LINUX PITER

Microsoft loves Linux on Azure

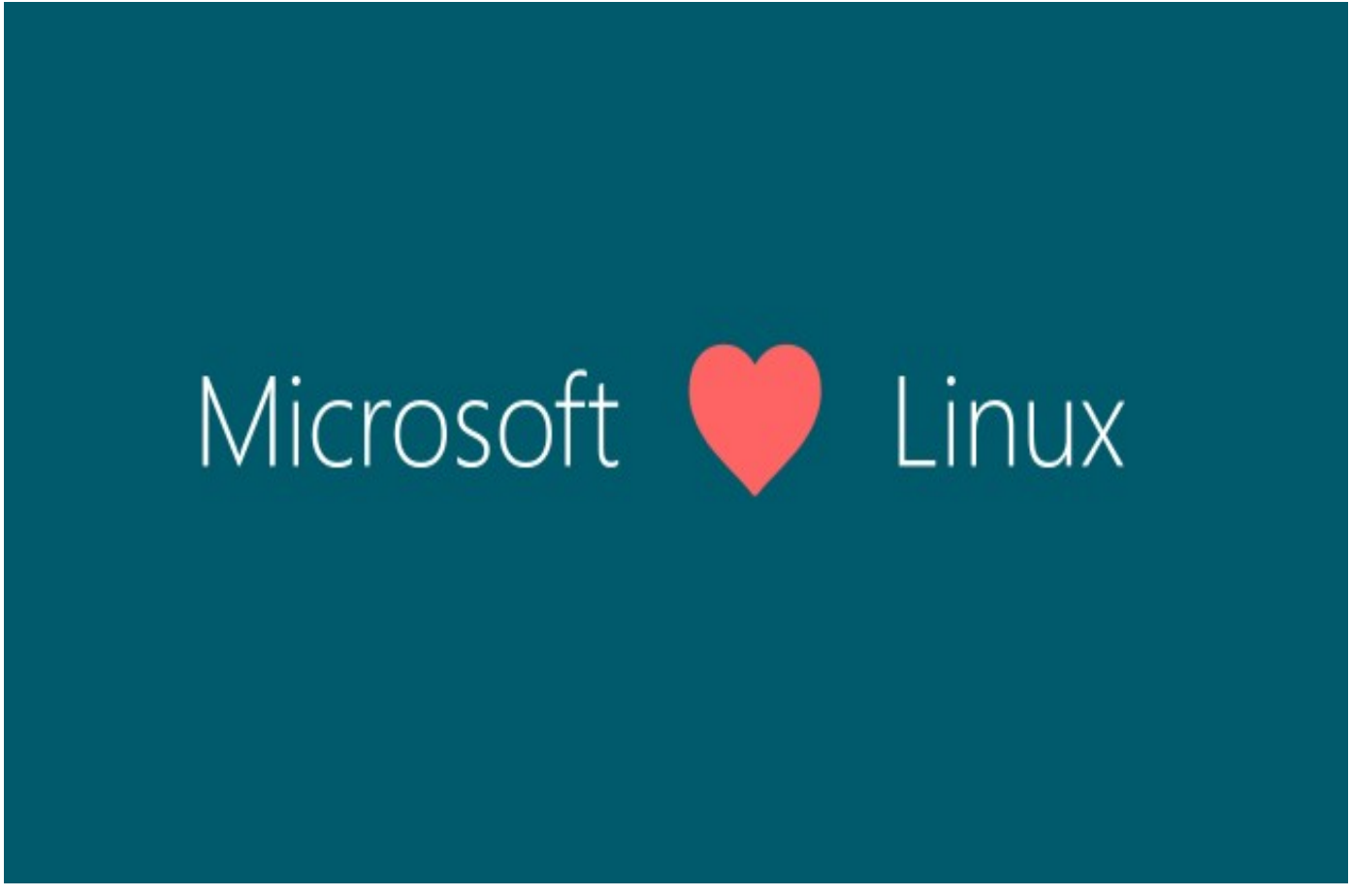
Stephen Hemminger
sthemmin@microsoft.com
@networkplumber

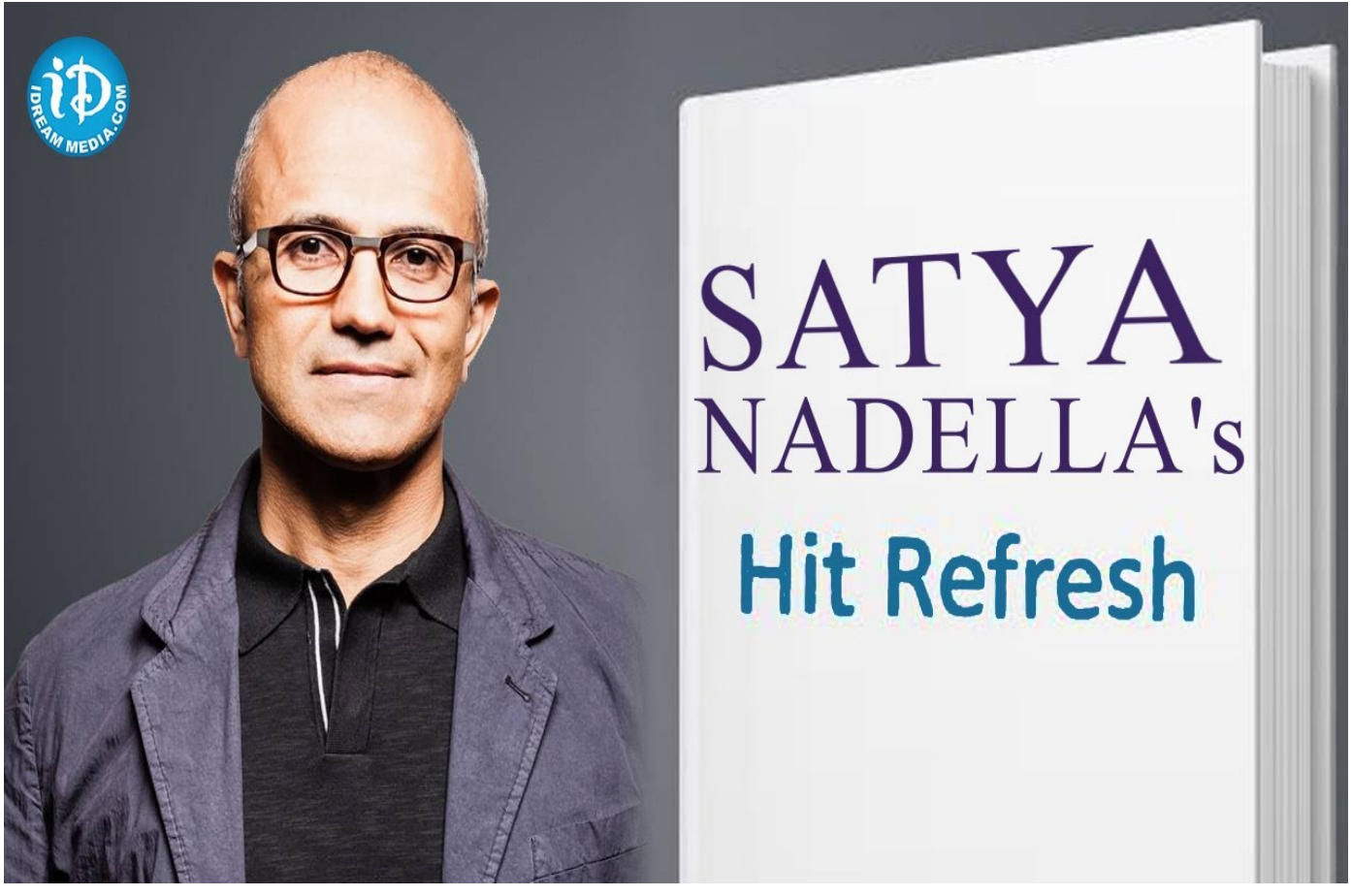
Saint Petersburg
3-4 November 2017

#LinuxPit

Agenda

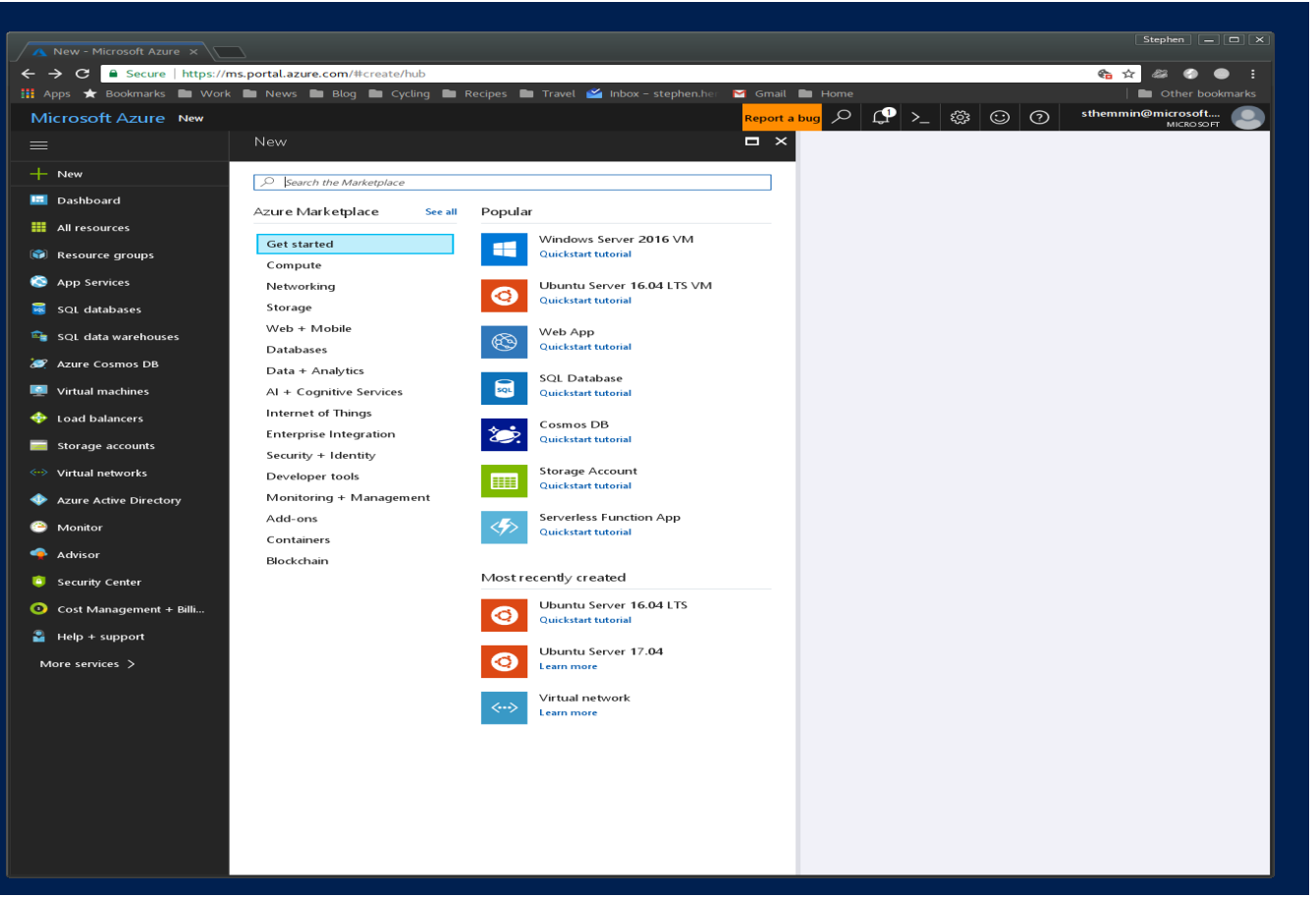
- Change of heart
- Orchestration
- Containers
- Secure VM
- Accelerated Networking
- Future


Microsoft
Linux

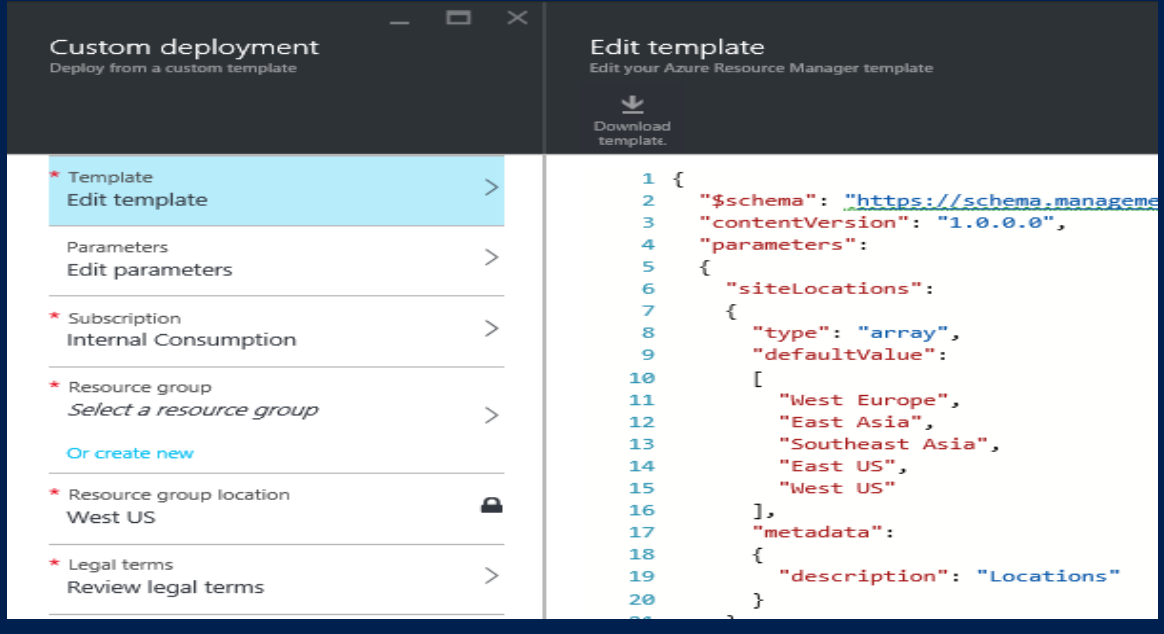

SATYA
NADELLA's
Hit Refresh

Agenda

- Change of heart
- Orchestration
- Containers
- Secure VM
- Accelerated Networking
- Future

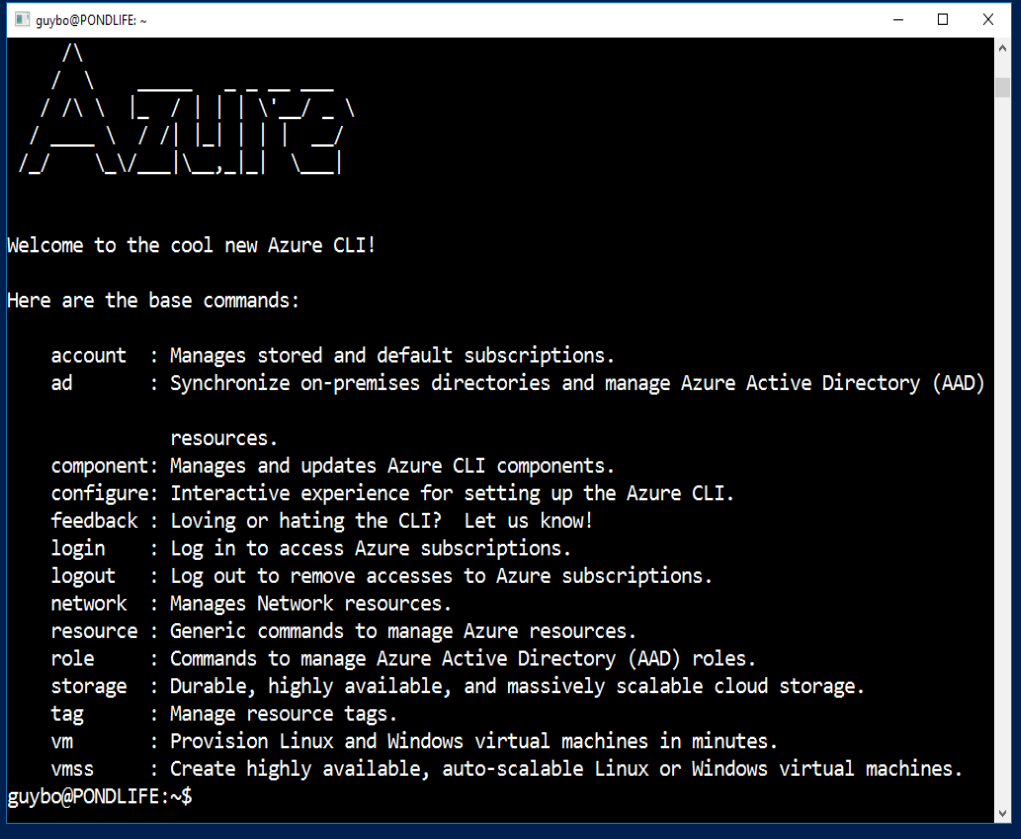

New - Microsoft Azure
Stephen
Secure | https://ms.portal.azure.com/#create/hub
Apps Bookmarks Work News Blog Cycling Recipes Travel Inbox – stephen.her Gmail Home Other bookmarks
Microsoft Azure New
Report a bug
sthemmin@microsoft....
MICROSOFT
New
Search the Marketplace
New
Dashboard
All resources
Resource groups
App Services
SQL databases
SQL data warehouses
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billi...
Help + support
More services >
Azure Marketplace
See all
Get started
Compute
Networking
Storage
Web + Mobile
Databases
Data + Analytics
AI + Cognitive Services
Internet of Things
Enterprise Integration
Security + Identity
Developer tools
Monitoring + Management
Add-ons
Containers
Blockchain
Popular
Windows Server 2016 VM
Quickstart tutorial
Ubuntu Server 16.04 LTS VM
Quickstart tutorial
Web App
Quickstart tutorial
SQL Database
Quickstart tutorial
Cosmos DB
Quickstart tutorial
Storage Account
Quickstart tutorial
Serverless Function App
Quickstart tutorial
Most recently created
Ubuntu Server 16.04 LTS
Quickstart tutorial
Ubuntu Server 17.04
Learn more
Virtual network
Learn more

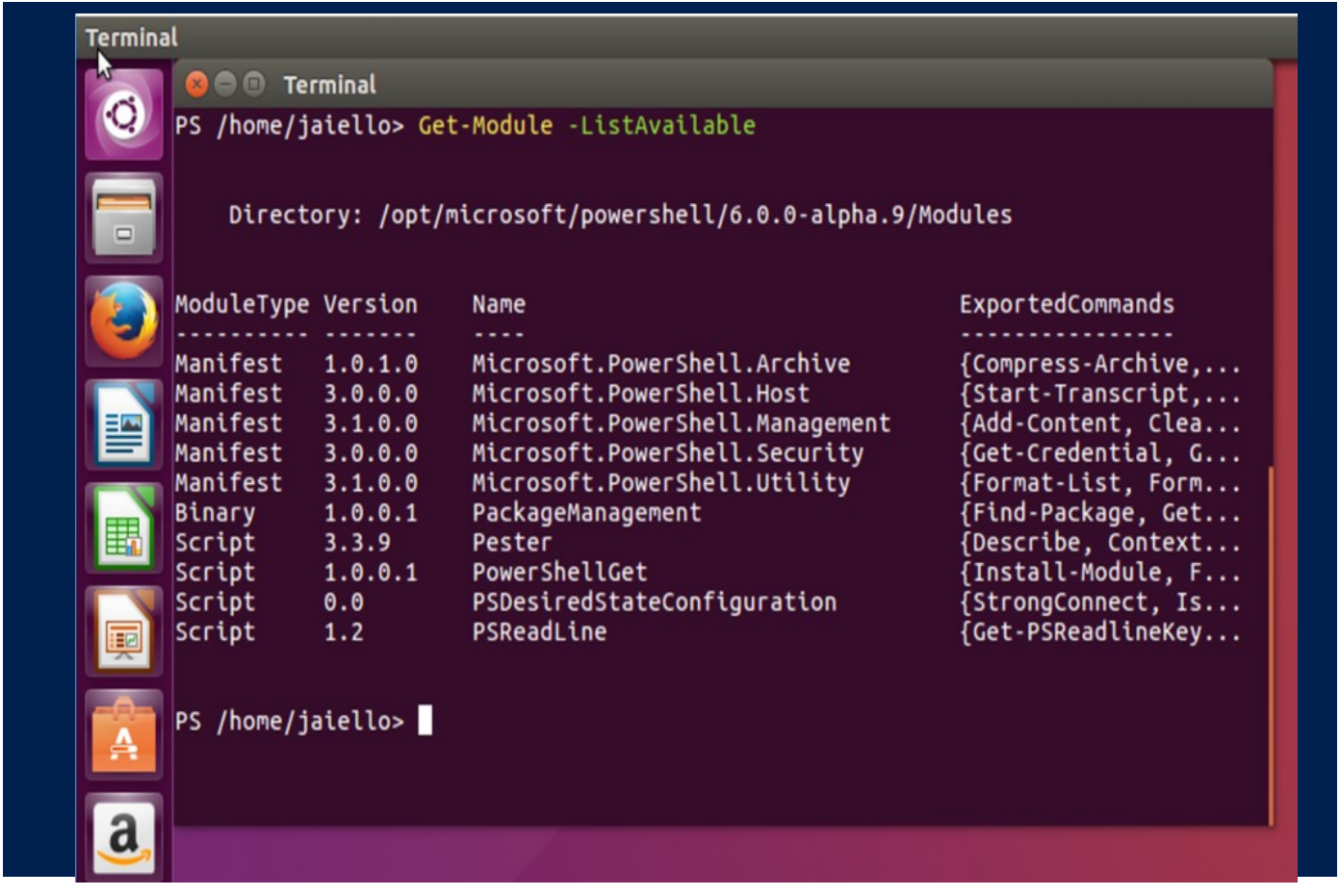
Azure Resource Manager Templates

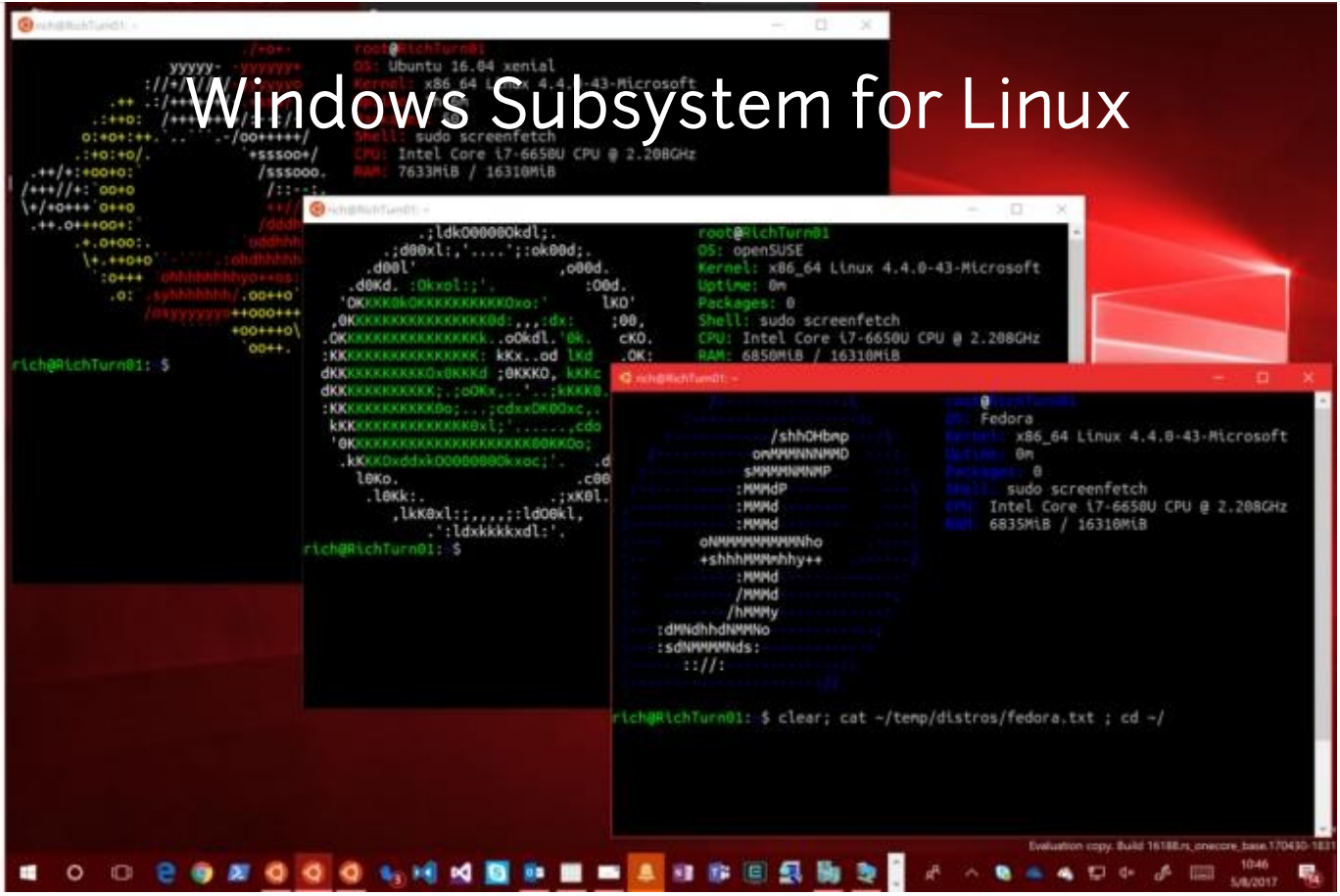


CLI options

	Bash	*Powershell*
Linux	Azure CLI	Azure Powershell Module
Windows	Windows Subsystem for Linux	Windows Azure Powershell Module

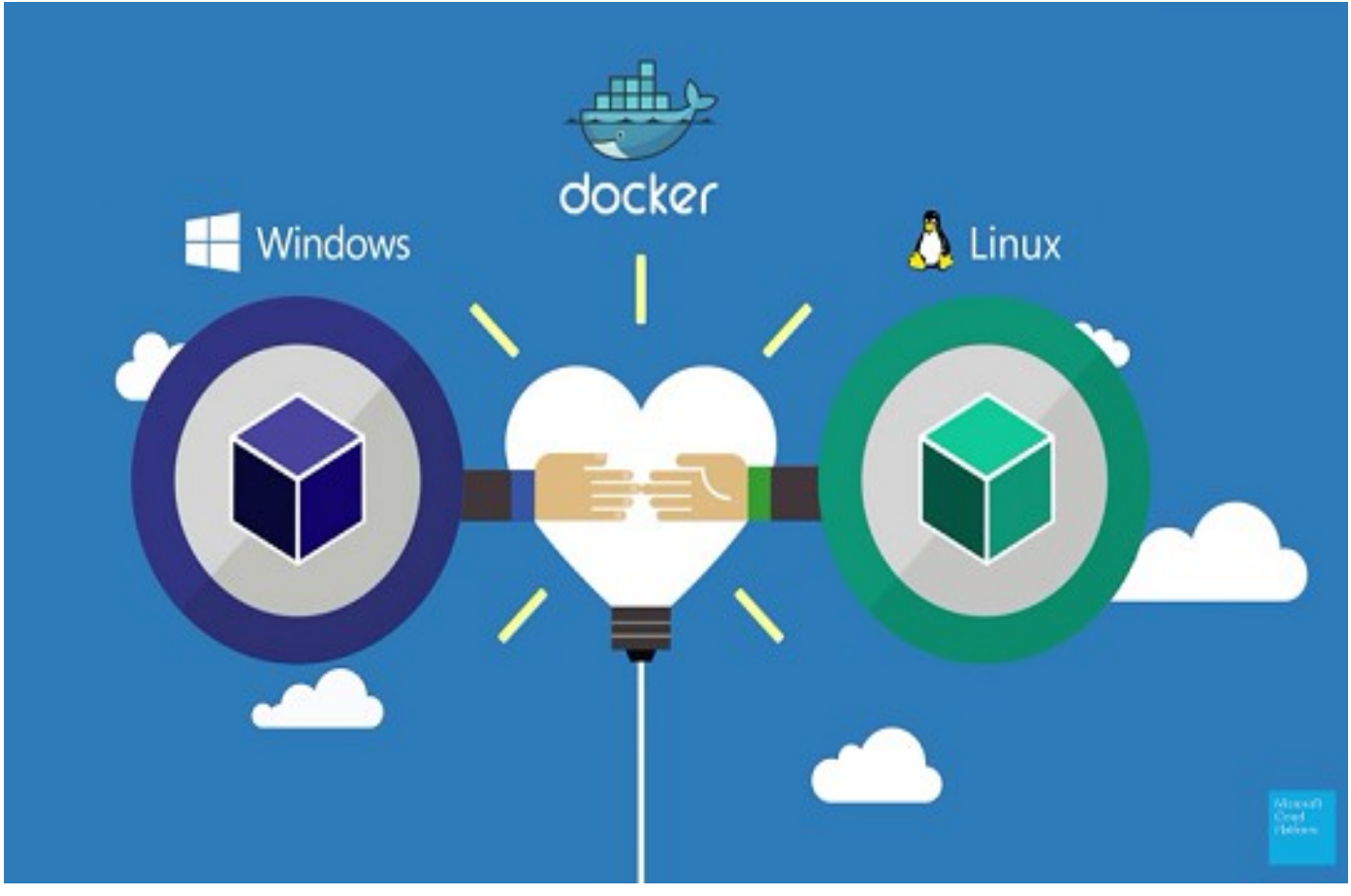

guybo@PONDLIFE: ~
/\
/ \ _____ _ _ __ ___
/ /\ \ |_ / | | | \'__/ _ \
/ ____ \ / /| |_| | | | | __/
/_/ _\/___|__,_|_| ___|
Welcome to the cool new Azure CLI!
Here are the base commands:
account : Manages stored and default subscriptions.
ad : Synchronize on-premises directories and manage Azure Active Directory (AAD)
resources.
component: Manages and updates Azure CLI components.
configure: Interactive experience for setting up the Azure CLI.
feedback : Loving or hating the CLI? Let us know!
login : Log in to access Azure subscriptions.
logout : Log out to remove accesses to Azure subscriptions.
network : Manages Network resources.
resource : Generic commands to manage Azure resources.
role : Commands to manage Azure Active Directory (AAD) roles.
storage : Durable, highly available, and massively scalable cloud storage.
tag : Manage resource tags.
vm : Provision Linux and Windows virtual machines in minutes.
vmss : Create highly available, auto-scalable Linux or Windows virtual machines.
guybo@PONDLIFE:~$


Terminal
Terminal
PS /home/jaiello> Get-Module -ListAvailable
Directory: /opt/microsoft/powershell/6.0.0-alpha.9/Modules
ModuleType Version Name ExportedCommands
---------- ------- ---- ---------------
Manifest 1.0.1.0 Microsoft.PowerShell.Archive {Compress-Archive,...
Manifest 3.0.0.0 Microsoft.PowerShell.Host {Start-Transcript,...
Manifest 3.1.0.0 Microsoft.PowerShell.Management {Add-Content, Clea...
Manifest 3.0.0.0 Microsoft.PowerShell.Security {Get-Credential, G...
Manifest 3.1.0.0 Microsoft.PowerShell.Utility {Format-List, Form...
Binary 1.0.0.1 PackageManagement {Find-Package, Get...
Script 3.3.9 Pester {Describe, Context...
Script 1.0.0.1 PowerShellGet {Install-Module, F...
Script 0.0 PSDesiredStateConfiguration {StrongConnect, Is...
Script 1.2 PSReadLine {Get-PSReadlineKey...
PS /home/jaiello>


Windows Subsystem for Linux
root@RichTurn01
OS: Ubuntu 16.04 xenial
Shell: sudo screenfetch
CPU: Intel Core i7-6650U CPU @ 2.208GHz
RAM: 7633MiB / 16310MiB
rich@RichTurn01: $
root@RichTurn01
OS: openSUSE
Kernel: x86_64 Linux 4.4.0-43-Microsoft
Uptime: 0m
Packages: 0
Shell: sudo screenfetch
CPU: Intel Core i7-6650U CPU @ 2.208GHz
RAM: 6850MiB / 16310MiB
rich@RichTurn01: $
Fedora
Kernel: x86_64 Linux 4.4.0-43-Microsoft
Uptime: 0m
Packages: 0
Shell: sudo screenfetch
CPU: Intel Core i7-6650U CPU @ 2.208GHz
RAM: 6835MiB / 16310MiB
rich@RichTurn01: $ clear; cat ~/temp/distros/fedora.txt ; cd ~/

Agenda

- Change of heart
- Orchestration
- Containers
- Secure VM
- Accelerated Networking
- Future


docker
Windows
Linux

Linux containers with Hyper-V isolation

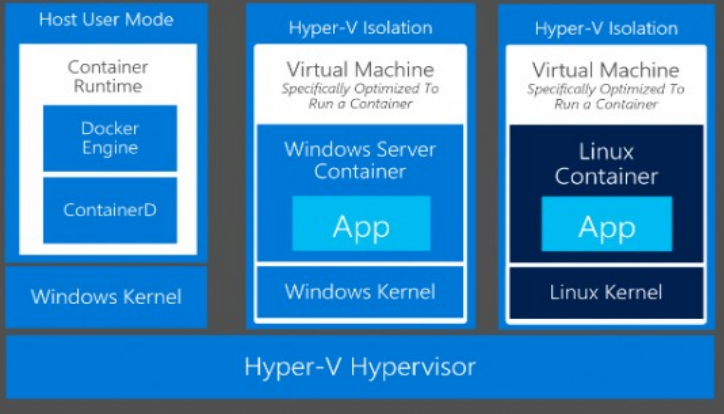
One Docker engine

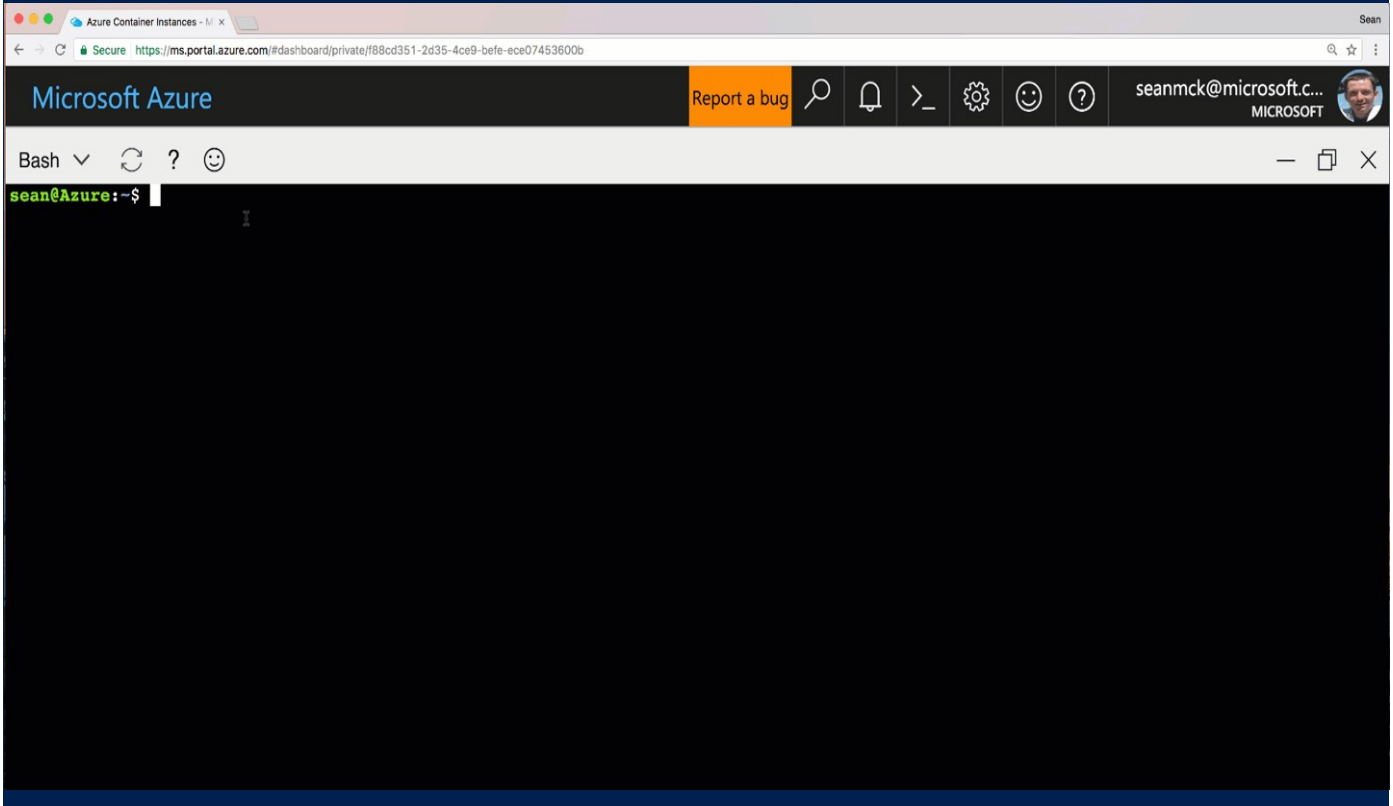
One container host

Any container,
regardless of OS

Choice of Linux kernels

Yes, this will be on Win10!




Azure Container Instances
Sean
Secure https://ms.portal.azure.com/#dashboard/private/f88cd351-2d35-4ce9-befe-ece07453600b
Microsoft Azure
Report a bug
seanmck@microsoft.c...
MICROSOFT
Bash
sean@Azure:~$

Agenda

- Change of heart
- Orchestration
- Containers
- Secure VM
- Accelerated Networking
- Future

What is the problem?

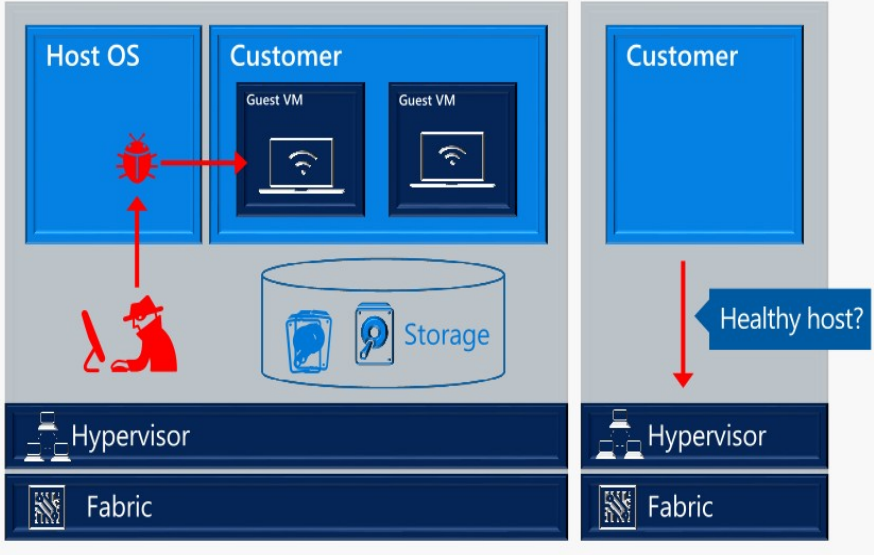
Virtual machines introduce new security risks

Compromised or malicious fabric admins can access guest virtual machines

Health of hosts not taken into account before running VMs

Tenant's VMs are exposed to storage and network attacks

VMs don't benefit from hardware-rooted security such as TPMs



Shielded VMs: Security Assurance Goals

Encryption of data, both at-rest & in-flight

Virtual TPM enables the use of disk encryption within a VM (e.g. dm-crypt, BitLocker)
Both Live Migration and VM state are encrypted

Fabric admins locked out

Host administrators cannot access guest VM secrets (e.g. can't see disks, video, etc.)
Host administrators cannot run arbitrary kernel-mode code

Attestation of host health required

VMs can only run on "healthy" hosts designated by the VM owner

NOTE: Shielding is not intended as a defense against DoS attacks

Drilldown: Normal Boot Path (1 of 3)

Key Goals

Prevent tampering with boot path that could expose secrets

Automate supplying dm-crypt passphrase from the vTPM

Don't modify the code in the normal Linux boot path (shim, grub, kernel)

What is modified	What is not modified
• initramfs updated to get dm-crypt passphrase from a file • lsvmload used as a precursor to the normal Linux boot shim • lsvmload inject disk passphrases as a file into virtualized copy of initramfs	• Linux shim • grub • Linux kernel

Current Status

Hyper-V is updated to enable Linux Shielded VMs

Updated Hyper-V release ships later this fall

Works with Linux distros that can UEFI Secure Boot

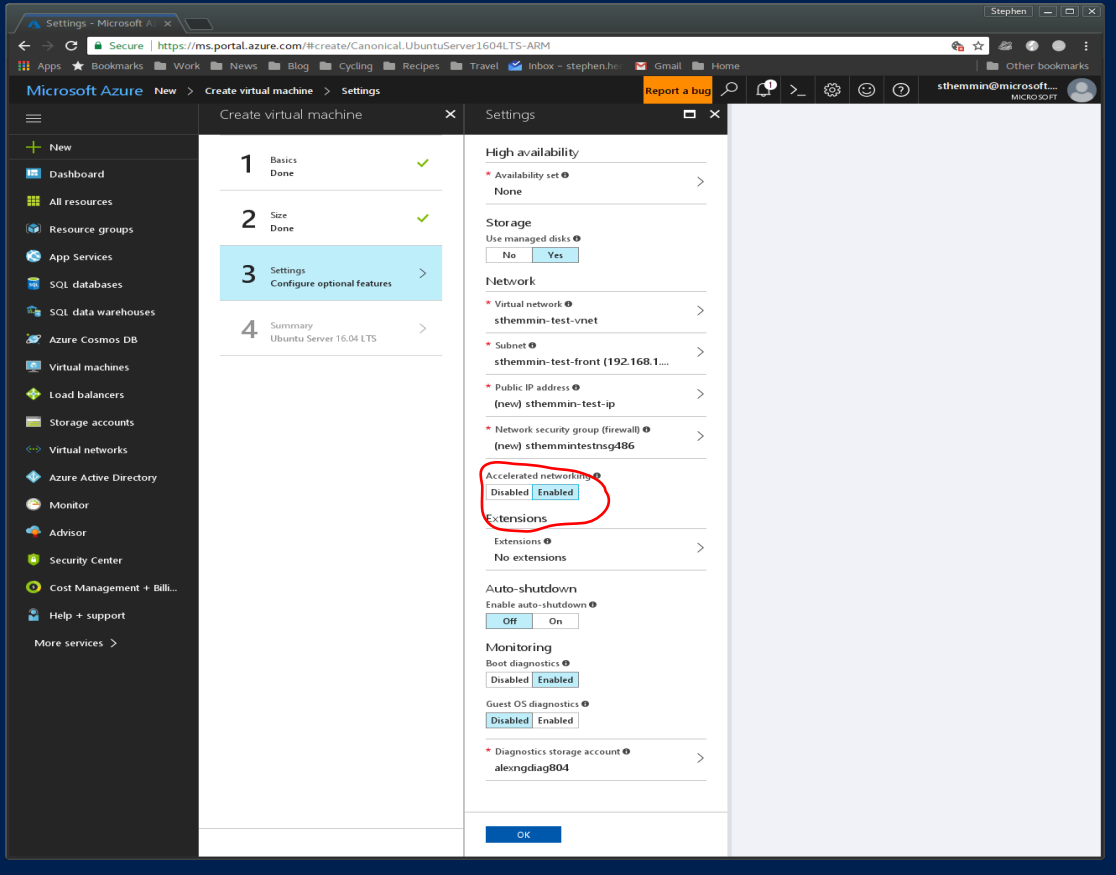
We're collaborating with commercial distro vendors to ensure official support
Red Hat, SUSE, and Canonical

Windows Shielded VMs commercially available today

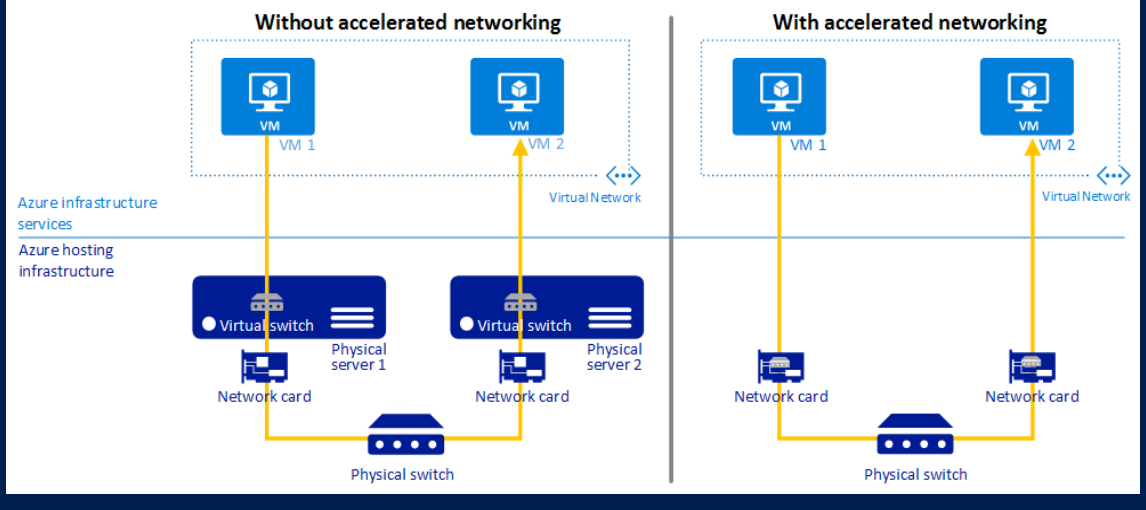
Rackspace, brightsolid (UK)
Expect to see Linux Shielded VMs commercially available after Hyper-V update ships

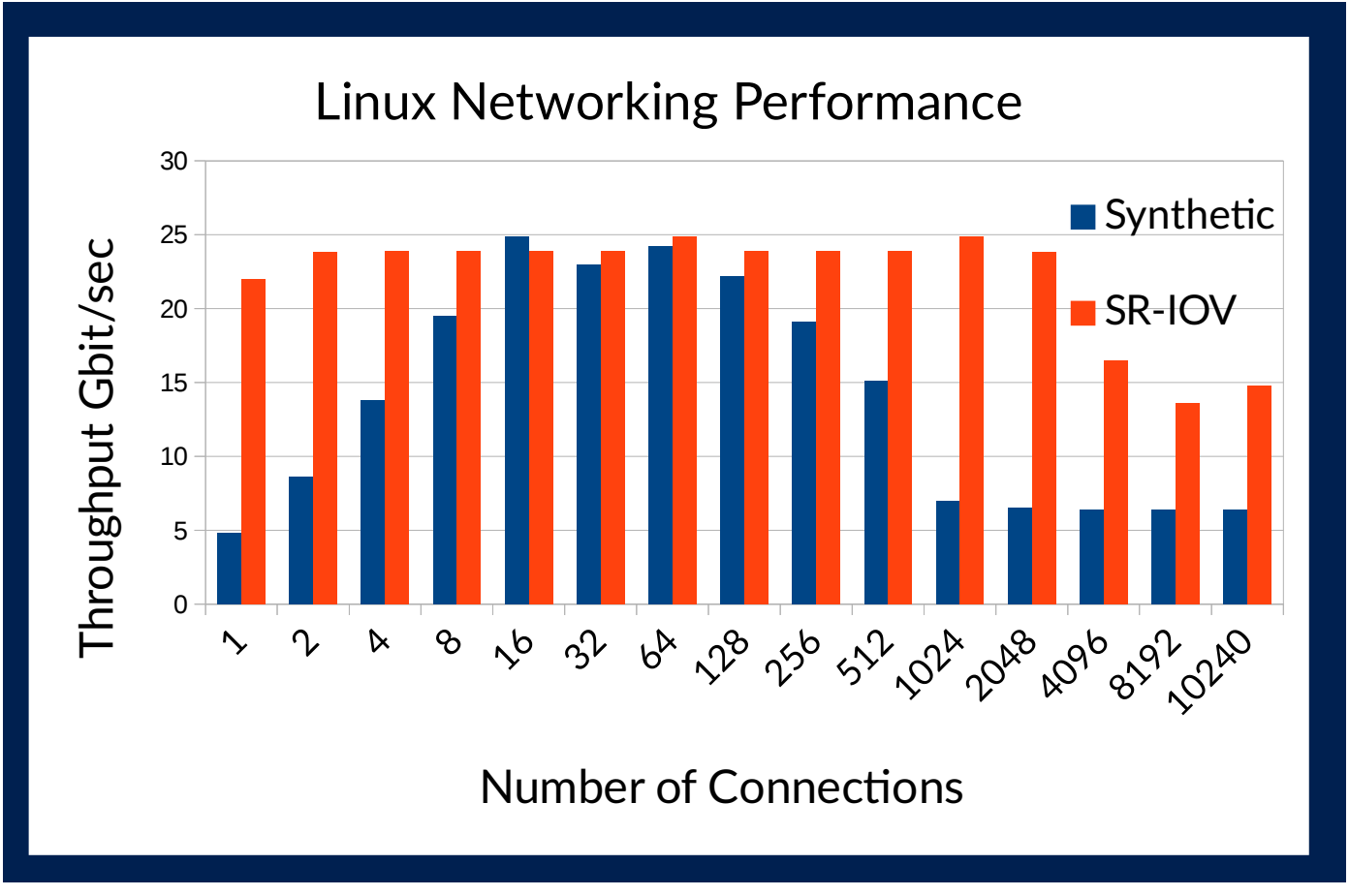
Agenda

- Change of heart
- Orchestration
- Containers
- Secure VM
- Accelerated Networking
- Future

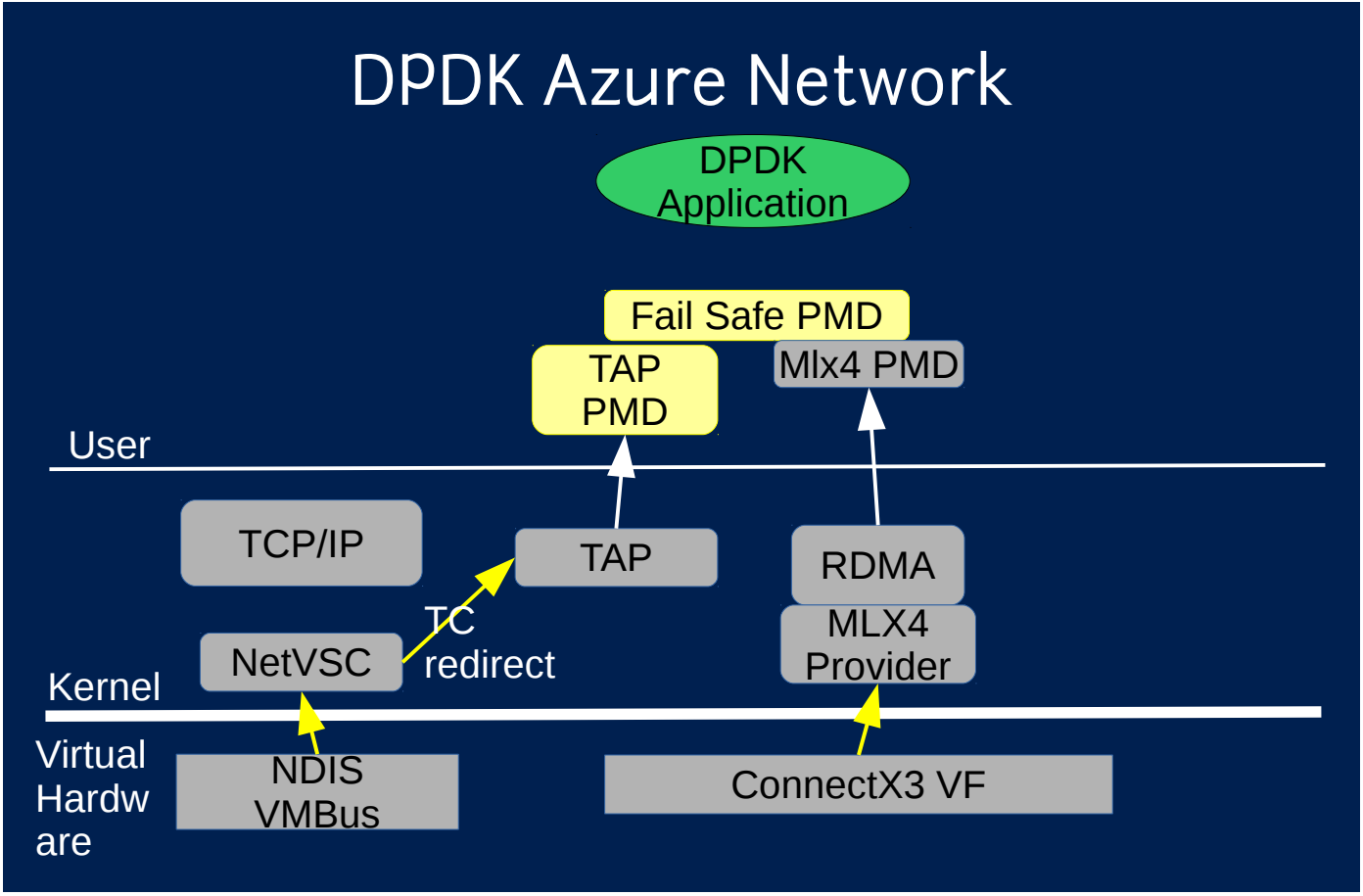

Settings - Microsoft A...
Stephen
Secure | https://ms.portal.azure.com/#create/Canonical.UbuntuServer1604LTS-ARM
Apps Bookmarks Work News Blog Cycling Recipes Travel Inbox - stephen.he Gmail Home Other bookmarks
Microsoft Azure New > Create virtual machine > Settings
Report a bug
sthemmin@microsoft.... MICROSOFT
New
Dashboard
All resources
Resource groups
App Services
SQL databases
SQL data warehouses
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billi...
Help + support
More services >
Create virtual machine
1 Basics Done
2 Size Done
3 Settings Configure optional features
4 Summary Ubuntu Server 16.04 LTS
Settings
High availability
* Availability set
None
Storage
Use managed disks
No Yes
Network
* Virtual network
sthemmin-test-vnet
* Subnet
sthemmin-test-front (192.168.1....
* Public IP address
(new) sthemmin-test-ip
* Network security group (firewall)
(new) sthemmintestnsg486
Accelerated networking
Disabled Enabled
Extensions
Extensions
No extensions
Auto-shutdown
Enable auto-shutdown
Off On
Monitoring
Boot diagnostics
Disabled Enabled
Guest OS diagnostics
Disabled Enabled
* Diagnostics storage account
alexngdiag804
OK

Azure Accelerated Networking




Linux Networking Performance
Throughput Gbit/sec
30
25
20
15
10
5
0
Synthetic
SR-IOV
1
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
10240
Number of Connections

DPDK Azure Network



Agenda

- Change of heart
- Orchestration
- Containers
- Secure VM
- Accelerated Networking
- Future

Process

- Azure
  - Simultaneous feature availability
- Linux kernel
  - Upstream first
  - Leading edge: Ubuntu, Intel, …
  - Enterprise partners: Redhat, SuSe
  - Linux Integration Services (backport)

KEEP
CALM
AND
ASK
QUESTIONS

Thank you