

Die Windows Sandbox wurde eingeführt, um versierten Anwendern und Admins die Möglichkeit einzuräumen, verdächtige Anwendungen, Webseiten und Dokumente zu prüfen.

Alles was in der Sandbox passiert, bleibt in der Sandbox. Nach einem Neustart der Sandbox, wird diese als frisches Windows wieder hochgefahren. Aus diesem Grund kann man die Sandbox auch als Wegwerf-Desktop bezeichnen.

Die aktuellen Anforderungen an die Windows Sandbox sind:

- Windows 10 Pro oder Enterprise
- AMD64 Architektur

•

•

- Eine im BIOS aktivierbare Virtualisierungsfunktion *
 - Minimum 4 GB RAM
 - 8GB empfohlen
 - Minimum 1 GB Festplattenspeicher
 - SSD empfohlen
 - Minimum 2 CPU-Kerne
 - o 4 Kerne mit Hyperthreading empfohlen

Hinweis: * Sobald ein Hypervisor innerhalb einer virtuellen Maschine eingesetzt wird, so muss die **Nested Virtualization** (geschachtelte Virtualisierung) aktiviert werden.

Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions \$true

Manuelles aktivieren der Sandbox auf einem physischen Host:



1. Im Bios die Virtualisierung einschalten.



2. Feature aktivieren



3. Sandbox starten





4. Mit der Sandbox arbeiten

Sandbox Vindows-Sandbox					<u></u> -1		×
Papterkorb							
A Microsoft Edge							
					10-	18	
Suchbegriff hier eingeben	Ξi	 e		■ ײ ⊄	⁽⁾⁾ 17.03.	2019	0

Sobald die Sandbox heruntergefahren und neu gestartet wird, handelt es sich immer um ein neues und somit frisches Windows 10.

Aktivieren der Sandbox mithilfe der Powershell:

Enable-WindowsOptionalFeature –FeatureName "Containers-DisposableClientVM" -All – Online

Deaktivieren der Sandbox mithilfe der Powershell:

Disable-WindowsOptionalFeature –FeatureName "Containers-DisposableClientVM" – Online

Aktivieren der Sandbox über die CMD:

Dism /online /Enable-Feature /FeatureName:"Containers-DisposableClientVM" -All

Deaktivieren der Sandbox über die CMD:

Dism /online /Disable-Feature /FeatureName:"Containers-DisposableClientVM"



Die Sandbox wird über das Remote Desktop Protokoll administriert.

0	++ all Windows-Sandbox _ d' X	
Papitatkorio	- □ × (● ① http://www.der-windows-papst.de/ ・ 量 C Suchen	
Microsoft Edge		
	DER WINDOWS PAPST – IT BLOG ESSEN JÖRN	
	WALTER	
	Du bist hier: Startseite	
	DED WINDOWC DADET Diese Webseite verwendet Cookies. Cookies werden zur Benutzerführung und Webanalyse	
	verwendet und helfen dabei, diese Webseite besser zu machen. Akzeptieren Ablehnen	
	Zum Datenschutz 🗸	
Suchbegriff hier	eingeben 🛱 🤁 📜 🧟	■ 厚 (30) 11:00 □ 17.03.2019 □

Der Computername wird generiert und bleibt bestehen.

	System			– 🗆 X			
÷	→ 🗠 🛧 👱 > Systemsteue	erung > System und Sicherheit	> System v Ö Systemster	uerung durchsuchen 🔎			
	Startseite der Systemsteuerung	Basisinformationen übe	r den Computer anzeigen	0			
•	Geräte-Manager	Windows-Edition					
•	Remoteeinstellungen	Windows 10 Pro					
•	Computerschutz	© 2019 Microsoft Corporat	100000				
•	Erweiterte Systemeinstellungen	Alle Rechte vorbehalten.	000510				
		Prozessor:	2.79 GHz				
		Installierter Arbeitsspeicher (RAM):					
		Systemtyp:	64-Bit-Betriebssystem, x64-basierter Prozessor				
		Stift- und Toucheingabe:	Für diese Anzeige ist keine Stift- oder Toucheir	ngabe verfügbar.			
		Einstellungen für Computernamen, Domäne und Arbeitsgruppe					
		Computername: 7fb1111f-5a8e-4b49-9a22-e3465615e5d2		Einstellungen			
		Vollständiger Computername:	7fb1111f-5a8e-4b49-9a22-e3465615e5d2	ändern			
		Computerbeschreibung:					
		Arbeitsgruppe:	WORKGROUP				
		Windows-Aktivierung					
	Siehe auch	Windows ist nicht aktiviert.	Microsoft-Softwarelizenzbedingungen lesen				
	Sicherheit und Wartung	Produkt-ID: Nicht verfügba	ar	Windows aktivieren			



Die Auslastung ist recht hoch, aus diesem Grund sollte man sich schon an die empfohlenen Anforderungen halten.

🙀 Task-Manager —							×	
Datei Optionen Ansicht								
Prozesse Leistung App-Verlauf Autos	tart Benutzer Details	Dienste						
^		53%	61%	1%	0%			
Name	Status	CPU	Arbeitss	Datenträ	Netzwerk	Stromverbrau	Stromver	brau
> 🖶 Spoolersubsystem-Anwendung		0%	1,1 MB	0 MB/s	0 MBit/s	Sehr niedrig		^
> 💷 Starten		0%	11,8 MB	0 MB/s	0 MBit/s	Sehr niedrig		
🔯 System Settings Broker		0%	4,1 MB	0 MB/s	0 MBit/s	Sehr niedrig		
📧 TechSmith HTML Help Helper (3		0%	0,4 MB	0 MB/s	0 MBit/s	Sehr niedrig		
📧 Usermode Font Driver Host		0%	0,2 MB	0 MB/s	0 MBit/s	Sehr niedrig		
> 📧 Verwaltungsdienst für virtuelle		0%	2,4 MB	0 MB/s	0 MBit/s	Sehr niedrig		
Vmmem		39,2%	1.458,9 MB	0 MB/s	0 MBit/s	Sehr hoch		
Windows Defender SmartScreen		0%	5,4 MB	0 MB/s	0 MBit/s	Sehr niedrig		
Windows Driver Foundation - B		0%	0,9 MB	0 MB/s	0 MBit/s	Sehr niedrig		
💽 Windows Driver Foundation - B		0%	0,1 MB	0 MB/s	0 MBit/s	Sehr niedrig		
📧 Windows Graphisolierung für A		0%	5,2 MB	0 MB/s	0 MBit/s	Sehr niedrig		
		007	4.5.4.0		0.000	e + - + +		~
(Weniger Details							Task bee	nden

Mit der Tastenkombination CTRL + ALT + Pause wird die Sandbox im Vollbildmodus angezeigt.

Mit der Tastenkombination SHIFT + ALT + Druck öffnet man den Bildschirmmodus für hohen Kontrast.

Speicherort der Sandbox:

Die Sandbox liegt im Pfad C:\ProgramData\Microsoft\Windows\Containers

sowie das Basis Image z.B. Die gestartete Sandbox liegt als Snapshot im Ordner Sandboxes.

📙 🛃 📙 🖛 Containe	ers			- 0	\times			
Datei Start Freige	ben Ansicht				~ ?			
← → * ↑ <mark>·</mark> « P	iners" durchsuchen	Ą						
	Name	Änderungsdatum	Тур	Größe				
📌 Schnellzugriff	Baselmages	17.03.2019 09:57	Dateiordner					
ineDrive 🍊 🍊	Dumps	17.03.2019 11:11	Dateiordner					
Dieser DC	PortableBaseLayer	17.03.2019 09:57	Dateiordner	ordner				
	Sandboxes	17.03.2019 09:58	Dateiordner					
💣 Netzwerk	Zygotes	17.03.2019 09:58						
5 Elemente								

Erstellt von Jörn Walter



Externe Quelle:

https://techcommunity.microsoft.com/t5/Windows-Kernel-Internals/Windows-Sandbox/ba-p/301849