Endpoint Security mit Windows 10

lingen 2019

cim

Marc Grote

Wer bin ich?

- Marc Grote
- Erster Rechner 1984 / seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig / ab 2022 Rentner
- MVP Forefront (2004-2014), MVP Hyper-V (2014), MVP Cloud and Datacenter (2015-2017), Microsoft MCT/MCSE Messaging/Security/Server/MCLC /MCITP*/MCTS*/MCSA*/MC* MCSE Private Cloud, Productivity, Cloud Platform and Infrastructure, Server Infrastructure, Exchange
  MCS Server Virtualization Hyper-V / System Center/ Azure
  MCITP Virtualization Administrator
- Buchautor und Autor fuer Fachzeitschriften
- Schwerpunkte:
  - Windows Server Clustering/Virtualisierung/Security
  - Exchange Server seit Version 5.0
  - System Center VMM/SCEP/DPM
  - von *.Forefront reden wir nicht mehr ☹

Agenda

- Ueberblick Windows (Microsoft) Defender Produktfamilie
- Bitlocker / Bitlocker to Go
- Windows Sandbox
- Windows Firewall
- Patchhell
- Zertifikate / Verschluesselung
- USB Kontrolle
- Gruppenrichtlinien
- Virenscanner
- Scripting und Powershell
- Microsoft Security and Compliance Toolkit
- Faktor Mensch

Das sicherste Windows aller Zeiten – mit dauerhaftem Schutz

- Windows 10 bietet umfassende, integrierte und stets aktuelle Sicherheitsfeatures, auf die Sie sich verlassen können – einschließlich Windows Defender Antivirus, Firewall und vielem mehr. Sie bleiben stets auf dem neuesten Stand und können sicher sein, dass Sie über aktuelle Features und aktuellen Schutz verfügen – ohne Zusatzkosten

Quelle: https://www.microsoft.com/de-de/windows/comprehensive-security

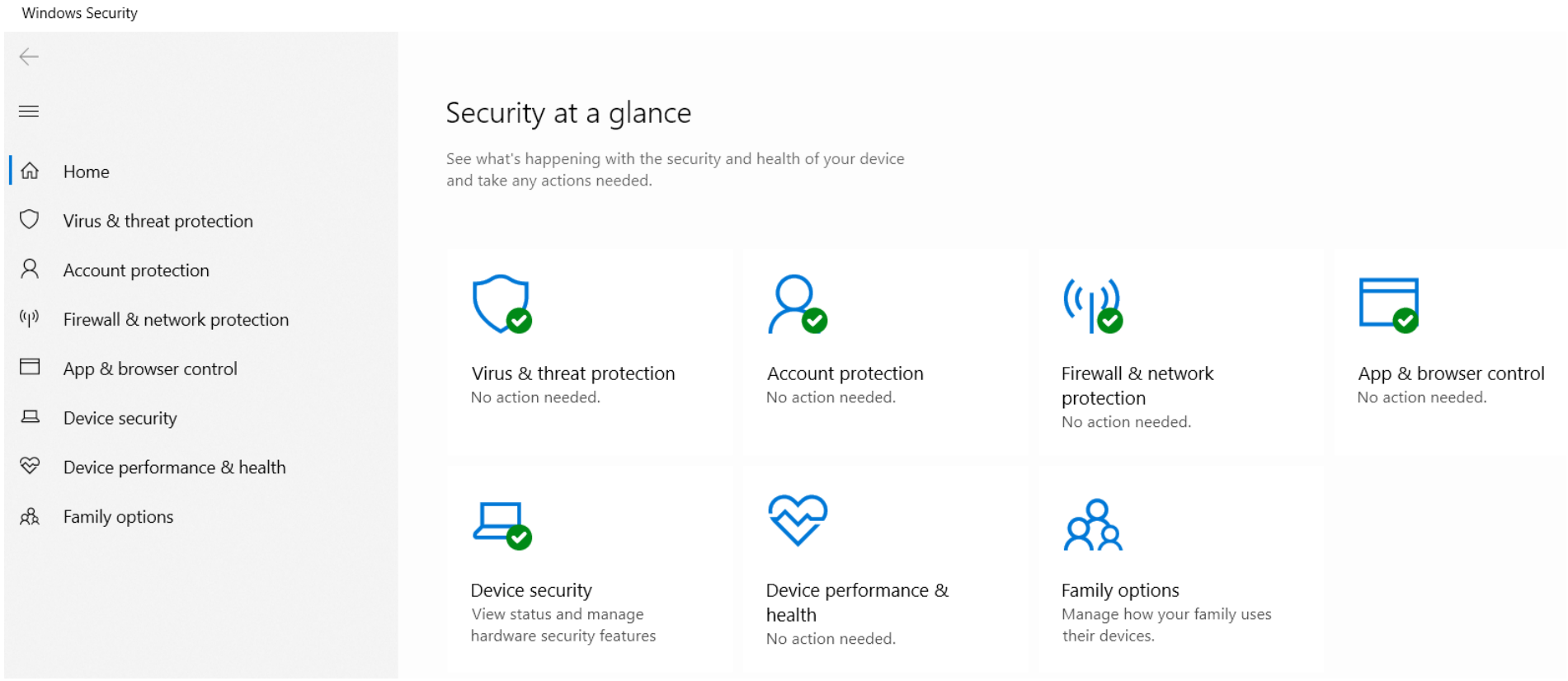
Windows Defender Produkt Familie

- Windows Defender Firewall
- Windows Defender Security Center
- Windows Defender Application Guard
- Windows Defender Application Control
- Windows Defender Exploit Guard
- Windows Defender Smartscreen
- Windows Defender Credential Guard
- Microsoft Defender Advanced Threat Protection
- In Windows 10 20 H1 … Microsoft Defender?

Windows Defender Security Center

- Windows Defender Funktionen (Virus und Threat Protection)
- Firewall und Network-Protection (Zustand der Windows Defender Firewall mit erweiterter Sicherheit)
- Geraete-Performance und -Gesundheitszustand
- App & Browser Control (Windows Defender Smartscreen Konfiguration für Anwendungen, Dateien und den Microsoft Edge Browser)
- Family Options (Steuerung des Zugriffs auf Webseiten, Zeitsteuerung für Anwendungen und Zugriff auf erlaubte Anwendungen für Kinder)

Windows Defender Security Center



Windows Defender Application Guard

- Nicht vertrauenswuerdige Webseiten im Microsoft Edge / IE Browser werden in einer isolierten Umgebung ausgefuehrt
- Hyper-V wird als (Container)Technik verwendet
- Systemanforderungen beachten (4 GB RAM – 8 GB besser), 64 Bit CPU, AMD-V oder Intel VT-x, 5 GB HD Space, SSD empfohlen
- Konfiguration per GPO: https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-guard/configure-wd-app-guard

Windows Defender Application Control

- Applocker fuer Fortgeschrittene
- Unternehmensweites Anwendungs-Whitelisting mit Windows Code Integrity Sicherstellung
- WDAC kann auch nicht signierte Skripte reglementieren und die Windows PowerShell im restricted Language Mode ausfuehren lassen
- Ehemals Windows Defender Device Guard
- Ab Windows 10 1703 kann WDAC Plug-Ins, Add-Ins und Module von Apps reglementieren

Windows Defender Exploit Guard

- Windows Defender Exploit Guard (WDEG) stellt ab Windows 10 1709 eine Reihe von IPS Funktionen zur Verfuegung, um die Angriffsoberflaeche von verwendete Anwendungen durch Benutzer zu reduzieren
- WDEG wird auch als EMET II bezeichnet
- WDEG stellt Techniken wie Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Structured Exception Handling Overwrite Protection (SEHOP) zur Verfuegung
- Die Konfiguration von WDEG erfolgt im Windows Defender Security Center
- WDEG erweitert die mit EMET bereitgestellten Sicherheitsfunktionen mit dem Control Flow Guard (CFG)

Windows Defender Smartscreen

- Windows Defender Smartscreen hilft dabei den Aufruf von Webseiten, welche als Phishing- oder Malware-Webseiten gemeldet wurden, zu verhindern oder den Download von potentiell gefaehrlichen Dateien zu blockieren
- Smartscreen analysiert die besuchten Webseiten und vergleicht diese mit dynamischen Listen mit gemeldeten Phishing-Webseiten und Webseiten mit Schadsoftware
- Smartscreen prueft ob eine heruntergeladene App oder ein App-Installer potenziell gefaehrlich ist und vergleicht die heruntergeladenen Dateien mit einer Liste von gemeldeten Webseiten und Programmen mit Schadsoftware, die als unsicher bekannt sind
- Die Konfiguration von Smartscreen kann mit Hilfe von Active Directory Gruppenrichtlinien oder einer Mobile Device Management (MDM) Loesung wie Microsoft Intune erfolgen

Windows Defender Credential Guard

- Windows Defender Credential Guard (WDCG) verwendet virtualisierungsbasierte Sicherheit (Hyper-V), um Secrets wie Kennwoerter, Passwort-Hashes und Kerberos Ticket Granting Tickets zu isolieren und nur privilegierten Systemprozessen Zugriff auf die Daten zu gewaehren
- Mit WDCG sind dann Tools zur Ermittlung von NTLM-Hashes oder Pass-the-Hash und Pass-the-Ticket nicht mehr moeglich
- Hardware-Anforderungen fuer Virtualization Based Security (VBS):
  - 64 Bit CPU, aktivierte CPU Virtualization Extensions und Extended Page Tables, sowie einen Windows Hypervisor, Secure Boot, TPM 2.0 (empfohlen), UEFI Lock (empfohlen)
- Die Konfiguration von WDCG erfolgt mit Hilfe von GPO

Microsoft Defender ATP

- Microsoft Defender Advanced Threat Protection ist ein Dienst fuer Windows 10 Enterprise/Education E5 oder Microsoft 365 E5 ab Version 1607, mit dessen Hilfe Administratoren Angriffe in einem Netzwerk erkennen und entsprechende Gegenmaßnahmen einleiten koennen
- Microsoft Defender ATP vereint Windows 10 Schutzmaßnahmen und Microsoft Cloud-Technologien in einer Loesung
- Zu den Funktionen gehoeren Techniken zur Erkennung von Anomalien auf (Registry-, Dateisystem- und Netzwerkzugriffe), Sicherheits-Analyse Funktionen in der Microsoft Cloud (Bing und Smartscreen Reputation), Microsoft Malicious Removal Tool (MRT) und Threat Intelligence
- Microsoft Defender ATP arbeitet mit Anwendungen wie Applocker, und Windows Defender zusammen
- Microsoft Defender fuer Mac
- Die Konfiguration kann mit Hilfe von Gruppenrichtlinien, SCCM, einer Skript-Konfiguration oder MDM-Loesungen wie Microsoft Intune erfolgen

Bitlocker / Bitlocker to Go

- Laufwerksverschluesselung
- TPM Chip
- XTS-AES 128, AES-CBC 128, AES-CBC 256
- Bitlocker Network Unlock
- Steuerung ueber Gruppenrichtlinien
- Bitlocker Recovery Key Speicherung im AD
- MBAM ist Tod lang lebe Microsoft Intune oder SCCM

Windows Sandbox

- Anwendungsausfuehrung in einer isolierten VM
- VM teilt sich Binaries mit Host System
- Keine Netzwerkverbindung zum Host System
- Beim Schliessen der Sandbox werden die Aenderungen verworfen
- Erweiterung von Windows Defender Application Guard (Ausfuehrung von Webseiten im Browser in einer isolierten VM)
- Verfuegbar ab Build 18305

Windows Sandbox

Ansehen

Windows Firewall

- Wer hat die Windows Firewall flaechendeckend auf Clients eingeschaltet?
- Wer hat die Windows Firewall flaechendeckend auf Servern eingeschaltet?
- Steuerung ueber Gruppenrichtlinien
- Eine aktivierte Windows Firewall tut (meist) nicht weh
- Lieber einen Grundschutz als keinen Schutz → einfach mal aktivieren und testen

Patchhell

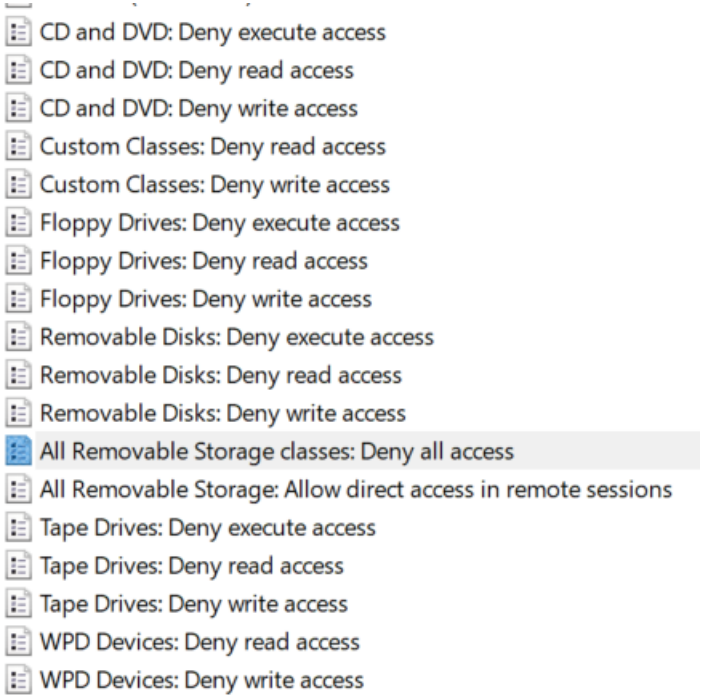
- „Patch as Patch can“ oder „never change a running system“
- Standalone Windows Update oder verwaltet durch WSUS, SCCM oder andere
- Update fuer Microsoft Produkte sind einfach …
- Aber wie die anderen Produkte patchen?
  - Z. B. GFI LanGuard, Ivanti Patch Management, Manage Engine
- Update Bereinigung / Reporting

Zertifikate / Verschluesselung

- Zertifikate → Das Grauen aller (vieler) Admins und User
- Zertifikate sind notwendig (Authentication, Authorization, Verschluesselung …)
- Self Signed Zertifikate vermeiden → PKI Zertifikate verwenden
- Verschluesselung wo machbar und sinnvoll? → SMB, LDAP, HTTPS, Anwendungen
- EFS – Encrypting File System

USB Kontrolle

- GPO zur Steuerung der Zugriffe auf USB Geraete (Hardware IDs etc. ☺)
- GPO - Computer Configuration\Administrative Templates\System\ Removable Storage Access
- Microsoft Defender ATP zur USB Steuerung
- Third Party Software



Gruppenrichtlinien

- Kennen wir doch alle oder?

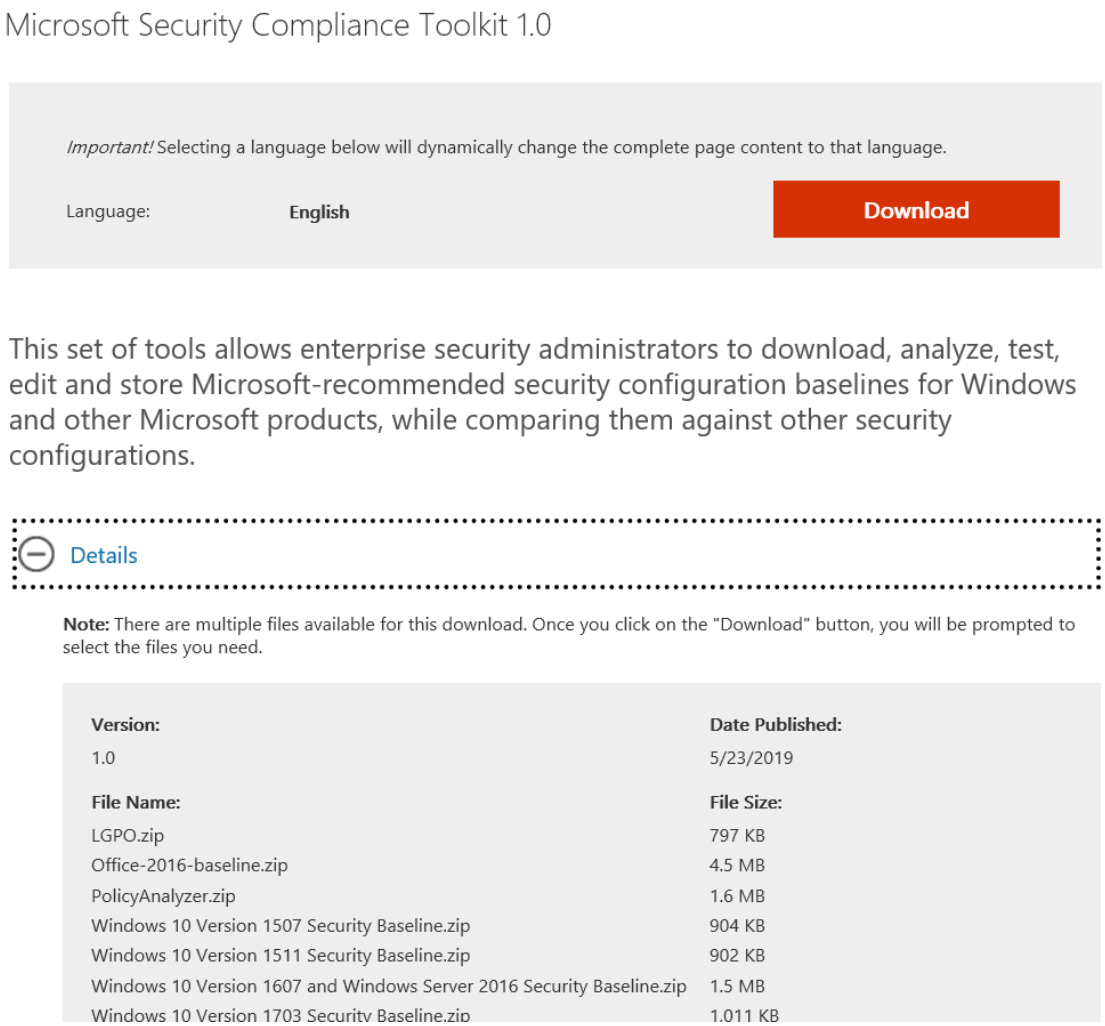
Virenscanner

- Unser Virenscanner bremst alle Systeme aus
- Unser Virenscanner hat neulich wieder eine unserer wichtigsten Anwendungen blockiert
- Unser Virenscanner hat nach einem Update den Port 25 blockiert
- Seit wir die neue Virenscanner Signatur haben bekommen wir staendig Fehlermeldungen
- Der Hersteller Support unserer Anwendung empfiehlt keinen Einsatz eines Virenscanners
- Auf den folgenden 20 Seiten finden Sie alle notwendigen Ausschluesse des Virenscans fuer unsere Anwendung

Scripting und Powershell

- Meine notwendigen Scripte und Powershell cmdlets finde ich alle im Internet
- Scripts und cmdlets auf Basis von Try and Error ausfuehren
- Set-ExecutionPolicy –ExecutionPolicy Unrestricted
- winrm s winrm/config/client @{TrustedHosts="*"}
- JEA/JIT ist die Rettung?: https://docs.microsoft.com/de-de/powershell/jea/overview

Microsoft Security Compliance Toolkit

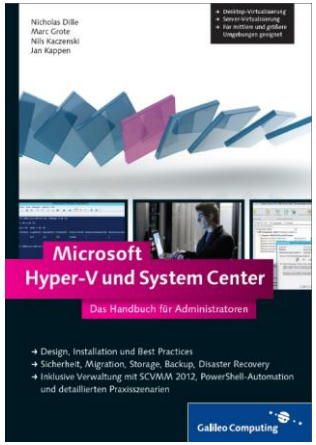


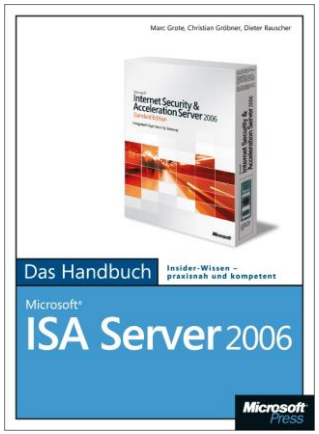
Faktor Mensch

- Wer sperrt schon seinen Rechner
- Meldungen am Bildschirm stoeren nur
- Jede E-Mail die ich bekomme ist fuer mich und wichtig
- Was kann ich denn mal so an Anwendungen und Apps installieren??
- Schnell mal die Dokumente von der Arbeit nach Hause senden
- Zertifikatsmeldungen im Browser sind was fuer Studierte
- Damit mein Azubi arbeiten kann, gebe ich dem meine Zugangsdaten

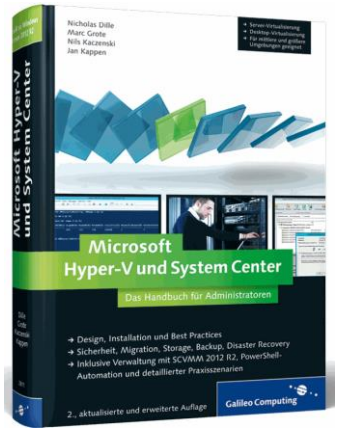

Fragen?

Werbung

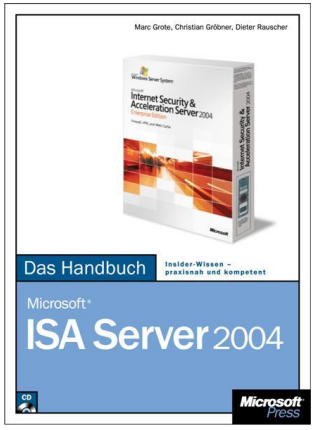

Nicholas Dilie
Marc Grote
Nils Kaczenski
Jan Kappen
Microsoft
Hyper-V und System Center
Das Handbuch für Administratoren
→ Design, Installation und Best Practices
→ Sicherheit, Migration, Storage, Backup, Disaster Recovery
→ Inklusive Verwaltung mit SCVMM 2012, PowerShell-Automation und detaillierten Praxisszenarien
Galileo Computing

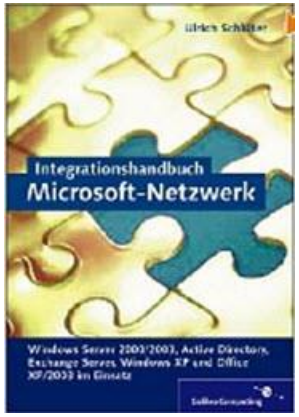

Marc Grote, Christian Gröbner, Dieter Rauscher
Das Handbuch
Insider-Wissen – praxisnah und kompetent
Microsoft
ISA Server 2006
Microsoft Press

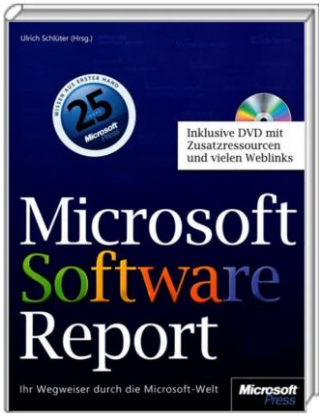

Marc Grote, Christian Gröbner, Dieter Rauscher
Forefront
Threat Management
Gateway 2010
Das Handbuch
Insider-Wissen – praxisnah und kompetent
Microsoft
Forefront
Threat Management
Gateway 2010
Microsoft Press

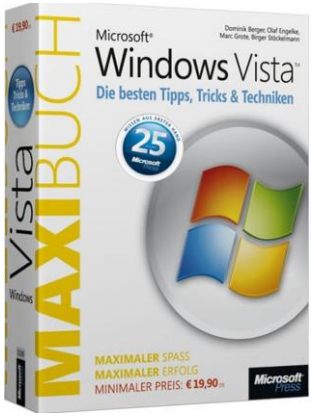

Nicholas Dilie
Marc Grote
Nils Kaczenski
Jan Kappen
Microsoft Hyper-V und System Center
Microsoft
Hyper-V und System Center
Das Handbuch für Administratoren
→ Design, Installation und Best Practices
→ Sicherheit, Migration, Storage, Backup, Disaster Recovery
→ Inklusive Verwaltung mit SCVMM 2012 R2, PowerShell-Automation und detaillierter Praxisszenarien
2., aktualisierte und erweiterte Auflage
Galileo Computing

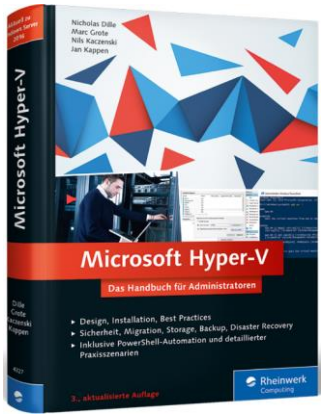

IT Administrator
Sonderheft
Troubleshooting
Microsoft-Server
Windows-, Exchange- und SQL-Server-Probleme erkennen und beheben
IT Administrator
Sonderheft
Monitoring
Methoden und Werkzeuge zur Leistungs- und Verfügbarkeitsüberwachung von IT-Systemen


Marc Grote, Christian Gröbner, Dieter Rauscher
Das Handbuch
Insider-Wissen – praxisnah und kompetent
Microsoft
ISA Server 2004
Microsoft Press


Integrationshandbuch
Microsoft-Netzwerk


Ulrich Schlüter (Hrsg.)
25
Inklusive DVD mit Zusatzressourcen und vielen Weblinks
Microsoft
Software
Report
Ihr Wegweiser durch die Microsoft-Welt
Microsoft Press


Microsoft
Windows Vista
Die besten Tipps, Tricks & Techniken
25
Vista
MAXIBUCH
MAXIMALER SPASS
MAXIMALER ERFOLG
MINIMALER PREIS: € 19,90
Microsoft Press


Microsoft Hyper-V
Microsoft Hyper-V
Das Handbuch für Administratoren
→ Design, Installation, Best Practices
→ Sicherheit, Migration, Storage, Backup, Disaster Recovery
→ Inklusive PowerShell-Automation und detaillierter Praxisszenarien
2., aktualisierte Auflage
Rheinwerk Computing

Kontakt

- E-Mail: marc.grote@it-consulting-grote.de
- Web: https://www.it-consulting-grote.de
- Blog: https://blog.it-consulting-grote.de
- XING: https://www.xing.com/profile/Marc_Grote2
- Mobile: +4917623380279