Free and Standard. The Standard tier is free for the first 60 days, and any usage beyond 60 days will be automatically charged per a fee schedule. So for your test lab, make sure you use and configure at least the free tier.

Microsoft Azure

Search resources, services, and docs

Home > Security Center - Overview

### Security Center - Overview

Showing subscription 'Pay-As-You-Go'

Search (Ctrl+/)

Subscriptions

#### Policy & compliance

Subscription coverage

- Covered (standard): 0
- Covered (free): 1
- Not covered: 0

7 Covered resources

Policy compliance

Overall compliance: 36%

Least compliant subscriptions: Pay-As-You-Go

Show policy compliance of your environment >

#### Resource security hygiene

Secure score: 180 of 215

Resource health monitoring

- 6 Compute & apps
- 1 Data & storage
- 0 Networking
- 0 Identity

## Auto Provisioning

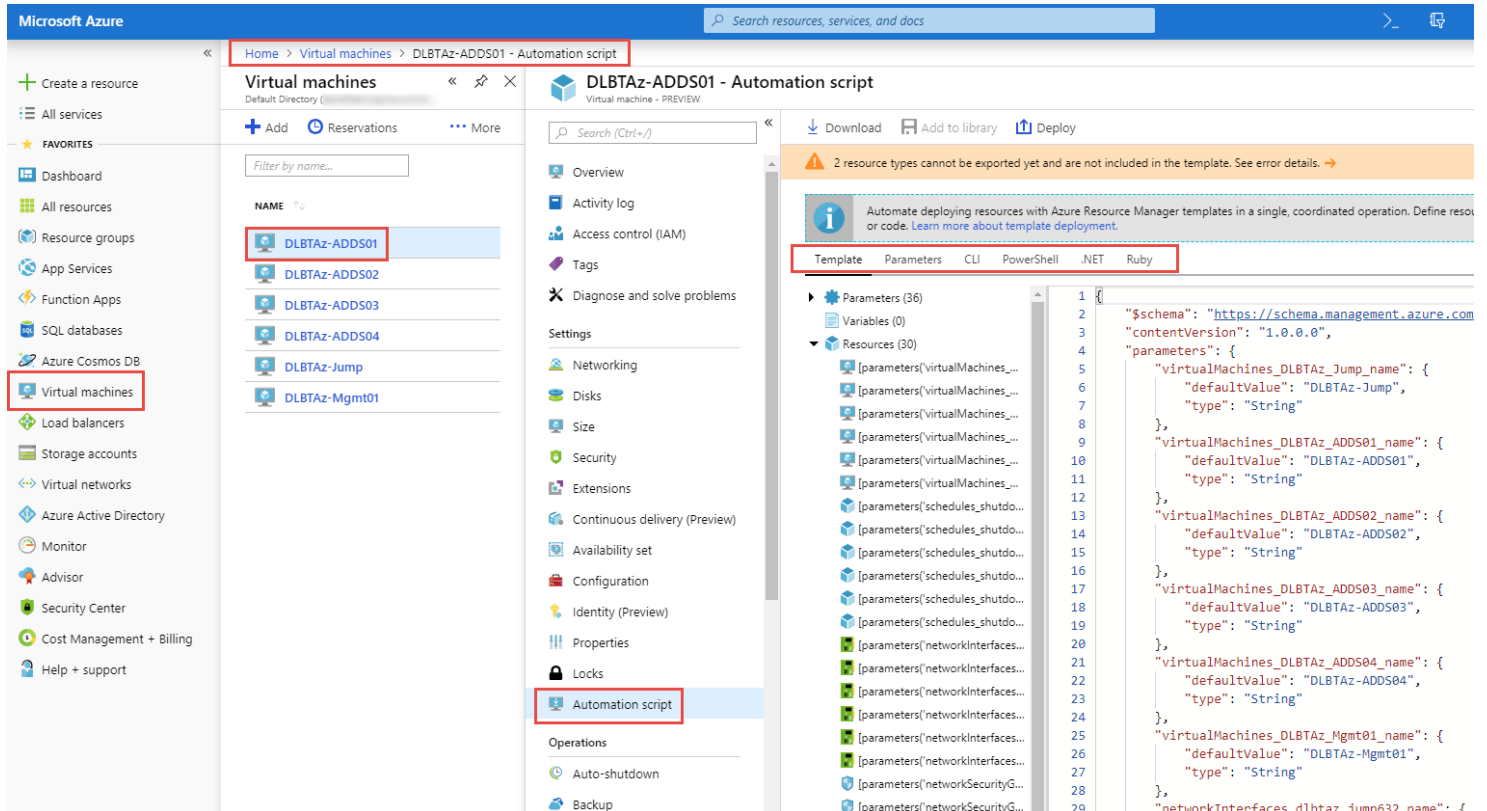
This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed agent will be provisioned. [Learn more >](#)

On  Off

<https://daniellbenway.net/use-azure-to-build-your-test-lab/>

## IaC - Infrastructure as Code:

- ARM (Azure resource manager) templates are the JSON code that can be used to deploy Azure IaaS resources
- ARM templates are typically paired with configuration files
- like PSh in modern OSs and applications, you can manually create something in Azure and then have Azure give you the ARM template for that action you just completed



The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top indicates the path: Home > Virtual machines > DLBTaz-ADDS01 - Automation script. The left sidebar shows the 'Virtual machines' service selected. The main content area displays the 'Automation script' page for the virtual machine 'DLBTaz-ADDS01'. The page includes a search bar, a list of virtual machines, and a detailed view of the automation script. The script is displayed in a code editor with a red box highlighting the 'Template' tab. The JSON code defines parameters for virtual machine names and network interfaces, such as 'virtualMachines\_DLBTaz\_Jump\_name', 'virtualMachines\_DLBTaz\_ADDS01\_name', 'virtualMachines\_DLBTaz\_ADDS02\_name', 'virtualMachines\_DLBTaz\_ADDS03\_name', 'virtualMachines\_DLBTaz\_ADDS04\_name', and 'networkInterfaces\_dlbtaz\_jump632\_name'.

<https://daniellbenway.net/use-azure-to-build-your-test-lab/>

## PSH (PowerShell Security and Tidbits):



- remember, PSh is a shell AND a scripting language (use it for BOTH)
- from Cmd.exe:
  - Powershell starts Windows PSh (a.k.a. FullCLR, built on .Net)
  - Pwsh starts PSh Core (a.k.a. CoreCLR, based on .Net Core, cross platform -- Windows, Mac, Linux, etc.)

### Key Takeaways

Use a layered approach to security.

PowerShell is a POST-exploitation tool, not a vulnerability.

PowerShell is the MOST security-featured scripting language.

Properly configured, PowerShell leaves glowing fingerprints.

Don't be afraid of PowerShell remoting. Lock it down with JEA.

Upgrade to PowerShell 5.1 and remove the PS 2.0 Windows Feature.

Security features are available cross-platform.

Lots of free information available if you are willing to find it.

THIS IS ALL FREE!

<https://www.slideshare.net/AshleyMcGlone/securing-powershell-with-free-techniques-dogfoodcon-2018>

- PSh 5.1 is considered 'complete' by MS.

“The improvements in WMF 5.0 (or WMF 4.0 with KB3000850) make PowerShell the worst tool of choice for a hacker when you enable script block logging and system-wide transcription. Hackers will leave fingerprints everywhere, unlike popular CMD utilities. For this reason, PowerShell should be the only tool you allow for remote administration.”

<https://blogs.technet.microsoft.com/ashleymcglone/2016/06/29/whos-afraid-of-powershell-security/>

Engine	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	Application Whitelisting	Antimalware Integration	Local Sandboxing	Remote Sandboxing	Untrusted Input Tracking
Bash	No**	No*	No	No	Yes	No	No*	Yes	No
CMD / BAT	No	No	No	No	Yes	No	No	No	No
Jscript	No	No	No	No	Yes	Yes	No	No	No
LUA	No	No	No	No	No	No	No*	Yes	Yes
Perl	No	No	No	No	No	No	No*	Yes	Yes
PHP	No	No	No	No	No	No	No*	Yes	Yes
PowerShell	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No**
Python	No	No	No	No	No	No	No	No	No**
Ruby	No	No	No	No	No	No	No**	No**	Yes
sh	No**	No*	No	No	No	No	No*	Yes	No
T-SQL	Yes	Yes	Yes	No	No	No	No**	No**	No
VBScript	No	No	No	No	Yes	Yes	No	No	No
zsh	No**	No*	No	No	No	No	No*	Yes	No

\* Feature exists, but cannot enforce by policy  
\*\* Experiments exist

<https://blogs.msdn.microsoft.com/powershell/2017/04/10/a-comparison-of-shell-and-scripting-language-security/>

# PowerShell Hygiene

Level 1: Implement and monitor: logging & transcription

Level 2: Enable and secure remoting (default endpoint, firewall)

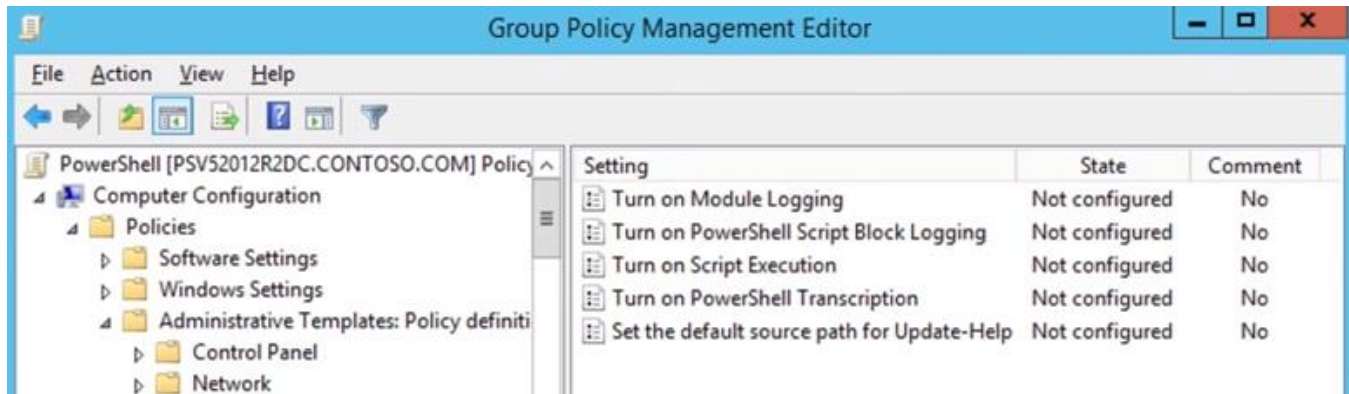
Level 3: Block evil code: AppLocker / DeviceGuard / AMSI



\*anti-malware scanning interface, which integrates with Windows Defender and many other AV products

<https://www.slideshare.net/AshleyMcGlone/securing-powershell-with-free-techniques-dogfoodcon-2018>

## Level 1:



<https://www.youtube.com/watch?v=NRnGP1RRNsM&t=275s>

- I think there's a way to encrypt these logs too
- GPO can also be used to set Execution Policy too

## Level 2:

Every Windows PowerShell session (PSSession) uses a session configuration, also known as an endpoint. When users create a session that connects to the computer, they can select a session configuration or use the default session configuration that is registered when you enable Windows PowerShell remoting.

<https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/Register-PSSessionConfiguration?view=powershell-5.1>



Reference:

- <https://www.slideshare.net/AshleyMcGlone/securing-powershell-with-free-techniques-dogfoodcon-2018>  
Securing PowerShell with Free Techniques - DogFoodCon 2018
- <https://www.youtube.com/watch?v=NRnGP1RRNsM&t=275s>  
Managing PowerShell in the Enterprise Using Group Policy
- <https://blogs.technet.microsoft.com/ashleymcglone/2016/06/29/whos-afraid-of-powershell-security/>
- <http://aka.ms/pssec>  
Who's afraid of PowerShell security?
- <https://github.com/GoateePFE>  
Ashley McGlone's GitHub
- <https://github.com/PowerShell/JEA>  
Just Enough Administration Samples and Resources
- <https://docs.microsoft.com/en-us/powershell/jea/overview>  
Just Enough Administration
- <https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/Register-PSSessionConfiguration?view=powershell-5.1>  
Register-PSSessionConfiguration
- <https://blogs.msdn.microsoft.com/powershell/2017/04/10/a-comparison-of-shell-and-scripting-language-security/>  
A Comparison of Shell and Scripting Language Security
- <https://blogs.technet.microsoft.com/heyscriptingguy/2014/04/02/build-constrained-powershell-endpoint-using-configuration-file/>  
Build Constrained PowerShell Endpoint Using Configuration File
- <https://social.technet.microsoft.com/Forums/en-US/a930fe34-702b-4e9f-8646-6d3736416e23/what-does-turning-powershell-20-off-in-windows-features-actually-do-?forum=winserverpowershell>  
What Does Turning Powershell 2.0 OFF in Windows Features Actually Do ?

## Spin Your Tale:

Spin Your Tale: The Fiction Writer's Guide to Telling YOUR Story - Dona Sarkar

<https://myignite.techcommunity.microsoft.com/videos?t=%257B%2522from%2522%253A%25222018-09-23T08%253A00%253A00-04%253A00%2522%252C%2522to%2522%253A%25222018-09-28T19%253A00%253A00-04%253A00%2522%257D&q=dona%2520sarkar>

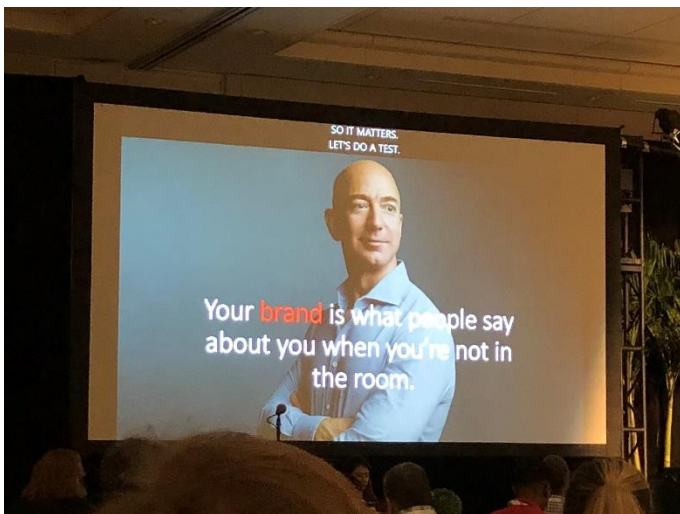
<https://www.youtube.com/watch?v=5R6mqWTPesk>

<https://www.amazon.com/DoTheThing-Because-comfort-zones-boring/dp/0996731121>



[https://www.facebook.com/donasarkarbooks/?eid=ARAFmwKQvm7ZMZSY68zIBuafxW68zcMcxhL5xl6cZfeTE8Mh6oX3kEBcw\\_m1Mr6zaVUBctz5WXrXMLDD](https://www.facebook.com/donasarkarbooks/?eid=ARAFmwKQvm7ZMZSY68zIBuafxW68zcMcxhL5xl6cZfeTE8Mh6oX3kEBcw_m1Mr6zaVUBctz5WXrXMLDD)

From Ashley McGlone (former MS SPFE): be online, on stage, on camera



What do you want your brand to be?