
Windows 10
im Unternehmen

Netz-Weise
Lernen von den Besten.

Holger Voges

CCA,MCSE, MCDBA, MCT, MCITP DB Administrator / DB Developer, MCTIP Enterprise Administrator, MCSE Windows Server 2012, MCSE Data Platform

Netz-Weise
Freundallee 13a
30173 Hannover
www.netz-weise.de

Agenda

- Die Versionsunterschiede
- Deployment
- Die Arbeitsoberfläche
- Windows Update
- Hyper-V
- Die Kommandozeile
- Interna
- Credential Guard
- Device-Guard
- Passport und Hello
- Enterprise Data Protection
- weitere Funktionen

Wichtige Neuerungen in Windows 8

Netz-Weise
Lernen von den Besten.

- Storage Spaces
- Dateiversionsverlauf
- UEFI-Boot
- Virtual Smartcards

Editionen

Netz-Weise
Lernen von den Besten.

- Home
- Pro
- Enterprise
- Education
- Enterprise LTSB (Long Time Service Branch)
- Vergleich
- Ein OS für alle:
  - X-Box
  - PC
  - Tablet
  - Windows Phone

Deployment

Netz-Weise
Lernen von den Besten.

- MDT 2013 Update 1 (Re-Release vom 15.09.2015) mit Win 10 ADK
- System Center 2012 R2 SP1 mit Windows 10 ADK
- Anforderungen:
  - TPM 2.0 empfohlen (bald Pflicht für Hersteller)
- ICD erlaubt das nachträgliche Anpassen von Images (Provisioning Packages)

Updates im MDT

- Support for new Enterprise LTSB and Education editions of Windows 10
- Support for modern app (.appx) dependencies and bundles
- Improved support for split image files (.swm)
- Switched to using DISM for imaging processes (instead of deprecated ImageX)
- Deployment Workbench revisions for deprecated content
- Enhanced accessibility within the Deployment Workbench
- Revised lists of time zones, regions and languages in the Deployment Wizard
- Removed Start menu shortcut for “Remove PXE Filter”
- Several MVP recommended fixes for Windows Updates, password handling, and PowerShell cmdlets
- Added missing OOBE settings to Unattend.xml
- Unattend.xml default screen resolution changed to allow for automatic scaling
- Updated task sequence binaries from System Center 2012 R2 Configuration Manager SP1
- New GetMajorMinorVersion function for integer comparison of Windows version numbers

http://blogs.technet.com/b/msdeployment/archive/2015/08/17/mdt-2013-update-1-now-available.aspx

Desktop

Netz-Weise
Lernen von den Besten.

- virtuelle Desktops (Strg+Win+Pfeil) zum wechseln
- Action Center zur Schnellkonfiguration
- Startmenü basiert auf Datenbank
- Starmenü anpassen: Win+i > Personalisierung > Start
- Continuum (Tablet-Modus)
- Cortana 
- Powershell + Gruppenrichtlinien zur Verteilung von Startmenüs

Windows Update

Netz-Weise
Lernen von den Besten.

- Updates werden als Kumulative Updates verteilt
- Windows 10 Update kann Updates zwischen Clients („Bittorrent“) verteilen
- Updates können in Pro und Enterprise zurückgestellt werden
- Feature-Updates können nur in der LTSB*-Version verhindert werden
- keine Unterscheidung zwischen Update-Typen (kritisch, wichtig,…) mehr

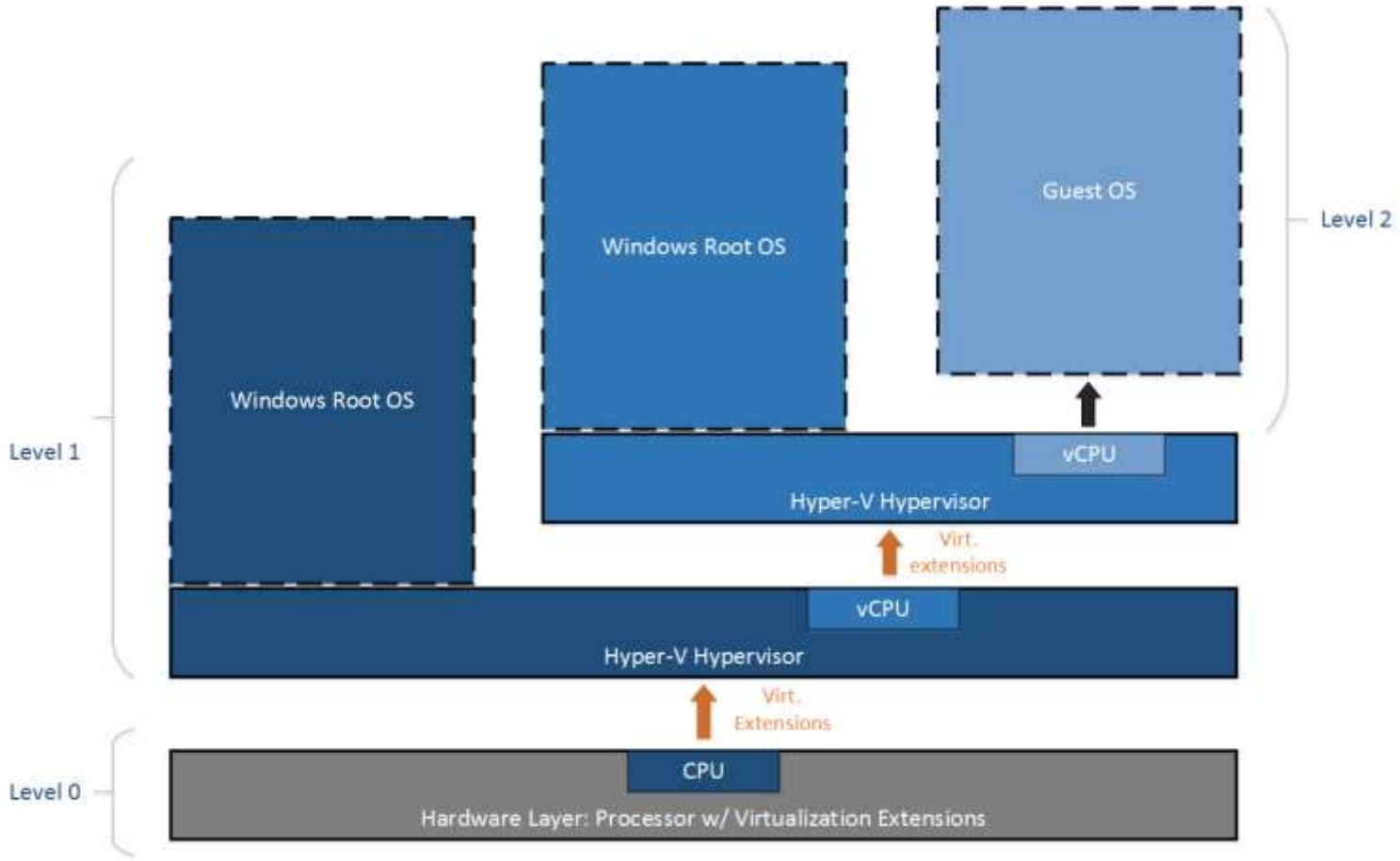
*Long Term Service Branch

Hyper-V

- PowerShell Direct
- Hot-Add Memory
- Hot-Add Netzwerkkarten (ab Gen 2)
- Production Checkpoint
- Connected Standby funktioniert mit Hyper-V
- Linux Secure Boot unterstützt mehr Distributionen
- Virtual Machine Configuration mit neuen Format (.VMCX)
- Integration-Services werden durch Windows Update aktualisiert (Ab Windows 7 / Server 2008 Guest OS)
- Nested Virtualization

Nested Virtualization

Netz-Weise
Lernen von den Besten.



Powershell + CMD

- Powershell und CMD unterstützen jetzt Cut and Paste per Tastatur
- Automatische Anpassung der Spalten und Zeilen an die Fenstergröße!
- Powershell 5.0:
  - Powershell Package-Manager
  - DSC deutlich erweitert
  - Debugging

Interna

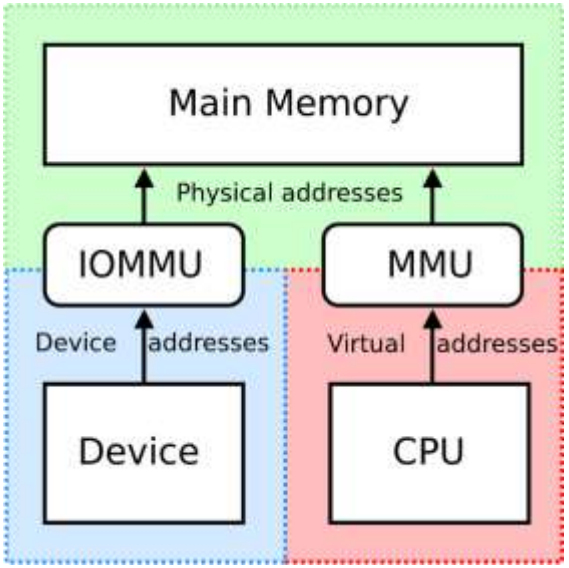
Netz-Weise
Lernen von den Besten.

- Memory Compression verringert Paging
- Isolated User Mode sichert LSASS.exe vor Zugriff
- Virtual Secure Mode sichert Windows vor unbefugtem Speicherzugriff mit SLAT und IOMMU
- Enterprise-Edition, SLAT und Virtualisierungserweiterungen (vt-x) sind für Isolated User Mode und VSM erforderlich

https://de.wikipedia.org/wiki/Second_Level_Address_Translation

https://de.wikipedia.org/wiki/IOMMU

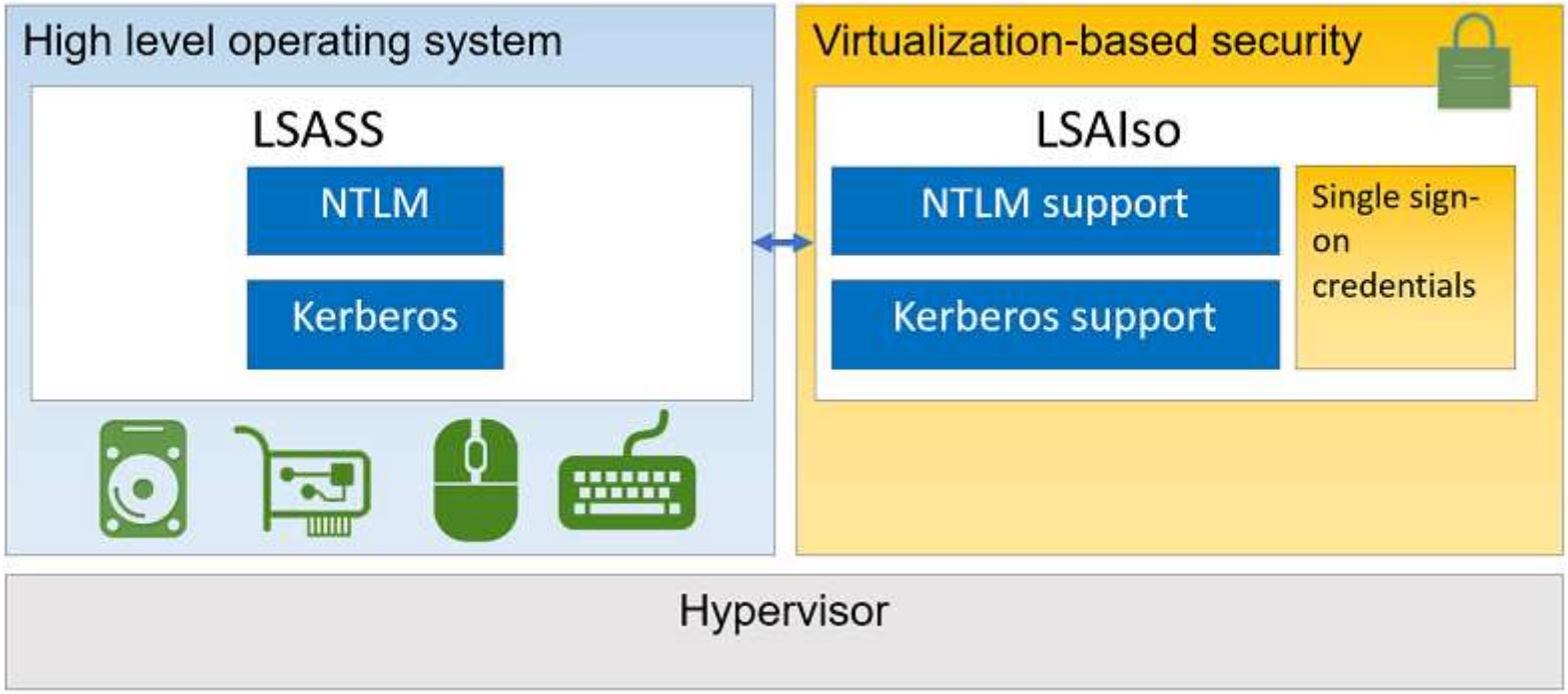
https://de.wikipedia.org/wiki/Memory_Management_Unit



Credential Guard

Netz-Weise
Lernen von den Besten.

- Credential-Guard ist die Bezeichnung für die Nutzung des Isoloated User-Mode zur Sicherung von Kennwörtern, Hashes und Tickets in gesicherten Secure User Mode



Credential Guard Anforderungen

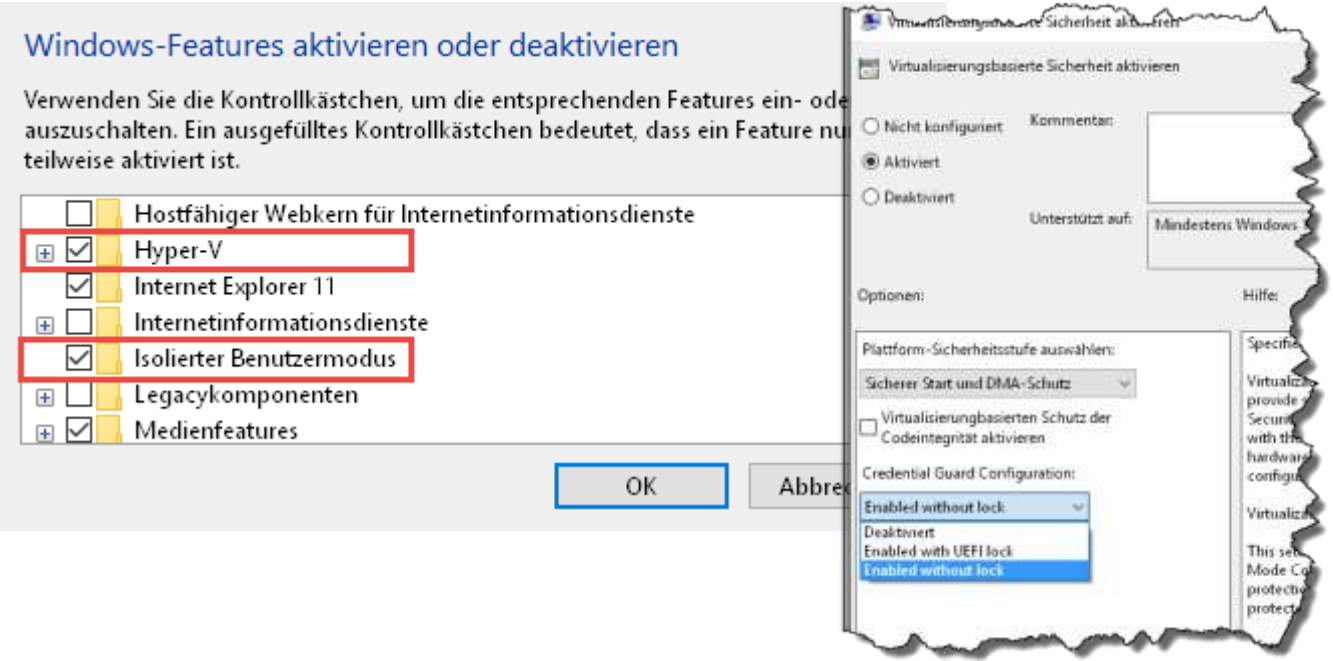
- Windows 10 Enterprise
- Physikalischer PC
- UEFI firmware version 2.3.1 or higher and Secure Boot
- Virtualisierungs-Erweiterungen VT-x / AMD-V, SLAT
- x64-Architektur
- IOMMU (Input / Output Memory Management Unit) *
- TPM 2.0 *
- Secure Firmware Update *
- Secure MOR *

* Optional

Device-Guard

Netz-Weise
Lernen von den Besten.

- Device-Guard erstellte eine Sicherheitskette, die das ausführen von unsigniertem Code verhindert
- Der Bootvorgang wird über SecureBoot abgesichert
- Windows startet nur signierte Programme und Apps
- Virtualization Based Security sichert Device-Guard vor Kernelmode-Angriffen



Windows Hello

Netz-Weise
Lernen von den Besten.

- Authentifizierung mit biometrischen Daten
  - Iris-Erkennung
  - Fingerabdruck-Erkennung
  - Gesichts-Erkennung
- Für die Gesichts- und Iriserkennung wird eine spezielle Kamera mit Infrarotbeleuchtung bzw. eine räumliche Kamera (Intel Realsense) benötigt

Hello Gesichtserkennung

Netz-Weise
Lernen von den Besten.

Fazit

Windows Hello wirkt durchaus alltagstauglich und ist nicht leicht zu überlisten. Dass sich das Notebook automatisch entsperrte, wenn wir uns davor setzten, hat uns Spaß gemacht. Mit dieser Funktion wird eine Bildschirmsperre nach sehr kurzer Zeit alltagstauglich…

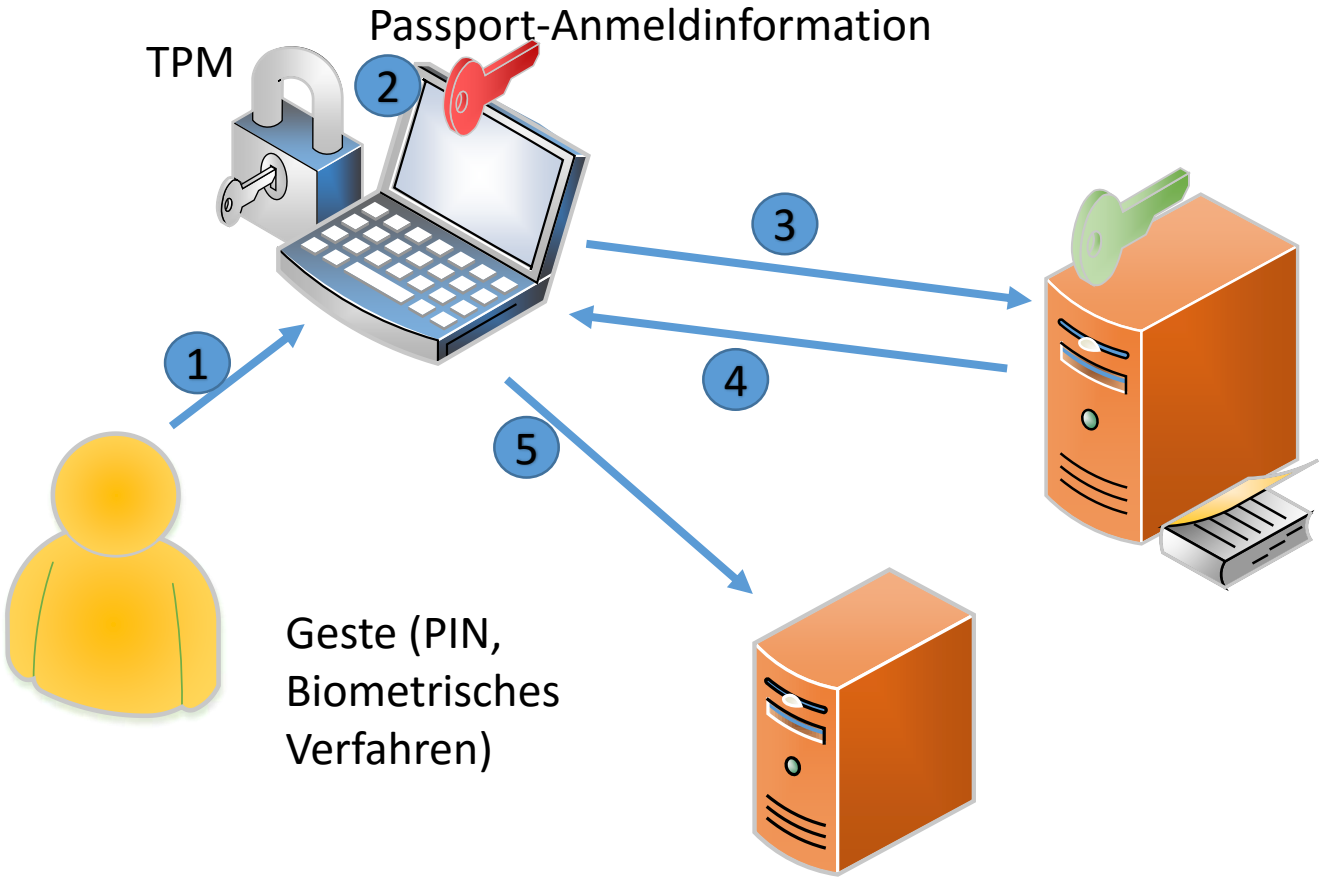
http://www.heise.de/ct/artikel/Windows-Hello-Anmeldung-per-Gesichtserkennung-auf-dem-Pruefstand-2761764.html?hg=1&hgi=1&hgf=false

[…] Die Zeitung *The Australian* hat das System jetzt mit sechs Paaren von Zwillingen getestet: In keinem Fall konnte sich der "falsche" Zwilling in den Account des anderen einloggen. […]

http://www.heise.de/newsticker/meldung/Windows-Hello-laesst-sich-von-Zwillingen-nicht-taeuschen-2789690.html

Microsoft Passport

Netz-Weise
Lernen von den Besten.



https://technet.microsoft.com/de-de/library/mt219735%28v=vs.85%29.aspx

Enterprise Data Protection

Netz-Weise
Lernen von den Besten.

- Windows 10 Geräte können per MDM* verwaltet warden
- Verschlüsselung kann auf privaten- und Unternehmensgeräten aktiviert werden
- Private Daten werden beim Remote-Löschen des Gerätes nicht betroffen
- “Privilegierte Anwendungen” können Unternehmens-Daten verwenden. Es können Nicht-Privilegierte Anwendungen bestimmt werden.
- Die Unterscheidung zwischen Privaten- und Unternehmensdaten wird über die Quelle bestimmt, nicht über unterschiedliche Konten.

* Mobile Device Management, API zur Remote-Verwaltung von Mobilgeräten

Weitere Features

- Neue Funktionen im Auditing
- Bitlocker-Integration in Azure-AD
- UAC integriert AMSI (Antimalware Scan Interface). Wird malware erkannt, kann der Benutzer keine Admin-Privilegien mehr erhalten.
- Device Lockdown
  - wird über Benutzerkonten bestimmt und löst den Kioskmodus ab.
  - Der Benutzer kann nur eine App starten, die beim Anmelden aufgerufen wird