Neuerungen in Windows Server 2016

Der neue Kollege

Quelle: convisum – 123RF

Windows Server 2016 bietet zahlreiche interessante Neuerungen. Dazu gehören verschiedene Container-Technologien und die minimale Server-Bereitstellung mit der Bezeichnung "Nano". Darüber hinaus wurde an Hyper-V und für die Virtualisierung relevanten Storage-Funktionen geschraubt.

Mit Windows Server 2016 führt Microsoft neben dem Core-Server eine weitere minimale Serverinstallation mit der Bezeichnung "Nano" ein. Diese basiert auf 64 Bit und ist vor allem für Cloud-Anwendungen interessant. Microsoft nennt Installationen in Zusammenhang mit dem Nano-Server auch Microservices. Auf Nano-Servern lassen sich aber auch die Microsoft-Clusterfeatures installieren. Interessant kann das sein, wenn Unternehmen mit Nano-Servern Storage auf Basis eines Software-defined Networks (SDN) aufbauen wollen, denn Server 2016 erlaubt mit "Storage Spaces Direct", die Storage Spaces nicht nur auf verschiedene Festplatten auszudehnen, sondern auch über verschiedene Server hinweg. Die Lizenzierung eines Nano-Servers entspricht dabei genau der eines herkömmlichen Windows-Servers.

Die Fähigkeiten von Nano-Servern

Nano-Server arbeiten stark mit Docker-Containern zusammen, die Microsoft in Windows Server 2016 integriert hat. Die Bezeichnung lautet "Windows Server Container". Nano-Server lassen sich als VM betreiben, aber auch als Installation auf physischen Servern. Virtualisieren Administratoren Nano-Server, besteht der Vorteil vor allem darin, dass sich auf einem Virtualisierungshost mehr virtuelle Server betreiben lassen als mit Core-Servern oder einer herkömmlichen Installation von Windows Server 2016. Außerdem sind die Server sicherer, da angreifbare Elemente des Betriebssystems fehlen.

Bei der Nano-Installation handelt es sich um keine spezielle Edition von Windows Server 2016, sondern um eine besondere Installationsvariante, genauso wie die Core-Installation. Im Gegensatz zur Core-Installation werden Nano-Server aber nicht als Option bei der Installation ausgewählt, sondern nachträglich bereitgestellt. Nano-Server unterstützen generell alle APIs, die mit Windows Server 2016 kompatibel sind. Nur APIs, die Zugriff auf den Desktop oder lokale Verwaltungsprogramme erfordern, laufen nicht. Generell verhalten sich die Server im Netzwerk also wie herkömmliche Server. Der Zugriff durch die Anwender erfolgt transparent, hier muss nichts Besonderes beachtet werden. Entwickler müssen also keine speziellen Client-Anwendungen programmieren, sollen Anwender auf Nano-Server zugreifen.

Auch wenn Nano-Server deutlich eingeschränkt sind, unterstützen Sie wichtige Windows-Funktionen wie Storage und auch Scale-Out File-Server (SOFS), Clustering, CoreCLR und ASP.NET 5. Auch PowerShell Desired State Configuration (DSC) lässt sich in Zusammenhang mit Nano-Servern nutzen. Gerade hier ist die Technik sogar sehr sinnvoll, da Sie mehrere Nano-Server schnell und zentral auf einen sicheren Stand bringen können.

Nano-Server werden als Image bereitgestellt. Standardmäßig verfügt die Nano-Installation über keinerlei Treiber. Diese müssen von Administratoren manuell hinzugefügt werden, sobald der Nano-Server bereitsteht, oder als Paket in die Installation eingebunden sein. Nano-Server benötigen aber keine speziellen Treiber, alle Treiber für Windows Server 2016 lassen sich auch auf Nano-Servern nutzen.

Die PowerShell ist das zentrale Verwaltungswerkzeug für Nano-Server. Da die Server vor allem für Cloud-Szenarien gedacht sind, unterstützen sie auch viele Programmiersprachen, zum Beispiel sind Chef, Go, Java (OpenJDK), MySQL, Nginx, Node.js, OpenSSL, PHP, Python 3.5, Redis, Ruby 2.1.5 und SQLite Visual Studio 2015 vollständig kompatibel mit Nano-Server und erlauben, Anwendungen direkt auf diesen Servern bereitzustellen. Entwickler können mit Visual Studio über das Netzwerk nach Fehlern in Anwendungen suchen (Remote Debugging). Beim Entwickeln für Nano-Server weist Visual Studio darüber hinaus auf API-Zugriffe hin, die mit Nano-Servern nicht kompatibel sind.

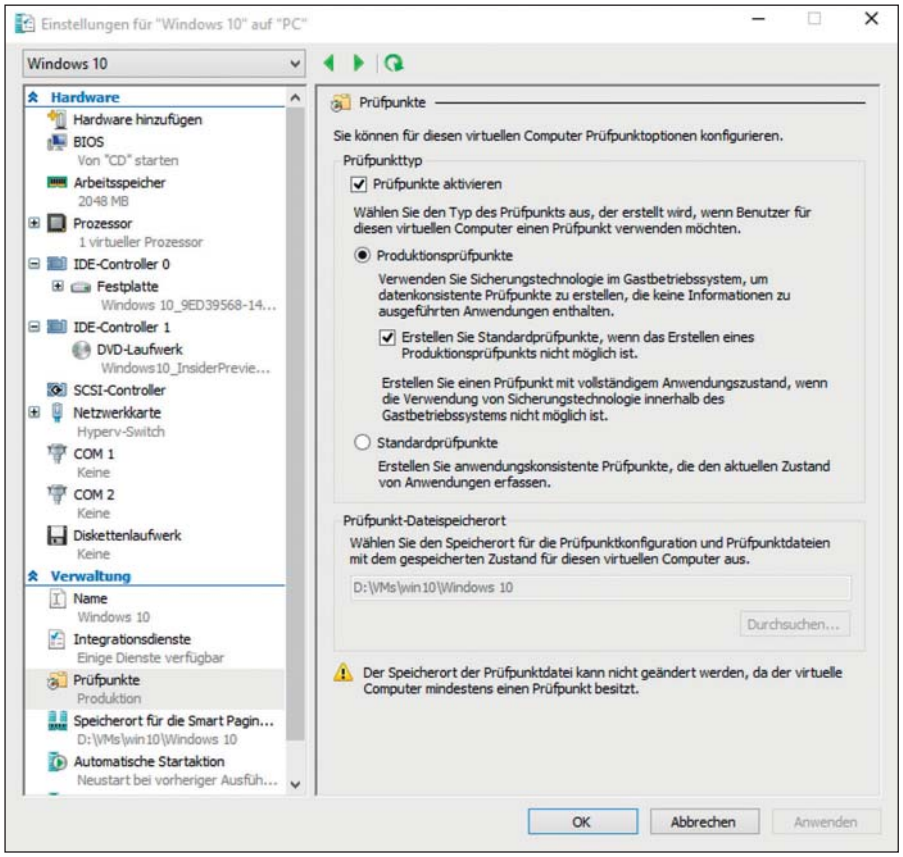

Bild 1: Hyper-V erlaubt in Windows Server 2016 eine effizientere Konfiguration von Snapshots.

Core versus Nano

Im Gegensatz zu Core-Servern enthalten Nano-Server keinerlei lokale Verwaltungswerkzeuge und auch Remoteverbindungen sind nicht erlaubt. Die Server sollen abgeschottet, sicher und minimal ausgestattet sein. Nano-Server sollen also möglichst kleine Fußabdrücke (Footprints) im Netzwerk hinterlassen. Vorteil der Umgebung ist die Möglichkeit, dedizierte Server schnell und einfach bereitzustellen. Microsoft geht davon aus, dass Nano-Server in weniger als drei Minuten vollständig einsatzbereit sind.

Core-Server haben eine Größe von etwa 4 GByte in der Minimal-Installation, Nano-Server sollen mit lediglich 400 MByte auskommen. Laut Microsoft beanspruchen Nano-Server außerdem fast 90 Prozent weniger Ressourcen. Dieser Ansatz gehört zu den wichtigsten Punkten, die Microsoft für Nano-Server sieht. Die meisten Unternehmen werden Nano-Server virtualisiert zur Verfügung stellen. Hier ergibt sich der Vorteil, dass sich die Netzwerkkonfiguration des Servers auch lokal über den Hyper-V-Host anpassen lässt.

Nano-Servern fehlt jegliche 32-Bit-Unterstützung, auch MSI-Dateien und -Installationen lassen sich nicht verwenden oder durchführen. Microsoft hat dazu den kompletten GUI-Stack und die 32-Bit-Unterstützung (WOW64) aus der Installation von Nano-Servern entfernt. Die Verwaltung erfolgt über das Netzwerk. Dafür hat Microsoft die Möglichkeiten für den PowerShell-Zugriff über das LAN verbessert und auch Möglichkeiten integriert, über das Netzwerk Dateien auf den Server zu übertragen.

Nano-Server lassen sich problemlos virtualisieren: Das heißt, Sie können auf Virtualisierungshosts deutlich mehr virtuelle Server zur Verfügung stellen als beim Einsatz mit Core-Servern. Dadurch stellen Sie dedizierte Server zur Verfügung, die vor allem einzelne Serveranwendungen im Fokus haben. Trotz der damit verbundenen steigenden Anzahl an VMs auf einem Host, reduziert sich der unnötige Datenverbrauch der Server, da nicht notwendige Betriebssystemkomponenten auf dem Server fehlen.

Nano-Server sollen vor allem drei Funktionen ausfüllen: Virtualisierung über Hyper-V, App-Server (IIS) und Dateiserver.

Auf Basis der Virtualisierungsmöglichkeiten mit Nano lassen sich zum Beispiel auch Docker-Container auf Nano-Servern realisieren, in Server 2016 auch als "Windows Server Container" bezeichnet.

Virtualisierung mit Hyper-V

Die Hyper-V-Neuerungen in Windows Server 2016 erleichtern Ihnen deutlich die Arbeit, stellen virtuelle Server und deren Konfigurationsdateien stabiler bereit und bieten vor allem bessere Möglichkeiten zum Erstellen von Snapshots. Die neuen Funktionen lassen sich jedoch nur dann nutzen, wenn Sie für VMs die neue Version für Windows Server 2016 aktivieren. VMs, die Sie mit Server 2016 erstellen, erhalten automatisch diese neue Version, bei VM-Migrationen von Vorgängerversionen wie Windows Server 2012 R2 zu Windows Server 2016 bleibt die ursprüngliche Version bestehen. Diese unterstützt nicht die neuen Snapshot-Funktionen und auch nicht die neuen binären Konfigurationsdateien.

Diese binären Konfigurationsdateien für die neue Version bauen auf XML auf. Hauptsächlicher Vorteil ist dabei deren Robustheit bei Systemabstürzen – ähnlich zu VHDX. Die Anpassung der Konfigurationsdateien erfolgt beim Konvertieren der VM zur neuen Version. In den Eigenschaften der VMs steht im Bereich "Prüfpunkte" die neue Funktion "Produktionsprüfpunkte" zur Verfügung. Bei dieser neuen Art von Snapshots wird der Volumenschattenkopie-Dienst der VM verwendet, was die Erstellung von VMs für Datenbank-Server ermöglicht. Auch Linux-Server lassen sich auf diesem Weg absichern. Das ermöglicht bessere Snapshots, zum Beispiel für Domänencontroller, Datenbank-Server oder Exchange. Die Einstellungen für die Snapshots lassen sich pro VM festlegen.

Bei den neuen VMs können Sie auch im laufenden Betrieb virtuelle Netzwerkadapter hinzufügen. Das war bis Windows 8.1 beziehungsweise Server 2012 R2 nur im ausgeschalteten Zustand möglich. Auch der Arbeitsspeicher lässt sich für VMs in Hyper-V-Hosts unter Windows Server 2016 im laufenden Zustand anpassen. Die Hyper-V-Integrationsdienste

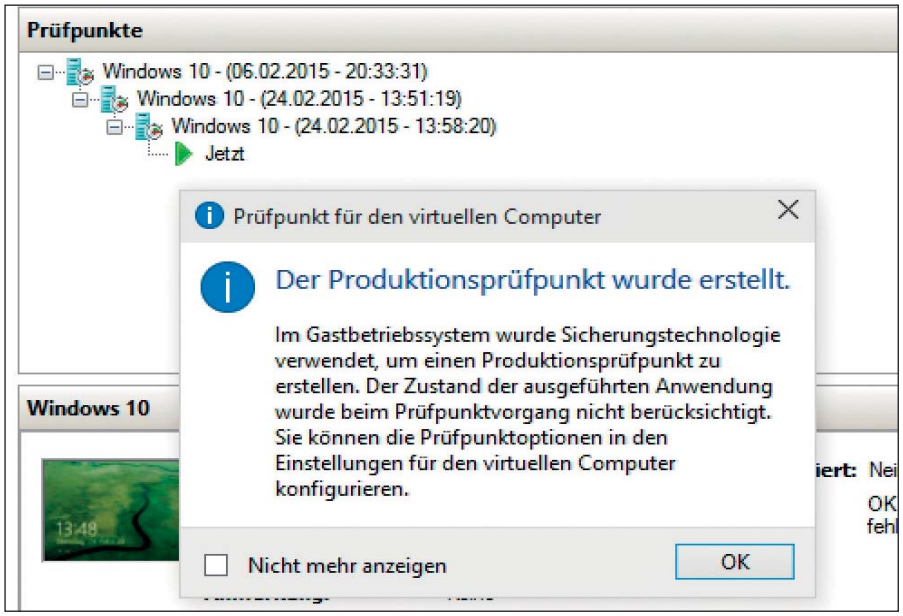

Bild 2: Die neuen Produktionsprüfpunkte binden den Volume-Schattenkopiedienst von Windows-Servern oder den Systempuffer von Linux-Servern mit ein.

installieren und aktualisieren Sie in VMs auf Basis von Windows 10 oder Windows Server 2016 über die Windows-Update-Funktion und WSUS, nicht mehr über eine ISO-Datei. Verbinden Sie die VM mit einem WSUS-Server, werden die Integrationsdienste über diesen Dienst aktualisiert. Im Hyper-V-Manager können Sie für jeden angebundenen Server benutzerdefinierte Anmeldedaten hinterlegen. Das erleichtert die Verwaltung von Hyper-V über das Netzwerk.

Generation-2-VMs können Sie unter Win-dows Server 2016 auch für Linux-VMs nutzen. Das bietet Linux-VMs die Möglichkeit, über UEFI zu booten und auch dessen Secure-Boot-Funktion zu nutzen. Dazu müssen Sie Ubuntu ab Version 14.04 oder SUSE Linux Enterprise Server ab Version 12 einsetzen. Diese Systeme sind automatisch für Secure Boot aktiviert.

In Windows Server 2016 ist eine eingebettete Virtualisierung (Nested Virtualization) möglich. Sie können damit auf einem virtuellen Server, den Sie mit Server 2016 und Hyper-V virtualisiert haben, Hyper-V installieren und auch virtuelle Switche erstellen. Durch diese Verbindung können Sie virtuelle Switche noch einmal virtualisieren, was für Testumgebungen, aber auch für die neuen Windows Server Container sinnvoll ist. Denn virtuelle Server-Container können Sie auf einem virtuellen Container-Host betreiben, der wiederum auf einer physischen Hyper-V-Maschine installiert ist.

Bodyguard für virtuelle Maschinen

Der "Host Guardian Service" überwacht die virtuellen Server auf einem Hyper-V-Host und kann bei verdächtigen Aktionen eingreifen. Die Hauptaufgabe des Dienstes ist die Abschottung des Hosts von einzelnen VMs beziehungsweise das Trennen von VMs untereinander, sodass sich hochsichere virtuelle Umgebungen erstellen lassen. Der Host Guardian Service ist als neue Serverrolle in den Server-Manager integriert.

Ist eine VM bereits durch einen Angreifer kompromittiert, verhindert dieser Dienst die Ausbreitung des Bösewichts. VMs sind so zudem nicht in Lage, zu viel der Leistung des Hosts zu kapern, da der Dienst das erkennt und verhindert. VMs können über den Host Guardian Service verschlüsselte Festplatten nutzen, auch mit vTPM. Dadurch lassen sich besonders heikle und wichtige VMs sehr effizient schützen. Jede herkömmliche VM lässt sich vom Non-Shielded-Modus in den Shielded-Modus versetzen. Bei diesem Vorgang können Sie dann auch gleich die virtuellen Festplatten der VM verschlüsseln. Gesteuert wird das am besten über System Center 2016 Virtual Machine Manager. Auch der Datenverkehr der Livemigration ist jetzt verschlüsselbar.

Virtuelle Netze

Mit Hyper-V Network Virtualization (HNV) trennen Sie virtuelle Netzwerke vom physischen Netzwerk. Viele Hardware-Switche zum Beispiel von Cisco arbeiten mit dieser Konfiguration zusammen. Mit dieser Technik lassen sich virtuelle Netzwerke zusammenfassen, sodass virtuelle Server in diesem Netzwerk kommunizieren können, ohne physische Netzwerke zu beeinträchtigen. Vor allem in großen Rechenzentren spielt HNV eine wichtige Rolle. In einem physischen Netzwerk lassen sich mehrere virtuelle Netzwerke parallel einsetzen, die den gleichen oder einen anderen IP-Adressraum verwenden.

HNV unterstützt darüber hinaus dynamische IP-Adressen. Das ist in Rechenzentren für eine IP-Adress-Failover-Konfiguration sinnvoll. Der komplette Datenverkehr in den virtuellen Switchen von Windows Server 2016 läuft über die Netzwerk-Virtualisierung und die optional integrierten Dritthersteller-Produkte. Auch Netzwerkkarten-Teams arbeiten mit der Netzwerk-Virtualisierung zusammen. Große Unternehmen und Cloud-Anbieter können auf die Berechtigungslisten (ACL) virtueller Switche zugreifen und Firewall-Einstellungen, Berechtigungen und Netzwerkschutz für die Datencenter einbinden und zentral verwalten. Windows Server 2016 bietet die Möglichkeit, den entsprechenden Port in Firewallregeln zu integrieren.

Docker liefert Anwendungen im Container

Docker virtualisiert Anwendungen im Betriebssystem über Container. Sie lassen sich dadurch leichter bereitstellen, da die Container mit den virtualisierten Anwendungen transportabel sind. Einfach ausgedrückt handelt es sich bei Docker-Containern um virtualisierte Serveranwendungen, die keinen Server und kein eigenes Betriebssystem benötigen. Vorteil dabei ist, dass virtuelle Docker-Container mit ihren Serveranwendun-

gen im Rahmen von Nano-Installationen die Möglichkeit bieten, exakt die benötigten Ressourcen zu verwenden.

Virtuelle Server binden in den meisten Fällen deutlich mehr Ressourcen als sie eigentlich verbrauchen und die Images sind oft unnötig groß. Dazu kommt, dass virtuelle Server ein komplettes Betriebssystem benötigen. Genau hier setzen Nano und Docker in Windows Server 2016 an. Der Overhead wird reduziert, die Bereitstellung beschleunigt. Sinnvoller Einsatz von Docker-Umgebungen und Nano-Installationen in Windows Server 2016 sind Big-Data-Infrastrukturen, bei denen zahlreiche Rechenknoten verwendet werden. Microsoft unterstützt Docker auch in Azure.

Docker-Container und Nano-Installationen erhalten IP-Adressen und Netzwerkzugriff. Die virtuellen Anwendungen stehen im Netzwerk zur Verfügung, werden aber nicht durch das Betriebssystem beeinträchtigt. So lassen sich beispielsweise Hadoop, aber auch Datenbanken in Docker-Container oder Nano-Installationen bereitstellen. Auch in Windows-Server-Containern lassen sich Firewallregeln definieren. Gehostet werden die Container über einen Container-Host auf Basis von Windows Server 2016, der auch für die Sicherheit der Container sorgt.

Mehr Sicherheit dank Hyper-V-Containern

Betreiben Sie Docker-Container mit Windows Server 2016 innerhalb von Hyper-V, werden diese noch mehr abgeschottet als herkömmliche Windows-Server-Container auf Basis von Docker. Dadurch erreichen Sie eine erhöhte Sicherheit und Stabilität. Windows-Server-Container teilen sich einige Bereiche des Betriebssystems mit dem Host und anderen Containern. Daher ist es möglich, dass ein Container oder ein Serverdienst in einem Container andere Docker-Container auf dem Host beeinträchtigt. Das lässt sich mit Hyper-V-Containern verhindern. In diesen ist jeweils eine eigene Kopie des Betriebssystems integriert und er läuft in einer Art VM. Dadurch können sich Container untereinander nicht beeinträchtigen. Durch die Virtualisierung von Containern mit Hyper-V werden diese weiter voneinander abgeschottet als bei Windows-Server-Containern. Sinnvoll ist das für Webserver oder Cloud-Dienste. Windows-Server-Container, Hyper-V-Container und Nano-Server lassen sich gemeinsam betreiben.

Microsoft bietet mit Hyper-V-Containern auch die Möglichkeit, Rechte zu delegieren – zum Beispiel für mandantengestützte Systeme. Die Hyper-V-Container eines Mandanten können miteinander kommunizieren, während die Container der anderen Mandanten vollständig abgeschottet sind. Das erlaubt, Container in Gruppen zusammenzufassen. Die Container lassen sich zudem auf andere Hyper-V-Hosts replizieren und mit Hyper-V-Clustern absichern. Auch die Übertragung von Hyper-V-Containern auf andere Knoten mit Livemigration ist problemlos möglich.

Die Bereitstellung der Container erfolgt über ein Image. Dabei spielt es für das Image keine Rolle, ob Sie Container auf herkömmlichem Weg oder innerhalb von Hyper-V erzeugen. Die Images und Container müssen dafür nicht angepasst werden. Das liegt vor allem daran, dass ein Hyper-V-Container ein ganz herkömmlicher Windows-Server-Container ist, der in einer Hyper-V-Partition installiert wird. Aus Windows-Server-Containern erstellen Sie mit wenigen Schritten Hyper-V-Container und umgekehrt. Bei der Umwandlung gehen keine Einstellungen und Daten verloren.

Docker auf der Windows-10-Arbeitsstation

Administratoren in Umgebungen mit Windows 10 wird freuen, dass Microsoft die Container-Technologie, inklusive der Hyper-V-Container, in Windows 10 integriert hat. Dazu benötigen die Clients das Windows 10 Anniversary Update. Für Hyper-V-Container ist ein physischer PC notwendig oder eine VM in einer eingebetteten Virtualisierungsumgebung. Mit Windows 10 und Docker können Sie ein aktuelles Nano-Server-Image auf Basis von Windows Server 2016 herunterladen und bereitstellen. Hierüber stehen dann die Hyper-V-Container zur Verfügung. Die Basis entspricht also den Möglichkeiten von Server 2016.

Ab Windows 10 mit Anniversary Update können Administratoren die Linux-Container-Technologie Docker uneingeschränkt nutzen, inklusive der Möglichkeiten, die Microsoft mit Windows Server 2016 integriert und das Nano-Server-Image ist sogar vollständig identisch. Dadurch besteht die Möglichkeit, Container und Images für das Rechenzentrum auch auf Arbeitsstationen bereitzustellen oder zumindest vorzubereiten.

Bisher mussten Sie bei der Verwendung von Docker mit Windows ein kleines virtuelles Linux-System auf dem Rechner betreiben. Das ist ab Windows 10 mit dem Anniversary Update nicht mehr notwendig. Entwickler können mit Windows 10 also Anwendungen für Container vorbereiten und diese später mit Server 2016 bereitstellen.

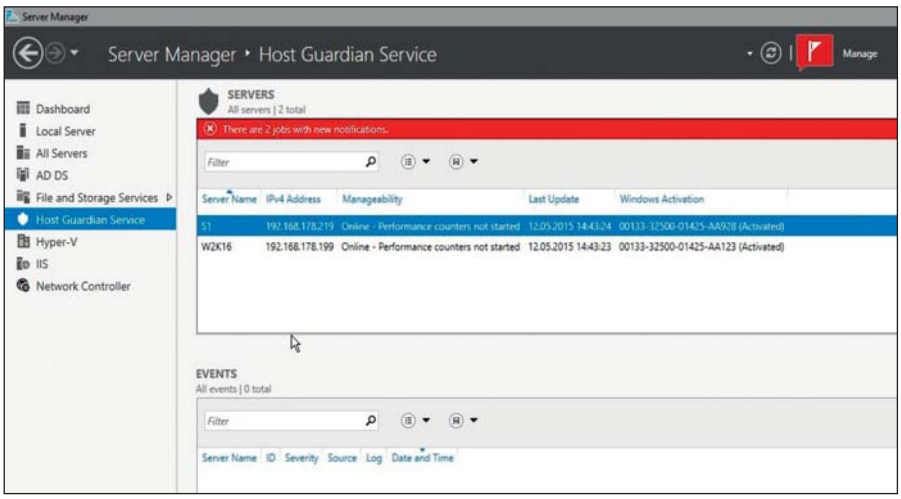

Bild 3: Mit dem Host Guardian Service lassen sich VMs absichern.

Netzwerke mit dem Network Controller verwalten

Der neue Network-Controller-Dienst erlaubt die zentrale Verwaltung, Überwachung und Konfiguration von Netzwerkgeräten. Anbinden lassen sich physische Netzwerkgeräte, aber auch virtuelle Netzwerke sowie Netzwerke in Microsoft Azure. Neben Hardware-Geräten können Sie auch softwarebasierte Netzwerkdienste verwalten. Die Verwaltung all dieser Geräte und Dienste ist dann auch über die PowerShell möglich. Im Bereich des "Fabric Network Managements" erlaubt der Network Controller auch die Konfiguration und Verwaltung von IP-Subnetzen, VLANs, Layer 2- und Layer 3-Switchen sowie die Verwaltung von Netzwerkadaptern in Hosts.

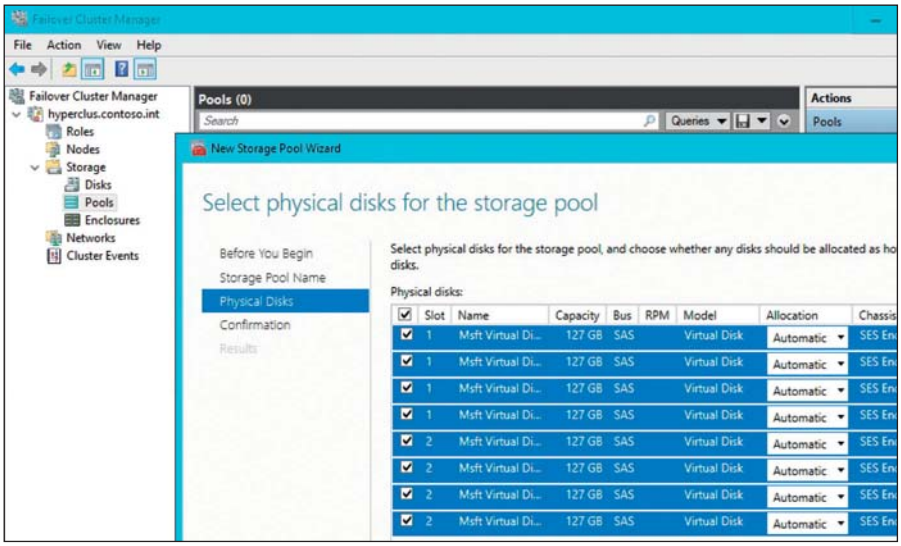

Bild 4: Datenträger der einzelnen Clusterknoten lassen sich in Windows Server 2016 zu einem gemeinsamen Speicherpool zusammenfassen.

Mit dem Network Controller lassen sich folgende Bereiche zentral konfigurieren und überwachen:

- Hyper-V-VMs und virtuelle Switche
- Physische Netzwerk-Switche
- Firewall-Software
- VPN-Gateways
- Routing and Remote Access Service (RRAS) Multitenant Gateways
- Loadbalancer

Zusammen mit Network Controller ist in Windows Server 2016 auch PowerShell 5.0 integriert. Sie steht auch für Windows Server 2012 R2 zur Verfügung, unterstützt aber nicht alle Funktionen. Mit dem Data Center Abstraction Layer (DAL) steht ein Schnittpunkt zwischen Hardware-Geräten und der Steuerung über die PowerShell bereit. DAL bietet eine Remoteverwaltung von Rechenzentren und kompatiblen Netzwerkkomponenten über die PowerShell. Dazu müssen die Netzwerkkomponenten allerdings von Microsoft zertifiziert sein. Zu den zertifizierten Herstellern gehören derzeit Cisco und Huawei. Microsoft geht in der TechNet [1] näher auf die Funktionen und Möglichkeiten von kompatiblen Geräten ein.

Speicher virtualisieren

Mit Windows Server 2016 verbessert Microsoft die Storage Spaces aus Windows Server 2012 R2. Die Software-defined-Storage-Lösung erlaubt das Zusammenfassen mehrerer Datenträger zu einem zentralen Speicherpool. Diesen können Sie in verschiedene Volumes aufteilen und wie herkömmliche Datenträger nutzen. Unter Server 2016 kann ein solcher Speicher nicht nur mehrere Festplatten umfassen, sondern auch mehrere Server. Das erhöht die Flexibilität der Datenspeicherung.

Storage Spaces Direct benötigen einen Cluster mit mindestens drei Hosts. Unter vier Hosts unterstützt die Technik nur die Spiegelung der Daten zur Absicherung (Mirrored Resiliency). Benötigen Sie Paritiäts-basierte Datenträger (Parity-based Resiliency), sind mindestens vier Hosts notwendig. Storage Spaces Direct sind standardmäßig vor dem Ausfall eines Hosts geschützt. Die Technik kann den Ausfall eines ganzen Racks mit Servern verkraften, die Bestandteil von Storage Spaces Direct sind. Das hängt natürlich von der Konfiguration ab sowie der Anzahl der Server, die Bestandteil des Clusters sind.

In Windows Server 2016 lassen sich in den Storage Spaces drei Storage-Tiers nutzen: NVMe, SSD und HDD. NVMe-Speicher wird zum Zwischenspeichern der Daten verwendet, während die SSD und HDD zur Datenspeicherung dienen.

Im Geocluster Datenträger zwischen RZs replizieren

Microsoft hat in Windows Server 2016 darüber hinaus noch die Möglichkeit integriert, komplette Festplatten – auch innerhalb eines Storage Pools – auf andere Server zu replizieren. Diese Replikation erfolgt synchron und blockbasiert. So sind Unternehmen in der Lage, Geocluster aufzubauen. Storage Replica kann Datenträger zwischen verschiedenen Hosts replizieren und kann auch Cluster absichern. Im Rahmen der Einrichtung können Sie eine synchrone und asynchrone Replikation festlegen.

Diese Technik lässt sich zusammen mit Hyper-V-Replika, Deduplizierung und Storage Spaces betreiben. Unterstützt werden NTFS und ReFS-Datenträger. Die Replikation ist unabhängig von darunter liegenden Speichermedien. Sie können diese Technologie auch im Zusammenspiel mit verteilten Clustern einsetzen, die den gemeinsamen Datenspeicher auch über mehrere Regionen hinweg nutzen sollen. Größere Unternehmen können mit der Technologie zudem auf Clusterebene Daten zwischen Rechenzentren replizieren lassen (Stretched Cluster).

Remotedesktop-Dienste in Windows Server 2016

Die Funktionen der Remotedesktop-Dienste in Windows Server 2016 entsprechen noch weitgehend den Funktionen in Server 2012 R2. Die Verwaltung hat Microsoft nicht stark verändert, dafür aber einige Verbesserungen eingeführt, mit denen sich die Remotedesktopdienste besser nutzen lassen. Der "Remote Desktop Connection Broker" der Remotedesktopdienste kann mit Windows Server

2016 in einer Azure-SQL-DB laufen. Dadurch lassen sich hochverfügbare Umgebungen auch rechenzentrumsübergreifend zur Verfügung stellen.

Microsoft hat viele Neuerungen, die bereits in Windows Server 2012 R2 verfügbar, aber in den Remotedesktopdiensten nicht nutzbar waren, integriert. So lassen sich für virtuelle Desktops in Virtual Desktop Infrastructures (VDI) jetzt Vorlagen auf Basis von Generation-2-VMs erstellen. Virtuelle Computer in VDI-Infrastrukturen unterstützen in Server 2016 das UEFI-System und damit Secure Boot in UEFI. Diese VMs nutzen auch virtuelle SCSI-Festplatten für den Boot, arbeiten also sofort im Virtualisierungsmodus und müssen nicht erst eine Emulation für den Systemstart durchführen.

Virtuelle GPUs unterstützen in Windows Server 2016 OpenGL/OpenCL. Zusammen mit den Verbesserungen in RemoteFX ermöglicht das den Betrieb grafikintensiver Anwendungen wie Adobe PhotoShop auf Remotedesktop-Servern. Mit dem "Server Based Personal Desktop" lässt sich für Anwender ein personalisierter Server bereitstellen, der einen Windows-10-Desktop bietet. Sinnvoll ist das in Umgebungen, in denen Anwender eigene Desktops erhalten sollen, aber keine Windows-10-Lizenz vorliegt, zum Beispiel bei Desktop-as-a-Service (DaaS). Dadurch können Unternehmen auf Basis von Windows Server 2016 einen virtuellen Rechner für Anwender zur Verfügung stellen, der den Funktionen und Möglichkeiten von Windows 10 entspricht. Die Bereitstellung dieses Servers erfolgt als VM. Die neuen Server Based Personal Desktops ergänzen die Möglichkeiten von herkömmlich bereitgestellten Desktops um die Option, neue Sammlungen zu erstellen, in denen Anwender echte virtuelle Computer mit administrativen Rechten erhalten.

Die Verwaltung erfolgt über das New-RDSessionCollection-Cmdlet mit den drei neuen Optionen:

- PersonalUnmanaged: Legt den neuen Typ der Sammlung fest und erlaubt, dass Anwender direkt zu einem speziellen Sitzungshost weitergeleitet werden.
- GrantAdministrativePrivilege: Erteilt dem Anwender Administrator-Rechte auf dem Sitzungshost, indem er in die lokale Administrator-Gruppe aufgenommen wird.
- AutoAssignUser: Legt fest, dass Anwender automatisch zu einem noch freien Sitzungshost verbunden werden, den noch kein anderer Anwender nutzt.

RemoteFX, das Protokoll für die Verbesserung der Grafikleistung auf virtuellen Desktops und RDS-Sitzungen, hat Microsoft erweitert. RemoteFX in Windows Server 2016 unterstützt OpenGL 4.4 und OpenCL 1.1 API. Außerdem können Sie mehr Grafikspeicher einsetzen. Die neue Version unterstützt jetzt mehr als 1 GByte VRAM. Zudem haben Sie hier Einstellungsmöglichkeiten und können auf Basis von Hyper-V festlegen, wieviel Arbeitsspeicher eine virtuelle Grafikkarte erhalten soll. Mehr zu diesen Möglichkeiten finden Sie auf der Internetseite der RDS-Entwickler [2].

In Windows Server 2016 können Anwender durch diese Neuerungen umfassend mit Stifteingaben arbeiten. Das funktioniert auf Hybrid-PCs und Notebooks, aber auch auf Tablets. Die Eingaben werden durch das RDP-Protokoll in die Sitzung des Anwenders weitergeleitet.

Sie finden die Remote-FX-Einstellungen im Hyper-V-Manager über "Hyper-V-Einstellungen" bei "Physical GPUs". In Windows Server 2016 können Sie dadurch auch den Server Based Personal Desktops virtuelle Grafikkarten auf Basis von RemoteFX zuweisen. Für jeden Server können Sie dediziert steuern, ob er RemoteFX zur Verfügung stellen soll, und wenn ja mit wieviel Arbeitsspeicher.

Damit Sie diese Funktion nutzen können, muss die Grafikkarte die Funktion sowie mindestens DirectX 11 unterstützen. Auch müssen Sie einen passenden Treiber installieren. Die Prozessoren auf dem Server müssen mit Second-Level-Address-Translation-Erweiterungen und Data Execution Prevention (DEP) klarkommen. Außerdem muss die Virtualisierung in der Firmware/BIOS des Servers aktiviert sein.

MultiPoint-Server in RDS integriert

In Windows Server 2016 integriert Microsoft auch die Funktionen des "Windows MultiPoint Server" in RDS als neue Serverrolle. Die Technik bietet die Möglichkeit, dass Anwender Monitor, Tastatur und Maus direkt an den Server anschließen, aber dennoch eine eigene Umgebung erhalten. Einfach ausgedrückt handelt es sich bei Multipoint um einen sehr simplen Remotedesktop-Sitzungshost, der einigen Anwendern einen eigenen virtuellen Desktop zur Verfügung stellt. Im Gegensatz zu den herkömmlichen Remotedesktopdiensten erfolgt die Verbindung zum Server nicht über das RDP-Protokoll per Netzwerkzugriff, sondern durch einen direkten Anschluss der Komponenten am Server. Normalerweise wird dazu der Monitor direkt am Server angeschlossen, der dazu über eine passende Grafikkarte verfügen muss. Maus und Tastatur werden üblicherweise an einem USB-Verteiler verbunden, der dann wiederum am Server hängt. Natürlich lassen sich die Dienste auch über Thin-Clients oder mit dem normalen RDP-Client nutzen. Diese Funktion wird also nicht mehr nur als eigenständiger Server betrieben, sondern direkt in die Standard- und Datacenter-Edition von Server 2016 integriert.

Vergleichbar ist das Produkt mit der Essentials-Rolle, die kleinen Unternehmen oder Niederlassungen die Möglichkeit bietet, auf einfache Weise Benutzer anzubinden. Neben Bildungseinrichtungen und Schulungscentern ist diese Technologie auch für kleine Unternehmen und Niederlassungen geeignet. Allerdings bietet Multipoint auch Funktionen, die in den Remotedesktopdiensten nicht integriert oder nur kompliziert umsetzbar sind. Da die Serverlösung vor allem für Bildungseinrichtungen und für Fortbildungen entwickelt wurde, verfügt sie zudem über spezielle Features in diesem Bereich.

So lässt sich zum Beispiel der Bildschirm des Dozenten auf den angeschlossenen Clients anzeigen. Die Benutzeraktivitäten lassen sich durch den Dozenten beobachten und verwalten, auch eine Aufnahme ist möglich. Administratoren haben mehr Einschränkungsmöglichkeiten, wenn es

um den Zugriff auf Webseiten geht. Die Remotesteuerung eines angeschlossenen Desktops ist außerdem wesentlich einfacher möglich als in den Remotedesktopdiensten, das gilt auch für die Kommunikation zwischen Client und Administrator. Diese Technologie ermöglicht es, dass Anwender eigene Umgebungen auf Basis von Windows 10 auf einem einzelnen Computer einrichten und getrennt voneinander nutzen können.

Storagebandbreiten garantieren

In Windows Server 2016 können Sie die Bandbreite festlegen, mit denen Server und Serveranwendungen auf Datenspeicher zugreifen. Sie sind jetzt also in der Lage, für Server eine gewisse Leistung der Datenspeicherung zu garantieren oder einzuschränken. Sie können Richtlinien in der Art "Nicht mehr als…:" oder "Nicht weniger als…:" definieren, außerdem lassen sich Regeln wie "Erlauben, wenn verfügbar..:" konfigurieren. Diese Richtlinien lassen sich an VMs binden, aber auch an einzelne virtuelle Festplatten, ganze Rechenzentren oder einzelnen Mandanten in gehosteten Umgebungen.

Zwar erlaubt auch Server 2012 R2 Einstellungen für "Storage Quality of Service", allerdings müssen Sie hier für jeden Server Einstellungen vornehmen und Daten auslesen. In Windows Server 2016 lassen sich diese wichtigen Einstellungen zentral mit dem Query Policy Manager auslesen und mit der Storage-QoS-Richtlinie umsetzen.

Leichter clustern

Die neue Funktion "Cluster Operating System Rolling Upgrade" erlaubt die Aktualisierung von Clusterknoten mit Windows Server 2012 R2 zu Windows Server 2016, ohne dass Serverdienste ausfallen. Bei diesen Vorgängen werden weder Hyper-V-Dienste noch Dateiserver-Freigaben beendet und stehen den Anwendern weiter zur Verfügung. Ein Clusterknoten lässt sich also ohne Ausfallzeit auf Windows Server 2016 aktualisieren.

Sie können Clusterknoten mit Windows Server 2016 installieren und in bestehende Cluster mit Server 2012 R2 integrieren. Auch das Verschieben von Clusterressourcen und virtuellen Maschinen zwischen den Clusterknoten ist dann möglich. Sind alle Knoten auf Windows Server 2016 aktualisiert, wird die Clusterkonfiguration auf die neue Version gesetzt und unterstützt ab dann keine Vorgängerversi- onen wie Windows Server 2012 R2 mehr. Dazu steht das neue Update-ClusterFunctionalLevel-Cmdlet zur Verfügung.

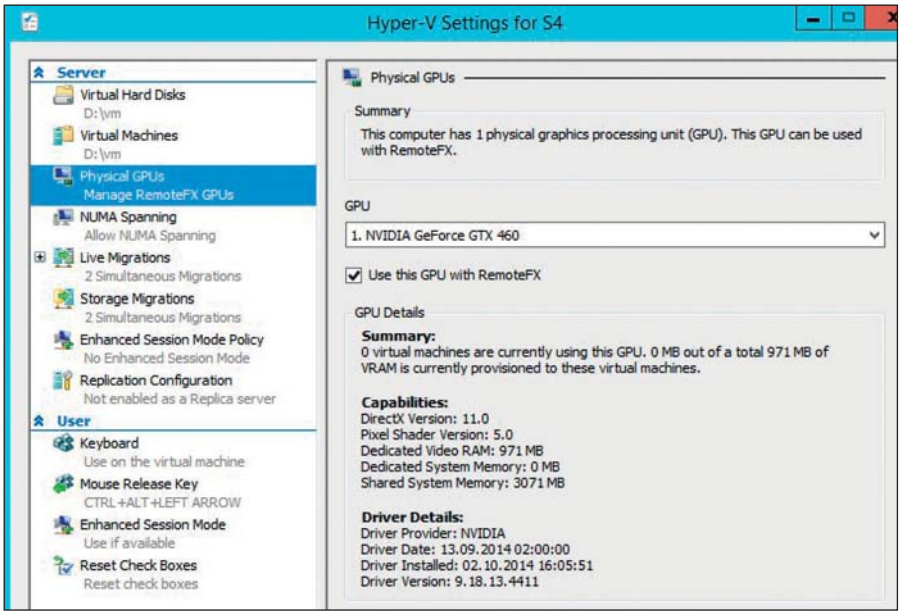

Bild 5: Damit Windows Server 2016 RemoteFX unterstützt, muss die Grafikkarte mindestens DirectX 11 leisten und ein passender Treiber vorliegen.

Windows Server 2016 erlaubt den Betrieb von Zeugenserver (Witness) in Microsoft Azure. Für global verteilte Cluster und Rechenzentren kann die Effizienz von Clustern erheblich verbessert und die Verwaltung erleichtert werden.

Durch "Cluster Compute Resiliency" und "Cluster Quarantine" verschiebt ein Windows-Cluster Ressourcen nicht mehr unnötig zwischen Knoten, wenn ein Clusterknoten Probleme hat. Vielmehr versetzt Windows einen Knoten in Isolation, wenn das Betriebssystem erkennt, dass der Knoten nicht mehr stabil funktioniert. Alle Ressourcen werden vom Knoten verschoben und die Administratoren informiert. Der Network Controller erkennt in diesem Zusammenhang auch fehlerhafte physische und virtuelle Netzwerke und kann entsprechend eingreifen. Ein Scale-Out-File-Server lässt sich in einem Cluster mit Windows Server 2016 als Clusterressource verwenden und gleichzeitig auch mit Storage Space Direct verbinden.

LDAP-Verzeichnisse mit ADFS anbinden

Windows Server 2016 erlaubt es, auch Benutzerkonten in den Active-Directory-Verbunddiensten (Active Directory Federation Services, ADFS) zu authentifizieren, die nicht aus einem AD kommen. Beispiel dafür sind X.500-kompatible LDAP-Verzeichnisse oder auch SQL-Datenbanken. Microsoft nennt dazu hier: AD LDS, Apache DS, IBM Tivoli DS, Novell DS, Open LDAP und andere als Beispiele.

Microsoft hat in Windows Server 2016 auch Verbesserungen in den Active-Directory-Verbunddiensten integriert. Hier ist es zum Beispiel möglich, eine Zugriffssteuerung auf Basis bestimmter Bedingungen zu verwenden. Diese "Conditional Access Control" ist vor allem für mobile Anwender interessant. Außerdem lassen sich Rechner mit Windows 10 über Geräteauthentifizierung an Windows Server 2016 anbinden [3].

Besserer Schutz für administrative Konten

Ab Windows Server 2016 ist es schwieriger, mit Pass-the-hash-Angriffen an vertrauliche Anmeldedaten von Administratoren zu gelangen. Derlei Attacken zielen nicht auf die Kennwörter ab, sondern auf die Hashes, die im Active Directory erzeugt werden, nachdem sich ein Benutzer authentifiziert hat. Dazu

bietet Windows Server 2016 Privileged Access Management (PAM) [4] und Microsoft Identity Manager (MIM) [5]. Dazu wird eine neue Active-Directory-Gesamtstruktur mit MIM erstellt und mit PAM geschützt.

Um PAM mit Windows Server 2016 zu nutzen, sind mindestens zwei Active-Directory-Gesamtstrukturen notwendig. Diese werden über eine Vertrauensstellung miteinander verbunden und die Administratorkonten sind in einer solchen Infrastruktur von der produktiven Domäne getrennt. Dadurch steigt die Sicherheit im Netzwerk. Die neue Gesamtstruktur mit den Administratorkonten wird auch als "Bastion Active Directory Forest" bezeichnet. Er wird durch den Microsoft Identity Manager zur Verfügung gestellt, überwacht und gesteuert.

Der Vorteil dabei ist, dass Sie die vorhandene Gesamtstruktur zu Windows Server 2016 aktualisieren können und die neue Gesamtstruktur mittels PAM zukünftig die Verwaltung steuert. Das erhöht die Sicherheit unmittelbar, da selbst kompromittierte AD-Umgebungen nach der Implementierung von PAM sicher sind.

Zukünftig arbeiten Administratoren nicht mehr mit Administratorkonten in der Active-Directory-Umgebung, sondern erhalten einen sogenannten Zugang mit "Just Enough Administration" (JEA). Dabei wird eine Gruppe an Cmdlets in der PowerShell definiert sowie eine genaue Zielgruppe an Objekten, die für einen bestimmten administrativen Vorgang nötig sind. Auch die Zeitdauer für diese Rechte legt JEA fest. Sobald der Zeitraum abgelaufen ist, lässt sich der Zugang nicht mehr für die Administration nutzen, auch nicht für den fest definierten Zielbereich [6].

Zusammen mit PAM, MIM und dem Bastion Active Directory Forest stehen auch "Shadow Groups" zur Verfügung. Diese verfügen über administrative Rechte, jedoch ist die Mitgliedschaft zeitlich begrenzt. Dazu wird der TTL von Kerberos-Tickets verringert und die Gruppe überwacht. Die Zeitdauer lässt sich granular steuern, ist jedoch niemals unendlich.

Unabhängig davon bietet Windows Server 2016 für die bessere Grundsicherung von Windows-Servern den Bordmittel-Virenschutz "Windows Defender", der standardmäßig aktiv ist. Der Dienst deaktiviert sich erst, wenn ein anderer Virenschutz installiert wird, genauso wie auf Windows-Clients. Im Gegensatz zur Clientversion Windows 10 wird auf Servern allerdings nicht das Verwaltungsprogramm für Windows Defender installiert. Windows Defender schützt das System im Hintergrund automatisch.

Bessere Datendeduplizierung

Bereits mit Windows Server 2012 hat Microsoft die Datendeduplizierung eingeführt. Diese Technik soll verhindern, dass identische Dateien oder Daten mehrfach auf einem Speichersystem lagern und dadurch den Speicherplatz unnötig verschwenden. In Windows Server 2016 hat Microsoft die Leistung dieser Funktion deutlich verbessert.

Vor allem beim Betrieb virtueller Desktopinfrastrukturen lässt sich dadurch deutlich der benötigte Speicherplatz reduzieren, da virtuelle Windows-Betriebssysteme zahlreiche identische Dateien verwenden. Die Deduplizierung kann jetzt mehrere Threads parallel nutzen und deutlich größere Datenträger bearbeiten. Außerdem ist die Technologie mit physischen Datenträgern aber auch mit virtuellen Festplatten kompatibel.

Der neue Small-Business-Server

Auch mit Windows Server 2016 bietet Microsoft wieder eine spezielle Essentials-Edition. Außerdem stellt das Unternehmen die Essentials-Funktionen wieder als Serverrolle für die anderen Windows-Server-2016-Editionen zur Verfügung. Diese Rolle ermöglicht zum Beispiel den Betrieb von kleineren Servern in Niederlassungen, die Bestandteil von Active-Directory-Umgebungen sein können. Die Essentials-Funktionen bieten also nicht nur Möglichkeiten für kleine Unternehmen, sondern auch für kleine Niederlassungen in größeren Firmen.

Sobald der Server installiert ist, rufen Sie das "Windows Server Essentials Dashboard" auf. Über den Link "Startseite" finden Sie zunächst mit "Erste Schritte" weitere Aufgaben, die bei der Einrichtung helfen. Auf der linken Seite finden Sie die vier Kacheln "Setup", "Services", "Kurze Statusinfos" und "Hilfe". Klicken Sie auf eine Kachel, erscheinen in der Mitte des Fensters weitere Aufgaben. Klicken Sie auf den Link einer Aufgabe, startet ein Assistent zur Einrichtung. Im Rahmen des Anlegens von neuen Benutzern können Sie auch Postfächer in Office 365 schaffen oder Benutzerkonten, die bereits in Office 365 vorhanden sind, mit Benutzerkonten auf dem Server verknüpfen.

Entfernte Funktionen

Neben zahlreichen neuen Funktionen, hat Microsoft aber auch Dienste abgeschafft. Der File Replication Service (FRS) und die Unterstützung für Windows Server 2003/2003 R2 sind nicht mehr in Windows Server 2016 enthalten. Auch die Funktionsebenen für Windows Server 2003 wurden aus den Domänen und der Gesamtstruktur entfernt. Network Access Protection (NAP) hat Microsoft aus DHCP getilgt.

Fazit

Windows Server 2016 bringt zahlreiche Neuerungen und verbessert auch vorhandene Technologien. Die wichtigsten Neuerungen sind sicherlich der Nano-Server und die Windows-Container, inklusive der Hyper-V-Container. Es lohnt sich für Unternehmen, einen Blick auf die neue Version zu werfen. Um die Funktionen zu nutzen, müssen Sie nicht alle Server auf die neue Version umstellen, besonders profitieren Hyper-V-Hosts. *(jp)*

Link-Codes

[1] Datacenter Abstraction Layer Center
GS211

[2] Blog der RDS-Entwickler
DS1E1

[3] Active Directory Federation Services
GS212

[4] Privileged Access Management
GS213

[5] Microsoft Identity Manager
GS214

[6] Just Enough Administration
GS213