

Sami Laiho

Senior Technical Fellow, MVP Adminize.com / Win-fu.com <u>sami@adminize.com</u> BLOG.WIN-FU.COM

@samilaiho

What's really new in Windows 10?



Configuration Manager

Forgive my English

- •When most get **Administrator** or Spanish get **Administrador**
- •we get JÄRJESTELMÄNVALVOJA



Sami Laiho

Senior Technical Fellow adminize.com

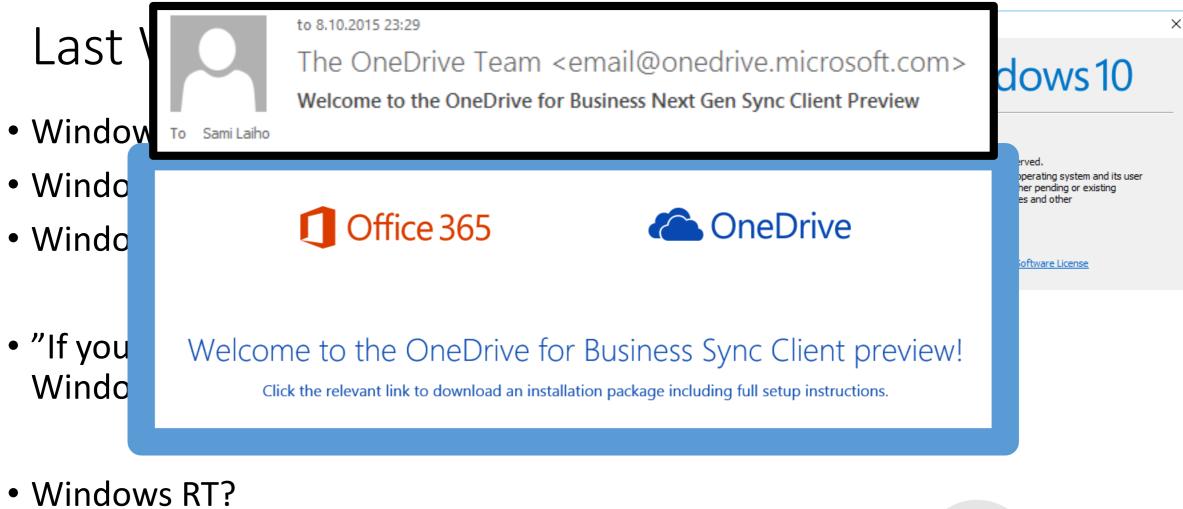
- IT Admin since 1996
- MCT since 2001 (MCT Regional Lead Finland)
- MVP in Windows OS since 2011
- Specializes in and trains:
 - Troubleshooting
 - Security
 - Centralized Management
 - Active Directory
 - Hacking
 - Penetration testing
 - Social Engineering
- Trophies:
 - Ignite 2015 Best male presenter ;) (#2 out of 1000 speakers)
 - TechEd Europe 2014 Best session
 - TechEd North America 2014 Best session, Best speaker
 - TechEd Australia 2013 Best session, Best speaker
 - TechEd Europe 2013 Best Session by an external speaker



AMAZING!!!!

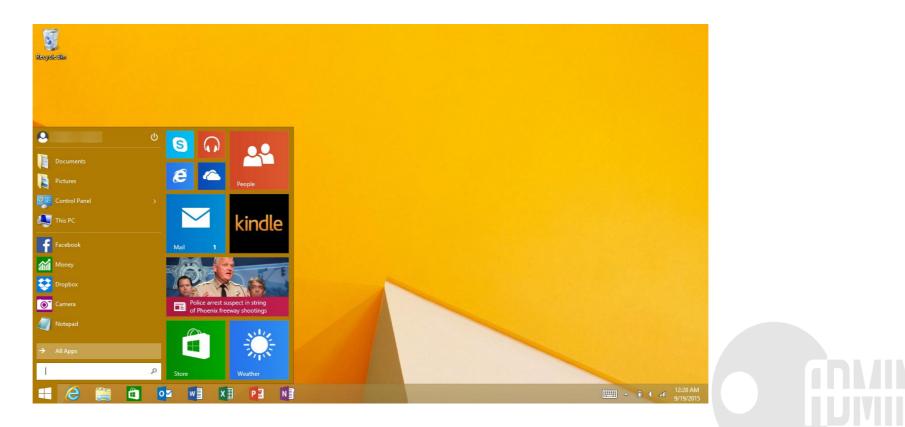
- A Start-Menu!!! (NOW WITH 2048 things!!)
- Virtual Desktops!!!
- Running applications in Windows!!!
- A transparent Command Prompt!!!





Windows RT "Windows 10 upgrade"

<u>https://support.microsoft.com/en-us/kb/3033055</u>



Upgrade is recommended

- Until now it has always been a less recommended way to upgrade and has always said to result in poor performance compared to a clean install
- You can opt out or delay the adoption
 - Long Time Servicing Branch
- This is part of a bigger picture:
 - Flight upgrades
 - Home users forced to use Windows Update
 - Windows Update for Business



DEMO

Upgrade Settings



Provision packages

- Transform a purchased OEM-installed PC to an Enterprise device
- Trying to make CYOD easier
- Windows "Phone" has an Enterprise-version so I hope this works...



Fixed ConHost.exe

Windo Copyr

Command Prompt	– 🗆 X	🖼 "Command Prompt" Properties 🛛 🗙 🗙			
Microsoft Windows [Version 10.0.9926] (c) 2015 Microsoft Corporation. All rights reserved. C:\Users\Sami>_		Options Font Layout Colors			
Windows PowerShell ndows PowerShell spright (6) 20114 Microsoft Corporation. All rights reserved. C:\Users\Sami}	<pre></pre>	Cursor Size Command History Buffer Size: 50 • Medium Large Large Discard Old Duplicates Edit Options QuickEdit Mode Insert Mode Enable Ctrl key shortcuts Filter clipboard contents on paste Text Selection Enable line wrapping selection Extended text selection keys Current code page 850 (OEM - Multilingual Latin I) Indext more about new console features			
	ОК	Cancel			

DEMO

Conhost.exe



Biometrics

- No more passwords!
- Two-factor authentication for everyone!
- First factor to be Biometrics, PIN, face recognition ...
- Smartcards and other physical tokens are easily forgotten so let's use something that's easier to remember to take with you
 - Your computers TPM
 - Windows 10 phone
- Windows Hello and Windows Passport



DEMO

Windows Hello



account password



this PIN to sign ir

I forgot my P

s Hello

indows, apps and

New Store and Universal Apps

- Only way to make Windows fly in the current world of devices is to make the Store work
- Only way to make the Store work is to make the developers happy with it and get more apps in it
 - Two phases:
 - 1. "Emulation" for iOS and Android apps, and support for App-V packages
 - 2. Make the store more sexy and appealing to devs Xbox plays a crucial role in this
- Volume licensing, reusable licenses and Azure AD authentication are a must

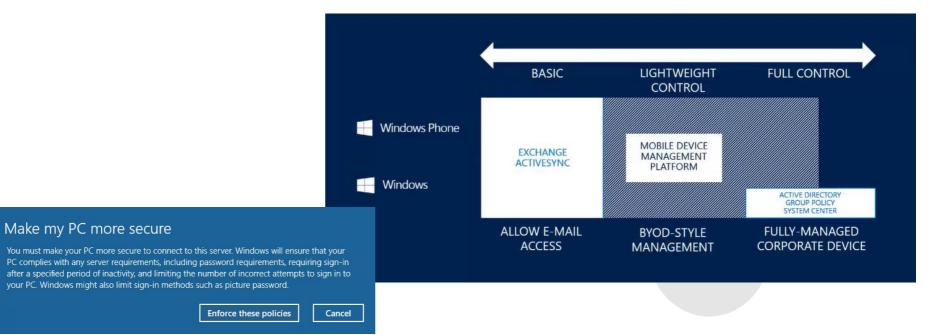
Azure AD

- Path to here
 - Windows 7 \rightarrow Domain
 - Windows 8.1 + Microsoft Account
 - Windows 10 + Azure AD -account
- Windows 10 is the first OS really connected to Azure
- "AAD should be called Azure Authentication Services (for now at least)" – Sami Laiho



MDM

- InTune, SCCM and 3rd party supported better than before
- Not only for BYOD anymore
- Three scenarios



Hardware features

- Windows Hello and RealSense 3D Cameras
- DirectX 12
- Wireless Charging
- Software Guard Extensions (SGX)
 - <u>https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003</u> <u>81_SGX_DL_100_small.pdf</u>
- USB Type C and USB 3.1
- ThunderBolt 3.0 (40Gbps → Two daisy-chained 4K displays)

Hardware features

- Intel Skylake enhancements
 - Keyword spotter algorithm
 - WiGig technology, which can transfer data at 7Gbps
 - DDR4 memory, which will improve internal data transfer between memory, processor and other components
 - SIMD.js for Edge
 - Single Instruction, Multiple Data (SIMD)
 - CPU Speed Shift (30ms→1ms)
 - Sensor Hub
 - Image Signal Processor



DEMO

CPU Shift



Continuum



Virtual memory size and ASLR

Process: note PID: 422	epad.exe 282	Process: notepad.exe PID: 3744		Process: notepad.exe PID: 42106		
Committed: Private Byte: 32 Working Set:	bit notepad 2GB	Committed: Private Bytes: Working Set:	4bit notepad on W8 8TB	or	t notepa n W8.1 <u>28TB!</u>	ad
Туре		Туре	jize	Туре		Size
Total Image Mapped File Shareable Heap Managed Heap Stack Private Data Page Table	13 K 50 K 15 K 58 K 1 K 2 B K 2 K 4 B K	Total Image Mapped File Shareable Heap Managed Heap Stack Private Data Page Table Unusable	4 52 K 4 12 K 1 72 K 2 D0 K 4 D4 K 1 2 K 1 30 K 4 34 K 1 738 K	Total Image Mapped File Shareable Heap Managed Heap Stack Private Data Page Table	2 1	598 780 K 60 148 K 19 912 K 509 500 K 1 528 K 2 560 K 1 416 K 444 K
Unusable Free	2 658 K 1 961 728 K	Free	8 589 842 560 K	Unusable Free	135 291	3 272 K 355 072 K

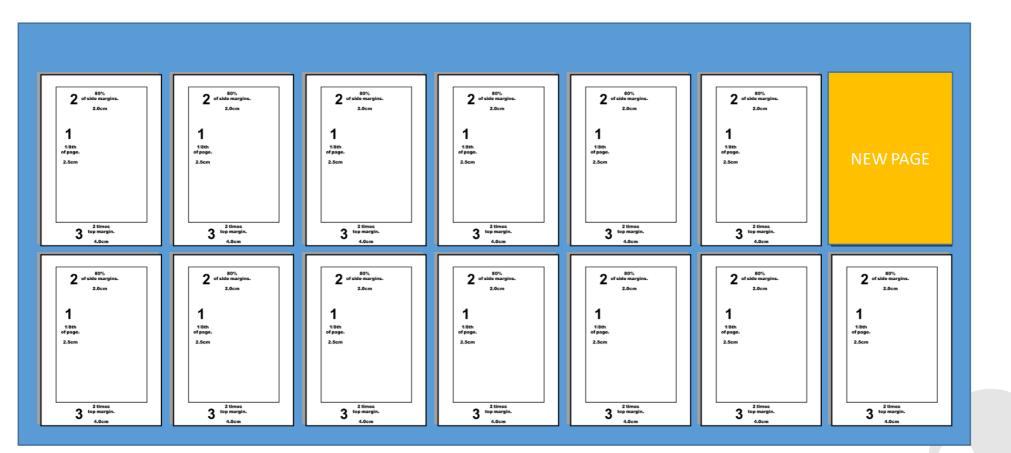
IOMMU

- I/O Memory Management Unit
 - MMU for devices, as opposed to processors
 - Where an MMU translates virtual to physical addresses for a CPU accessing your system's memory, an IOMMU translates virtual to physical addresses for devices
- Hardware based protection against DMA-access
- Protects against buggy drivers and malicious code
- Works with SLAT
- Makes sure a device or VM won't have access to physical memory addresses not meant for them
- Known as: Intel VT-d / AMD-Vi



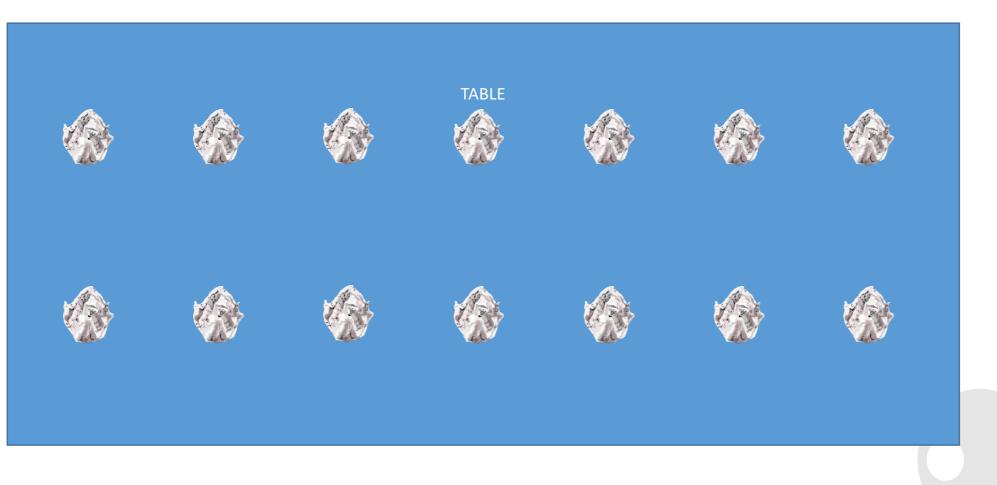
Memory Compression

To fit a new page old might need to be paged out...

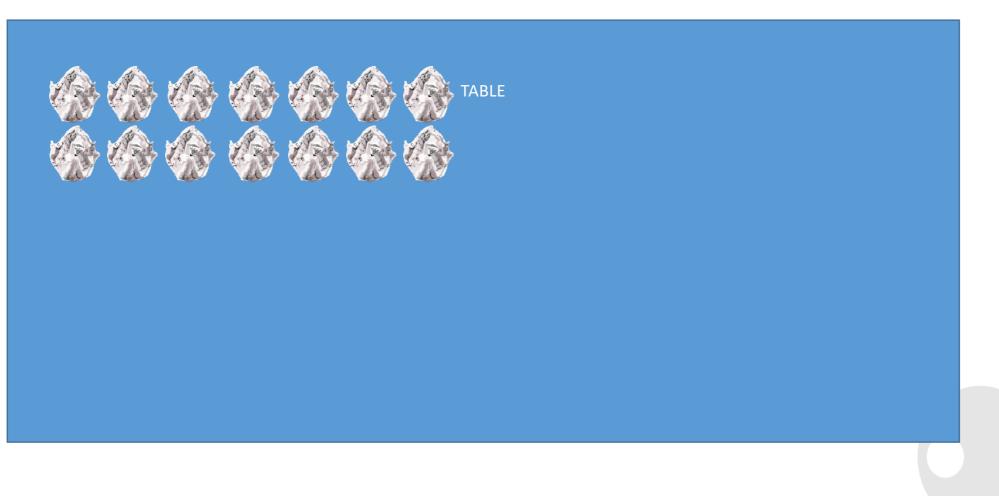




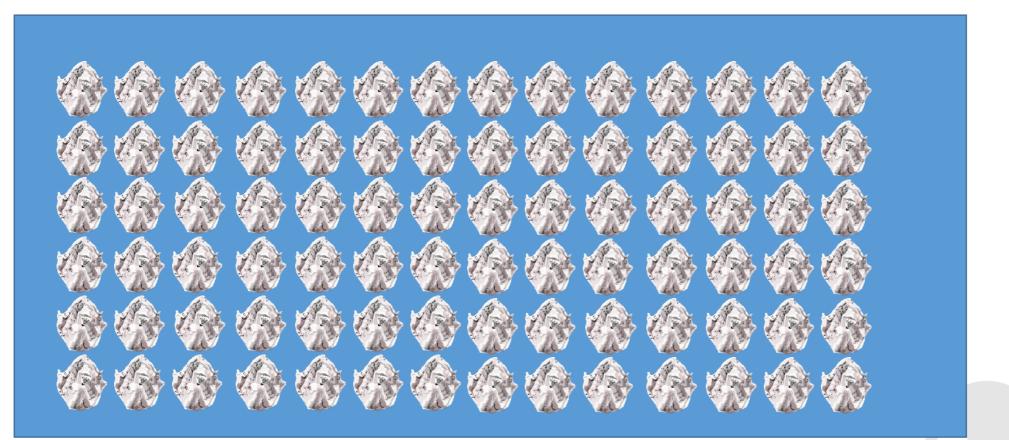
Compress the pages

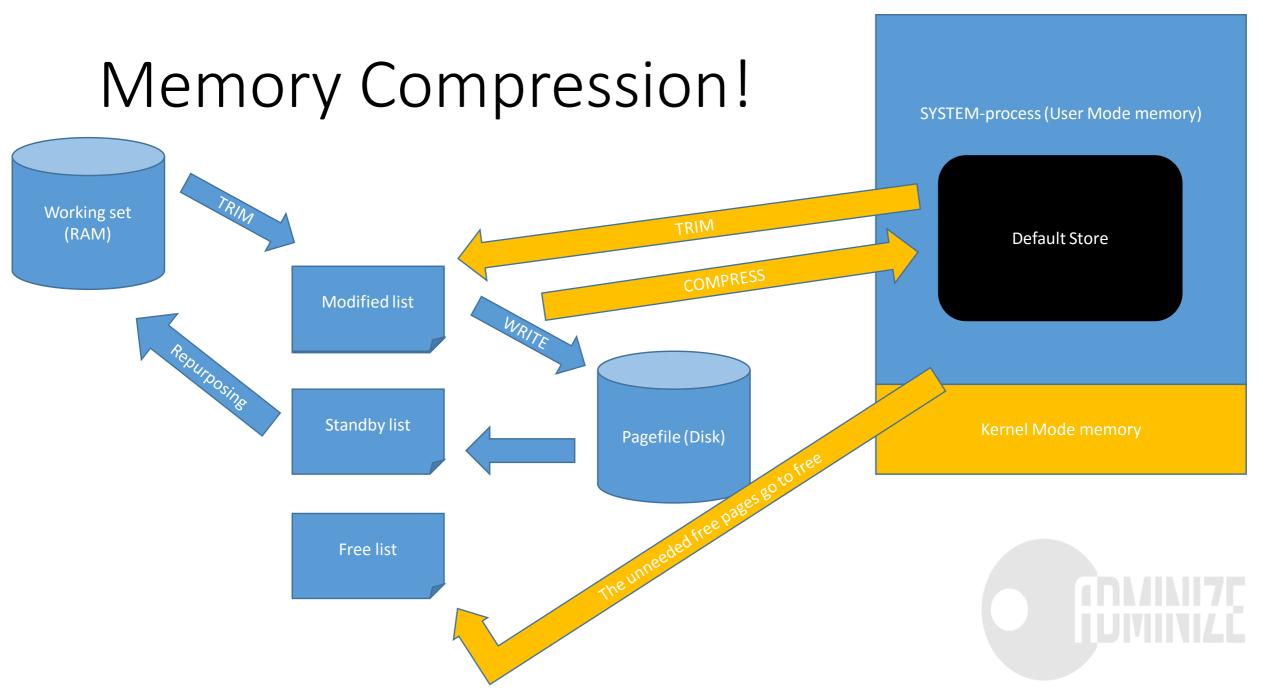


Compressed pages on a table



Compressed pages on a table

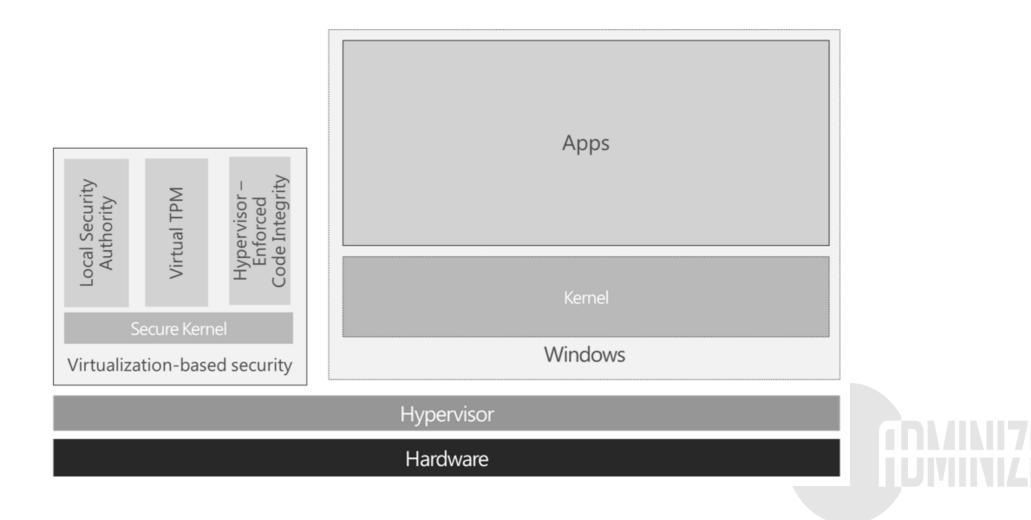




Device Drivers

- Microsoft Signatures to be REQUIRED for Windows 10 Kernel-Mode Drivers
- To distribute you will have to:
 - Sign your driver package with your company's code signing certificate
 - Login to the Microsoft Hardware Developer Portal
 - Upload your signed driver package
 - Agree to a few particulars
 - Download the Microsoft signed files (within minutes)
- Why?
 - driver signing is vulnerable to exploitation
 - Bad guys have managed to steal certificates
 - some have even managed to acquire code signing certs on their own

Device Guard



Isolated User Mode

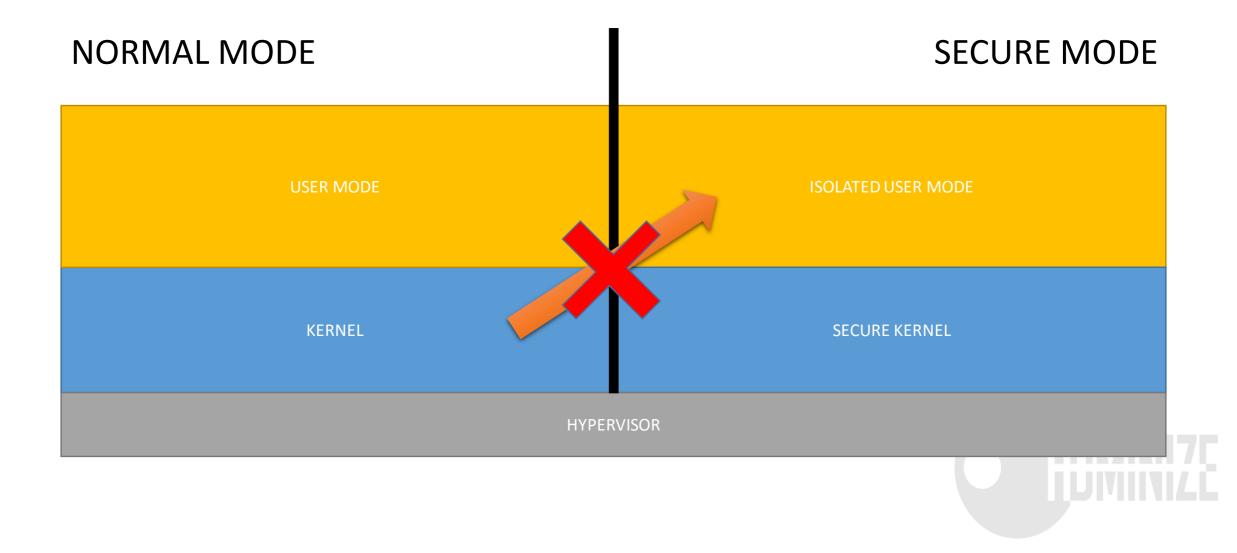
Traditional Kernel Mode vs User Mode

USER MODE

KERNELMODE



Normal and Secure mode



Isolated User Mode

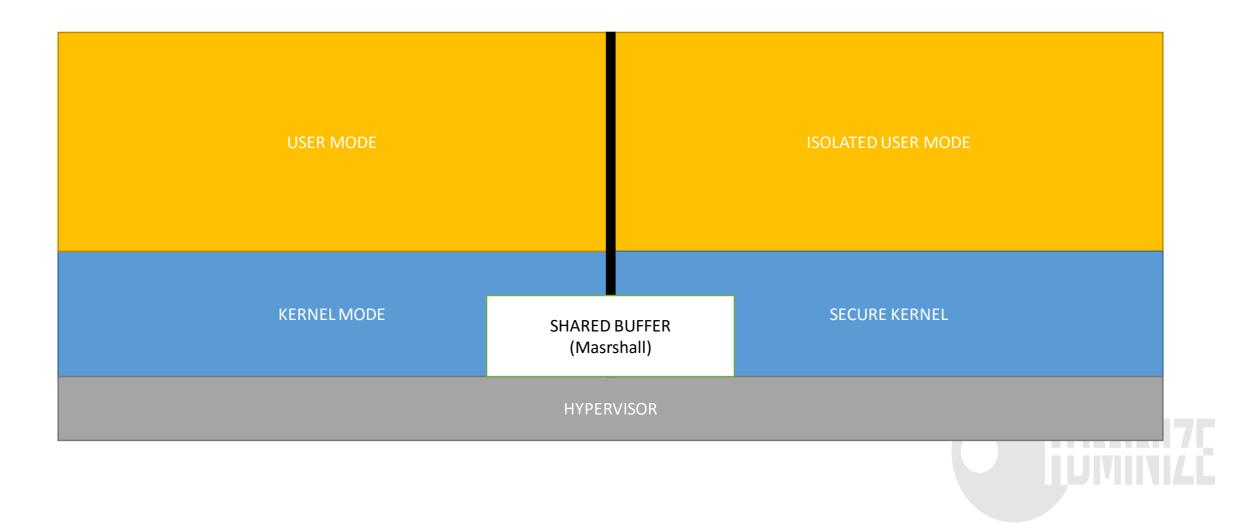
- Protects User Mode from the code in the Kernel Mode
 - Normally Kernel has full visibility to User Mode processes' memory



Secure Kernel

- IUM is on top of Secure Kernel (Secure System)
- Not a real Kernel but more a proxy that talks to the real Kernel but marshalls the transactions and does sanity checks
- Does not implement stuff that the normal kernel already does
- Secure Kernel cannot be extended like the normal
 - Only accessible by Microsoft not 3rd party
- All CryptoCode, Challenge/Response is here so it stays private to the Virtual Secure Mode

Traditional Kernel Mode vs User Mode



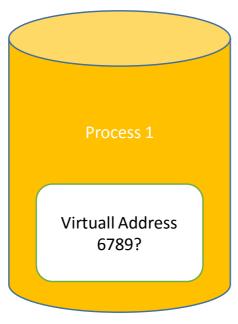
How come the Kernel is not able to access the memory of the Secure Kernel?



Traditional Virtual memory



PAGETABLE	PROCESS 0	
V-Address	P-Address	ACCESSMASK
хххх	уууу	Z-Z-Z
6789	0x7777777	R-X



PAGETABLE	PROCESS 0	
V-Address	P-Address	ACCESSMASK
хххх	уууу	Z-Z-Z
6789	0x7778888	RW-

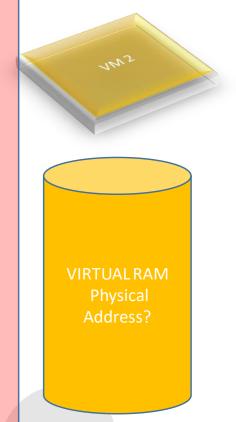
Kernel has access to the Page Table so why wouldn't it have access to the memory?



Hypervisors and VMs

VNA	
VIRTUAL RAM Physical Address?	

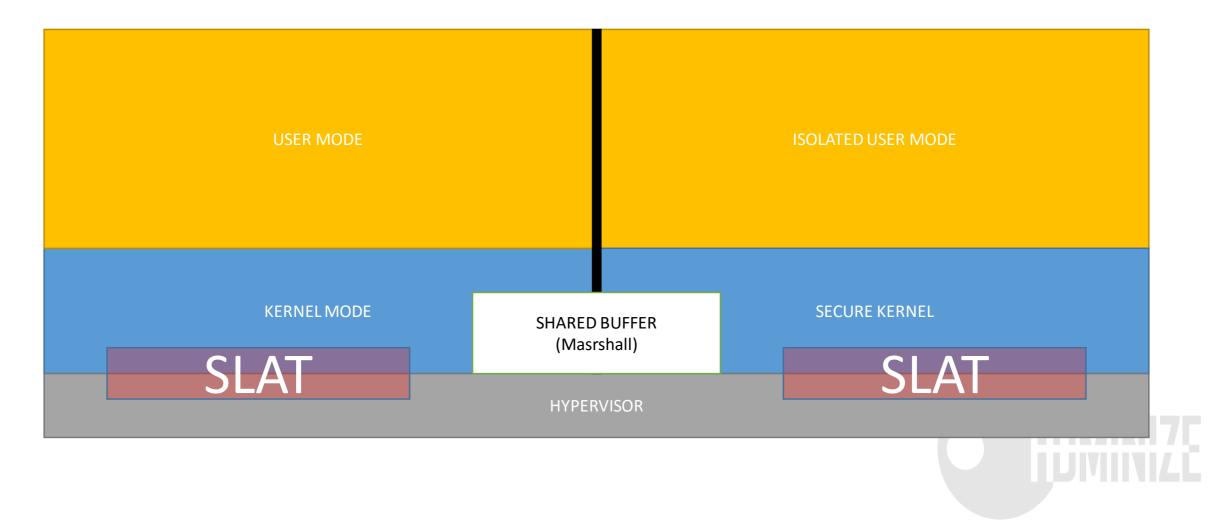
PAGETABLE	VM 1	
GPA	SPA	ACCESSMASK
хххх	уууу	Z-Z-Z
67890	0x7777777	R-X



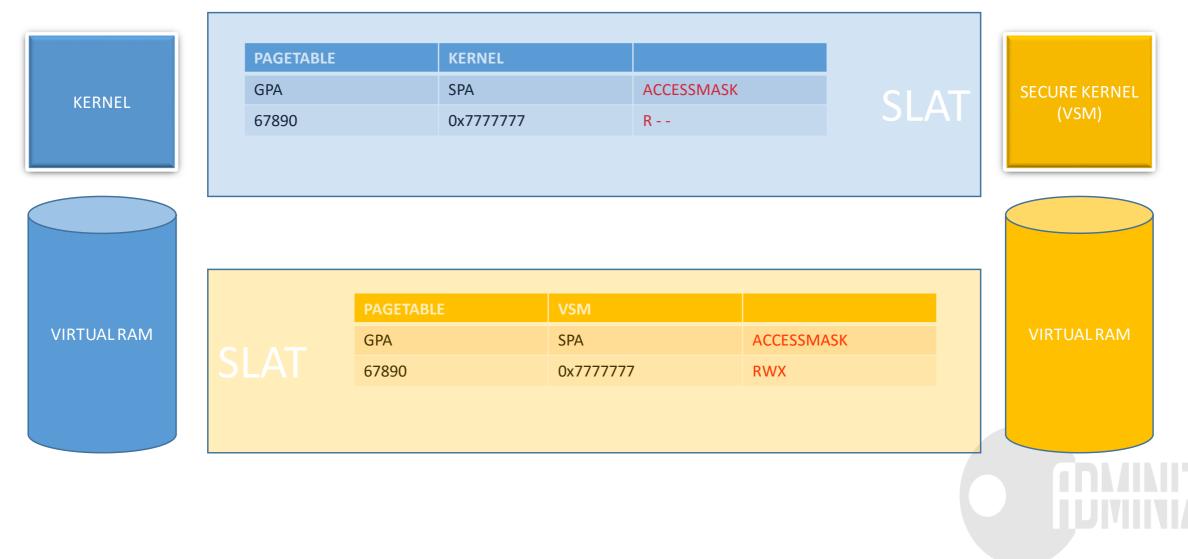
PAGETABLE	VM 2	
GPA	SPA	ACCESSMASK
хххх	уууу	Z-Z-Z
67890	0x7778888	R-X

SI AT

Kernel and Secure Kernel have their own SLAT's



Hypervisors and VMs



So what is VSM? Really?

- It's not really a VM but a functionality possible because of virtualization technology (Kind-Of-Semi-Almost-VM)
- This could be multiplied easily to many VMs



Enabling VSM

Windows Features	-	-		×				
Turn Windows feature	Turn On Virtualization Based Securit	ty					- 0	×
To turn a feature on, select its box. A filled box means that of Image: Image:	 Not <u>Configured</u> Comment: <u>E</u>nabled <u>D</u>isabled Supported on: 		/indows 10		Previous Setting	Next Setting		
Embedded Boot Exp Embedded Logon Embedded Shell Lau	Options:		He Sp		ther Virtualization	Based Security is	enabled.	~ ^
	Enable Virtualization Based Protectio	♥ n of Code	pro Se wir ha co	ovide suppo curity requi th the use c rdware sup nfigured de	Based Security use ort for security ser ires Secure Boot, a of DMA Protection port and will only evices. Based Protection	vices. Virtualizati nd can optionall <u>i</u> s. DMA protecti be enabled on co	ion Based y be enabled ons require orrectly	
Internet Explorer 11 Internet Information Internet Information Isolated User Mode			Th Ma pro Wa fea	iis setting en ode Code Ir otections ar otected by f arning: All o ature or the	nables virtualization tegrity. When this re enforced and th the virtualization b drivers on the syste system may crash	on based protecti is enabled kerne e Code Integrity pased security fea em must be com b. Ensure that this	on of Kerne el mode me validation p ature. patible with s policy setti	mory path is this ing is
				ily deployed	d to computers wh			tible. ↓ ↓pply

bcdedit /set vsmlaunchtype auto

ent 13, Wininit						×
General Details						
^						
Credential Guard	(Lsa	lso.exe) \	was stai	rted	and wi	ill protect LSA credentials.
똃 Task Manager						– 🗆 🗙
File Options View						
Processes Performance	e Ap	p history	Startup (Jsers	Details	Services
Name	PID	Status	User	C	Mem	Description
Lsalso.exe	620	Running	SYST	0	904 K	Credential Guard
Isass.exe	628	Running	SYST	0	6 348	Local Security Authority Process
CMicrosoftEdge.exe	1	Running	Sami	0	18 55	Microsoft Edge
CMicrosoftEdgeCP	7	Running	Sami	0	34 11	Microsoft Edge Content Process
CMicrosoftEdgeCP	3	Running	Sami	0	47 77	Microsoft Edge Content Process
MsMpEng.exe	2	Running	SYST	0	54 77	Antimalware Service Executable
NisSrv.exe	2	Running	LOC	0	5 536	Microsoft Network Realtime Inspection Service
OfficeClickToRun	1	Running	SYST	0	23 46	Microsoft Office Click-to-Run
🛆 OneDrive.exe	5	Running	Sami	0	67 64	Microsoft OneDrive
🗊 OptionalFeatures	4	Running	Sami	0	2 576	Windows Features
OUTLOOK.EXE	532	Running	Sami	0	84 77	Microsoft Outlook
POWERPNT.EXE	948	Running	Sami	0	11 60	Microsoft PowerPoint
POWERPNT.EXE	4	Running	Sami	0	152 7	Microsoft PowerPoint
PresentationFont	3	Running	LOC	0	5 192	PresentationFontCache.exe
RealSenseDCM.e	6	Running	SYST	0	16 90	Intel(R) RealSense(TM) Depth Camera Manager Service
RemindersServer	4	Suspen	Sami	0	2 172	Reminders WinRT OOP Server
RuntimeBroker.exe	3	Running	Sami	0	9 232	Runtime Broker
♣ SearchIndexer.exe	4	Running	SYST	0	60 70	Microsoft Windows Search Indexer
SearchUI.exe	4	Suspen	Sami	0	50 91	Search and Cortana application
Secure System	368	Suspen	SYST	0	16 K	
services.exe	600	Running	SYST	0	2 208	Services and Controller app
■ CattingConclusat 《	ſ	Dunning	Cami	^	ADC K	List Duscess for Catting Conchronization
Fewer details						End task

Trustlets

- Processes running in Virtual Secure Mode
 - Currently not available for developers
 - In the future anything that needs Secrets to stay secret
- Currently three trustlets
 - LSAISO = Credential Guard
 - vTPM = Virtual TPM
 - HVCI = Kernel Mode Code Integrity
- If a trustlet shuts down all keys are gone and the secrets are safe



Device Guard

- Device Guard requires:
 - UEFI Secure Boot with non-Microsoft UEFI CA removed from the UEFI database.
 - TPM 1.2
 - Virtualization support enabled by default in the system firmware (BIOS):
 - Virtualization extensions (e.g., Intel VT-x, AMD RVI)
 - SLAT (e.g., Intel EPT, AMD RVI)
 - IOMMU (e.g., Intel VT-d, AMD-Vi)
 - UEFI BIOS configured to prevent an unauthorized user from disabling Device Guard hardware security features.
 - Kernel mode drivers must be Microsoft signed and compatible with hypervisorenforced code integrity.
 - Windows 10 Enterprise only



DEMO

Process Dump



Nested Virtualization

Containers

- Containers are a new level of virtualization
- I see it like App-V for Operating Systems
- Two different levels: Server Containers and Hyper-V Containers
- More info:
 - <u>http://blogs.technet.com/b/virtualization/archive/2015/10/13/windows-</u> insider-preview-nested-virtualization.aspx
 - https://channel9.msdn.com/Events/Build/2015/2-704

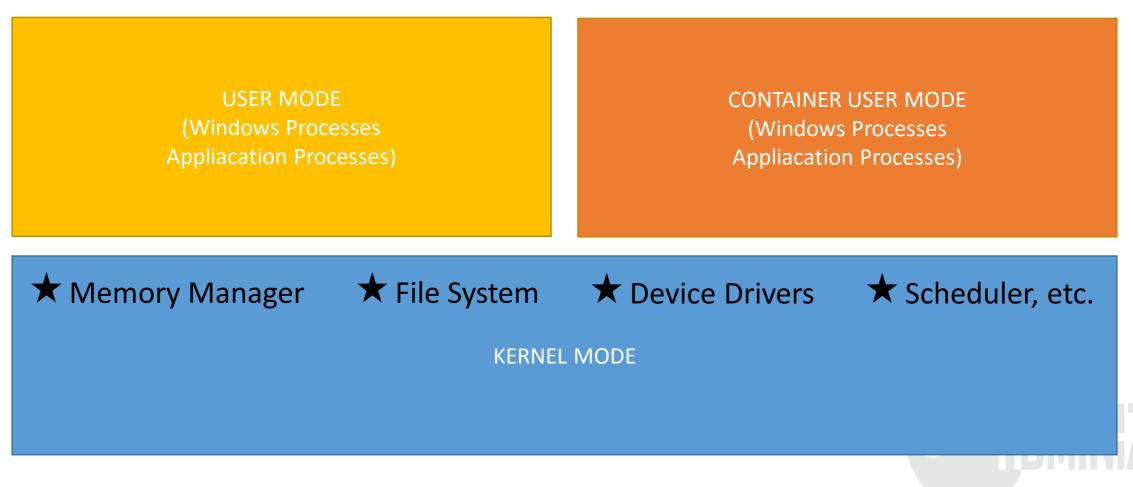


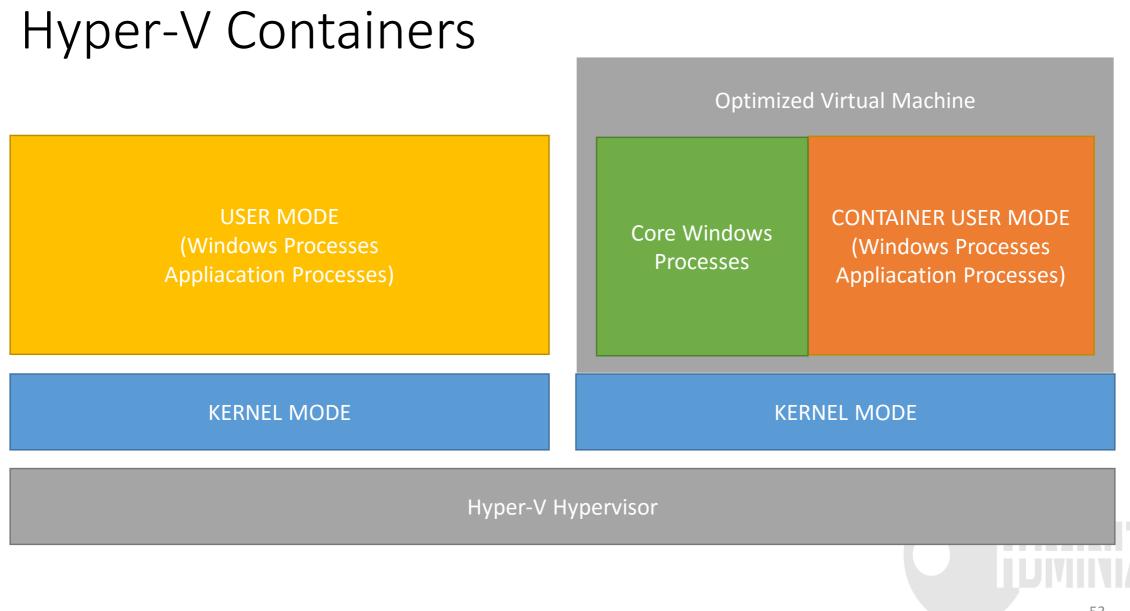
Server Containers

USER MODE

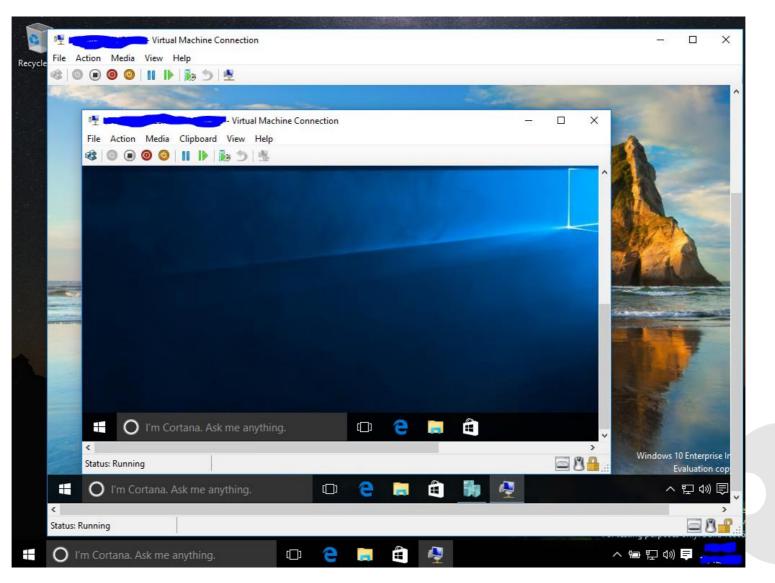
KERNEL MODE

Server Containers





Hyper-V inside of Hyper-V



Contact

- <u>sami@adminize.com</u>
- Twitter: @samilaiho
- Blog: <u>http://blog.win-fu.com/</u>
- Free newsletter: <u>http://eepurl.com/F-GOj</u>
- Websites:
 - <u>www.adminize.com</u>
 - www.win-fu.com
 - <u>www.wioski.com</u>
 - <u>www.samilaiho.com</u>
- Video-based training:
 - Later: <u>http://www.pluralsight.com/</u>
 - NOW: <u>http://dojo.win-fu.com/</u>



Nächster Event: Freitag 17. Juni Digicomp Bern (begrenzte Anzahl Teilnehmer möglich)