

Contents

Virtualisierung

Geschütztes Fabric und abgeschirmte VMs

Hyper-V

Technologieübersicht

Neues bei Hyper-V

Systemanforderungen

Unterstützte Windows-Gastbetriebssysteme

Unterstützte Linux- und FreeBSD-VMs

CentOS- und Red Hat Enterprise Linux-VMs

Debian-VMs

Oracle Linux-VMs

SUSE-VMs

Ubuntu-VMs

FreeBSD-VMs

Beschreibungen der Features von Linux- und FreeBSD-VMs

Bewährte Methoden für die Ausführung von Linux

Bewährte Methoden für die Ausführung von FreeBSD

Kompatibilität von Features nach Generation und Gast

Erste Schritte

Installieren von Hyper-V

Erstellen eines virtuellen Switches

Erstellen eines virtuellen Computers

Planen

VM-Generation

Netzwerk

Skalierbarkeit

Sicherheit

GPU-Beschleunigung

Diskrete Gerätezuweisung

Bereitstellen

- Exportieren und Importieren virtueller Computer
- Einrichten von Hosts für die Livemigration
- Upgrade der VM-Version
- Bereitstellen von Grafikgeräten mit DDA
- Bereitstellen von Grafikgeräten mit RemoteFX vGPU
- Bereitstellen von Speichergeräten mit DDA

Verwalten

- Konfigurieren von beständigen Speichergeräten für Hyper-V-VMs
- Wählen zwischen Standard- oder Produktionsprüfpunkten
- Erstellen eines VHD-Satzes
- Aktivieren oder Deaktivieren von Prüfpunkten
- Verwalten des Hosts mit Hyper-V-Manager
- Verwalten von Host-CPU Ressourcensteuerungen
- Verwenden von VM-CPU-Gruppen
- Verwalten von Hypervisor Scheduler-Typen
- Informationen zur Hyper-V Scheduler-Auswahl
- Verwalten von Integrationsdiensten
- Verwalten von Windows-VMs mit PowerShell Direct
- Einrichten von Hyper-V-Replikaten
- Aktivieren der Intel Performance Monitoring-Hardware
- Verschieben von VMs mit Livemigration
 - Übersicht über die Livemigration
 - Einrichten von Hosts für die Livemigration
 - Verwenden der Livemigration ohne Failoverclustering

Leistungsoptimierung bei Hyper-V-Servern

Virtueller Hyper-V-Switch

- Remotezugriff auf den direkten Speicher (RDMA) und Switch Embedded Teaming (SET)
- Verwalten virtueller Hyper-V-Switches
 - Konfigurieren und Anzeigen von VLAN-Einstellungen für virtuelle Hyper-V-Switchports
 - Erstellen von Sicherheitsrichtlinien mit erweiterten Port-Zugriffssteuerungslisten

TIP

Suchen Sie nach Informationen zu älteren Versionen von Windows Server? Sehen Sie sich unsere [Windows Server-Bibliotheken](#) auf „docs.microsoft.com“ an. Sie können auch nach bestimmten Informationen [auf dieser Website](#) suchen.

Virtualisierung in Windows Server ist eine der grundlegenden Technologien, die zum Erstellen Ihrer softwaredefinierten Infrastruktur erforderlich sind. Zusammen mit Netzwerk- und Speicherressourcen bieten Virtualisierungsfeatures die Flexibilität, die Sie benötigen, um die Workloads Ihrer Kunden zu beschleunigen.

Geschütztes Fabric und abgeschirmte VMs

Als Cloud-Dienstanbieter oder privater Cloud-Administrator im Unternehmen können Sie ein geschütztes Fabric verwenden, um eine sicherere Umgebung für VMs bereitzustellen. Ein geschütztes Fabric besteht aus einem Host Guardian Service (HGS, Host-Überwachungsdienst) – in der Regel ein Cluster mit drei Knoten – sowie einem oder mehreren geschützten Hosts und einer Reihe von abgeschirmten virtuellen Computern (VMs).

Microsoft Hyper-V Server

Die Hyper-V-Technologie stellt Computing-Ressourcen durch Hardwarevirtualisierung bereit. Hyper-V erstellt eine Softwareversion von einem Computer, einen so genannten „virtuellen Computer“, auf dem Sie ein Betriebssystem und Anwendungen ausführen können. Sie können mehrere virtuelle Computer gleichzeitig ausführen und sie nach Bedarf erstellen und löschen.

Windows-Container

Windows-Container ermöglichen die Virtualisierung auf Betriebssystemebene und damit die Ausführung mehrerer isolierter Anwendungen auf einem einzigen System. Das Feature stellt zwei verschiedene Arten von Containerlaufzeiten mit zwei unterschiedlichen Anwendungsisolierungsgraden bereit.

Windows 10 für Unternehmen: Möglichkeiten zur Verwendung von Geräten für die Arbeit

Die Hyper-V-Technologie stellt Computing-Ressourcen durch Hardwarevirtualisierung bereit. Hyper-V erstellt eine Softwareversion von einem Computer, einen so genannten „virtuellen Computer“, auf dem Sie ein Betriebssystem und Anwendungen ausführen können. Sie können mehrere virtuelle Computer gleichzeitig ausführen und sie nach Bedarf erstellen und löschen.

Virtueller Hyper-V-Switch

Der virtuelle Hyper-V-Switch ist ein softwarebasierter Layer-2-Ethernet-Netzwerkswitch, der in allen Versionen von Hyper-V enthalten ist.

Der virtuelle Hyper-V-Switch ist in Hyper-V-Manager verfügbar, nachdem Sie die Hyper-V-Serverrolle installiert haben.

Der virtuelle Hyper-V-Switch umfasst programmgesteuert verwaltete und erweiterbare Funktionen zum Verbinden von virtuellen Computern mit virtuellen Netzwerken und dem physischen Netzwerk.

Außerdem bietet der virtuelle Hyper-V-Switch Richtlinien erzwingung für Sicherheits-, Isolations- und Dienststufen.

Verwandte Themen

- Hyper-V erfordert spezielle Hardware zum Erstellen der Virtualisierungsumgebung. Weitere Informationen finden Sie unter [Systemanforderungen für Hyper-V unter Windows Server 2016](#).
- Weitere Informationen zu Hyper-V unter Windows 10 finden Sie unter [Hyper-V unter Windows 10](#).

Geschütztes Fabric und abgeschirmte VMs

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016

Eines der wichtigsten Ziele bei der Bereitstellung einer gehosteten Umgebung besteht darin, die Sicherheit der virtuellen Computer zu gewährleisten, die in der Umgebung ausgeführt werden. Als Cloud-Dienstanbieter oder privater Cloud-Administrator im Unternehmen können Sie ein geschütztes Fabric verwenden, um eine sicherere Umgebung für VMs bereitzustellen. Ein geschütztes Fabric besteht aus einem Host Guardian Service (Host-Überwachungsdienst) – in der Regel ein Cluster mit drei Knoten – sowie einem oder mehreren geschützten Hosts und einer Reihe von abgeschirmten virtuellen Computern (VMs).

IMPORTANT

Stellen Sie sicher, dass Sie das neueste kumulative Update installiert haben, bevor Sie geschützte virtuelle Computer in der Produktion bereitstellen.

Videos, Blog und Übersichts Thema zu geschützten Fabrics und abgeschirmten VMS

- Video: [Schützen Ihres virtualisierungsfabrics vor Insider Bedrohungen mit Windows Server 2019](#)
- Video: [Einführung in abgeschirmte Virtual Machines in Windows Server 2016](#)
- Video: [Einblicke in abgeschirmte VMS mit Windows Server 2016 Hyper-V](#)
- Video: [bereitstellen von abgeschirmten VMS und einem geschützten Fabric mit Windows Server 2016](#)
- Blog: [Daten Center-und Private Cloud-Sicherheitsblog](#)
- Übersicht: [Übersicht über geschützte Fabric-und abgeschirmte VMS](#)

Themen zur Planung

- [Planungs Handbuch für Hosters](#)
- [Planungs Handbuch für Mandanten](#)

Themen zur Bereitstellung

- [Bereitstellungs Handbuch](#)
 - [Schnellstart](#)
 - [Bereitstellen von HGS](#)
 - [Bereitstellen geschützter Hosts](#)
 - [Konfigurieren des Fabric-DNS für Hosts, die zu überwachten Hosts werden](#)
 - [Bereitstellen eines überwachten Hosts im AD-Modus](#)
 - [Bereitstellen eines überwachten Hosts mit dem TPM-Modus](#)
 - [Bestätigen, dass geschützte Hosts bestätigen können](#)
 - [Abgeschirmte VMS: der hostingdienstanbieter stellt überwachte Hosts in VMM bereit.](#)
 - [Bereitstellen von abgeschirmten VMs](#)
 - [Erstellen einer abgeschirmten VM-Vorlage](#)
 - [Vorbereiten einer VHD für ein VM-Schutz Hilfsprogramm](#)

- Einrichten des Windows Azure Packs
- Erstellen einer Schutz Datendatei
- Bereitstellen einer abgeschirmten VM mithilfe Windows Azure Pack
- Bereitstellen einer abgeschirmten VM mithilfe Virtual Machine Manager

Themen zur Betriebs-und Verwaltungsaufgaben

- Verwalten des Host-Überwachungs Diensts

Hyper-V unter Windows Server



09.04.2020 • 4 minutes to read • [Edit Online](#)




Gilt für: Windows Server 2016, Windows Server 2019

Mit der Hyper-V-Rolle in Windows Server können Sie eine virtualisierte Computerumgebung erstellen, in der Sie virtuelle Maschinen erstellen und verwalten können. Sie können mehrere Betriebssysteme auf einem physischen Computer ausführen und die Betriebssysteme voneinander isolieren. Mit dieser Technologie können Sie die Effizienz Ihrer Computerressourcen verbessern und Ihre Hardware Ressourcen freigeben.

Weitere Informationen zu Hyper-V unter Windows Server finden Sie in den Themen in der folgenden Tabelle.

Hyper-V-Ressourcen für IT-Profis

AUFGABE	RESSOURCEN
	<p>Auswerten von Hyper-V</p> <p>Übersicht über - Hyper-V-Technologie</p> <ul style="list-style-type: none">- Neuerungen bei Hyper-V unter Windows Server- System Anforderungen für Hyper-V unter Windows Server- unterstützten Windows-Gastbetriebssystemen für Hyper-V- unterstützte virtuelle Linux-und FreeBSD- Computer Kompatibilität von - Features nach Generierung und Gast <p>Planen für Hyper-V</p> <ul style="list-style-type: none">- sollte ich einen virtuellen Computer der Generation 1 oder 2 in Hyper-V erstellen?- Planen der Hyper-V-Skalierbarkeit in Windows Server- Plan für Hyper-V-Netzwerke in Windows Server- Planen der Hyper-V-Sicherheit in Windows Server
	<p>Beginnen Sie mit Hyper-V</p> <ul style="list-style-type: none">- herunterladen und Installieren von Windows Server 2019 <p>Server Core-oder GUI-Installationsoption von Windows Server 2019 als Host für virtuelle Maschinen</p> <ul style="list-style-type: none">- Installieren der Hyper-V-Rolle unter Windows Server- Erstellen eines virtuellen Switches für virtuelle Hyper-V-Computer- Erstellen eines virtuellen Computers in Hyper-V

AUFGABE	RESSOURCEN
	<p>Aktualisieren von Hyper-V-Hosts und virtuellen Maschinen</p> <ul style="list-style-type: none"> - Aktualisieren von Windows Server-Cluster Knoten - Aktualisieren der Version des virtuellen Computers - <p>Konfigurieren und Verwalten von Hyper-V</p> <ul style="list-style-type: none"> - Einrichten von Hosts für die Live Migration ohne Failoverclustering - die Remote Verwaltung von Nano Server - zwischen Standard-oder Produktions Prüfpunkten auswählen - Aktivieren oder Deaktivieren von Prüfpunkten - Verwalten von virtuellen Windows-Computern mit PowerShell Direct - Einrichten des Hyper-V-Replikats
	<p>Gt</p> <p>Sehen Sie sich die neuesten Beiträge von Programmmanagern, Produktmanagern, Entwicklern und Testern in den Microsoft-Virtualisierungs-und Hyper-V-Teams an.</p> <ul style="list-style-type: none"> - virtualisierungsblog - Windows Server-Blog - Blog von - Ben Armstrong (archiviert)
	<p>Forum und Newsgroups</p> <p>Haben Sie Fragen? Sprechen Sie mit ihren Peers, MVPs und dem Hyper-V-Produktteam.</p> <ul style="list-style-type: none"> - Windows Server-Community - Hyper-V-TechNet-Forum für Windows Server

Verwandte Technologien

In der folgenden Tabelle sind die Technologien aufgelistet, die Sie möglicherweise in ihrer virtualisierungsserverumgebung verwenden möchten.

TECHNOLOGIE	BESCHREIBUNG
Hyper-V für Clients	Virtualisierungstechnologie, die in Windows 8 enthalten ist, Windows 8.1 und Windows 10, die Sie über Programme und Funktionen in der Systemsteuerung installieren können.
Failoverclustering	Windows Server-Funktion, die Hochverfügbarkeit für Hyper-V-Hosts und virtuelle Maschinen bereitstellt.
Virtual Machine Manager	System Center-Komponente, die eine Verwaltungs Lösung für das virtualisierte Rechenzentrum bereitstellt. Sie können Virtualisierungshosts, Netzwerke und Speicherressourcen konfigurieren und verwalten, um virtuelle Maschinen und Dienste in privaten Clouds, die Sie erstellt haben, zu erstellen und bereitzustellen.

TECHNOLOGIE	BESCHREIBUNG
Windows-Container	Verwenden Sie Windows Server-und Hyper-V-Container, um standardisierte Umgebungen für Entwicklungs-, Test-und Produktionsteams bereitzustellen.

Übersicht über die Hyper-V-Technologie

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Hyper-V ist das Hardware-Virtualisierungsprodukt von Microsoft. Es ermöglicht Ihnen das Erstellen und Ausführen einer Softwareversion eines Computers, der als *virtueller* Computer bezeichnet wird. Jeder virtuelle Computer verhält sich wie ein kompletter Computer, auf dem ein Betriebssystem und Programme ausgeführt werden. Wenn Sie computeressourcen benötigen, bieten Ihnen virtuelle Computer mehr Flexibilität, Zeit und Geld zu sparen und eine effizientere Möglichkeit zur Verwendung von Hardware, als nur ein Betriebssystem auf physischer Hardware ausgeführt wird.

Hyper-V führt jeden virtuellen Computer in einem eigenen isolierten Speicherplatz aus. Das bedeutet, dass Sie mehrere virtuelle Computer gleichzeitig auf derselben Hardware ausführen können. Dies ist möglicherweise sinnvoll, um Probleme zu vermeiden, wie z. B. einen Absturz, der sich auf die anderen Workloads auswirkt, oder um anderen Personen, Gruppen oder Diensten Zugriff auf verschiedene Systeme zu bieten.

Einige Möglichkeiten, wie Hyper-V Ihnen helfen kann

Hyper-V kann Ihnen Folgendes helfen:

- **Richten Sie eine Private Cloud Umgebung ein oder erweitern Sie Sie.** Bieten Sie flexiblere, bedarfs gesteuerte IT-Dienste an, indem Sie die Verwendung von freigegebenen Ressourcen verschieben oder erweitern und die Auslastung bei Bedarf anpassen.
- **Verwenden Sie Ihre Hardware effektiver.** Konsolidieren Sie Server und Arbeits Auslastungen auf weniger, leistungsfähigere physische Computer, um weniger Strom und physischen Speicherplatz zu nutzen.
- **Verbessern Sie die Geschäftskontinuität.** Minimieren Sie die Auswirkungen sowohl geplanter als auch nicht geplanter Ausfallzeiten Ihrer Workloads.
- **Einrichten oder Erweitern einer virtuellen Desktop Infrastruktur (VDI).** Mithilfe einer zentralisierten Desktop Strategie mit VDI können Sie die geschäftliche Flexibilität und Datensicherheit steigern und die Einhaltung gesetzlicher Vorschriften und die Verwaltung von Desktop Betriebssystemen und-Anwendungen vereinfachen. Stellen Sie Hyper-V und Remotedesktop-Virtualisierungshost (RD-Virtualisierungshost) auf demselben Server bereit, um Ihren Benutzern persönliche virtuelle Desktops oder virtuelle Desktop Pools zur Verfügung zu stellen.
- **Entwickeln und testen Sie die Entwicklung und das Testen effizienter.** Reproduzieren Sie unterschiedliche Computerumgebungen, ohne dass Sie die erforderliche Hardware erwerben oder verwalten müssen, wenn Sie nur physische Systeme verwendet haben.

Hyper-V und andere Virtualisierungsprodukte

Hyper-V in Windows und Windows Server ersetzt ältere Hardwarevirtualisierungsprodukte, wie z. B. Microsoft Virtual PC, Microsoft Virtual Server und Windows Virtual PC. Hyper-V bietet Netzwerk-, Leistungs-, Speicher- und Sicherheitsfeatures, die in diesen älteren Produkten nicht verfügbar sind.

Hyper-V und die meisten Virtualisierungsanwendungen von Drittanbietern, die die gleichen Prozessor Features erfordern, sind nicht kompatibel. Dies liegt daran, dass die Prozessor Funktionen, die als hardwarevirtualisierungserweiterungen bezeichnet werden, nicht freigegeben werden sollen. Weitere

Informationen finden Sie unter [Virtualisierungsanwendungen funktionieren nicht zusammen mit Hyper-V, Device Guard und Credential Guard](#).

Welche Features haben Hyper-V?

Hyper-V bietet zahlreiche Features. Dies ist eine Übersicht, gruppiert nach den Funktionen, die von den Funktionen bereitgestellt oder unterstützt werden.

Computerumgebung : ein virtueller Hyper-V-Computer umfasst die gleichen grundlegenden Komponenten wie ein physischer Computer, wie z. B. Arbeitsspeicher, Prozessor, Speicher und Netzwerk. Alle diese Teile verfügen über Features und Optionen, mit denen Sie verschiedene Möglichkeiten zum Erfüllen verschiedener Anforderungen konfigurieren können. Speicher und Netzwerke können als eigene Kategorien angesehen werden, da Sie auf viele verschiedene Arten konfiguriert werden können.

Notfall Wiederherstellung und Sicherung : bei der Notfall Wiederherstellung erstellt das Hyper-V-Replikat Kopien von virtuellen Computern, die an einem anderen physischen Speicherort gespeichert werden sollen, sodass Sie den virtuellen Computer aus der Kopie wiederherstellen können. Für die Sicherung bietet Hyper-V zwei Arten von. Eine verwendet gespeicherte Zustände und die andere verwendet Volumeschattenkopie-Dienst (VSS), sodass Sie Anwendungs konsistente Sicherungen für Programme durchführen können, die VSS unterstützen.

Optimierung : jedes unterstützte Gast Betriebssystem verfügt über eine angepasste Reihe von Diensten und Treibern namens *Integration Services*, die die Verwendung des Betriebssystems auf einem virtuellen Hyper-V-Computer vereinfachen.

Portabilität : Features wie Live Migration, Speicher Migration und Import/Export vereinfachen die Verschiebung oder Verteilung eines virtuellen Computers.

Remote Konnektivität : Hyper-V umfasst die Verbindung mit virtuellen Computern, ein Remote Verbindungs Tool für die Verwendung mit Windows und Linux. Im Gegensatz zu Remotedesktop bietet dieses Tool den Konsolenzugriff, damit Sie sehen können, was im Gast passiert, auch wenn das Betriebssystem noch nicht gestartet wurde.

Der **Sicherheits** sichere Start und geschützte virtuelle Computer helfen beim Schutz vor Schadsoftware und anderen nicht autorisierten Zugriffen auf einen virtuellen Computer und dessen Daten.

Eine Zusammenfassung der in dieser Version eingeführten Features finden Sie unter [Neues in Hyper-V unter Windows Server](#). Einige Features oder Teile haben eine Beschränkung, wie viele konfiguriert werden können. Weitere Informationen finden Sie unter [Planen der Hyper-V-Skalierbarkeit in Windows Server 2016](#).

So erhalten Sie Hyper-V

Hyper-V ist in Windows Server und Windows als Server Rolle verfügbar, die für x64-Versionen von Windows Server verfügbar ist. Server Anweisungen finden Sie unter [Installieren der Hyper-V-Rolle unter Windows Server](#). Unter Windows ist es als [Feature](#) in einigen 64-Bit-Versionen von Windows verfügbar. Es steht auch als herunterladbares, eigenständiges Server Produkt [Microsoft Hyper-V Server](#) zur Verfügung.

Unterstützte Betriebssysteme

Viele Betriebssysteme werden auf virtuellen Computern ausgeführt. Im Allgemeinen wird ein Betriebssystem, das eine x86-Architektur verwendet, auf einem virtuellen Hyper-V-Computer ausgeführt. Nicht alle Betriebssysteme, die ausgeführt werden können, werden von Microsoft getestet und unterstützt. Listen der unterstützten Funktionen finden Sie unter:

- [Unterstützte virtuelle Linux-und FreeBSD-Computer für Hyper-V unter Windows](#)
- [Unterstützte Windows-Gast Betriebssysteme für Hyper-V unter Windows Server](#)

Funktionsweise von Hyper-V

Hyper-V ist eine Hypervisor-basierte Virtualisierungstechnologie. Hyper-V verwendet den Windows-Hypervisor, der einen physischen Prozessor mit spezifischen Funktionen erfordert. Hardware Details finden Sie unter [System Anforderungen für Hyper-V unter Windows Server](#).

In den meisten Fällen verwaltet der Hypervisor die Interaktionen zwischen der Hardware und den virtuellen Computern. Dieser über den Hypervisor gesteuerte Zugriff auf die Hardware bietet virtuellen Maschinen die isolierte Umgebung, in der Sie ausgeführt werden. In einigen Konfigurationen hat ein virtueller Computer oder das Betriebssystem, das auf dem virtuellen Computer ausgeführt wird, direkten Zugriff auf Grafiken, Netzwerke oder Speicherhardware.

Worin besteht Hyper-V?

Hyper-V verfügt über erforderliche Komponenten, die zusammenarbeiten, damit Sie virtuelle Computer erstellen und ausführen können. Diese Teile werden als Virtualisierungsplattform bezeichnet. Sie werden bei der Installation der Hyper-V-Rolle als Gruppe installiert. Zu den erforderlichen Komponenten gehören der Windows-Hypervisor, der Hyper-V-Verwaltungsdienst für virtuelle Computer, der virtualisierungswmi-Anbieter, der Virtual Machine Bus (VMBus), der virtualisierungsdienstanbieter (VSP) und der virtuelle Infrastruktur Treiber (vid).

Hyper-V verfügt auch über Tools für Verwaltung und Konnektivität. Sie können diese auf demselben Computer installieren, auf dem die Hyper-v-Rolle installiert ist, und auf Computern, auf denen die Hyper-v-Rolle nicht installiert ist. Diese Tools sind:

- Hyper-V-Manager
- [Hyper-V-Modul für Windows PowerShell](#)
- Die [Verbindung des virtuellen](#) Computers (manchmal als "VMConnect" bezeichnet)
- [Windows PowerShell Direct](#)

Verwandte Technologien

Dabei handelt es sich um einige Technologien von Microsoft, die häufig mit Hyper-V verwendet werden:

- [Failoverclustering](#)
- [Remotedesktopdienste](#)
- [System Center Virtual Machine Manager](#)

Verschiedene Speichertechnologien: freigegebene Clustervolumes, SMB 3,0, direkte Speicherplätze

Windows-Container bieten einen anderen Ansatz für die Virtualisierung. Weitere Informationen finden Sie in der [Windows-Container](#) Bibliothek auf MSDN.

Neues in Hyper-V unter Windows Server

09.04.2020 • 31 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Microsoft Hyper-V Server 2016, Windows Server 2016

In diesem Artikel werden die neuen und geänderten Funktionen von Hyper-V auf Windows Server 2019, Windows Server 2016 und Microsoft Hyper-V Server 2016 erläutert. Wenn Sie neue Features auf virtuellen Computern verwenden möchten, die mit Windows Server 2012 R2 erstellt wurden und auf einen Server mit Hyper-V unter Windows Server 2019 oder Windows Server 2016 verschoben oder importiert wurden, müssen Sie die Konfigurations Version des virtuellen Computers manuell aktualisieren. Anweisungen finden Sie unter [Aktualisieren der Version der virtuellen Maschine](#).

Dies ist in diesem Artikel enthalten, und es wird erläutert, ob die Funktionalität neu ist oder aktualisiert wurde.

Windows Server, Version 1903

Hinzufügen von Hyper-V-Manager zu Server Core-Installationen (aktualisiert)

Wie Ihnen vielleicht bekannt ist, empfehlen wir die Verwendung der Server Core-Installationsoption beim Einsatz von Windows Server im halbjährlichen Kanal in Produktionsumgebungen. Standardmäßig sind in Server Core jedoch eine Reihe nützlicher Verwaltungstools fortgelassen. Viele der häufig verwendeten Tools lassen sich durch Installieren des App-Kompatibilitätsfeatures hinzufügen, aber einige Tools fehlten immer noch.

Basierend auf dem Kundenfeedback haben wir dem App-Kompatibilitäts Feature in dieser Version noch ein paar weitere Tools hinzugefügt: Hyper-V-Manager (virtmgmt. msc).

Weitere Informationen finden Sie unter [Server Core-App-Kompatibilitätsfeature](#).

Windows Server 2019

Sicherheit: Verbesserungen der abgeschirmten Virtual Machines (neu)

- **Verbesserungen für Filialen**

Sie können nun abgeschirmte virtuelle Computer auf Computern mit intermittierender Konnektivität zum Host-Überwachungsdienst (Host Guardian Service, HGS) ausführen, indem Sie die neuen [Fallback-HGS](#)- und [Offline-Modus](#)-Features nutzen. Fallback HGS ermöglicht es Ihnen, einen zweiten Satz von URLs für Hyper-V zu konfigurieren, um zu prüfen, ob Ihr primärer HGS-Server erreicht werden kann.

Im Offline-Modus können Sie Ihre abgeschirmten VMs auch dann starten, wenn HGS nicht erreichbar ist, sofern die VM einmal erfolgreich gestartet wurde und sich die Sicherheitskonfiguration des Hosts nicht geändert hat.

- **Verbesserungen bei der Problembehandlung**

Darüber hinaus haben wir die Problembehandlung bei Ihren [abgeschirmten virtuellen Computern](#) vereinfacht, indem wir den erweiterten VMConnect-Sitzungsmodus und PowerShell Direct unterstützen. Diese Tools sind besonders nützlich, wenn Sie die Netzwerkverbindung zu Ihrer VM verloren haben und ihre Konfiguration aktualisieren müssen, um den Zugriff wiederherzustellen.

Diese Features müssen nicht konfiguriert werden, und sie werden automatisch zur Verfügung gestellt, wenn eine abgeschirmte VM auf einem Hyper-V-Host mit Windows Server, Version 1803 oder höher, ausgeführt wird.

- **Linux-Unterstützung**

Wenn Sie Umgebungen mit gemischten Betriebssystemen ausführen, unterstützt Windows Server 2019 jetzt die Ausführung von Ubuntu, Red Hat Enterprise Linux und SUSE Linux Enterprise Server in abgeschirmten virtuellen Computern.

Windows Server 2016

Kompatibel mit verbundenen Standby-(neue)

Wenn die Hyper-V-Rolle auf einem Computer installiert ist, der das Energiemodell Always on/Always Connected (AOAC) verwendet, ist der Energiezustand " **verbundener** Standbymodus" nun verfügbar.

Diskrete Geräte Zuweisung (neue)

Mit diesem Feature können Sie einem virtuellen Computer einen direkten und exklusiven Zugriff auf einige PCIe-Hardware Geräte ermöglichen. Wenn Sie ein Gerät auf diese Weise verwenden, wird der Hyper-V-Virtualisierungsstapel umgangen, was zu einem schnelleren Zugriff führt. Weitere Informationen zur unterstützten Hardware finden Sie unter "diskrete Geräte Zuweisung" unter [System Anforderungen für Hyper-V auf Windows Server 2016](#). Weitere Informationen, einschließlich der Verwendung dieses Features und Überlegungen, finden Sie im Beitrag "[diskrete Geräte Zuweisung – Beschreibung und Hintergrund](#)" im virtualisierungsblog.

Verschlüsselungs Unterstützung für den Betriebssystem Datenträger in virtuellen Maschinen der Generation 1 (neu)

Sie können den Betriebssystem Datenträger jetzt mithilfe der BitLocker-Laufwerk Verschlüsselung auf virtuellen Computern der Generation 1 schützen. Ein neues Feature, Schlüsselspeicher, erstellt ein kleines, dediziertes Laufwerk zum Speichern des BitLocker-Schlüssels des System Laufwerks. Dies erfolgt anstelle der Verwendung eines virtuellen Trusted Platform Module (TPM), das nur auf virtuellen Computern der Generation 2 verfügbar ist. Um den Datenträger zu entschlüsseln und den virtuellen Computer zu starten, muss der Hyper-V-Host entweder Teil eines autorisierten geschützten Fabrics sein oder den privaten Schlüssel von einem der Wächter der virtuellen Maschine aufweisen. Der Schlüsselspeicher erfordert einen virtuellen Computer der Version 8. Informationen zur Version der virtuellen Maschine finden Sie unter [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#).

Host Ressourcenschutz (neue)

Mit dieser Funktion wird verhindert, dass ein virtueller Computer mehr als den Anteil der Systemressourcen verwendet, indem er nach übermäßigen Aktivitätsstufen sucht. Dadurch kann verhindert werden, dass die übermäßige Aktivität eines virtuellen Computers die Leistung des Hosts oder anderer virtueller Maschinen beeinträchtigt. Wenn die Überwachung einen virtuellen Computer mit übermäßiger Aktivität erkennt, erhält die virtuelle Maschine weniger Ressourcen. Diese Überwachung und Durchsetzung ist standardmäßig deaktiviert. Aktivieren oder deaktivieren Sie diese mithilfe von Windows PowerShell. Um dies zu aktivieren, führen Sie den folgenden Befehl aus:

```
Set-VMProcessor TestVM -EnableHostResourceProtection $true
```

Weitere Informationen zu diesem Cmdlet finden Sie unter [Set-vmprocessor](#).

Hot Add und Remove für Netzwerkadapter und Arbeitsspeicher (neue)

Sie können nun einen Netzwerkadapter hinzufügen oder entfernen, während der virtuelle Computer ausgeführt wird, ohne Ausfallzeiten zu verursachen. Dies funktioniert für virtuelle Computer der Generation 2, auf denen Windows-oder Linux-Betriebssysteme ausgeführt werden.

Sie können auch die Menge an Arbeitsspeicher anpassen, die einem virtuellen Computer während der Ausführung zugewiesen wird, auch wenn Sie dynamischer Arbeitsspeicher nicht aktiviert haben. Dies funktioniert

für virtuelle Computer der Generation 1 und Generation 2, auf denen Windows Server 2016 oder Windows 10 ausgeführt wird.

Verbesserungen der Hyper-V-Manager (aktualisiert)

- **Unterstützung alternativer Anmelde Informationen:** Sie können nun einen anderen Satz von Anmelde Informationen im Hyper-V-Manager verwenden, wenn Sie eine Verbindung mit einem anderen Windows Server 2016-oder Windows 10-Remote Host herstellen. Sie können diese Anmelde Informationen auch speichern, um die Anmeldung zu vereinfachen.
- **Verwalten früherer Versionen :** mit dem Hyper-v-Manager in Windows Server 2019, Windows Server 2016 und Windows 10 können Sie Computer verwalten, auf denen Hyper-v unter Windows Server 2012, Windows 8, Windows Server 2012 R2 und Windows 8.1 ausgeführt wird.
- **Aktualisiertes Verwaltungs Protokoll :** der Hyper-v-Manager kommuniziert jetzt mit Remote-Hyper-v-Hosts mithilfe des WS-man-Protokolls, das die CredSSP-, Kerberos-oder NTLM-Authentifizierung zulässt. Wenn Sie zum Herstellen einer Verbindung mit einem Hyper-V-Remote Host mithilfe von "andssp" eine Verbindung herstellen, können Sie eine Live Migration durchführen, ohne die eingeschränkte Delegierung Active Directory in Mit der WS-man-basierten Infrastruktur wird auch das Aktivieren eines Hosts für die Remote Verwaltung vereinfacht. WS-MAN stellt über Port 80 eine Verbindung her, der standardmäßig geöffnet ist.

Von Windows Update (aktualisierte Integrationsdienste)

Aktualisierungen von Integration Services für Windows-Gäste werden über Windows Update verteilt. Für Dienstanbieter und Private Cloud Hosts wird dadurch das Anwenden von Updates auf die Hände der Mandanten, die die virtuellen Computer besitzen, gesteuert. Mandanten können nun Ihre virtuellen Windows-Computer mit allen Updates, einschließlich der Integrationsdienste, mithilfe einer einzigen Methode aktualisieren. Ausführliche Informationen zu Integration Services für Linux-Gäste finden Sie [unter Linux und FreeBSD Virtual Machines auf Hyper-V](#).

IMPORTANT

Die Image Datei "vmguest. ISO" wird nicht mehr benötigt und ist daher nicht in Hyper-V unter Windows Server 2016 enthalten.

Virtueller Linux-Start (neue)

Linux-Betriebssysteme auf virtuellen Computern der Generation 2 können jetzt mit aktivierter Option "sicherer Start" gestartet werden. Ubuntu 14,04 und höher, SuSE Linux Enterprise Server 12 und höher, Red Hat Enterprise Linux 7,0 und höher, und CentOS 7,0 und höher sind für den sicheren Start auf Hosts aktiviert, auf denen Windows Server 2016 ausgeführt wird. Bevor Sie den virtuellen Computer zum ersten Mal starten, müssen Sie den virtuellen Computer für die Verwendung der Microsoft UEFI-Zertifizierungsstelle konfigurieren. Hierzu können Sie den Hyper-V-Manager, Virtual Machine Manager oder eine Windows PowerShell-Sitzung mit erhöhten Rechten verwenden. Führen Sie für Windows PowerShell den folgenden Befehl aus:

```
Set-VMFirmware TestVM -SecureBootTemplate MicrosoftUEFICertificateAuthority
```

Weitere Informationen zu virtuellen Linux-Computern in Hyper-v finden Sie [unter Linux und FreeBSD Virtual Machines auf Hyper-v](#). Weitere Informationen zum Cmdlet finden Sie unter [Set-vmfirmware](#).

Mehr Arbeitsspeicher und Prozessoren für virtuelle Maschinen der Generation 2 und Hyper-V-Hosts (aktualisiert)

Ab Version 8 können virtuelle Maschinen der Generation 2 erheblich mehr Arbeitsspeicher und virtuelle Prozessoren verwenden. Hosts können auch mit wesentlich mehr Arbeitsspeicher und virtuellen Prozessoren konfiguriert werden, als zuvor unterstützt wurden. Diese Änderungen unterstützen neue Szenarien, wie z. b. das

Ausführen von großen in-Memory-Datenbanken für die Online Transaktionsverarbeitung (OLTP) und Data Warehousing (DW). Der Windows Server-Blog veröffentlichte vor kurzem die Leistungsergebnisse eines virtuellen Computers mit 5,5 Terabyte Arbeitsspeicher und 128 virtuellen Prozessoren mit einer in-Memory Database von 4 TB. Die Leistung war größer als 95% der Leistung eines physischen Servers. Weitere Informationen finden Sie unter [Windows Server 2016 Hyper-V-VM-Leistung in großem Maßstab für die Verarbeitung im Arbeitsspeicher](#). Weitere Informationen zu Versionen von virtuellen Computern finden Sie unter [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#). Die vollständige Liste der unterstützten maximalen Konfigurationen finden Sie unter [Planen der Hyper-V-Skalierbarkeit in Windows Server 2016](#).

(neue)

Mit dieser Funktion können Sie einen virtuellen Computer als Hyper-V-Host verwenden und virtuelle Maschinen innerhalb dieses virtualisierten Hosts erstellen. Dies kann besonders für Entwicklungs- und Testumgebungen nützlich sein. Um die Netzwerkvirtualisierung verwenden zu können, benötigen Sie Folgendes:

- Zum Ausführen von mindestens Windows Server 2019, Windows Server 2016 oder Windows 10 auf dem physischen Hyper-V-Host und dem virtualisierten Host.
- Ein Prozessor mit Intel VT-x (Nested Virtualization steht zurzeit nur für Intel-Prozessoren zur Verfügung).

Weitere Informationen und Anweisungen finden Sie unter [Ausführen von Hyper-V auf einem virtuellen Computer mit der Netzwerkvirtualisierung](#).

Netzwerk Features (neue)

Zu den neuen Netzwerk Features gehören:

- **Remote Zugriff auf den direkten Speicher (RDMA) und Switch Embedded Team Vorgang (Set)** . Sie können RDMA für Netzwerkadapter einrichten, die an einen virtuellen Hyper-V-Switch gebunden sind, unabhängig davon, ob auch Set verwendet wird. Set bietet einen virtuellen Switch mit einigen der gleichen Funktionen wie der NIC-Team Vorgang. Weitere Informationen finden Sie unter [Remote Direct Memory Access \(RDMA\) und Switch Embedded Teaming \(Set\)](#).
- **Virtual Machine-multiwarteschlangen (vmmq)** . Verbessert den VMQ-Durchsatz durch Zuordnen mehrerer Hardware Warteschlangen pro virtuellem Computer. Die Standard Warteschlange wird zu einem Satz von Warteschlangen für einen virtuellen Computer, und der Datenverkehr wird zwischen den Warteschlangen verteilt.
- **Quality of Service (QoS) für softwaredefinierte Netzwerke**. Verwaltet die Standardklasse des Datenverkehrs über den virtuellen Switch innerhalb der standardmäßigen Klassen Bandbreite.

Weitere Informationen zu neuen Netzwerk Features finden Sie unter [What es New in Networking](#).

Produktions Prüfpunkte (neue)

Produktions Prüfpunkte sind "Point-in-Time"-Images einer virtuellen Maschine. Auf diese Weise können Sie einen Prüfpunkt anwenden, der den Unterstützungs Richtlinien entspricht, wenn ein virtueller Computer eine produktionsworkloads ausführt. Produktions Prüfpunkte basieren auf Sicherungs Technologie innerhalb des Gast Betriebssystems anstelle eines gespeicherten Zustands. Bei virtuellen Windows-Computern wird der volumemomentaufnahme-Dienst (VSS) verwendet. Bei virtuellen Linux-Computern werden die Dateisystem Puffer geleert, um einen Prüfpunkt zu erstellen, der mit dem Dateisystem konsistent ist. Wenn Sie stattdessen Prüfpunkte auf der Grundlage gespeicherter Zustände verwenden möchten, wählen Sie stattdessen Standard Prüfpunkte aus. Weitere Informationen finden Sie unter [Auswählen zwischen Standard-oder Produktions Prüfpunkten in Hyper-V](#).

IMPORTANT

Bei neuen virtuellen Computern werden Produktions Prüfpunkte als Standard verwendet.

Paralleles Upgrade für Hyper-V-Cluster (neue)

Sie können nun einen Knoten unter Windows Server 2019 oder Windows Server 2016 zu einem Hyper-V-Cluster hinzufügen, auf dem Windows Server 2012 R2 ausgeführt wird. Dies ermöglicht es Ihnen, den Cluster ohne Ausfallzeiten zu aktualisieren. Der Cluster wird auf einer Windows Server 2012 R2-Funktionsebene ausgeführt, bis Sie ein Upgrade für alle Knoten im Cluster durchführen und die Cluster Funktionsebene mit dem Windows PowerShell-Cmdlet [Update-clusterfunctionallevel](#) aktualisieren.

IMPORTANT

Nachdem Sie die Cluster Funktionsebene aktualisiert haben, können Sie Sie nicht mehr an Windows Server 2012 R2 zurückgeben.

Für einen Hyper-V-Cluster mit einer Funktionsebene von Windows Server 2012 R2 mit Knoten, auf denen Windows Server 2012 R2, Windows Server 2019 und Windows Server 2016 ausgeführt wird, beachten Sie Folgendes:

- Verwalten Sie den Cluster, Hyper-V und virtuelle Computer von einem Knoten, auf dem Windows Server 2016 oder Windows 10 ausgeführt wird.
- Sie können virtuelle Maschinen zwischen allen Knoten im Hyper-V-Cluster verschieben.
- Wenn Sie neue Hyper-V-Features verwenden möchten, müssen auf allen Knoten Windows Server 2016 oder ausgeführt werden, und die Cluster Funktionsebene muss aktualisiert werden.
- Die Konfigurations Version des virtuellen Computers für vorhandene virtuelle Maschinen wird nicht aktualisiert. Sie können die Konfigurations Version erst aktualisieren, nachdem Sie die Cluster Funktionsebene aktualisiert haben.
- Virtuelle Computer, die Sie erstellen, sind kompatibel mit Windows Server 2012 R2, VM-Konfigurations Ebene 5.

Nachdem Sie die Cluster Funktionsebene aktualisiert haben:

- Sie können neue Hyper-V-Features aktivieren.
- Um neue Features für virtuelle Computer verfügbar zu machen, verwenden Sie das Update-vmconfigurationversion-Cmdlet, um die Konfigurations Ebene des virtuellen Computers manuell zu aktualisieren. Anweisungen finden Sie unter [Aktualisieren der Version der virtuellen Maschine](#).
- Sie können dem Hyper-V-Cluster, auf dem Windows Server 2012 R2 ausgeführt wird, keinen Knoten hinzufügen.

NOTE

Hyper-V unter Windows 10 unterstützt kein Failoverclustering.

Weitere Informationen und Anweisungen finden Sie unter Paralleles [Upgrade des Cluster Betriebssystems](#).

Freigegebene virtuelle Festplatten (aktualisiert)

Sie können jetzt die Größe der freigegebenen virtuellen Festplatten (vhdx-Dateien), die für Gastclustering verwendet werden, ohne Ausfallzeiten ändern. Freigegebene virtuelle Festplatten können vergrößert oder

verkleinert werden, während der virtuelle Computer online ist. Gast Cluster können jetzt auch freigegebene virtuelle Festplatten mithilfe des Hyper-V-Replikats für die Notfall Wiederherstellung schützen.

Aktivieren Sie die Replikation für die Sammlung. Das Aktivieren der Replikation für eine Sammlung wird **nur über die WMI-Schnittstelle** verfügbar gemacht. Weitere Informationen finden Sie in der Dokumentation zur [Msvm_CollectionReplicationService-Klasse](#). **Die Replikation einer Sammlung kann nicht über das PowerShell-Cmdlet oder die Benutzeroberfläche verwaltet werden.** Die VMs sollten sich auf Hosts befinden, die Teil eines Hyper-V-Clusters sind, um auf Features zuzugreifen, die für eine Sammlung spezifisch sind. Dies gilt auch für freigegebene virtuelle Festplatten: freigegebene virtuelle Festplatten auf eigenständigen Hosts werden vom Hyper-V-Replikat nicht unterstützt.

Befolgen Sie die Richtlinien für freigegebene VHDs unter [Übersicht über die Freigabe virtueller Festplatten](#), und stellen Sie sicher, dass die freigegebenen VHDs Teil eines Gast Clusters sind.

Eine Sammlung mit einer freigegebenen VHD, aber keinem zugeordneten Gast Cluster, kann keine Referenzpunkte für die Sammlung erstellen (unabhängig davon, ob die freigegebene virtuelle Festplatte in der Referenzpunkt Erstellung enthalten ist oder nicht).

Sicherung virtueller Computer(neue)

Wenn Sie einen einzelnen virtuellen Computer sichern (unabhängig davon, ob der Host geclustert ist), sollten Sie keine VM-Gruppe verwenden. Sie sollten auch keine Momentaufnahme Sammlung verwenden. VM-Gruppen und die Momentaufnahme Sammlung dienen ausschließlich zum Sichern von Gast Clustern, die freigegebene vhdx verwenden. Stattdessen sollten Sie eine Momentaufnahme mithilfe des [Hyper-V-WMI v2-Anbieters](#) erstellen. Verwenden Sie auch den [WMI-Anbieter für den Failoverclusternicht](#).

Geschützte virtuelle Computer (neue)

Abgeschirmte virtuelle Computer verwenden mehrere Features, um Hyper-V-Administratoren und Schadsoftware auf dem Host das Überprüfen, manipulieren oder stehlen von Daten aus dem Zustand eines abgeschirmten virtuellen Computers zu erschweren. Daten und Status sind verschlüsselt, Hyper-V-Administratoren können die Videoausgabe und die Datenträger nicht anzeigen, und die virtuellen Computer können so eingeschränkt werden, dass Sie nur auf bekannten, fehlerfreien Hosts ausgeführt werden, die von einem Host-Überwachungs Server bestimmt werden. Weitere Informationen finden Sie unter geschütztes [Fabric und abgeschirmte VMS](#).

NOTE

Abgeschirmte virtuelle Computer sind mit dem Hyper-V-Replikat kompatibel. Zum Replizieren einer abgeschirmten virtuellen Maschine muss der Host, auf den Sie replizieren möchten, autorisiert sein, die geschützte virtuelle Maschine auszuführen.

Priorität der Reihenfolge der virtuellen Cluster Computer (neue)

Diese Funktion ermöglicht Ihnen mehr Kontrolle darüber, welche virtuellen Cluster Computer zuerst gestartet oder neu gestartet werden. Dies erleichtert das Starten von virtuellen Computern, die Dienste vor virtuellen Computern bereitstellen, die diese Dienste verwenden. Definieren von Sätzen, platzieren virtueller Maschinen in Gruppen und Angeben von Abhängigkeiten. Verwenden Sie Windows PowerShell-Cmdlets, um die Sätze zu verwalten, z. b. [New-clustergroupset](#), [Get-clustergroupset](#) und [Add-clustergroupsetabhängigkeit](#).

Quality of Service (QoS) für Speicher (aktualisiert)

Sie können nun Speicher-QoS-Richtlinien auf einem Dateiserver mit horizontaler Skalierung erstellen und diese einem oder mehreren virtuellen Datenträgern auf virtuellen Hyper-V-Computern zuweisen. Bei Änderungen der Speicherlast wird die Speicherleistung automatisch neu angepasst, um die Richtlinien einzuhalten. Weitere Informationen finden Sie unter [Storage Quality of Service](#).

Das Konfigurationsdatei Format des virtuellen Computers (aktualisiert)

Konfigurationsdateien für virtuelle Computer verwenden ein neues Format, das das Lesen und Schreiben von

Konfigurationsdaten effizienter macht. Das Format führt auch zu einer Beschädigung der Daten, wenn ein Speicherfehler auftritt. Die Datendateien der Konfiguration der virtuellen Maschine verwenden eine vmcx-Dateinamenerweiterung und Datendateien für den Laufzeit-Zustand verwenden die Dateinamenerweiterung VMRS.

IMPORTANT

Die vmcx-Dateierweiterung gibt eine Binärdatei an. Das Bearbeiten von vmcx- oder VMRS-Dateien wird nicht unterstützt.

Die Konfigurationsversion des virtuellen Computers (aktualisiert)

Die Version stellt die Kompatibilität der Konfiguration der virtuellen Maschine, des gespeicherten Zustands und der Momentaufnahme-Dateien mit der Hyper-V-Version dar. Virtuelle Computer mit Version 5 sind kompatibel mit Windows Server 2012 R2 und können unter Windows Server 2012 R2 und Windows Server 2016 ausgeführt werden. Virtuelle Computer, deren Versionen in Windows Server 2016 und Windows Server 2019 eingeführt wurden, werden nicht in Hyper-V unter Windows Server 2012 R2 ausgeführt.

Wenn Sie eine virtuelle Maschine auf einen Server mit Hyper-V unter Windows Server 2016 oder Windows Server 2019 von Windows Server 2012 R2 verschieben oder importieren, wird die Konfiguration der virtuellen Maschine nicht automatisch aktualisiert. Dies bedeutet, dass Sie den virtuellen Computer auf einen Server zurück verschieben können, auf dem Windows Server 2012 R2 ausgeführt wird. Dies bedeutet jedoch auch, dass Sie die neuen Features für virtuelle Computer erst verwenden können, wenn Sie die Version der Konfiguration der virtuellen Maschine manuell aktualisieren.

Anweisungen zum Überprüfen und Aktualisieren der Version finden Sie unter [Aktualisieren der Version der virtuellen Maschine](#). In diesem Artikel wird außerdem die Version aufgeführt, in der einige Features eingeführt wurden.

IMPORTANT

- Nachdem Sie die Version aktualisiert haben, können Sie die virtuelle Maschine nicht auf einen Server mit Windows Server 2012 R2 verschieben.
- Sie können die Konfiguration nicht auf eine frühere Version herabstufen.
- Das [Update-VMVersion](#)-Cmdlet wird auf einem Hyper-V-Cluster blockiert, wenn die Clusterfunktionsebene Windows Server 2012 R2 ist.

Virtualisierungsbasierte Sicherheit für virtuelle Maschinen der Generation 2 (neu)

Virtualisierungsbasierte Sicherheit stellt Features wie Device Guard und Credential Guard bereit und bietet einen verstärkten Schutz des Betriebssystems gegen Exploits von Schadsoftware. Virtualisierungsbasierte Sicherheit ist auf virtuellen Gast Computern der Generation 2 ab Version 8 verfügbar. Informationen zur Version der virtuellen Maschine finden Sie unter [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#).

Windows-Container (neue)

Mit Windows-Containern können viele isolierte Anwendungen auf einem Computersystem ausgeführt werden. Sie können schnell erstellt werden und sind hochgradig skalierbar und portabel. Es sind zwei Typen von Containern Laufzeit verfügbar, von denen jede einen anderen Grad an Anwendungs-Isolation hat. Windows Server-Container verwenden Namespace- und Prozess-Isolation. Für Hyper-V-Container wird für jeden Container ein einfacher virtueller Computer verwendet.

Wichtige Merkmale:

- Unterstützung für Websites und Anwendungen mit HTTPS
- Nano Server kann sowohl Windows Server- als auch Hyper-V-Container hosten.

- Möglichkeit zum Verwalten von Daten über freigegebene Container Ordner
- Möglichkeit zum Einschränken von Container Ressourcen

Weitere Informationen, einschließlich Schnellstart Handbücher, finden Sie in der [Dokumentation zu Windows-Containern](#).

Windows PowerShell Direct (neue)

Dadurch haben Sie die Möglichkeit, Windows PowerShell-Befehle auf einem virtuellen Computer auf dem Host auszuführen. Windows PowerShell Direct wird zwischen dem Host und dem virtuellen Computer ausgeführt. Dies bedeutet, dass keine Netzwerk-oder Firewallanforderungen erforderlich sind und unabhängig von Ihrer Remote Verwaltungs Konfiguration funktionieren.

Windows PowerShell Direct ist eine Alternative zu den vorhandenen Tools, die von Hyper-v-Administratoren verwendet werden, um eine Verbindung mit einer virtuellen Maschine auf einem Hyper-v-Host herzustellen:

- Remoteverwaltungstools wie PowerShell oder Remotedesktop
- Verbindung mit dem virtuellen Hyper-V-Computer (VMConnect)

Diese Tools funktionieren gut, haben jedoch Kompromisse: VMConnect ist zuverlässig, kann aber nur schwer automatisiert werden. Remote-PowerShell ist leistungsstark, kann aber nur schwer einzurichten und zu warten. Diese Kompromisse werden möglicherweise wichtiger, wenn Ihre Hyper-V-Bereitstellung zunimmt. Windows PowerShell Direct wendet dies durch die Bereitstellung einer leistungsstarken Skript-und Automatisierungsfunktion an, die so einfach ist wie die Verwendung von VMConnect.

Anforderungen und Anweisungen finden Sie unter [Verwalten virtueller Windows-Computer mit PowerShell Direct](#).

System Anforderungen für Hyper-V unter Windows Server

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Für Hyper-v gelten bestimmte Hardwareanforderungen, und einige Hyper-v-Features haben zusätzliche Anforderungen. Verwenden Sie die Details in diesem Artikel, um zu entscheiden, welche Anforderungen Ihr System erfüllen muss, damit Sie Hyper-V wie geplant verwenden können. Überprüfen Sie anschließend den [Windows Server-Katalog](#). Beachten Sie, dass die Anforderungen für Hyper-V die allgemeinen Mindestanforderungen für Windows Server 2016 überschreiten, da eine Virtualisierungsumgebung mehr computeressourcen erfordert.

Wenn Sie Hyper-V bereits verwenden, ist es wahrscheinlich, dass Sie Ihre vorhandene Hardware verwenden können. Die allgemeinen Hardwareanforderungen wurden von Windows Server 2012 R2 nicht signifikant geändert. Sie benötigen jedoch neuere Hardware, um abgeschirmte virtuelle Computer oder eine diskrete Geräte Zuweisung zu verwenden. Diese Features basieren auf einer bestimmten Hardwareunterstützung, wie unten beschrieben. Der wichtigste Unterschied bei der Hardware besteht darin, dass die Adressübersetzung (slat) der zweiten Ebene jetzt anstelle von "empfohlen" erforderlich ist.

Ausführliche Informationen zu den maximal unterstützten Konfigurationen für Hyper-v, wie z. b. die Anzahl der aktiven virtuellen Maschinen, finden Sie unter [Planen der Hyper-v-Skalierbarkeit in Windows Server 2016](#). Die Liste der Betriebssysteme, die Sie auf Ihren virtuellen Computern ausführen können, finden Sie [unter Unterstützte Windows-Gast Betriebssysteme für Hyper-V unter Windows Server](#).

Allgemeine Anforderungen

Unabhängig von den Hyper-V-Features, die Sie verwenden möchten, benötigen Sie Folgendes:

- Ein 64-Bit-Prozessor mit Adressübersetzung der zweiten Ebene (Address Translation, slat). Zum Installieren der Hyper-V-Virtualisierungskomponenten, z. b. Windows-Hypervisor, muss der Prozessor über slat verfügen. Es ist jedoch nicht erforderlich, Hyper-v-Verwaltungs Tools wie die Verbindung mit virtuellen Computern (VMConnect), den Hyper-v-Manager und die Hyper-v-Cmdlets für Windows PowerShell zu installieren. Weitere Informationen finden Sie unter "Vorgehensweise beim Überprüfen der Hyper-V-Anforderungen" unten, um zu ermitteln, ob Ihr Prozessor slat hat.
- Erweiterungen des VM-Monitor Modus
- Ausreichender Speicher Plan für mindestens 4 GB RAM. Mehr Arbeitsspeicher ist besser. Für den Host und alle virtuellen Computer, die Sie gleichzeitig ausführen möchten, benötigen Sie ausreichend Arbeitsspeicher.
- Virtualisierungsunterstützung im BIOS oder UEFI aktiviert:
 - Hardwareunterstützte Virtualisierung. Dies ist in Prozessoren verfügbar, die eine Virtualisierungsoption enthalten, insbesondere Prozessoren mit Intel-Virtualisierungstechnologie (Intel VT) oder AMD Virtualization (AMD-V)-Technologie.
 - Von der Hardware erzwungene Datenausführungsverhinderung (DEP) muss verfügbar und aktiviert sein. Bei Intel-Systemen ist dies der XD-Bit-Wert (deaktivierte Bit ausführen). Bei AMD-

Systemen ist dies das NX-Bit (No Execute Bit).

Überprüfen der Hyper-V-Anforderungen

Öffnen Sie Windows PowerShell oder eine Eingabeaufforderung, und geben Sie Folgendes ein:

```
Systeminfo.exe
```

Scrollen Sie zum Abschnitt "Hyper-V-Anforderungen", um den Bericht zu überprüfen.

Anforderungen für bestimmte Features

Dies sind die Anforderungen für die diskrete Geräte Zuweisung und geschützte virtuelle Computer.

Beschreibungen dieser Features finden Sie unter [Neues in Hyper-V unter Windows Server](#).

Diskrete Geräte Zuweisung

Die Host Anforderungen ähneln den vorhandenen Anforderungen für die SR-IOV-Funktion in Hyper-v.

- Der Prozessor muss entweder die erweiterte Seiten Tabelle (EPT) von Intel oder die Nested Page Table (Atom) der AMD (Nested Page Table) enthalten.
- Der Chipsatz muss Folgendes aufweisen:
 - Neuordnung unterbrechen: die VT-d von Intel mit der Funktion zum Neuordnen von Unterbrechungen (VT-D2) oder eine beliebige Version der AMD-e/a-Speicherverwaltungseinheit (e/a-MMU).
 - DMA-Neuordnung: die VT-d von Intel mit Invalidierungen in der Warteschlange oder eine beliebige AMD-e/a-MMU.
 - Zugriffs Steuerungs Dienste (ACS) auf PCI Express-stammports.
- In den firmwaretabellen muss das e/a-MMU für den Windows-Hypervisor verfügbar gemacht werden. Beachten Sie, dass diese Funktion in UEFI oder BIOS deaktiviert werden kann. Anweisungen finden Sie in der Hardware Dokumentation, oder wenden Sie sich an den Hardwarehersteller.

Geräte benötigen GPU oder Non-volatile Memory Express (nvme). Bei GPU unterstützen nur bestimmte Geräte die diskrete Geräte Zuweisung. Informationen zur Überprüfung finden Sie in der Hardware Dokumentation, oder wenden Sie sich an den Hardwarehersteller Ausführliche Informationen zu diesem Feature, einschließlich der Verwendungsweise und Überlegungen, finden Sie im Beitrag "[diskrete Geräte Zuweisung--Beschreibung und Hintergrund](#)" im virtualisierungsblog.

Abgeschirmte VMs

Diese virtuellen Computer basieren auf virtualisierungsbasierter Sicherheit und sind ab Windows Server 2016 verfügbar.

Die **Host** Anforderungen lauten:

- UEFI 2.3.1 c: unterstützt sicheren, gemessenen Start

Die folgenden beiden sind optional für die virtualisierungsbasierte Sicherheit im Allgemeinen, aber für den Host erforderlich, wenn Sie den Schutz der Features gewährleisten möchten:

- TPM v 2.0: schützt Platt Form sicherheitsassets
- IOMMU (Intel VT-D): der Hypervisor kann somit den Zugriff auf den direkten Speicher (DMA) bereitstellen.

Anforderungen an **virtuelle Computer** :

- Zweite Generation
- Windows Server 2012 oder höher als Gast Betriebssystem

Unterstützte Windows-Gast Betriebssysteme für Hyper-V unter Windows Server

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows Server 2019

Hyper-V unterstützt mehrere Versionen von Windows Server-, Windows- und Linux-Distributionen, die auf virtuellen Computern ausgeführt werden, als Gast Betriebssysteme. In diesem Artikel werden die unterstützten Windows Server- und Windows-Gast Betriebssysteme behandelt. Informationen zu Linux- und FreeBSD-Distributionen finden Sie [unter Unterstützte virtuelle Linux- und FreeBSD-Computer für Hyper-V unter Windows](#).

Für einige Betriebssysteme ist Integration Services integriert. Andere erfordern, dass Sie Integrationsdienste in einem separaten Schritt installieren oder aktualisieren, nachdem Sie das Betriebssystem auf dem virtuellen Computer eingerichtet haben. Weitere Informationen finden Sie in den Abschnitten unten und [Integration Services](#).

Unterstützte Gastbetriebssysteme für Windows Server

Im folgenden finden Sie die Versionen von Windows Server, die als Gast Betriebssysteme für Hyper-V in Windows Server 2016 und Windows Server 2019 unterstützt werden.

GASTBETRIEBSSYSTEM (SERVER)	MAXIMALE ANZAHL VIRTUELLER PROZESSOREN	INTEGRATIONSDIENSTE	HINWEISE
Windows Server, Version 1909	240 für Generation 2; 64 für Generation 1	Integrierte	Für die Unterstützung von mehr als 240 virtuellen Prozessoren sind Windows Server-, Version 1903- und spätere Gast Betriebssysteme erforderlich.
Windows Server, Version 1903	240 für Generation 2; 64 für Generation 1	Integrierte	
Windows Server, Version 1809	240 für Generation 2; 64 für Generation 1	Integrierte	
Windows Server 2019	240 für Generation 2; 64 für Generation 1	Integrierte	
Windows Server, Version 1803	240 für Generation 2; 64 für Generation 1	Integrierte	
Windows Server 2016	240 für Generation 2; 64 für Generation 1	Integrierte	
Windows Server 2012 R2	64	Integrierte	
Windows Server 2012	64	Integrierte	

GASTBETRIEBSSYSTEM (SERVER)	MAXIMALE ANZAHL VIRTUELLER PROZESSOREN	INTEGRATIONSDIENSTE	HINWEISE
Windows Server 2008 R2 mit Service Pack 1 (SP 1)	64	Installieren Sie alle wichtigen Windows-Updates nach dem Einrichten des Gast Betriebssystems.	Datacenter, Enterprise, Standard und Web Edition.
Windows Server 2008 mit Service Pack 2 (SP2)	8	Installieren Sie alle wichtigen Windows-Updates nach dem Einrichten des Gast Betriebssystems.	Datacenter, Enterprise, Standard und Web Edition (32-Bit und 64-Bit).

Unterstützte Windows Client-Gast Betriebssysteme

Im folgenden finden Sie die Versionen des Windows-Clients, die als Gast Betriebssysteme für Hyper-V in Windows Server 2016 und Windows Server 2019 unterstützt werden.

GASTBETRIEBSSYSTEM (CLIENT)	MAXIMALE ANZAHL VIRTUELLER PROZESSOREN	INTEGRATIONSDIENSTE	HINWEISE
Windows 10	32	Integrierte	
Windows 8.1	32	Integrierte	
Windows 7 mit Service Pack 1 (SP 1)	4	Aktualisieren Sie die Integrationsdienste, nachdem Sie das Gast Betriebssystem eingerichtet haben.	Ultimate, Enterprise und Professional Edition (32-Bit und 64-Bit).

Unterstützung von Gastbetriebssystemen in anderen Versionen von Windows

Die folgende Tabelle enthält Links zu Informationen zu Gastbetriebssystemen, die für Hyper-V unter anderen Windows-Versionen unterstützt werden.

HOSTBETRIEBSSYSTEM	THEMA
Windows 10	Unterstützte Gast Betriebssysteme für Hyper-V-Client in Windows 10
Windows Server 2012 R2 und Windows 8.1	<ul style="list-style-type: none"> - unterstützte Windows-Gast Betriebssysteme für Hyper-V in Windows Server 2012 R2 und Windows 8.1 - Linux-und FreeBSD-Virtual Machines auf Hyper-V
Windows Server 2012 und Windows 8	Unterstützte Windows-Gast Betriebssysteme für Hyper-V in Windows Server 2012 und Windows 8
Windows Server 2008 und Windows Server 2008 R2	Informationen zu Virtual Machines und Gastbetriebssystemen

So bietet Microsoft Unterstützung für Gast Betriebssysteme

Microsoft bietet auf folgende Weise Unterstützung für Gastbetriebssysteme:

- Der Microsoft-Support hilft beim Lösen von Problemen in Microsoft-Betriebssystemen und -Integrationsdiensten.
- Für Probleme in anderen Betriebssystemen, die vom Anbieter des Betriebssystems für die Ausführung unter Hyper-V zertifiziert wurden, wird der Support vom Anbieter geleistet.
- Andere in den Betriebssystemen ermittelte Probleme werden von Microsoft an die Supportcommunity mehrerer Anbieter weitergeleitet, [TSANet](#).

Siehe auch

- [Virtuelle Linux- und FreeBSD Computer unter Hyper-V](#)
- [Unterstützte Gast Betriebssysteme für Hyper-V-Client in Windows 10](#)

Unterstützte virtuelle Linux-und FreeBSD-Computer für Hyper-V unter Windows

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows Server 2012, Hyper-v Server 2012, Windows Server 2008 R2, Windows 10, Windows 8.1, Windows 8, Windows 7,1, Windows 7

Hyper-V unterstützt sowohl emulierten als auch Hyper-v-spezifische Geräte für virtuelle Linux-und FreeBSD-Maschinen. Bei der Ausführung mit emulierten Geräten muss keine zusätzliche Software installiert werden. Emulierten Geräte bieten jedoch keine hohe Leistung und können nicht die umfassende Verwaltungsinfrastruktur für virtuelle Computer nutzen, die die Hyper-V-Technologie bietet. Um alle von Hyper-v bereitgestellten Vorteile vollständig nutzen zu können, ist es am besten, Hyper-v-spezifische Geräte für Linux und FreeBSD zu verwenden. Die Sammlung der Treiber, die zum Ausführen von Hyper-V-spezifischen Geräten erforderlich sind, wird als Linux-Integration Services (LIS) oder FreeBSD Integration Services (bis) bezeichnet.

LIS wurde zum Linux-Kernel hinzugefügt und wird für neue Releases aktualisiert. Linux-Distributionen, die auf älteren Kernel basieren, haben jedoch möglicherweise nicht die neuesten Verbesserungen oder Korrekturen. Microsoft stellt einen Download bereit, der installierbare LIS-Treiber für einige Linux-Installationen auf der Grundlage dieser älteren Kernel enthält. Da Verteilungs Anbieter Versionen von Linux-Integration Services enthalten, empfiehlt es sich, ggf. die neueste herunterladbare Version von Lis für Ihre Installation zu installieren.

Bei anderen Linux-Distributionen werden die Änderungen regelmäßig in den Kernel und die Anwendungen des Betriebssystems integriert, sodass keine separaten Downloads oder Installationen erforderlich sind.

Für ältere FreeBSD-Releases (vor 10,0) stellt Microsoft Ports bereit, die installierbare-bis-Treiber und entsprechende Daemons für FreeBSD Virtual Machines enthalten. Für Neuere FreeBSD-Releases ist bis in das FreeBSD-Betriebssystem integriert, und es ist kein separater Download oder eine separate Installation erforderlich, mit Ausnahme eines herunterladbare KVP-Ports, der für FreeBSD 10,0 benötigt wird.

TIP

- Laden Sie [Windows Server 2019](#) aus dem Evaluation Center herunter.

Ziel dieses Inhalts sind die Bereitstellung von Informationen, die Ihnen helfen, Ihre Linux-oder FreeBSD-Bereitstellung auf Hyper-V zu vereinfachen. Zu den Details gehören:

- Linux-Distributionen oder FreeBSD-Releases, die den Download und die Installation von Lis-oder bis-Treibern erfordern.
- Linux-Distributionen oder FreeBSD-Releases, die integrierte LIS-oder bis-Treiber enthalten.
- Featureverteilungszuordnungen, die auf die Features in großen Linux-Distributionen oder FreeBSD-Releases hinweisen.
- Bekannte Probleme und Problem Umgehungen für jede Distribution oder Version.
- Funktionsbeschreibung für jede LIS-oder bis-Funktion.

Möchten Sie einen Vorschlag zu Features und Funktionen erstellen? Gibt es etwas, das wir besser machen können? Auf der [Windows Server User Voice](#) -Website können Sie neue Features und Funktionen für

Linux-und FreeBSD-Virtual Machines auf Hyper-V vorschlagen und sehen, was andere Personen sagen.

Inhalt dieses Abschnitts

- [Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V](#)
- [Unterstützte virtuelle Debian-Computer in Hyper-V](#)
- [Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V](#)
- [Unterstützte virtuelle SuSE-Computer auf Hyper-V](#)
- [Unterstützte virtuelle Ubuntu-Computer auf Hyper-V](#)
- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)
- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)
- [Bewährte Methoden für die Ausführung von FreeBSD unter Hyper-V](#)

Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V

09.04.2020 • 25 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Hyper-v Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows 10, Windows 8.1

Die folgenden featureverteilungszuordnungen zeigen die Funktionen an, die in integrierten und herunterladbaren Versionen von Linux-Integration Services vorhanden sind. Die bekannten Probleme und Problem Umgehungen für die einzelnen Verteilungen werden nach den Tabellen aufgelistet.

Die integrierten Red Hat Enterprise Linux Integration Services Treiber für Hyper-v (verfügbar seit Red Hat Enterprise Linux 6,4) sind für Red Hat Enterprise Linux Gäste ausreichend, damit Sie mit den hochleistungsfähigen synthetischen Geräten auf Hyper-v-Hosts ausgeführt werden können. Diese integrierten Treiber werden für diese Verwendung von Red hat zertifiziert. Zertifizierte Konfigurationen können auf der red hat-Webseite angezeigt werden: [red hat Certification Catalog](#). Es ist nicht erforderlich, Linux-Integration Services Pakete aus dem Microsoft Download Center herunterzuladen und zu installieren. Dadurch kann der red hat-Support eingeschränkt werden, wie in red hat Knowledge dgebase-Artikel 1067: [red hat Knowledge dgebase 1067](#) beschrieben.

Da bei der Aktualisierung des Kernels mögliche Konflikte zwischen der integrierten LIS-Unterstützung und der herunterladbaren LIS-Unterstützung auftreten, deaktivieren Sie automatische Updates, deinstallieren Sie die von Lis herunterladbaren Pakete, aktualisieren Sie den Kernel, starten Sie, und installieren Sie dann die neueste Version von Lis und starten Sie erneut.

NOTE

Offizielle Red Hat Enterprise Linux Zertifizierungs Informationen sind im [red hat-Kunden Portal](#) verfügbar.

In diesem Abschnitt:

- [RHEL/CentOS 8. x-Serie](#)
- [RHEL/CentOS 7. x-Serie](#)
- [RHEL/CentOS 6. x-Reihe](#)
- [RHEL/CentOS 5. x-Reihe](#)
- [Hinweise](#)

Tabellen Legende

- **Integrierte** -LIS sind als Teil dieser Linux-Distribution enthalten. Die Kernel-Modul Versionsnummern für die integrierten Lis (z. b. **lsmod**) unterscheiden sich von der Versionsnummer des von Microsoft bereitgestellten LIS-Download Pakets. Ein Konflikt weist nicht darauf hin, dass der integrierte LIS veraltet ist.
- ✓ -Feature verfügbar
- (*leer*): Feature nicht verfügbar

RHEL/CentOS 8. x-Serie

FEATURE	WINDOWS SERVER-VERSION	8,1	8,0
Verfügbarkeit			
Core	2019, 2016, 2012 R2	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓	✓
Ungs			
Großrahmen	2019, 2016, 2012 R2	✓	✓
VLAN-Tagging und-Abschneiden	2019, 2016, 2012 R2	✓	✓
Livemigration	2019, 2016, 2012 R2	✓	✓
Statische IP-Injektion	2019, 2016, 2012 R2	✓ Hinweis 2	✓ Hinweis 2
vRSS	2019, 2016, 2012 R2	✓	✓
TCP-Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓	✓
SR-IOV	2019, 2016	✓	✓
Speicher			
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓	✓
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓ Hinweis 3	✓ Hinweis 3
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Hinweis 5	✓ Hinweis 5
Trim-Unterstützung	2019, 2016, 2012 R2	✓	✓
SCSI-WWN	2019, 2016, 2012 R2	✓	✓
Gedenkens			
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	N/V	N/V
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2	✓ Notiz 8, 9, 10	✓ Notiz 8, 9, 10
Dynamischer Arbeitsspeicher-Ballooning	2019, 2016, 2012 R2	✓ Notiz 8, 9, 10	✓ Notiz 8, 9, 10

[illegible]

FEATU RE	WINDO WS SERVER - VERSIO N	7.5-7.8	7.3-7.4	7.0-7.2	7.5-7.8	7,4	7,3	7,2	7,1	7,0
Dynam ischer Arbeits speiche r- Balloon ing	2019, 2016, 2012 R2	✓ Noti z 8, 9, 10	✓ Noti z 8, 9, 10	✓ Noti z 8, 9, 10	✓ Hin weis 9, 10	✓ Hin weis 9, 10	✓ Hin weis 9, 10	✓ Hin weis 9, 10	✓ Hin weis 9, 10	✓ Noti z 8, 9, 10
Größen änderu ng des Lauf Zeit Speiche rs	2019, 2016	✓	✓	✓						
Video										
Hyper- V- spezifis ches Videog erät	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Versch iedens ten										
Schlüss el- Wert- Paar	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Nicht mastba re Unterb rechun g	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dateik opie von Host zu Gast	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓	✓	
Isymbu s- Befehl	2019, 2016, 2012 R2	✓	✓	✓						

FEATU RE	WINDO WS SERVER - VERSIO N	7.5-7.8	7.3-7.4	7.0-7.2	7.5-7.8	7,4	7,3	7,2	7,1	7,0
Hyper- V- Sockets	2019, 2016	✓	✓	✓						
PCI- Passth rough/ DDA	2019, 2016	✓	✓		✓	✓	✓			
Virtue lle Masch inen der Gener ation 2										
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14	✓ Hin weis 14
Sichere r Start	2019, 2016	✓	✓	✓	✓	✓	✓	✓	✓	✓

RHEL/CentOS 6. x-Reihe

Der 32-Bit-Kernel für diese Reihe ist "PE" aktiviert. Es gibt keine integrierte LIS-Unterstützung für RHEL/CentOS 6.0-6.3.

FEATURE	WINDOW S SERVER- VERSION	6.7-6.10	6.4-6.6	6.0-6.3	6,10, 6,9, 6,8	6,6, 6,7	6,5	6,4
Verfügb arkeit		LIS 4,3	LIS 4,3	LIS 4,3	Integriert	Integriert	Integriert	Integriert
Core	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016							
Ungs								

FEATURE	WINDOW S SERVER- VERSION	6.7-6.10	6.4-6.6	6.0-6.3	6,10, 6,9, 6,8	6,6, 6,7	6,5	6,4
Großbrah men	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
VLAN- Tagging und- Abschnei den	2019, 2016, 2012 R2	✓Hinwei s 1	✓Hinwei s 1	✓Hinwei s 1	✓Hinwei s 1	✓Hinwei s 1	✓Hinwei s 1	✓Hinwei s 1
Livemigra tion	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Statische IP- Injektion	2019, 2016, 2012 R2	✓Hinwei s 2	✓Hinwei s 2	✓Hinwei s 2	✓Hinwei s 2	✓Hinwei s 2	✓Hinwei s 2	✓Hinwei s 2
vRSS	2019, 2016, 2012 R2	✓	✓	✓	✓	✓		
TCP- Segmenti erung und Prüfsum men Offloads	2019, 2016, 2012 R2	✓	✓	✓	✓	✓		
SR-IOV	2019, 2016							
Speicher								
Vhdx- Größe ändern	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓Hinwei s 3	✓Hinwei s 3	✓Hinwei s 3	✓Hinwei s 3	✓Hinwei s 3	✓Hinwei s 3	
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓Hinwei s 5	✓Hinwei s 5	✓Hinwei s 5	✓Hinwei s 4, 5	✓Hinwei s 4, 5	✓Hinwei s 4, 5, 6	✓Hinwei s 4, 5, 6
Trim- Unterstüt zung	2019, 2016, 2012 R2	✓	✓	✓	✓			
SCSI- WWN	2019, 2016, 2012 R2	✓	✓	✓				

FEATURE	WINDOW S SERVER- VERSION	6.7-6.10	6.4-6.6	6.0-6.3	6.10, 6.9, 6.8	6.6, 6.7	6,5	6,4
Gedenke ns								
Unterstüt zung für den unterstüt zten Kernel	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
MMIO- Lücke konfigurie ren	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Dynamisc her Arbeitssp eicher- Hot-Add	2019, 2016, 2012 R2	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 8, 9, 10	✓Hinwei s 7, 8, 9, 10	
Dynamisc her Arbeitssp eicher- Balloonin g	2019, 2016, 2012 R2	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10	✓Hinwei s 7, 9, 10, 11
Größenän derung des Lauf Zeit Speichers	2019, 2016							
Video								
Hyper-V- spezifisch es Videogerä t	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	
Verschie densten								
Schlüssel- Wert-Paar	2019, 2016, 2012 R2	✓	✓	✓	✓Hinwei s 12	✓Hinwei s 12	✓Hinwei s 12, 13	✓Hinwei s 12, 13
Nicht mastbare Unterbrec hung	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓

FEATURE	WINDOW S SERVER- VERSION	6.7-6.10	6.4-6.6	6.0-6.3	6,10, 6,9, 6,8	6,6, 6,7	6,5	6,4
Dateikopi e von Host zu Gast	2019, 2016, 2012 R2	✓	✓	✓	✓	✓		
Isvmbus- Befehl	2019, 2016, 2012 R2	✓	✓	✓				
Hyper-V- Sockets	2019, 2016	✓	✓	✓				
PCI- Passthrou gh/DDA	2019, 2016	✓						
Virtuelle Maschin en der Generati on 2								
Starten mithilfe von UEFI	2012 R2							
	2019, 2016	✓ Hinweis s 14	✓ Hinweis s 14	✓ Hinweis s 14	✓ Hinweis s 14			
Sicherer Start	2019, 2016							

RHEL/CentOS 5. x-Reihe

Für diese Reihe ist ein 32-Bit-PE-Kernel verfügbar. Vor 5,9 gibt es keine integrierte LIS-Unterstützung für RHEL/CentOS.

FEATURE	WINDOWS SERVER- VERSION	5,2-5,11	5.2-5.11	5,9-5,11
Verfügbarkeit		LIS 4,3	LIS 4,1	Integriert
Core	2019, 2016, 2012 R2	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016			
Ungs				
Großrahmen	2019, 2016, 2012 R2	✓	✓	✓

FEATURE	WINDOWS SERVER- VERSION	5,2-5,11	5.2-5.11	5,9-5,11
VLAN-Tagging und-Abschneiden	2019, 2016, 2012 R2	✓ Hinweis 1	✓ Hinweis 1	✓ Hinweis 1
Livemigration	2019, 2016, 2012 R2	✓	✓	✓
Statische IP-Injektion	2019, 2016, 2012 R2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2
vRSS	2019, 2016, 2012 R2			
TCP-Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓	✓	
SR-IOV	2019, 2016			
Speicher				
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓	✓	
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓ Hinweis 3	✓ Hinweis 3	
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Hinweis 5, 15	✓ Hinweis 5	✓ Hinweis 4, 5, 6
Trim-Unterstützung	2019, 2016, 2012 R2			
SCSI-WWN	2019, 2016, 2012 R2			
Gedenkens				
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	✓	✓	✓
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2			
Dynamischer Arbeitsspeicher-Ballooning	2019, 2016, 2012 R2	✓ Hinweis 7, 9, 10, 11	✓ Hinweis 7, 9, 10, 11	
Größenänderung des Lauf Zeit Speichers	2019, 2016			
Video				

FEATURE	WINDOWS SERVER- VERSION	5,2-5,11	5.2-5.11	5,9-5,11
Hyper-V-spezifisches Videogerät	2019, 2016, 2012 R2	✓	✓	
Verschiedensten				
Schlüssel-Wert-Paar	2019, 2016, 2012 R2	✓	✓	
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓	✓
Dateikopie von Host zu Gast	2019, 2016, 2012 R2	✓	✓	
Isvmbus-Befehl	2019, 2016, 2012 R2			
Hyper-V-Sockets	2019, 2016			
PCI-Passthrough/DDA	2019, 2016			
Virtuelle Maschinen der Generation 2				
Starten mithilfe von UEFI	2019, 2016, 2012 R2			
Sicherer Start	2019, 2016			

Hinweise

1. Für diese RHEL/CentOS-Version funktioniert das VLAN-Tagging, aber VLAN-abkürzen nicht.
2. Die statische IP-Injektion funktioniert möglicherweise nicht, wenn der Netzwerk-Manager für einen bestimmten synthetischen Netzwerkadapter auf dem virtuellen Computer konfiguriert wurde. Stellen Sie für eine reibungslose Verwendung statischer IP-Einschleusung sicher, dass entweder der Netzwerk-Manager entweder vollständig ausgeschaltet ist oder für einen bestimmten Netzwerkadapter über seine ifcfg-ethX-Datei ausgeschaltet wurde.
3. Stellen Sie unter Windows Server 2012 R2 bei der Verwendung von virtuellen Fibre Channel-Geräten sicher, dass die logische Gerätenummer 0 (LUN 0) aufgefüllt wurde. Wenn LUN 0 nicht aufgefüllt wurde, kann ein virtueller Linux-Computer möglicherweise keine systemeigenen Fibre Channel-Geräte einbinden.
4. Für integrierte LIS muss das "HyperV-Daemons"-Paket für diese Funktionalität installiert werden.
5. Wenn während eines Sicherungs Vorgangs für virtuelle Computer geöffnete Datei Handles vorhanden sind, müssen die gesicherten VHDs in einigen Fällen möglicherweise bei der Wiederherstellung eine Dateisystem Konsistenzprüfung (fsck) durchlaufen. Bei Live Sicherungs Vorgängen kann ein Fehler auftreten, wenn der virtuelle Computer über ein angefügtes iSCSI-Gerät oder einen direkt angeschlossenen Speicher (auch als Pass-Through-Datenträger bezeichnet) verfügt.
6. Während der heruntergeladen von Linux-Integration Services bevorzugt wird, ist die Unterstützung der Live Sicherung für RHEL/CentOS 5,9-5.11/6.4/6.5 auch über [Hyper-V Backup Essentials für Linux](#) verfügbar.

7. Die Unterstützung dynamischer Arbeitsspeicher ist nur auf virtuellen 64-Bit-Computern verfügbar.
8. Die Unterstützung von "Hot-Add" ist in dieser Verteilung standardmäßig nicht aktiviert. Um die Unterstützung für "Hot-Add" zu aktivieren, müssen Sie eine udev-Regel unter/etc/udev/rules.d/wie folgt hinzufügen:
 - a. Erstellen Sie eine Datei **/etc/udev/rules.d/100-Balloon.Rules**. Sie können einen beliebigen anderen gewünschten Namen für die Datei verwenden.
 - b. Fügen Sie der Datei den folgenden Inhalt hinzu:

```
SUBSYSTEM=="memory", ACTION=="add", ATTR{state}="online"
```

- c. Starten Sie das System neu.

Während das Herunterladen von Linux-Integration Services diese Regel bei der Installation erstellt, wird die Regel auch entfernt, wenn LIS deinstalliert wird. Daher muss die Regel neu erstellt werden, wenn dynamischer Arbeitsspeicher nach der Installation benötigt wird.

9. Dynamische Arbeitsspeicher Vorgänge können fehlschlagen, wenn für das Gast Betriebssystem zu wenig Arbeitsspeicher verfügbar ist. Im folgenden finden Sie einige bewährte Methoden:
 - Start Speicher und minimaler Arbeitsspeicher müssen größer oder gleich dem vom Verteilungs Anbieter empfohlenen Arbeitsspeicher sein.
 - Anwendungen, die in der Regel den gesamten verfügbaren Arbeitsspeicher auf einem System belegen, können bis zu 80 Prozent des verfügbaren Arbeitsspeichers verbrauchen.
10. Wenn Sie dynamischer Arbeitsspeicher auf einem Windows Server 2016-oder Windows Server 2012 R2-Betriebssystem verwenden, geben Sie den **Start Speicher**, den **minimalen Arbeitsspeicher** und den **maximalen Arbeitsspeicher** Parameter in Vielfachen von 128 Megabyte (MB) an. Wenn dies nicht der Fall ist, kann dies zu Fehlern beim Hinzufügen von Fehlern führen, und in einem Gast Betriebssystem wird möglicherweise keine Erhöhung des Arbeitsspeichers angezeigt.
11. Bestimmte Verteilungen, einschließlich derjenigen, die LIS 4,0 und 4,1 verwenden, bieten nur Unterstützung für die Bereitstellung und bieten keine Unterstützung für das heiße hinzufügen. In einem solchen Szenario kann die Funktion "dynamischer Arbeitsspeicher" verwendet werden, indem der Start Speicher Parameter auf einen Wert festgelegt wird, der gleich dem maximalen Arbeitsspeicher Parameter ist. Dies führt dazu, dass der gesamte erforderliche Arbeitsspeicher dem virtuellen Computer zum Startzeitpunkt hinzugefügt wird und später abhängig von den Arbeitsspeicher Anforderungen des Hosts, dass Hyper-V Arbeitsspeicher vom Gast mithilfe von hoch Skalierung frei zuweisen oder deren Zuweisung aufgehoben werden kann. Konfigurieren Sie den **Start Speicher** und den **minimalen Arbeitsspeicher** um bzw. über dem empfohlenen Wert für die Verteilung.
12. Um die KVP-Infrastruktur (Key/Value Pair) zu aktivieren, installieren Sie das Paket hypervkvpd oder HyperV-Daemons RPM von der RHEL-ISO-Datei. Alternativ kann das Paket direkt aus RHEL-Repository installiert werden.
13. Die KVP-Infrastruktur (Key/Value-Paar) funktioniert möglicherweise ohne Linux-Software Update nicht ordnungsgemäß. Wenden Sie sich an Ihren Verteilungs Hersteller, um das Software Update zu erhalten, falls Probleme mit diesem Feature auftreten.
14. Auf virtuellen Computern der Windows Server 2012 R2-Generation 2 ist der sichere Start standardmäßig aktiviert, und einige virtuelle Linux-Computer werden erst gestartet, wenn die Option für den sicheren Start deaktiviert ist. Sie können den sicheren Start im Abschnitt **Firmware** der Einstellungen für den virtuellen Computer im **Hyper-V-Manager** deaktivieren, oder Sie können ihn mithilfe von PowerShell deaktivieren:

```
Set-VMFirmware -VMName "VMname" -EnableSecureBoot Off
```

Der Download der Linux-Integration Services kann auf vorhandene VMS der Generation 2 angewendet werden, aber nicht die Funktion der Generation 2.

15. In Red Hat Enterprise Linux oder CentOS 5,2, 5,3 und 5,4 ist die Funktion zum Einfrieren des Dateisystems nicht verfügbar, daher ist die Sicherung virtueller Computer auch nicht verfügbar.

Weitere Informationen

- [Set-vmfirmware](#)
- [Unterstützte virtuelle Debian-Computer in Hyper-V](#)
- [Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V](#)
- [Unterstützte virtuelle SuSE-Computer auf Hyper-V](#)
- [Unterstützte virtuelle Ubuntu-Computer auf Hyper-V](#)
- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)
- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)
- [Red hat-Hardware Zertifizierung](#)

Unterstützte virtuelle Debian-Computer auf Hyper-V

10.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Hyper-v Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows 10, Windows 8.1

Die folgende featureverteilungskarte gibt die Funktionen an, die in den einzelnen Versionen vorhanden sind. Die bekannten Probleme und Problem Umgehungen für die einzelnen Verteilungen werden nach der Tabelle aufgelistet.

Tabellen Legende

- **Integrierte** -LIS sind als Teil dieser Linux-Distribution enthalten. Das von Microsoft bereitgestellte LIS-Downloadpaket funktioniert für diese Verteilung nicht. Installieren Sie es also nicht. Die Kernel-Modul Versionsnummern für die integrierten Lis (z. b. **lsmod**) unterscheiden sich von der Versionsnummer des von Microsoft bereitgestellten LIS-Download Pakets. Ein Konflikt weist nicht darauf hin, dass der integrierte LIS veraltet ist.
- ✓ -Feature verfügbar
- (/eer): Feature nicht verfügbar

FEATURE	WINDOWS SERVER- BETRIEBSSYSTEM VERSION	10.0-10.3 (BUSTER)	9.0-9.12 (STRETCH)	8.0-8.11 (JESSIE)	7.0-7.11 (WHEEZY)
Verfügbarkeit		Integriert	Integriert	Integriert	Integriert (Notiz 5)
Core	2019, 2016, 2012 R2	✓	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓ Hinweis 4	✓ Hinweis 4		
Ungs					
Großrahmen	2019, 2016, 2012 R2	✓	✓	✓	✓
VLAN-Tagging und-Abschneiden	2019, 2016, 2012 R2	✓	✓	✓	✓
Livemigration	2019, 2016, 2012 R2	✓	✓	✓	✓
Statische IP-Injektion	2019, 2016, 2012 R2				

FEATURE	WINDOWS SERVER- BETRIEBSSYSTEM VERSION	10.0-10.3 (BUSTER)	9.0-9.12 (STRETCH)	8.0-8.11 (JESSIE)	7.0-7.11 (WHEEZY)
vRSS	2019, 2016, 2012 R2	✓ Hinweis 4	✓ Hinweis 4		
TCP- Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓ Hinweis 4	✓ Hinweis 4		
SR-IOV	2019, 2016	✓ Hinweis 4	✓ Hinweis 4		
Speicher					
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓ Hinweis 1	✓ Hinweis 1	✓ Hinweis 1	✓ Hinweis 1
Virtueller Fibre Channel	2019, 2016, 2012 R2				
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Note2	✓ Note2	✓ Note2	✓ Note2
Trim- Unterstützung	2019, 2016, 2012 R2	✓ Hinweis 4	✓ Hinweis 4		
SCSI-WWN	2019, 2016, 2012 R2	✓ Hinweis 4	✓ Hinweis 4		
Gedenkens					
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	✓	✓	✓	✓
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓	✓	✓
Dynamischer Arbeitsspeicher- Hot-Add	2019, 2016, 2012 R2	✓ Hinweis 4	✓ Hinweis 4		
Dynamischer Arbeitsspeicher- Ballooning	2019, 2016, 2012 R2	✓ Hinweis 4	✓ Hinweis 4		
Größenänderung des Lauf Zeit Speichers	2019, 2016	✓ Hinweis 4	✓ Hinweis 4		
Video					

FEATURE	WINDOWS SERVER- BETRIEBSSYSTEM VERSION	10.0-10.3 (BUSTER)	9.0-9.12 (STRETCH)	8.0-8.11 (JESSIE)	7.0-7.11 (WHEEZY)
Hyper-V- spezifisches Videogerät	2019, 2016, 2012 R2	✓	✓	✓	
Verschiedenste n					
Schlüssel-Wert- Paar	2019, 2016, 2012 R2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2	
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓	✓	
Dateikopie von Host zu Gast	2019, 2016, 2012 R2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2	
Isvmbus-Befehl	2019, 2016, 2012 R2				
Hyper-V-Sockets	2019, 2016	✓ Hinweis 4	✓ Hinweis 4		
PCI- Passthrough/DD A	2019, 2016	✓ Hinweis 4	✓ Hinweis 4		
Virtuelle Maschinen der Generation 2					
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hinweis 3	✓ Hinweis 3	✓ Hinweis 3	
Sicherer Start	2019, 2016	✓			

Hinweise

1. Das Erstellen von Dateisystemen auf VHDs, die größer als 2 TB sind, wird nicht unterstützt.
2. Ab Debian 8,3 enthält das manuell installierte Debian-Paket "HyperV-Daemons" die Schlüssel-Wert-Paare, fCopy und VSS-Daemons. Unter Debian 7. x und 8.0-8.2 muss das HyperV-Daemons-Paket von den [debian-backports](#) stammen.
3. Auf virtuellen Computern der Windows Server 2012 R2-Generation 2 ist der sichere Start standardmäßig aktiviert, und einige virtuelle Linux-Computer werden erst gestartet, wenn die Option für den sicheren Start deaktiviert ist. Sie können den sicheren Start im Abschnitt **Firmware** der Einstellungen für den virtuellen Computer im **Hyper-V-Manager** deaktivieren, oder Sie können ihn mithilfe von PowerShell deaktivieren:

```
Set-VMFirmware -VMName "VMname" -EnableSecureBoot Off
```

4. Die neuesten upstreamkernel-Funktionen sind nur verfügbar, wenn der mit dem Kernel enthaltene [debian-backports](#) verwendet wird.

5. Während Debian 7. x nicht unterstützt wird und einen älteren Kernel verwendet, hat der Kernel, der in den Debian-backports für Debian 7. x enthalten ist, die Hyper-V-Funktionen verbessert.

Siehe auch

- [Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V](#)
- [Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V](#)
- [Unterstützte virtuelle SuSE-Computer auf Hyper-V](#)
- [Unterstützte virtuelle Ubuntu-Computer auf Hyper-V](#)
- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)
- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)

Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V

11.06.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows 10, Windows 8.1

Die folgende featureverteilungskarte gibt die Funktionen an, die in den einzelnen Versionen vorhanden sind. Die bekannten Probleme und Problem Umgehungen für die einzelnen Verteilungen werden nach der Tabelle aufgelistet.

Inhalt dieses Abschnitts:

- [Oracle Linux 8. x-Serie](#)
- [Oracle Linux 7. x-Serie](#)
- [Oracle Linux 6. x-Reihe](#)

Tabellen Legende

- **Integrierte** -LIS sind als Teil dieser Linux-Distribution enthalten. Die Kernel-Modul Versionsnummern für die integrierten Lis (z. **b. Ismod**) unterscheiden sich von der Versionsnummer des von Microsoft bereitgestellten LIS-Download Pakets. Ein Konflikt weist nicht darauf hin, dass der integrierte LIS veraltet ist.
- **✓** -Feature verfügbar
- **(/eer)**: Feature nicht verfügbar
- **Rhck** -red hat-Kompilierbarer Kernel
- **UEK** -Unbreakable Enterprise Kernel (UEK)
 - UEK4 basiert auf einer Linux-Upstream-Version 4.1.12
 - UEK5 basiert auf der Linux-Upstream-Version 4,14
 - UEK6 basiert auf der Linux-Upstream-Version 5,4

Oracle Linux 8. x-Serie

FEATURE	WINDOWS SERVER-VERSION	8.0-8.1 (RHCK)
Verfügbarkeit		
Kernspeicher	2019, 2016, 2012 R2	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓
Netzwerk		
Großrahmen	2019, 2016, 2012 R2	✓
VLAN-Tagging und-Abschneiden	2019, 2016, 2012 R2	✓

FEATURE	WINDOWS SERVER-VERSION	8.0-8.1 (RHCK)
Livemigration	2019, 2016, 2012 R2	✓
Statische IP-Injektion	2019, 2016, 2012 R2	✓ Hinweis 2
vRSS	2019, 2016, 2012 R2	✓
TCP-Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓
SR-IOV	2019, 2016	✓
Storage		
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓ Hinweis 3
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Hinweis 5
Trim-Unterstützung	2019, 2016, 2012 R2	✓
SCSI-WWN	2019, 2016, 2012 R2	✓
Arbeitsspeicher		
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	–
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2	✓ Hinweis 7, 8, 9
Dynamischer Arbeitsspeicher-Ballooning	2019, 2016, 2012 R2	✓ Hinweis 7, 8, 9
Größenänderung des Lauf Zeit Speichers	2019, 2016	✓
Video		
Hyper-V-spezifisches Videogerät	2019, 2016, 2012 R2	✓
Verschiedenes		
Schlüssel-Wert-Paar	2019, 2016, 2012 R2	✓
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓
Dateikopie von Host zu Gast	2019, 2016, 2012 R2	✓
Isvmbus-Befehl	2019, 2016, 2012 R2	✓

FEATURE	WINDOWS SERVER-VERSION	8.0-8.1 (RHCK)
Hyper-V-Sockets	2019, 2016	✓
PCI-Passthrough/DDA	2019, 2016	✓
Virtuelle Computer der Generation 2		
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hinweis 12
Sicherer Start	2019, 2016	✓

Oracle Linux 7. x-Serie

Diese Reihe hat nur 64-Bit-Kernel.

Funktion	Windows Server-Version	7.5-7.8			7.3-7.4		
		RHCK		UEK 5	RHCK		UEK 4
Verfügbarkeit		LIS 4,3	Integrität	Integrität	LIS 4,3	Integrität	Integrität
Kernspeicher	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓			✓		
Netzwerk							
Großrahmen	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
VLAN-Tagging und-Abschneiden	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Livemigration	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Statische IP-Injektion	2019, 2016, 2012 R2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2

vRSS	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
TCP-Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
SR-IOV	2019, 2016	✓	✓	✓	✓	✓	✓
Storage							
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓ Hinweis 3	✓ Hinweis 3	✓ Hinweis 3	✓ Hinweis 3	✓ Hinweis 3	✓ Hinweis 3
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Hinweis 5	✓ Hinweis 4, 5	✓ Hinweis 5	✓ Hinweis 5	✓ Hinweis 4, 5	✓ Hinweis 5
Trim-Unterstützung	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
SCSI-WWN	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	
Arbeitsspeicher							
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	–	–	–	–	–	–
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Dynamischer Arbeitsspeicher Hot-Add	2019, 2016, 2012 R2	✓ Hinweis 7, 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9

Dynamischer Arbeitsspeicher	2019, 2016, 2012 R2	✓ Hinweis 7, 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9	✓ Hinweis 8, 9
Größenänderung des Laufzeit Speichers	2019, 2016	✓		✓	✓		
Video							
Hyper-V-spezifisches Video	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Verschiedenes							
Schlüssel-Wert-Paar	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Dateikopie von Host zu Gast	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓
Isvmbus-Befehl	2019, 2016, 2012 R2	✓		✓	✓		✓
Hyper-V-Sockets	2019, 2016	✓		✓	✓		✓
PCI-Passthrough/DDA	2019, 2016	✓	✓	✓	✓	✓	✓
Virtuelle Computer der Generation 2							
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hinweis 12	✓ Hinweis 12	✓ Hinweis 12	✓ Hinweis 12	✓ Hinweis 12	✓ Hinweis 12
Sicherer Start	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓

Oracle Linux 6. x-Reihe

Diese Reihe hat nur 64-Bit-Kernel.

FEATURE	WINDOWS SERVER-VERSION	6.8-6.10 (RHCK)	6.8-6.10 (UEK4)
Verfügbarkeit		LIS 4,3	Integriert
Kernspeicher	2019, 2016, 2012 R2	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016		
Netzwerk			
Großrahmen	2019, 2016, 2012 R2	✓	✓
VLAN-Tagging und-Abschneiden	2019, 2016, 2012 R2	✓ Hinweis 1	✓ Hinweis 1
Livemigration	2019, 2016, 2012 R2	✓	✓
Statische IP-Injektion	2019, 2016, 2012 R2	✓ Hinweis 2	✓
vRSS	2019, 2016, 2012 R2	✓	✓
TCP-Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓	✓
SR-IOV	2019, 2016		
Storage			
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓	✓
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓ Hinweis 3	✓ Hinweis 3
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Hinweis 5	✓ Hinweis 5
Trim-Unterstützung	2019, 2016, 2012 R2	✓	✓
SCSI-WWN	2019, 2016, 2012 R2	✓	✓
Arbeitsspeicher			
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	–	–
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2	✓ Hinweis 6, 8, 9	✓ Hinweis 6, 8, 9

FEATURE	WINDOWS SERVER-VERSION	6.8-6.10 (RHCK)	6.8-6.10 (UEK4)
Dynamischer Arbeitsspeicher-Ballooning	2019, 2016, 2012 R2	✓ Hinweis 6, 8, 9	✓ Hinweis 6, 8, 9
Größenänderung des Laufzeit Speichers	2019, 2016		
Video			
Hyper-V-spezifisches Videogerät	2019, 2016, 2012 R2	✓	✓
Verschiedenes			
Schlüssel-Wert-Paar	2019, 2016, 2012 R2	✓ Notiz 10, 11	✓ Notiz 10, 11
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓
Dateikopie von Host zu Gast	2019, 2016, 2012 R2	✓	✓
Isvmbus-Befehl	2019, 2016, 2012 R2	✓	✓
Hyper-V-Sockets	2019, 2016	✓	✓
PCI-Passthrough/DDA	2019, 2016	✓	✓
Virtuelle Computer der Generation 2			
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hinweis 12	✓ Hinweis 12
Sicherer Start	2019, 2016		

Hinweise

1. Für diese Oracle Linux Version funktioniert das VLAN-Tagging, aber VLAN-abkürzen nicht.
2. Die statische IP-Injektion funktioniert möglicherweise nicht, wenn der Netzwerk-Manager für einen bestimmten synthetischen Netzwerkadapter auf dem virtuellen Computer konfiguriert wurde. Stellen Sie für eine reibungslose Verwendung statischer IP-Einschleusung sicher, dass entweder der Netzwerk-Manager entweder vollständig ausgeschaltet ist oder für einen bestimmten Netzwerkadapter über seine ifcfg-ethX-Datei ausgeschaltet wurde.
3. Stellen Sie unter Windows Server 2012 R2 bei der Verwendung von virtuellen Fibre Channel-Geräten sicher, dass die logische Gerätenummer 0 (LUN 0) aufgefüllt wurde. Wenn LUN 0 nicht aufgefüllt wurde, kann ein virtueller Linux-Computer möglicherweise keine systemeigenen Fibre Channel-Geräte einbinden.
4. Für integrierte LIS muss das "HyperV-Daemons"-Paket für diese Funktionalität installiert werden.
5. Wenn während eines Sicherungs Vorgangs für virtuelle Computer geöffnete Datei Handles vorhanden sind, müssen die gesicherten VHDs in einigen Fällen möglicherweise bei der Wiederherstellung eine Dateisystem Konsistenzprüfung (fsck) durchlaufen. Bei Live Sicherungs Vorgängen kann ein Fehler auftreten, wenn der virtuelle Computer über ein angefügtes iSCSI-Gerät oder einen direkt angeschlossenen

Speicher (auch als Pass-Through-Datenträger bezeichnet) verfügt.

6. Die Unterstützung dynamischer Arbeitsspeicher ist nur auf virtuellen 64-Bit-Computern verfügbar.
7. Die Unterstützung von "Hot-Add" ist in dieser Verteilung standardmäßig nicht aktiviert. Um die Unterstützung für "Hot-Add" zu aktivieren, müssen Sie eine udev-Regel unter/etc/udev/rules.d/wie folgt hinzufügen:
 - a. Erstellen Sie eine Datei **/etc/udev/rules.d/100-Balloon.Rules**. Sie können einen beliebigen anderen gewünschten Namen für die Datei verwenden.
 - b. Fügen Sie der Datei den folgenden Inhalt hinzu:

```
SUBSYSTEM=="memory", ACTION=="add", ATTR{state}="online"
```

- c. Starten Sie das System neu.

Während das Herunterladen von Linux-Integration Services diese Regel bei der Installation erstellt, wird die Regel auch entfernt, wenn LIS deinstalliert wird. Daher muss die Regel neu erstellt werden, wenn dynamischer Arbeitsspeicher nach der Installation benötigt wird.

8. Dynamische Arbeitsspeicher Vorgänge können fehlschlagen, wenn für das Gast Betriebssystem zu wenig Arbeitsspeicher verfügbar ist. Im folgenden finden Sie einige bewährte Methoden:
 - Start Speicher und minimaler Arbeitsspeicher müssen größer oder gleich dem vom Verteilungs Anbieter empfohlenen Arbeitsspeicher sein.
 - Anwendungen, die in der Regel den gesamten verfügbaren Arbeitsspeicher auf einem System belegen, können bis zu 80 Prozent des verfügbaren Arbeitsspeichers verbrauchen.
9. Wenn Sie dynamischer Arbeitsspeicher auf einem Windows Server 2016-oder Windows Server 2012 R2-Betriebssystem verwenden, geben Sie den **Start Speicher**, den **minimalen Arbeitsspeicher** und den **maximalen Arbeitsspeicher** Parameter in Vielfachen von 128 Megabyte (MB) an. Wenn dies nicht der Fall ist, kann dies zu Fehlern beim Hinzufügen von Fehlern führen, und in einem Gast Betriebssystem wird möglicherweise keine Erhöhung des Arbeitsspeichers angezeigt.
10. Um die KVP-Infrastruktur (Key/Value Pair) zu aktivieren, installieren Sie das Paket hypervkvpd oder HyperV-Daemons RPM von Ihrer Oracle Linux ISO-Datei. Alternativ kann das Paket direkt aus Oracle Linux yum-Repository installiert werden.
11. Die KVP-Infrastruktur (Key/Value-Paar) funktioniert möglicherweise ohne Linux-Software Update nicht ordnungsgemäß. Wenden Sie sich an Ihren Verteilungs Hersteller, um das Software Update zu erhalten, falls Probleme mit diesem Feature auftreten.
12. Auf virtuellen Computern der Windows Server 2012 R2-Generation 2 ist der sichere Start standardmäßig aktiviert, und einige virtuelle Linux-Computer werden erst gestartet, wenn die Option für den sicheren Start deaktiviert ist. Sie können den sicheren Start im Abschnitt **Firmware** der Einstellungen für den virtuellen Computer im **Hyper-V-Manager** deaktivieren, oder Sie können ihn mithilfe von PowerShell deaktivieren:

```
Set-VMFirmware -VMName "VMname" -EnableSecureBoot Off
```

Der Download der Linux-Integration Services kann auf vorhandene VMS der Generation 2 angewendet werden, aber nicht die Funktion der Generation 2.

Weitere Informationen

- [Set-vmfirmware](#)
- [Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V](#)

- [Unterstützte virtuelle Debian-Computer in Hyper-V](#)
- [Unterstützte virtuelle SuSE-Computer auf Hyper-V](#)
- [Unterstützte virtuelle Ubuntu-Computer auf Hyper-V](#)
- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)
- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)

Unterstützte virtuelle SuSE-Computer auf Hyper-V

10.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Hyper-v Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows 10, Windows 8.1

Im folgenden finden Sie eine featureverteilungskarte, die die Features in jeder Version angibt. Die bekannten Probleme und Problem Umgehungen für die einzelnen Verteilungen werden nach der Tabelle aufgelistet.

Die integrierten SUSE Linux Enterprise Service-Treiber für Hyper-V sind von SUSE zertifiziert. Ein Beispiel für eine Konfiguration kann in diesem Bulletin angezeigt werden: [SUSE Yes Certification Bulletin](#).

Tabellen Legende

- **Integrierte** -LIS sind als Teil dieser Linux-Distribution enthalten. Das von Microsoft bereitgestellte LIS-Downloadpaket funktioniert für diese Verteilung nicht. Installieren Sie es also nicht. Die Kernel-Modul Versionsnummern für die integrierten Lis (z. **b. Ismod**) unterscheiden sich von der Versionsnummer des von Microsoft bereitgestellten LIS-Download Pakets. Ein Konflikt weist nicht darauf hin, dass der integrierte LIS veraltet ist.
- ✓ -Feature verfügbar
- (*leer*): Feature nicht verfügbar

SLES12 + ist nur 64 Bit.

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	SLES 15 SP1	SLES 15	SLES 12 SP3-SP5	SLES 12 SP2	SLES 12 SP1	SLES 11 SP4	SLES 11 SP3
Verfügbarkeit		Integrierte	Integrierte	Integrierte	Integrierte	Integrierte	Integrierte	Integrierte
Core	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓	✓	✓	✓			
Ungs								
Großrah men	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	SLES 15 SP1	SLES 15	SLES 12 SP3-SP5	SLES 12 SP2	SLES 12 SP1	SLES 11 SP4	SLES 11 SP3
VLAN- Tagging und- Abschnei den	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Livemigra tion	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Statische IP- Injektion	2019, 2016, 2012 R2	✓ Hinweis s 1	✓ Hinweis s 1	✓ Hinweis s 1	✓ Hinweis s 1	✓ Hinweis s 1	✓ Hinweis s 1	✓ Hinweis s 1
vRSS	2019, 2016, 2012 R2	✓	✓	✓	✓	✓		
TCP- Segmenti erung und Prüfsum men Offloads	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	
SR-IOV	2019, 2016	✓	✓	✓	✓			
Speicher								
Vhdx- Größe ändern	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Notiz 2, 3, 8	✓ Notiz 2, 3, 8	✓ Notiz 2, 3, 8	✓ Notiz 2, 3, 8	✓ Notiz 2, 3, 8	✓ Notiz 2, 3, 8	✓ Notiz 2, 3, 8
Trim- Unterstüt zung	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	
SCSI- WWN	2019, 2016, 2012 R2	✓	✓	✓	✓			
Gedenke ns								

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	SLES 15 SP1	SLES 15	SLES 12 SP3-SP5	SLES 12 SP2	SLES 12 SP1	SLES 11 SP4	SLES 11 SP3
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	N/V	N/V	N/V	N/V	N/V	✓	✓
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 4, 5, 6	✓ Hinweis 4, 5, 6
Dynamischer Arbeitsspeicher-Ballooning	2019, 2016, 2012 R2	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 4, 5, 6	✓ Hinweis 4, 5, 6
Größenänderung des Laufzeit Speichers	2019, 2016	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6	✓ Hinweis 6			
Video								
Hyper-V-spezifisches Videogerät	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Verschiedensten								
Schlüssel-Wert-Paar	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓ Hinweis 7	✓ Hinweis 7
Nicht-mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	SLES 15 SP1	SLES 15	SLES 12 SP3-SP5	SLES 12 SP2	SLES 12 SP1	SLES 11 SP4	SLES 11 SP3
Dateikopi e von Host zu Gast	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	
Isvmbus- Befehl	2019, 2016, 2012 R2	✓	✓	✓	✓			
Hyper-V- Sockets	2019, 2016	✓	✓	✓				
PCI- Passthrou gh/DDA	2019, 2016	✓	✓	✓	✓	✓		
Virtuelle Maschin en der Generati on 2								
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hinweis s 9	✓ Hinweis s 9	✓ Hinweis s 9	✓ Hinweis s 9	✓ Hinweis s 9	✓ Hinweis s 9	
Sicherer Start	2019, 2016	✓	✓	✓	✓	✓		

Anmerkungen

1. Die statische IP-Injektion funktioniert möglicherweise nicht, wenn der **Netzwerk-Manager** für einen bestimmten, für Hyper-V spezifischen Netzwerkadapter auf dem virtuellen Computer konfiguriert wurde. Stellen Sie sicher, dass der Netzwerk-Manager vollständig ausgeschaltet ist oder für einen bestimmten Netzwerkadapter über seine **ifcfg-ethX**- Datei ausgeschaltet wurde, um eine reibungslose Funktionsweise der statischen IP-Injektion sicherzustellen.
2. Wenn während eines Sicherungs Vorgangs für virtuelle Computer geöffnete Datei Handles vorhanden sind, müssen die gesicherten VHDs in einigen Fällen möglicherweise bei der Wiederherstellung eine Dateisystem Konsistenzprüfung (fsck) durchlaufen.
3. Bei Live Sicherungs Vorgängen kann ein Fehler auftreten, wenn der virtuelle Computer über ein angefügtes iSCSI-Gerät oder einen direkt angeschlossenen Speicher (auch als Pass-Through-Datenträger bezeichnet) verfügt.
4. Dynamische Arbeitsspeicher Vorgänge können fehlschlagen, wenn für das Gast Betriebssystem zu wenig Arbeitsspeicher verfügbar ist. Im folgenden finden Sie einige bewährte Methoden:
 - Start Speicher und minimaler Arbeitsspeicher müssen größer oder gleich dem vom Verteilungs Anbieter empfohlenen Arbeitsspeicher sein.
 - Anwendungen, die in der Regel den gesamten verfügbaren Arbeitsspeicher auf einem System

belegen, können bis zu 80 Prozent des verfügbaren Arbeitsspeichers verbrauchen.

5. Die Unterstützung dynamischer Arbeitsspeicher ist nur auf virtuellen 64-Bit-Computern verfügbar.
6. Wenn Sie dynamischer Arbeitsspeicher unter den Betriebssystemen Windows Server 2016 oder Windows Server 2012 verwenden, geben Sie den **Start Speicher**, den **minimalen Arbeitsspeicher** und den **maximalen Arbeitsspeicher** Parameter in Vielfachen von 128 Megabyte (MB) an. Wenn dies nicht der Fall ist, kann dies zu Fehlern beim Hinzufügen von Fehlern führen, und in einem Gast Betriebssystem wird möglicherweise keine Erhöhung des Arbeitsspeichers angezeigt.
7. In Windows Server 2016 oder Windows Server 2012 R2 funktioniert die Schlüssel-Wert-Paar-Infrastruktur ohne Linux-Software Update möglicherweise nicht ordnungsgemäß. Wenden Sie sich an Ihren Verteilungs Hersteller, um das Software Update zu erhalten, falls Probleme mit diesem Feature auftreten.
8. Bei der VSS-Sicherung tritt ein Fehler auf, wenn eine einzelne Partition mehrmals bereitgestellt wird.
9. Auf virtuellen Computern der Generation 2 auf Windows Server 2012 R2 ist der sichere Start standardmäßig aktiviert. virtuelle Linux-Computer der Generation 2 werden nicht gestartet, es sei denn, die Option für den sicheren Start ist deaktiviert Sie können den sicheren Start im Abschnitt **Firmware** der Einstellungen für den virtuellen Computer im Hyper-V-Manager oder mithilfe der PowerShell deaktivieren:

```
Set-VMFirmware -VMName "VMname" -EnableSecureBoot Off
```

Siehe auch

- [Set-vmfirmware](#)
- [Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V](#)
- [Unterstützte virtuelle Debian-Computer in Hyper-V](#)
- [Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V](#)
- [Unterstützte virtuelle Ubuntu-Computer auf Hyper-V](#)
- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)
- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)

Unterstützte virtuelle Ubuntu-Computer auf Hyper-V

10.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Hyper-v Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows 10, Windows 8.1

Die folgende featureverteilungszuordnung gibt die Features in den einzelnen Versionen an. Die bekannten Probleme und Problem Umgehungen für die einzelnen Verteilungen werden nach der Tabelle aufgelistet.

Tabellen Legende

- **Integrierte** -LIS sind als Teil dieser Linux-Distribution enthalten. Das von Microsoft bereitgestellte LIS-Downloadpaket funktioniert für diese Verteilung nicht. Installieren Sie es also nicht. Die Kernel-Modul Versionsnummern für die integrierten Lis (z. b. **lsmod**) unterscheiden sich von der Versionsnummer des von Microsoft bereitgestellten LIS-Download Pakets. Ein Konflikt weist nicht darauf hin, dass der integrierte LIS veraltet ist.
- **✓**-Feature verfügbar
- *(leer)*: Feature nicht verfügbar

FEATURE	WINDOWS SERVER- BETRIEBSSYSTEM VERSION	19,10	18,04 LTS	16,04 LTS	14,04 LTS
Verfügbarkeit		Integrierte	Integrierte	Integrierte	Integrierte
Core	2019, 2016, 2012 R2	✓	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓	✓	✓	
Ungs					
Großrahmen	2019, 2016, 2012 R2	✓	✓	✓	✓
VLAN-Tagging und- Abschneiden	2019, 2016, 2012 R2	✓	✓	✓	✓
Livemigration	2019, 2016, 2012 R2	✓	✓	✓	✓
Statische IP- Injektion	2019, 2016, 2012 R2	✓ Hinweis 1	✓ Hinweis 1	✓ Hinweis 1	✓ Hinweis 1
vRSS	2019, 2016, 2012 R2	✓	✓	✓	✓

FEATURE	WINDOWS SERVER- BETRIEBSSYSTEM VERSION	19,10	18,04 LTS	16,04 LTS	14,04 LTS
TCP-Segmentierung und Prüfsummen Offloads	2019, 2016, 2012 R2	✓	✓	✓	✓
SR-IOV	2019, 2016	✓	✓	✓	
Speicher					
Vhdx-Größe ändern	2019, 2016, 2012 R2	✓	✓	✓	✓
Virtueller Fibre Channel	2019, 2016, 2012 R2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2	✓ Hinweis 2
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓ Hinweis 3, 4, 6	✓ Hinweis 3, 4, 5	✓ Hinweis 3, 4, 5	✓ Hinweis 3, 4, 5
Trim-Unterstützung	2019, 2016, 2012 R2	✓	✓	✓	✓
SCSI-WWN	2019, 2016, 2012 R2	✓	✓	✓	✓
Gedenkens					
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2	✓	✓	✓	✓
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓	✓	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2	✓ Hinweis 7, 8, 9	✓ Hinweis 7, 8, 9	✓ Hinweis 7, 8, 9	✓ Hinweis 7, 8, 9
Dynamischer Arbeitsspeicher-Ballooning	2019, 2016, 2012 R2	✓ Hinweis 7, 8, 9	✓ Hinweis 7, 8, 9	✓ Hinweis 7, 8, 9	✓ Hinweis 7, 8, 9
Größenänderung des Lauf Zeit Speichers	2019, 2016	✓	✓	✓	✓
Video					
Hyper-V-spezifisches Videogerät	2019, 2016, 2012 R2	✓	✓	✓	✓

FEATURE	WINDOWS SERVER- BETRIEBSSYSTEM VERSION	19,10	18,04 LTS	16,04 LTS	14,04 LTS
Verschiedenste n					
Schlüssel-Wert- Paar	2019, 2016, 2012 R2	✓ Hinweis 6, 10	✓ Hinweis 5, 10	✓ Hinweis 5, 10	✓ Hinweis 5, 10
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓	✓	✓
Dateikopie von Host zu Gast	2019, 2016, 2012 R2	✓	✓	✓	✓
Isvmbus-Befehl	2019, 2016, 2012 R2	✓	✓	✓	✓
Hyper-V-Sockets	2019, 2016				
PCI- Passthrough/DD A	2019, 2016	✓	✓	✓	✓
Virtuelle Maschinen der Generation 2					
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓ Hinweis 11, 12	✓ Hinweis 11, 12	✓ Hinweis 11, 12	✓ Hinweis 11, 12
Sicherer Start	2019, 2016	✓	✓	✓	✓

Hinweise

1. Die statische IP-Injektion funktioniert möglicherweise nicht, wenn der **Netzwerk-Manager** für einen bestimmten, für Hyper-V spezifischen Netzwerkadapter auf dem virtuellen Computer konfiguriert wurde. Stellen Sie sicher, dass der Netzwerk-Manager vollständig ausgeschaltet ist oder für einen bestimmten Netzwerkadapter über seine `ifcfg-ethX`-Datei ausgeschaltet wurde, um eine reibungslose Funktionsweise der statischen IP-Injektion sicherzustellen.
2. Stellen Sie bei der Verwendung von Virtual Fiber Channel-Geräten sicher, dass die logische Gerätenummer 0 (LUN 0) aufgefüllt wurde. Wenn LUN 0 nicht aufgefüllt wurde, kann ein virtueller Linux-Computer möglicherweise keine systemeigenen Fiber-Fibre Channel-Geräte einbinden.
3. Wenn während eines Sicherungs Vorgangs für virtuelle Computer geöffnete Datei Handles vorhanden sind, müssen die gesicherten VHDs in einigen Fällen möglicherweise bei der Wiederherstellung einer Dateisystem Konsistenzprüfung (`fsck`) unterzogen werden.
4. Bei Live Sicherungs Vorgängen kann ein Fehler auftreten, wenn der virtuelle Computer über ein angefügtes iSCSI-Gerät oder einen direkt angeschlossenen Speicher (auch als Pass-Through-Datenträger bezeichnet) verfügt.
5. Bei LTS-Releases (Long Term Support) wird der neueste HWE-Kernel (Virtual Hardware Enablement) für aktuelle Linux-Integration Services verwendet.

Führen Sie die folgenden Befehle als root (or sudo) aus, um den mit Azure optimierten Kernel auf 14,04, 16,04 und 18,04 zu installieren:

```
# apt-get update
# apt-get install linux-azure
```

6. Verwenden Sie unter Ubuntu 19,10 den neuesten virtuellen Kernel, um über aktuelle Hyper-V-Funktionen zu verfügen.

Um den virtuellen Kernel auf 19,10 zu installieren, führen Sie die folgenden Befehle als root (oder sudo) aus:

```
# apt-get update
# apt-get install linux-azure
```

Wenn der Kernel aktualisiert wird, muss der virtuelle Computer neu gestartet werden, um ihn zu verwenden.

7. Die Unterstützung dynamischer Arbeitsspeicher ist nur auf virtuellen 64-Bit-Computern verfügbar.
8. Dynamischer Arbeitsspeicher Vorgänge können fehlschlagen, wenn für das Gast Betriebssystem zu wenig Arbeitsspeicher verfügbar ist. Im folgenden finden Sie einige bewährte Methoden:
- Start Speicher und minimaler Arbeitsspeicher müssen größer oder gleich dem vom Verteilungs Anbieter empfohlenen Arbeitsspeicher sein.
 - Anwendungen, die in der Regel den gesamten verfügbaren Arbeitsspeicher auf einem System belegen, können bis zu 80 Prozent des verfügbaren Arbeitsspeichers verbrauchen.
9. Wenn Sie dynamischer Arbeitsspeicher unter den Betriebssystemen Windows Server 2019, Windows Server 2016 oder Windows Server 2012/2012 R2 verwenden, geben Sie den **Start Speicher**, den **minimalen Arbeitsspeicher** und den **maximalen Arbeitsspeicher** Parameter in Vielfachen von 128 Megabyte (MB) an. Wenn dies nicht der Fall ist, kann dies zu Fehlern beim Hinzufügen von Fehlern führen, und es wird möglicherweise keine Arbeitsspeicher Zunahme für ein Gast Betriebssystem angezeigt.
10. In Windows Server 2019, Windows Server 2016 oder Windows Server 2012 R2 funktioniert die Schlüssel-Wert-Paar-Infrastruktur ohne Linux-Software Update möglicherweise nicht ordnungsgemäß. Wenden Sie sich an Ihren Verteilungs Hersteller, um das Software Update zu erhalten, falls Probleme mit diesem Feature auftreten.
11. Auf virtuellen Computern der Generation 2 auf Windows Server 2012 R2 ist der sichere Start standardmäßig aktiviert, und einige virtuelle Linux-Computer werden erst gestartet, wenn die Option für den sicheren Start deaktiviert ist. Sie können den sicheren Start im Abschnitt **Firmware** der Einstellungen für den virtuellen Computer im **Hyper-V-Manager** deaktivieren, oder Sie können ihn mithilfe von PowerShell deaktivieren:

```
Set-VMFirmware -VMName "VMname" -EnableSecureBoot Off
```

12. Führen Sie die folgenden Schritte aus, bevor Sie versuchen, die VHD eines vorhandenen virtuellen Computers der Generation 2 zu kopieren, um neue virtuelle Maschinen der Generation 2 zu erstellen:
- a. Melden Sie sich bei dem vorhandenen virtuellen Computer der Generation 2 an.
 - b. Wechseln Sie in das Verzeichnis für das Start-EFI:


```
# cd /boot/efi/EFI
```

c. Kopieren Sie das Ubuntu-Verzeichnis in ein neues Verzeichnis mit dem Namen Boot:

```
# sudo cp -r ubuntu/ boot
```

d. Wechseln Sie in das neu erstellte Start Verzeichnis:

```
# cd boot
```

e. Benennen Sie die Datei shimx64. EFI um:

```
# sudo mv shimx64.efi bootx64.efi
```

Siehe auch

- [Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V](#)
- [Unterstützte virtuelle Debian-Computer in Hyper-V](#)
- [Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V](#)
- [Unterstützte virtuelle SuSE-Computer auf Hyper-V](#)
- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)
- [Set-vmfirmware](#)
- [Ubuntu 14,04 in einem virtuellen Computer der Generation 2, den virtualisierungsblog von Ben Armstrong](#)

Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V

10.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Hyper-v Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows 10, Windows 8.1

Die folgende featureverteilungszuordnung gibt die Features in den einzelnen Versionen an. Die bekannten Probleme und Problem Umgehungen für die einzelnen Verteilungen werden nach der Tabelle aufgelistet.

Tabellen Legende

- **Integrierte in** -bis (FreeBSD Integration Service) sind als Teil dieses FreeBSD-Release enthalten.
- **✓**-Feature verfügbar
- **(/eer)**: Feature nicht verfügbar

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	12-12.1	11.1-11.3	11,0	10,3	10,2	10,0-10,1	9,1-9,3, 8,4
Verfügbarkeit		Integriert	Integriert	Integriert	Integriert	Integriert	Integriert	Landungen
Core	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Windows Server 2016 genaue Zeit	2019, 2016	✓	✓					
Ungs								
Großbrah men	2019, 2016, 2012 R2	✓ Hinweis s 3	✓ Hinweis s 3	✓ Hinweis s 3	✓ Hinweis s 3	✓ Hinweis s 3	✓ Hinweis s 3	✓ Hinweis s 3
VLAN- Tagging und- Abschnei den	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Livemigra tion	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	12-12.1	11.1-11.3	11,0	10,3	10,2	10,0-10,1	9,1-9,3, 8,4
Statische IP- Injektion	2019, 2016, 2012 R2	✓ Hinweis s 4	✓ Hinweis s 4	✓ Hinweis s 4	✓ Hinweis s 4	✓ Hinweis s 4	✓ Hinweis s 4	✓
vRSS	2019, 2016, 2012 R2	✓	✓	✓				
TCP- Segmenti erung und Prüfsum men Offloads	2019, 2016, 2012 R2	✓	✓	✓	✓	✓		
Große Empfangs Abladung (LRO)	2019, 2016, 2012 R2	✓	✓	✓	✓			
SR-IOV	2019, 2016	✓	✓	✓				
Speicher		Note1	Hinweis 1	Hinweis 1	Hinweis 1	Hinweis 1	Hinweis 1, 2	Hinweis 1, 2
Vhdx- Größe ändern	2019, 2016, 2012 R2	✓ Hinweis s 6	✓ Hinweis s 6	✓ Hinweis s 6				
Virtueller Fibre Channel	2019, 2016, 2012 R2							
Sicherung virtueller Computer	2019, 2016, 2012 R2	✓	✓					
Trim- Unterstüt zung	2019, 2016, 2012 R2	✓	✓					
SCSI- WWN	2019, 2016, 2012 R2							
Gedenke ns								

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	12-12.1	11.1-11.3	11,0	10,3	10,2	10,0-10,1	9,1-9,3, 8,4
Unterstützung für den unterstützten Kernel	2019, 2016, 2012 R2							
MMIO-Lücke konfigurieren	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓
Dynamischer Arbeitsspeicher-Hot-Add	2019, 2016, 2012 R2							
Dynamischer Arbeitsspeicher-Balloonin g	2019, 2016, 2012 R2							
Größenänderung des Laufzeit Speichers	2019, 2016							
Video								
Hyper-V-spezifisches Videogerät	2019, 2016, 2012 R2							
Verschiedensten								
Schlüssel-Wert-Paar	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓ Hinweis 5	✓
Nicht mastbare Unterbrechung	2019, 2016, 2012 R2	✓	✓	✓	✓	✓	✓	✓

FEATURE	WINDOW S SERVER- BETRIEBS SYSTEMV ERSION	12-12.1	11.1-11.3	11,0	10,3	10,2	10,0-10,1	9,1-9,3, 8,4
Dateikopi e von Host zu Gast	2019, 2016, 2012 R2							
Isvmbus- Befehl	2019, 2016, 2012 R2							
Hyper-V- Sockets	2019, 2016							
PCI- Passthrou gh/DDA	2019, 2016	✓	✓					
Virtuelle Maschin en der Generati on 2								
Starten mithilfe von UEFI	2019, 2016, 2012 R2	✓	✓					
Sicherer Start	2019, 2016							

Anmerkungen

1. Legen Sie fest, dass Datenträger [Geräte beschriftet](#) werden sollen, um den Fehler beim Starten der Stamm
2. Das virtuelle DVD-Laufwerk wird möglicherweise nicht erkannt, wenn bis-Treiber auf FreeBSD 8. x und 9. x geladen werden, es sei denn, Sie aktivieren den Legacy-ATA-Treiber über den folgenden Befehl.

```
# echo 'hw.ata.disk_enable=1' >> /boot/loader.conf
# shutdown -r now
```

3. 9126 ist die maximal unterstützte MTU-Größe.
4. In einem failoverszenario ist es nicht möglich, eine statische IPv6-Adresse auf dem Replikat Server festzulegen. Verwenden Sie stattdessen eine IPv4-Adresse.
5. KVP wird von Ports auf FreeBSD 10,0 bereitgestellt. Weitere Informationen finden Sie in den [FreeBSD 10,0-Ports](#) auf FreeBSD.org.
6. Damit die Größe von vhdX Online in FreeBSD 11,0 ordnungsgemäß funktioniert, ist ein spezieller manueller Schritt erforderlich, um einen Geom-Fehler zu umgehen, der in 11.0 + behoben ist, nachdem der Host die Größe des vhdX-Datenträgers geändert hat: Öffnen Sie den Datenträger zum Schreiben, und führen Sie "gpart Recover" wie folgt aus.

```
# dd if=/dev/da1 of=/dev/da1 count=0  
# gpart recover da1
```

Weitere Hinweise: die Featurematrix von 10 stabilen und 11 stabilen ist mit der Version FreeBSD 11,1 identisch. Außerdem sind FreeBSD 10,2 und frühere Versionen (10,1, 10,0, 9. x, 8. x) das Ende der Lebensdauer. [Hier](#) finden Sie eine aktuelle Liste der unterstützten Releases und die neuesten Sicherheitsempfehlungen.

Siehe auch

- [Funktionsbeschreibungen für virtuelle Linux-und FreeBSD-Computer auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von FreeBSD unter Hyper-V](#)

Funktionsbeschreibungen für virtuelle Linux- und FreeBSD-Computer auf Hyper-V

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows Server 2012, Hyper-v Server 2012, Windows Server 2008 R2, Windows 10, Windows 8.1, Windows 8, Windows 7.1, Windows 7

In diesem Artikel werden die Funktionen beschrieben, die in Komponenten wie Kern, Netzwerk, Speicher und Arbeitsspeicher bei Verwendung von Linux und FreeBSD auf einem virtuellen Computer verfügbar sind.

Kern

FEATURE	BESCHREIBUNG
Integriertes Herunterfahren	Mit diesem Feature kann ein Administrator virtuelle Computer über den Hyper-V-Manager Herunterfahren. Weitere Informationen finden Sie unter Herunterfahren des Betriebssystems .
Zeitsynchronisierung	Mit dieser Funktion wird sichergestellt, dass die beibehaltene Zeit in einem virtuellen Computer mit der beibehaltenen Zeit auf dem Host synchronisiert bleibt. Weitere Informationen finden Sie unter Zeitsynchronisierung .
Windows Server 2016 genaue Zeit	Diese Funktion ermöglicht dem Gast die Verwendung der exakten Zeitfunktion von Windows Server 2016, wodurch die Zeitsynchronisierung mit dem Host auf eine Genauigkeit von 1 MS verbessert wird. Weitere Informationen finden Sie unter Windows Server 2016 genaue Zeit
Unterstützung für Multiprocessing	Mit dieser Funktion können von einem virtuellen Computer mehrere Prozessoren auf dem Host verwendet werden, indem mehrere virtuelle CPUs konfiguriert werden.
Takt	Mit dieser Funktion kann der Host für den Zustand der virtuellen Maschine nachverfolgen. Weitere Informationen finden Sie unter Heartbeat .
Integrierte Mausunterstützung	Mit dieser Funktion können Sie eine Maus auf dem Desktop eines virtuellen Computers verwenden und die Maus auch nahtlos zwischen dem Windows Server-Desktop und der Hyper-V-Konsole für den virtuellen Computer verwenden.
Hyper-V-spezifisches Speichergerät	Diese Funktion bietet hochleistungsfähigen Zugriff auf Speichergeräte, die einem virtuellen Computer zugeordnet sind.
Hyper-V-spezifisches Netzwerkgerät	Diese Funktion bietet hochleistungsfähigen Zugriff auf Netzwerkadapter, die an einen virtuellen Computer angefügt sind.

Netzwerk

FEATURE	BESCHREIBUNG
Großrahmen	Mit diesem Feature kann ein Administrator die Größe der Netzwerk Frames über 1500 Bytes hinaus erhöhen, was zu einer erheblichen Steigerung der Netzwerkleistung führt.
VLAN-Tagging und-Abschneiden	Mit dieser Funktion können Sie VLAN-Datenverkehr für virtuelle Computer konfigurieren.
Livemigration	Mit dieser Funktion können Sie eine virtuelle Maschine von einem Host zu einem anderen Host migrieren. Weitere Informationen finden Sie unter Übersicht über virtuelle Computer Livemigration .
Statische IP-Injektion	Mit dieser Funktion können Sie die statische IP-Adresse eines virtuellen Computers replizieren, nachdem für das Replikat auf einem anderen Host ein Failover durchgeführt wurde. Eine solche IP-Replikation stellt sicher, dass netzwerkworkloads nach einem failoverereignis weiterhin nahtlos funktionieren.
vrss (virtuelle Empfangs seitige Skalierung)	Verteilt die Last von einem virtuellen Netzwerkadapter auf mehrere virtuelle Prozessoren eines virtuellen Computers. Weitere Informationen finden Sie unter Virtual Receive-Side Scaling in Windows Server 2012 R2 .
TCP-Segmentierung und Prüfsummen Offloads	Überträgt Segmentierung und Prüfsummen Arbeit von der Gast-CPU an den virtuellen Host Switch oder den Netzwerkadapter während der Übertragung von Netzwerkdaten.
Große Empfangs Abladung (LRO)	Erhöht den eingehenden Durchsatz von Verbindungen mit hoher Bandbreite, indem mehrere Pakete in einem größeren Puffer aggregierte werden und der CPU-Overhead verringert wird.
SR-IOV	E/a-Geräte mit einem einzelnen Stamm verwenden DDA, um Gästen den Zugriff auf Teile spezifischer NIC-Karten zu ermöglichen, wodurch die Latenz und der Durchsatz erhöht werden. SR-IOV benötigt auf dem Host und den virtuellen Funktions Treibern (VF) auf dem Gast aktuellste physische Funktions Treiber (PF).

Speicher

FEATURE	BESCHREIBUNG
Vhdx-Größe ändern	Mit diesem Feature kann ein Administrator die Größe einer vhdx-Datei mit fester Größe ändern, die an einen virtuellen Computer angefügt ist. Weitere Informationen finden Sie unter Übersicht über das Ändern der Größe virtueller Festplatten im OnlineModus .

FEATURE	BESCHREIBUNG
Virtueller Fibre Channel	Mit diesem Feature können virtuelle Computer ein Fiber-Channel-Gerät erkennen und es nativ einbinden. Weitere Informationen finden Sie unter virtueller Hyper-V-Fibre Channel: Übersicht .
Sicherung virtueller Computer	Diese Funktion ermöglicht die Sicherung von virtuellen Live Computern (null). Beachten Sie, dass der Sicherungs Vorgang nicht erfolgreich ist, wenn der virtuelle Computer über virtuelle Festplatten (Virtual Hard Disks, VHDs) verfügt, die auf einem Remote Speicher wie z. b. einer SMB-Freigabe (Server Message Block) oder einem iSCSI-Volume gehostet. Stellen Sie außerdem sicher, dass sich das Sicherungs Ziel nicht auf dem Volume befindet, das Sie sichern.
Trim-Unterstützung	Mithilfe von Trim-hinweisen wird das Laufwerk benachrichtigt, dass bestimmte Sektoren, die zuvor zugeordnet waren, nicht mehr von der APP benötigt werden und gelöscht werden können. Dieser Prozess wird in der Regel verwendet, wenn eine APP große Speicherplatz Zuordnungen über eine Datei herstellt und die Zuordnungen für die Datei dann selbst verwaltet, z. b. zu virtuellen Festplatten Dateien.
SCSI-WWN	Der storvsc-Treiber extrahiert Informationen zum World Wide Name (WWN) vom Port und Knoten von Geräten, die an den virtuellen Computer angefügt sind, und erstellt die entsprechenden sysfs-Dateien.

Arbeitsspeicher

FEATURE	BESCHREIBUNG
Unterstützung für den unterstützten Kernel	Die PE-Technologie (Physical Address Extension) ermöglicht einem 32-Bit-Kernel den Zugriff auf einen physischen Adressraum, der größer als 4 GB ist. Ältere Linux-Distributionen, wie z. b. RHEL 5. x, haben zum Versenden eines separaten Kernels verwendet, bei dem es sich um eine Neuere Distributionen, wie z. b. RHEL 6. x, verfügen über eine vorgefertigte Unterstützung.
MMIO-Lücke konfigurieren	Mit dieser Funktion können Gerätehersteller den Speicherort der Lücke durch den Speicher Abbild-e/a (MMIO) konfigurieren. Die MMIO-Lücke wird normalerweise verwendet, um den verfügbaren physischen Arbeitsspeicher zwischen den gerade genug Betriebssystemen (JeOS) und der eigentlichen Software Infrastruktur aufzuteilen, die das Gerät unterstützt.

FEATURE	BESCHREIBUNG
Dynamischer Arbeitsspeicher-Hot-Add	<p>Der Host kann die Menge an Arbeitsspeicher, die einem virtuellen Computer zur Verfügung steht, dynamisch vergrößern oder verkleinern. Vor der Bereitstellung aktiviert der Administrator dynamischer Arbeitsspeicher im Bereich "Einstellungen der virtuellen Maschine" und gibt den Start Speicher, den minimalen Arbeitsspeicher und den maximalen Arbeitsspeicher für den virtuellen Computer an. Wenn die virtuelle Maschine in Betrieb ist dynamischer Arbeitsspeicher kann nicht deaktiviert werden, und nur die minimalen und maximalen Einstellungen können geändert werden. (Es empfiehlt sich, diese Speichergrößen als Vielfache von 128 MB anzugeben.)</p> <p>Beim ersten Start des virtuellen Computers ist der Arbeitsspeicher gleich dem Start Speicher. Da der Speicherbedarf aufgrund von anwendungsworkloads zunimmt, kann Hyper-V dem virtuellen Computer dynamisch über den Mechanismus zum Hinzufügen von Arbeitsspeicher dynamisch zuweisen, wenn dieser von dieser Version des Kernels unterstützt wird. Die maximale Menge an zugeordnetem Arbeitsspeicher wird durch den Wert des Parameters für den maximalen Arbeitsspeicher begrenzt.</p> <p>Auf der Registerkarte "Arbeitsspeicher" des Hyper-V-Managers wird die Menge an Arbeitsspeicher angezeigt, die dem virtuellen Computer zugewiesen ist, aber die Arbeitsspeicher Statistik auf dem virtuellen Computer zeigt den höchsten zugeordneten Arbeitsspeicher an.</p> <p>Weitere Informationen finden Sie unter Übersicht über Hyper-V-dynamischer Arbeitsspeicher.</p>

FEATURE	BESCHREIBUNG
Dynamischer Arbeitsspeicher-Ballooning	<p>Der Host kann die Menge an Arbeitsspeicher, die einem virtuellen Computer zur Verfügung steht, dynamisch vergrößern oder verkleinern. Vor der Bereitstellung aktiviert der Administrator dynamischer Arbeitsspeicher im Bereich "Einstellungen der virtuellen Maschine" und gibt den Start Speicher, den minimalen Arbeitsspeicher und den maximalen Arbeitsspeicher für den virtuellen Computer an. Wenn die virtuelle Maschine in Betrieb ist dynamischer Arbeitsspeicher kann nicht deaktiviert werden, und nur die minimalen und maximalen Einstellungen können geändert werden. (Es empfiehlt sich, diese Speichergrößen als Vielfache von 128 MB anzugeben.)</p> <p>Beim ersten Start des virtuellen Computers ist der Arbeitsspeicher gleich dem Start Speicher. Da der Speicherbedarf aufgrund von anwendungsworkloads zunimmt, kann Hyper-V dem virtuellen Computer dynamisch über den Mechanismus zum Hinzufügen von Arbeitsspeicher (oben) dynamisch mehr Arbeitsspeicher zuweisen. Wenn die Speichernachfrage abnimmt, kann der Arbeitsspeicher von der virtuellen Maschine durch den Sprechblasen Mechanismus automatisch von der virtuellen Maschine entfernt werden. Der Arbeitsspeicher wird von Hyper-V nicht unter dem Parameter für den minimalen Arbeitsspeicher bereitgestellt.</p> <p>Auf der Registerkarte "Arbeitsspeicher" des Hyper-V-Managers wird die Menge an Arbeitsspeicher angezeigt, die dem virtuellen Computer zugewiesen ist, aber die Arbeitsspeicher Statistik auf dem virtuellen Computer zeigt den höchsten zugeordneten Arbeitsspeicher an.</p> <p>Weitere Informationen finden Sie unter Übersicht über Hyper-V-dynamischer Arbeitsspeicher.</p>
Größenänderung des Lauf Zeit Speichers	<p>Ein Administrator kann die Menge an Arbeitsspeicher, die einer virtuellen Maschine zur Verfügung steht, während der Ausführung festlegen, um entweder den Arbeitsspeicher zu erhöhen ("Hot Add") oder ihn zu verringern ("Hot Remove"). Der Arbeitsspeicher wird über den Sprechblasen Treiber an Hyper-V zurückgegeben (Weitere Informationen finden Sie unter "dynamischer Arbeitsspeicher-Ballooning"). Der Sprechblasen Treiber behält einen minimalen Anteil an freiem Arbeitsspeicher nach dem Hochfahren, so genannten "Floor", bei. der zugewiesene Arbeitsspeicher kann daher nicht unterhalb der aktuellen Nachfrage Plus dieser bodenmenge reduziert werden. Auf der Registerkarte "Arbeitsspeicher" des Hyper-V-Managers wird die Menge an Arbeitsspeicher angezeigt, die dem virtuellen Computer zugewiesen ist, aber die Arbeitsspeicher Statistik auf dem virtuellen Computer zeigt den höchsten zugeordneten Arbeitsspeicher an. (Es empfiehlt sich, Arbeitsspeicher Werte als Vielfache von 128 MB anzugeben.)</p>

Video

FEATURE	BESCHREIBUNG
---------	--------------

FEATURE	BESCHREIBUNG
Hyper-V-spezifisches Videogerät	Diese Funktion bietet Hochleistungs Grafiken und eine bessere Auflösung für virtuelle Maschinen. Dieses Gerät bietet keine erweiterten Sitzungs Modus-oder remotefx-Funktionen.

Verschiedenes

FEATURE	BESCHREIBUNG
KVP (Schlüssel-Wert-Paar) Exchange	Diese Funktion bietet einen Schlüssel-Wert-Paar (KVP)-Exchange-Dienst für virtuelle Computer. In der Regel verwenden Administratoren den KVP-Mechanismus, um benutzerdefinierte Daten Vorgänge für Lese-und Schreibvorgänge auf einem virtuellen Computer auszuführen. Weitere Informationen finden Sie unter Daten austausch: Verwenden von Schlüssel-Wert-Paaren zum Freigeben von Informationen zwischen dem Host und dem Gast auf Hyper-V .
Nicht maskierbare Unterbrechung	Mit dieser Funktion kann ein Administrator einen virtuellen Computer, der nicht mit einem maskierbaren Interrupts (NMI) ausgeführt wird, ausgeben. NMIs sind nützlich, um Absturz Abbilder von Betriebssystemen zu erhalten, die aufgrund von Anwendungsfehlern nicht mehr reagiert. Diese Absturz Abbilder können nach dem Neustart diagnostiziert werden.
Dateikopie von Host zu Gast	Mit dieser Funktion können Dateien vom physischen Host Computer auf die virtuellen Gastcomputer kopiert werden, ohne dass der Netzwerkadapter verwendet wird. Weitere Informationen finden Sie unter Guest Services .
lsmbus-Befehl	Mit diesem Befehl werden Informationen zu Geräten auf dem Hyper-V-Virtual Machine Bus (VMBus) ähnlich wie bei Informations Befehlen wie lspci abgerufen.
Hyper-V-Sockets	Dies ist ein zusätzlicher Kommunikationskanal zwischen dem Host und dem Gast Betriebssystem. Informationen zum Laden und Verwenden des Hyper-V-Sockets-Kernel Moduls finden Sie unter Erstellen eigener Integrationsdienste .
PCI-Passthrough/DDA	<p>Mit Windows Server 2016 können Administratoren PCI Express-Geräte über den diskreten Geräte Zuweisungs Mechanismus durchlaufen. Gängige Geräte sind Netzwerkkarten, Grafikkarten und spezielle Speichergeräte. Der virtuelle Computer benötigt den entsprechenden Treiber, um die verfügbar gemachte Hardware zu verwenden. Die Hardware muss der virtuellen Maschine zugewiesen werden, damit Sie verwendet werden kann.</p> <p>Weitere Informationen finden Sie unter diskrete Geräte Zuweisung-Beschreibung und Hintergrund.</p> <p>DDA ist eine Voraussetzung für SR-IOV-Netzwerke. Virtuelle Ports müssen der virtuellen Maschine zugewiesen werden, und die virtuelle Maschine muss die richtigen virtuellen Funktions Treiber für das Multiplexing von Geräten verwenden.</p>

Virtuelle Computer der Generation 2

FEATURE	BESCHREIBUNG
Starten mithilfe von UEFI	Mit dieser Funktion können virtuelle Computer mit Unified Extensible Firmware Interface (UEFI) gestartet werden. Weitere Informationen finden Sie unter Übersicht über virtuelle Computer der Generation 2 .
Sicherer Start	Diese Funktion ermöglicht virtuellen Computern die Verwendung des UEFI-basierten sicheren Start Modus. Wenn ein virtueller Computer im sicheren Modus gestartet wird, werden verschiedene Betriebssystemkomponenten mithilfe von Signaturen überprüft, die im UEFI-Datenspeicher vorhanden sind. Weitere Informationen finden Sie unter Sicherer Start .

Weitere Informationen

- [Unterstützte virtuelle Computer der CentOS-und Red Hat Enterprise Linux auf Hyper-V](#)
- [Unterstützte virtuelle Debian-Computer in Hyper-V](#)
- [Unterstützte Oracle Linux virtuellen Maschinen auf Hyper-V](#)
- [Unterstützte virtuelle SuSE-Computer auf Hyper-V](#)
- [Unterstützte virtuelle Ubuntu-Computer auf Hyper-V](#)
- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)
- [Bewährte Methoden für die Ausführung von Linux unter Hyper-V](#)
- [Bewährte Methoden für die Ausführung von FreeBSD unter Hyper-V](#)

Bewährte Methoden für die Ausführung von Linux unter Hyper-V

01.05.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows Server 2012, Hyper-v Server 2012, Windows Server 2008 R2, Windows 10, Windows 8.1, Windows 8, Windows 7,1, Windows 7

Dieses Thema enthält eine Liste der Empfehlungen für die Ausführung virtueller Linux-Computer unter Hyper-V.

Optimieren von Linux-Dateisystemen auf dynamische vhdx-Dateien

Einige Linux-Dateisysteme belegen möglicherweise beträchtliche Mengen an tatsächlicher Speicherplatz, auch wenn das Dateisystem größtenteils leer ist. Beachten Sie die folgenden Empfehlungen, um die tatsächliche Speicherplatz Nutzung dynamischer vhdx-Dateien zu verringern:

- Wenn Sie die vhdx-Datei erstellen, verwenden Sie 1 MB blockSizeBytes (standardmäßig 32 MB) in PowerShell, z. b.:

```
PS > New-VHD -Path C:\MyVHDs\test.vhdx -SizeBytes 127GB -Dynamic -BlockSizeBytes 1MB
```

- Das Ext4-Format wird als ext3 bevorzugt, da ext4 bei der Verwendung mit dynamischen vhdx-Dateien mehr Speicherplatz als ext3 ist.
- Geben Sie beim Erstellen des Dateisystems die Anzahl der Gruppen an, die 4096 sein sollen, z. b.:

```
# mkfs.ext4 -G 4096 /dev/sdX1
```

Menü Timeout für grub bei Generation 2 Virtual Machines

Da die Legacy-Hardware auf virtuellen Computern der Generation 2 aus der Emulation entfernt wird, wird der Timer-Menü Countdowntimer zu schnell angerechnet, damit das Menü "grub" angezeigt wird. der Standardeintrag wird sofort geladen. Wenn die grub-Funktion nicht für die Verwendung des EFI-unterstützten Timers korrigiert wurde, ändern Sie **/Boot/grub/grub.conf**, **/usr/default/grub** oder die entsprechende "Timeout = 100000" anstelle der Standardeinstellung "Timeout = 5".

PXE-Start bei Virtual Machines der Generation 2

Da der boxtimer nicht in der Generation 2 Virtual Machines vorhanden ist, können Netzwerkverbindungen mit dem PXE-TFTP-Server vorzeitig beendet werden und verhindern, dass der Bootloader die GRUB-Konfiguration liest und einen Kernel vom Server lädt.

In RHEL 6. x kann der Legacy-, grub v 0,97 EFI-Bootloader anstelle von grub2 verwendet werden, wie hier beschrieben: https://access.redhat.com/documentation/Red_Hat_Enterprise_Linux/6/html/Installation_Guide/s1-netboot-pxe-config-efi.html

In anderen Linux-Distributionen als RHEL 6. x können ähnliche Schritte ausgeführt werden, um GRUB v 0,97 zum

Laden von Linux-Kernels von einem PXE-Server zu konfigurieren.

Außerdem funktionieren die Tastatur- und Maus Eingaben von RHEL/CentOS 6,6 nicht mit dem Vorinstallations-Kernel, mit dem die Angabe von Installationsoptionen im Menü verhindert wird. Eine serielle Konsole muss konfiguriert werden, um die Auswahl von Installationsoptionen zuzulassen.

- Fügen Sie in der Datei "**efidefault**" auf dem PXE-Server den folgenden Kernel Parameter "**console = ttyS1**" hinzu.
- Richten Sie auf dem virtuellen Computer in Hyper-V einen COM-Port mithilfe dieses PowerShell-Cmdlets ein:

```
Set-VMComPort -VMName <Name> -Number 2 -Path \\.\pipe\dbg1
```

Wenn Sie eine Kickstart-Datei für den Vorinstallations-Kernel angeben, ist es auch nicht erforderlich, dass während der Installation Tastatur- und Maus Eingaben benötigt werden.

Verwenden statischer MAC-Adressen mit Failoverclustering

Virtuelle Linux-Computer, die mithilfe des Failoverclustering bereitgestellt werden, sollten für jeden virtuellen Netzwerkadapter mit einer statischen Media Access Control (Mac-Adresse) konfiguriert werden. In einigen Versionen von Linux geht die Netzwerkkonfiguration möglicherweise nach einem Failover verloren, da dem virtuellen Netzwerkadapter eine neue Mac-Adresse zugewiesen wird. Stellen Sie sicher, dass jeder virtuelle Netzwerkadapter über eine statische MAC-Adresse verfügt, um den Verlust der Netzwerkkonfiguration zu vermeiden. Sie können die Mac-Adresse konfigurieren, indem Sie die Einstellungen der virtuellen Maschine im Hyper-V-Manager oder Failovercluster-Manager bearbeiten.

Verwenden Sie Hyper-V-spezifische Netzwerkadapter, nicht den Legacy-Netzwerkadapter.

Konfigurieren und verwenden Sie den virtuellen Ethernet-Adapter, bei dem es sich um eine Hyper-V-spezifische Netzwerkkarte mit verbesserter Leistung handelt. Wenn sowohl Legacy- als auch Hyper-V-spezifische Netzwerkadapter an einen virtuellen Computer angefügt sind, können die Netzwerknamen in der Ausgabe von **ifconfig -a** zufällige Werte wie **_tmp12000801310** anzeigen. Entfernen Sie alle älteren Netzwerkadapter, wenn Sie Hyper-V-spezifische Netzwerkadapter auf einem virtuellen Linux-Computer verwenden, um dieses Problem zu vermeiden.

E/a-Scheduler NOOP/None für bessere Datenträger-e/a-Leistung verwenden

Der Linux-Kernel bietet zwei Sätze von Datenträger-e/a-Zeit Planungs Modulen für die Neuordnung von Anforderungen. Ein Satz gilt für das ältere 'BLK'-Subsystem, und ein Satz ist für das neuere 'BLK-mq'-Subsystem. In beiden Fällen empfiehlt es sich, einen Scheduler zu verwenden, der die Planungsentscheidungen an den zugrunde liegenden Hyper-V-Hypervisor übergibt. Bei Linux-Kernels, die das "BLK"-Subsystem verwenden, handelt es sich hierbei um den "NOOP"-Scheduler. Bei Linux-Kernels, die das "BLK-MQ"-Subsystem verwenden, handelt es sich hierbei um den Scheduler "None".

Bei einem bestimmten Datenträger können die verfügbaren Planer an diesem Dateisystem Speicherort angezeigt werden: `<diskname> /sys/class/block//Queue/Scheduler`, wobei der aktuell ausgewählte Planer in eckigen Klammern steht. Sie können den Scheduler ändern, indem Sie an diesem Dateisystem Speicherort schreiben. Die Änderung muss zu einem Initialisierungs Skript hinzugefügt werden, damit Sie über Neustarts hinweg beibehalten werden. Weitere Informationen finden Sie in der Dokumentation zur Linux-Distribution.

NUMA

Linux-Kernelversionen vor Version 2.6.37 unterstützen keinen NUMA (Non-Uniform Memory Access, nicht einheitlicher Speicherzugriff) auf Hyper-V mit größeren VM-Größen. Dieses Problem betrifft in erster Linie ältere Distributionen, die den Red Hat 2.6.32-Upstreamkernel verwenden, und wurde in Red Hat Enterprise Linux (RHEL) 6.6 (kernel-2.6.32-504) behoben. Systeme, auf denen benutzerdefinierte Kernel ausgeführt werden, die älter als 2.6.37 sind, bzw. RHEL-basierte Kernel, die älter als 2.6.32-504 sind, müssen in „grub.conf“ in der Kernelbefehlszeile den Startparameter `numa=off` festlegen. Weitere Informationen finden Sie unter [Red Hat KB 436883](#).

Reservieren von mehr Speicher für kdump

Für den Fall, dass der dumperfassungs-Kernel beim Start eine Panik hat, reservieren Sie mehr Speicherplatz für den Kernel. Ändern Sie beispielsweise den Parameter `crashkernel = 384m-: 128 m` in `crashkernel = 384m-: 256M` in der Ubuntu grub-Konfigurationsdatei.

Das Verkleinern von vhdx oder das Erweitern von VHD- und vhdx-Dateien kann zu fehlerhaften GPT-Partitionstabellen führen

Hyper-V ermöglicht das Verkleinern von virtuellen Festplatten Dateien (vhdx) ohne Berücksichtigung von Partitionen, Volumes oder Dateisystem-Datenstrukturen, die möglicherweise auf dem Datenträger vorhanden sind. Wenn die vhdx-Datei auf das Ende der vhdx-Datei vor dem Ende einer Partition verkleinert wird, können Daten verloren gehen, und die Partition kann beschädigt werden, oder es können ungültige Daten zurückgegeben werden, wenn die Partition gelesen wird.

Nachdem die Größe einer VHD- oder vhdx-Datei geändert wurde, sollten Administratoren ein Hilfsprogramm wie fdisk oder parted verwenden, um die Größe der Partition, des Volumes und des Dateisystems zu aktualisieren und die Größe des Datenträgers widerzuspiegeln. Das Verkleinern oder Erweitern der Größe einer VHD oder vhdx mit einer GUID-Partitionstabelle (GPT) führt zu einer Warnung, wenn ein Partitions Verwaltungs Tool zum Überprüfen des Partitionslayouts verwendet wird, und der Administrator wird gewarnt, den ersten und sekundären GPT-Header zu korrigieren. Dieser manuelle Schritt kann ohne Datenverlust sicher durchgeführt werden.

Weitere Informationen

- [Unterstützte virtuelle Linux- und FreeBSD-Computer für Hyper-V unter Windows](#)
- [Bewährte Methoden für die Ausführung von FreeBSD unter Hyper-V](#)
- [Bereitstellen eines Hyper-V-Clusters](#)
- [Erstellen von Linux-Images für Azure](#)
- [Optimieren virtueller Linux-Computer in Azure](#)

Bewährte Methoden für die Ausführung von FreeBSD unter Hyper-V

09.04.2020 • 4 minutes to read • [Edit Online](#)

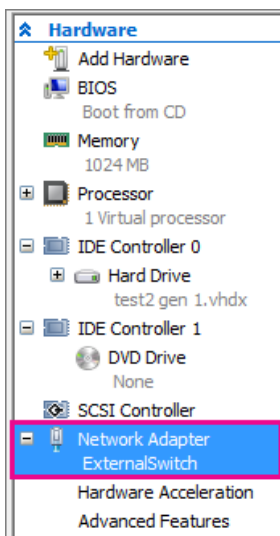
Gilt für: Windows Server 2019, Windows Server 2016, Hyper-v Server 2016, Windows Server 2012 R2, Hyper-v Server 2012 R2, Windows Server 2012, Hyper-v Server 2012, Windows Server 2008 R2, Windows 10, Windows 8.1, Windows 8, Windows 7,1, Windows 7

Dieses Thema enthält eine Liste der Empfehlungen zum Ausführen von FreeBSD als Gast Betriebssystem auf einem virtuellen Hyper-V-Computer.

Aktivieren von Karpfen in FreeBSD 10,2 unter Hyper-V

Das Common Address Redundanz-Protokoll (CARP) ermöglicht es mehreren Hosts, dieselbe IP-Adresse und virtuelle Host-ID (vhid) zu verwenden, um eine hohe Verfügbarkeit für einen oder mehrere Dienste zu gewährleisten. Wenn mindestens ein Host ausfällt, übernehmen die anderen Hosts transparent, sodass Benutzer keinen Dienst Fehler bemerken. Um Karpfen in FreeBSD 10,2 zu verwenden, befolgen Sie die Anweisungen im [FreeBSD-Handbuch](#), und führen Sie im Hyper-V-Manager die folgenden Schritte aus.

- Vergewissern Sie sich, dass der virtuelle Computer über einen Netzwerk Adapter verfügt und ihm ein virtueller Switch zugewiesen ist. Wählen Sie den virtuellen Computer aus, und wählen Sie **Aktionen** > **Einstellungen** aus.



- Spoofing von Mac-Adressen aktivieren. Gehen Sie hierzu wie folgt vor:
 1. Wählen Sie den virtuellen Computer aus, und wählen Sie **Aktionen** > **Einstellungen** aus.
 2. Erweitern Sie **Netzwerk Adapter**, und wählen Sie **Erweiterte Features** aus.
 3. Wählen Sie **Spoofing von Mac-Adressen aktivieren** aus.

Erstellen von Bezeichnungen für Datenträger Geräte

Während des Starts werden Geräteknoten erstellt, wenn neue Geräte erkannt werden. Dies kann bedeuten, dass sich Gerätenamen ändern können, wenn neue Geräte hinzugefügt werden. Wenn beim Starten ein Fehler bei der Stamm einreihe auftritt, sollten Sie für jede IDE-Partition Bezeichnungen erstellen, um Konflikte und Änderungen

zu vermeiden. Informationen zur Vorgehensweise finden Sie unter [bezeichnen von Datenträger Geräten](#). Im folgenden finden Sie Beispiele.

IMPORTANT

Erstellen Sie vor dem vornehmen von Änderungen eine Sicherungskopie Ihrer Datei.

1. Starten Sie das System im Einzelbenutzermodus neu. Wählen Sie hierzu die Option Start Menüoption 2 für FreeBSD 10.3 + (Option 4 für FreeBSD 8. x) aus, oder führen Sie in der Eingabeaufforderung "Boot-s" aus.
2. Erstellen Sie im Einzelbenutzermodus Geom-Bezeichnungen für jede der IDE-Datenträger Partitionen, die in Ihrem fstab (sowohl root als auch Swap) aufgelistet sind. Im folgenden finden Sie ein Beispiel für FreeBSD 10,3.

```
# cat /etc/fstab
# Device      Mountpoint      FStype  Options  Dump   Pass#
/dev/da0p2    /                ufs     rw       1      1
/dev/da0p3    none            swap    sw       0      0

# glabel label rootfs /dev/da0p2
# glabel label swap /dev/da0p3
# exit
```

Weitere Informationen zu Geom-Bezeichnungen finden Sie unter: [bezeichnen von Datenträger Geräten](#).

3. Das System wird mit dem multibenutzerstart fortgesetzt. Nachdem der Startvorgang abgeschlossen ist, bearbeiten Sie "/etc/fstab", und ersetzen Sie die herkömmlichen Gerätenamen durch die jeweiligen Bezeichnungen. Der endgültige "/etc/fstab" sieht wie folgt aus:

```
# Device      Mountpoint      FStype  Options  Dump   Pass#
/dev/label/rootfs /                ufs     rw       1      1
/dev/label/swap none            swap    sw       0      0
```

4. Das System kann jetzt neu gestartet werden. Wenn alles gut funktioniert, wird es normal angezeigt, und die einreihe zeigt Folgendes an:

```
# mount
/dev/label/rootfs on / (ufs, local, journaled soft-updates)
devfs on /dev (devfs, local, mutilabel)
```

Verwenden eines drahtlos Netzwerkadapters als virtuellen Switch

Wenn der virtuelle Switch auf dem Host auf dem Drahtlos Netzwerkadapter basiert, verringern Sie die ARP-Ablaufzeit mit dem folgenden Befehl auf 60 Sekunden. Andernfalls kann das Netzwerk der VM nach einer Weile nicht mehr funktionieren.

```
# sysctl net.link.ether.inet.max_age=60
```

Siehe auch

- [Unterstützte virtuelle FreeBSD-Maschinen auf Hyper-V](#)

Kompatibilität von Hyper-V-Features nach Generierung und Gast

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Die Tabellen in diesem Artikel veranschaulichen die Generationen und Betriebssysteme, die mit einigen der Hyper-V-Features kompatibel sind und nach Kategorien gruppiert sind. Im Allgemeinen erhalten Sie die beste Verfügbarkeit von Features mit einem virtuellen Computer der Generation 2, auf dem das neueste Betriebssystem ausgeführt wird.

Beachten Sie, dass einige Features von Hardware oder anderen Infrastrukturen abhängen. Hardware Details finden Sie unter [System Anforderungen für Hyper-V auf Windows Server 2016](#). In einigen Fällen kann ein Feature mit allen unterstützten Gastbetriebssystemen verwendet werden. Ausführliche Informationen dazu, welche Betriebssysteme unterstützt werden, finden Sie unter:

- [Unterstützte virtuelle Linux-und FreeBSD-Computer](#)
- [Unterstützte Windows-Gastbetriebssysteme](#)

Verfügbarkeit und Sicherung

FEATURE	STRO	GASTBETRIEBSSYSTEM
Prüfpunkte	1 und 2	Jeder unterstützte Gast
Gastclustering	1 und 2	Gäste, die Cluster fähige Anwendungen ausführen und die iSCSI-Ziel Software installiert haben
Replikation	1 und 2	Jeder unterstützte Gast
Domänencontroller	1 und 2	Alle unterstützten Windows Server-Gäste, die nur Produktions Prüfpunkte verwenden. Siehe unterstützte Windows Server-Gast Betriebssysteme

Compute

FEATURE	STRO	GASTBETRIEBSSYSTEM
Dynamischer Arbeitsspeicher	1 und 2	Bestimmte Versionen von unterstützten Gästen. Weitere Informationen finden Sie unter Übersicht über Hyper-V-dynamischer Arbeitsspeicher für ältere Versionen als Windows Server 2016 und Windows 10.
Heißes hinzufügen/entfernen des Speichers	1 und 2	Windows Server 2016, Windows 10

FEATURE	STRO	GASTBETRIEBSSYSTEM
Virtueller NUMA	1 und 2	Jeder unterstützte Gast

Entwicklung und Test

FEATURE	STRO	GASTBETRIEBSSYSTEM
COM/serielle Anschlüsse	1 und 2 Hinweis: Verwenden Sie für Generation 2 Windows PowerShell, um zu konfigurieren. Weitere Informationen finden Sie unter Hinzufügen eines COM-Ports für das Kernel Debugging .	Jeder unterstützte Gast

Mobilität

FEATURE	STRO	GASTBETRIEBSSYSTEM
Livemigration	1 und 2	Jeder unterstützte Gast
Importieren/Exportieren	1 und 2	Jeder unterstützte Gast

Netzwerk

FEATURE	STRO	GASTBETRIEBSSYSTEM
Heißes hinzufügen/entfernen des virtuellen Netzwerkadapters	2	Jeder unterstützte Gast
Virtueller Legacy-Netzwerkadapter	1	Jeder unterstützte Gast
Single root Input/Output Virtualization (SR-IOV)	1 und 2	64-Bit-Windows-Gast Betriebssysteme, beginnend mit Windows Server 2012 und Windows 8.
Multiqueue für virtuelle Computer (vmmq)	1 und 2	Jeder unterstützte Gast

Remote Verbindung

FEATURE	STRO	GASTBETRIEBSSYSTEM
Diskrete Geräte Zuweisung (DDA)	1 und 2	Windows Server 2016, Windows Server 2012 R2 nur mit installiertem Update 3133690, Windows 10 Hinweis: Ausführliche Informationen zu Update 3133690 finden Sie in diesem Support Artikel.

FEATURE	STRO	GASTBETRIEBSSYSTEM
Verbesserter Sitzungsmodus	1 und 2	Windows Server 2016, Windows Server 2012 R2, Windows 10 und Windows 8.1 mit aktiviertem Remotedesktopdienste Hinweis: möglicherweise müssen Sie auch den Host konfigurieren. Weitere Informationen finden Sie unter Verwenden lokaler Ressourcen auf einem virtuellen Hyper-V-Computer mit VMConnect .
RemoteFx	1 und 2	Generation 1 auf 32- und 64-Bit-Windows-Versionen ab Windows 8. Generation 2 auf 64-Bit-Windows 10-Versionen

Sicherheit

FEATURE	STRO	GASTBETRIEBSSYSTEM
Sicherer Start	2	Linux: Ubuntu 14,04 und höher, SuSE Linux Enterprise Server 12 und höher, Red Hat Enterprise Linux 7,0 und höher und CentOS 7,0 und höher Windows: alle unterstützten Versionen, die auf einem virtuellen Computer der Generation 2 ausgeführt werden können
Abgeschirmte VMs	2	Windows: alle unterstützten Versionen, die auf einem virtuellen Computer der Generation 2 ausgeführt werden können

Speicher

FEATURE	STRO	GASTBETRIEBSSYSTEM
Freigegebene virtuelle Festplatten (nur vhdx)	1 und 2	Windows Server 2016, Windows Server 2012 R2, Windows Server 2012
SMB3	1 und 2	Alle, die SMB3 unterstützen
Direkte Speicherplätze	2	Windows Server 2016
Virtueller Fibre Channel	1 und 2	Windows Server 2016, Windows Server 2012 R2, Windows Server 2012
Vhdx-Format	1 und 2	Jeder unterstützte Gast

Beginnen Sie mit Hyper-V unter Windows Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Verwenden Sie die folgenden Ressourcen zum Einrichten und Testen von Hyper-V auf der Server Core-oder GUI-Installationsoption von Windows Server 2019 oder Windows Server 2016. Bevor Sie etwas installieren, überprüfen Sie jedoch die [Systemanforderungen für Windows Server](#) und die [Systemanforderungen für Hyper-V](#).

- [Herunterladen und Installieren von Windows Server](#)
- [Installieren der Hyper-V-Rolle unter Windows Server](#)
- [Erstellen eines virtuellen Switches für Hyper-V-VMs](#)
- [Erstellen eines virtuellen Computers in Hyper-V](#)

Installieren der Hyper-V-Rolle unter Windows Server

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows Server 2019

Um virtuelle Computer zu erstellen und auszuführen, installieren Sie die Hyper-V-Rolle unter Windows Server, indem Sie Server-Manager oder das Cmdlet **install-Windows Feature** in Windows PowerShell verwenden. Informationen zu Windows 10 finden Sie unter [Installieren von Hyper-V unter Windows 10](#).

Weitere Informationen zu Hyper-v finden Sie in der [Übersicht über die Hyper-v-Technologie](#). Zum Ausprobieren von Windows Server 2019 können Sie eine Evaluierungsversion herunterladen und installieren. Weitere Informationen finden Sie im [Evaluation Center](#).

Stellen Sie vor dem Installieren von Windows Server oder dem Hinzufügen der Hyper-V-Rolle Folgendes sicher:

- Die Computer Hardware ist kompatibel. Weitere Informationen finden Sie unter [Systemanforderungen für Windows Server](#) und [Systemanforderungen für Hyper-V unter Windows Server](#).
- Sie beabsichtigen nicht, Virtualisierungsanwendungen von Drittanbietern zu verwenden, die auf den gleichen Prozessor Features basieren, die von Hyper-V benötigt werden. Beispiele hierfür sind VMware-Arbeitsstation und VirtualBox. Sie können Hyper-V installieren, ohne diese anderen apps zu deinstallieren. Wenn Sie jedoch versuchen, Sie zum Verwalten virtueller Maschinen zu verwenden, wenn der Hyper-V-Hypervisor ausgeführt wird, werden die virtuellen Computer möglicherweise nicht zuverlässig gestartet oder nicht zuverlässig ausgeführt. Ausführliche Informationen und Anweisungen zum Ausschalten des Hyper-v-Hypervisors, wenn Sie eine dieser Apps verwenden müssen, finden Sie unter [Virtualisierungsanwendungen funktionieren nicht zusammen mit Hyper-v, Device Guard und Credential Guard](#).

Wenn Sie nur die Verwaltungs Tools (z. b. Hyper-v-Manager) installieren möchten, finden Sie weitere Informationen unter [Remote Verwaltung von Hyper-v-Hosts mit Hyper-v-Manager](#).

Installieren von Hyper-V mit Server-Manager

1. Klicken Sie im **Server-Manager** im Menü **Verwalten** auf **Rollen und Funktionen hinzufügen**.
2. Überprüfen Sie auf der Seite **Vorbemerkungen**, ob der Zielservers und die Netzwerkumgebung für die Installation der Rolle und des Features vorbereitet sind. Klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite **Installationstyp auswählen** die Option **Rollenbasierte oder featurebasierte Installation**, und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie auf der Seite **Zielservers auswählen** einen Server aus dem Serverpool aus, und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Serverrollen auswählen** die Option **Hyper-V**.
6. Klicken Sie auf **Features hinzufügen**, um die Tools hinzuzufügen, die Sie zum Erstellen und Verwalten von virtuellen Computern verwenden. Klicken Sie auf der Seite mit den Features auf **Weiter**.
7. Wählen Sie auf der Seite **Virtuelle Switches erstellen, Migration eines virtuellen Computers und Standardspeicher** die gewünschten Optionen.
8. Wählen Sie auf der Seite **Installationsauswahl bestätigen** die Option **Zielservers bei Bedarf automatisch neu starten**, und klicken Sie dann auf **Installieren**.

9. Vergewissern Sie sich nach Abschluss der Installation, dass Hyper-V ordnungsgemäß installiert ist. Öffnen Sie in Server-Manager die Seite **alle Server**, und wählen Sie einen Server aus, auf dem Hyper-V installiert ist. Überprüfen Sie die Kachel **Rollen und Features** auf der Seite für den ausgewählten Server.

Installieren von Hyper-V mithilfe des Cmdlets "Install-Windows Feature"

1. Klicken Sie auf dem Windows-Desktop auf die Schaltfläche „Start“, und geben Sie einen beliebigen Teil des Namens **Windows PowerShell** ein.
2. Klicken Sie mit der rechten Maustaste auf Windows PowerShell, und wählen Sie **als Administrator ausführen**.
3. Zum Installieren von Hyper-V auf einem Server, mit dem Sie eine Remote Verbindung hergestellt haben, führen Sie den folgenden Befehl aus, und ersetzen Sie `<computer_name>` durch den Namen des Servers.

```
Install-WindowsFeature -Name Hyper-V -ComputerName <computer_name> -IncludeManagementTools -Restart
```

Wenn Sie lokal mit dem Server verbunden sind, führen Sie den Befehl ohne

```
-ComputerName <computer_name> aus.
```

4. Nachdem der Server neu gestartet wurde, können Sie sehen, dass die Hyper-V-Rolle installiert ist, und sehen, welche anderen Rollen und Features installiert werden, indem Sie den folgenden Befehl ausführen:

```
Get-WindowsFeature -ComputerName <computer_name>
```

Wenn Sie lokal mit dem Server verbunden sind, führen Sie den Befehl ohne

```
-ComputerName <computer_name> aus.
```

NOTE

Wenn Sie diese Rolle auf einem Server installieren, auf dem die Server Core-Installationsoption von Windows Server 2016 ausgeführt wird, und den Parameter `-IncludeManagementTools` verwenden, wird nur das Hyper-V-Modul für Windows PowerShell installiert. Sie können das GUI-Verwaltungs Tool Hyper-v-Manager auf einem anderen Computer verwenden, um einen Hyper-v-Host, der auf einer Server Core-Installation ausgeführt wird, Remote zu verwalten. Anweisungen zum Herstellen einer Remote Verbindung finden Sie unter [Remote Verwaltung von Hyper-v-Hosts mit dem Hyper-v-Manager](#).

Siehe auch

- [Install-Windows Feature](#)

Erstellen eines virtuellen Switches für virtuelle Hyper-V-Computer

09.04.2020 • 6 minutes to read • [Edit Online](#)

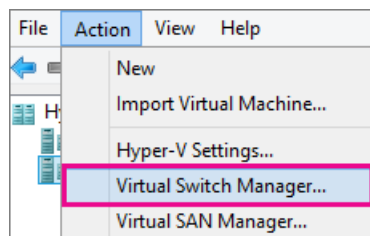
Gilt für: Windows 10, Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Mit einem virtuellen Switch können virtuelle Maschinen, die auf Hyper-V-Hosts erstellt wurden, mit anderen Computern kommunizieren. Wenn Sie die Hyper-V-Rolle unter Windows Server installieren, können Sie einen virtuellen Switch erstellen. Verwenden Sie zum Erstellen zusätzlicher virtueller Switches den Hyper-V-Manager oder Windows PowerShell. Weitere Informationen zu virtuellen Switches finden Sie unter [virtueller Hyper-V-Switch](#).

Das Netzwerk virtueller Computer kann ein komplexer Betreff sein. Außerdem gibt es mehrere neue Features für virtuelle Switches, die Sie verwenden können, wie z. b. [Switch Embedded Teaming \(Set\)](#). Das grundlegende Netzwerk ist jedoch relativ einfach. Dieses Thema behandelt genau genug, sodass Sie vernetzte virtuelle Maschinen in Hyper-V erstellen können. Weitere Informationen zum Einrichten der Netzwerkinfrastruktur finden Sie in der Dokumentation zum [Netzwerk](#).

Erstellen eines virtuellen Switches mit dem Hyper-V-Manager

1. Öffnen Sie Hyper-v-Manager, und wählen Sie den Computernamen des Hyper-v-Hosts aus.
2. Wählen Sie **Aktion > Manager für virtuelleSwitches** aus.



3. Wählen Sie den gewünschten virtuellen Switch aus.

VERBINDUNGSTYP	BESCHREIBUNG
Extern	Ermöglicht virtuellen Computern den Zugriff auf ein physisches Netzwerk, um mit Servern und Clients in einem externen Netzwerk zu kommunizieren. Ermöglicht, dass virtuelle Maschinen auf demselben Hyper-V-Server miteinander kommunizieren können.
Intern	Ermöglicht die Kommunikation zwischen virtuellen Maschinen auf demselben Hyper-V-Server und zwischen den virtuellen Computern und dem Verwaltungs Host Betriebssystem.

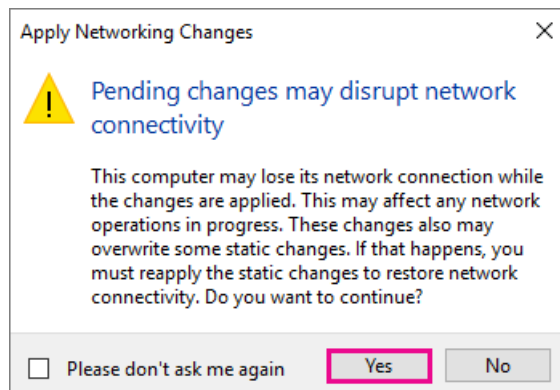
VERBINDUNGSTYP	BESCHREIBUNG
Privat	Ermöglicht nur die Kommunikation zwischen virtuellen Maschinen auf demselben Hyper-V-Server. Ein privates Netzwerk ist vom gesamten externen Netzwerk Datenverkehr auf dem Hyper-V-Server isoliert. Diese Art von Netzwerk ist nützlich, wenn Sie eine isolierte Netzwerkkumgebung wie eine isolierte Test Domäne erstellen müssen.

- Wählen Sie **virtuellen Switch erstellen** aus.
- Fügen Sie einen Namen für den virtuellen Switch hinzu.
- Wenn Sie extern auswählen, wählen Sie den Netzwerkkartens (NIC) aus, den Sie verwenden möchten, sowie alle weiteren Optionen, die in der folgenden Tabelle beschrieben werden.

EINSTELLUNGSNAME	BESCHREIBUNG
Gemeinsames Verwenden dieses Netzwerkkartens für das Verwaltungsbetriebssystem zulassen	Wählen Sie diese Option aus, wenn Sie zulassen möchten, dass der Hyper-V-Host die Verwendung des virtuellen Switches und der NIC bzw. des NIC-Teams mit dem virtuellen Computer gemeinsam verwenden kann. Wenn dieses Feature aktiviert ist, kann der Host jede der Einstellungen verwenden, die Sie für den virtuellen Switch konfigurieren, wie z. B. Quality of Service Einstellungen (QoS), Sicherheitseinstellungen oder andere Features des virtuellen Hyper-V-Switches.
E/A-Virtualisierung mit Einzelstamm (SR-IOV) aktivieren	Wählen Sie diese Option nur aus, wenn Sie zulassen möchten, dass der virtuelle Computer den Switch der virtuellen Maschine umgeht und direkt zur physischen NIC wechselt. Weitere Informationen finden Sie unter Single-root-e/a-Virtualisierung in der Poster-Begleit Referenz: Hyper-V-Netzwerke.

- Wenn Sie Netzwerk Datenverkehr vom Betriebssystem des Verwaltungs-Hyper-V-Hosts oder von anderen virtuellen Computern, die denselben virtuellen Switch verwenden, isolieren möchten, wählen Sie **virtuelle LAN-Identifizierung für Verwaltungsbetriebssystem aktivieren** aus. Sie können die VLAN-ID in eine beliebige Zahl ändern oder die Standardeinstellung überlassen. Dies ist die virtuelle LAN-ID, die vom Verwaltungsbetriebssystem für die gesamte Netzwerkkommunikation über diesen virtuellen Switch verwendet wird.

8. Klicken Sie auf **OK**.
9. Klicken Sie auf **Ja**.



Erstellen eines virtuellen Switches mithilfe von Windows PowerShell

1. Klicken Sie auf dem Windows-Desktop auf die Schaltfläche „Start“, und geben Sie einen beliebigen Teil des Namens **Windows PowerShell** ein.
2. Klicken Sie mit der rechten Maustaste auf Windows PowerShell, und wählen Sie **als Administrator ausführen**.
3. Suchen Sie nach vorhandenen Netzwerkadaptern, indem Sie das Cmdlet "[Get-netadapter](#)" ausführen. Notieren Sie sich den Namen des Netzwerkadapters, den Sie für den virtuellen Switch verwenden möchten.

```
Get-NetAdapter
```

4. Erstellen Sie einen virtuellen Switch mithilfe des Cmdlets [New-VMSwitch](#). Führen Sie beispielsweise den folgenden Befehl aus, um einen externen virtuellen Switch mit dem Namen externalswitch zu erstellen, indem Sie den Ethernet-Netzwerkadapter verwenden und das **Verwaltungs Betriebssystem zulassen, dass dieser Netzwerkadapter** aktiviert ist.

```
New-VMSwitch -name ExternalSwitch -NetAdapterName Ethernet -AllowManagementOS $true
```

Führen Sie den folgenden Befehl aus, um einen internen Switch zu erstellen.

```
New-VMSwitch -name InternalSwitch -SwitchType Internal
```

Führen Sie den folgenden Befehl aus, um einen privaten Switch zu erstellen.

```
New-VMSwitch -name PrivateSwitch -SwitchType Private
```

Erweiterte Windows PowerShell-Skripts, die verbesserte oder neue virtuelle Switchfeatures in Windows Server 2016 abdecken, finden Sie unter [Remote Direct Memory Access und Switch Embedded Teaming](#).

Nächster Schritt

[Erstellen eines virtuellen Computers in Hyper-V](#)

Erstellen eines virtuellen Computers in Hyper-V

09.04.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Erfahren Sie, wie Sie einen virtuellen Computer mit dem Hyper-v-Manager und Windows PowerShell erstellen und welche Optionen beim Erstellen eines virtuellen Computers im Hyper-v-Manager vorhanden sind.

Erstellen eines virtuellen Computers mit dem Hyper-V-Manager

1. Öffnen Sie den **Hyper-V-Manager**.
2. Klicken Sie im Bereich **Aktion** auf **neu**, und klicken Sie dann auf **virtueller Computer**.
3. Klicken Sie im **Assistenten für neue virtuelle Computerauf weiter**.
4. Treffen Sie auf jeder Seite die geeigneten Optionen für den virtuellen Computer. Weitere Informationen finden Sie weiter unten in diesem Thema unter [Optionen für neue virtuelle Maschinen und Standardeinstellungen im Hyper-V-Manager](#).
5. Nachdem Sie Ihre Auswahl auf der Seite **Zusammenfassung** überprüft haben, klicken Sie auf **Fertigstellen**.
6. Klicken Sie im Hyper-V-Manager mit der rechten Maustaste auf den virtuellen Computer, und wählen Sie **verbinden** aus.
7. Wählen Sie im Fenster Verbindung mit dem virtuellen Computer die Option **Aktion** > **starten** aus.

Erstellen eines virtuellen Computers mithilfe von Windows PowerShell

1. Klicken Sie auf dem Windows-Desktop auf die Schaltfläche „Start“, und geben Sie einen beliebigen Teil des Namens **Windows PowerShell** ein.
2. Klicken Sie mit der rechten Maustaste auf **Windows PowerShell**, und wählen Sie **als Administrator ausführen**.
3. Holen Sie sich den Namen des virtuellen Switches, den der virtuelle Computer verwenden soll, mithilfe von [Get-VMSwitch](#). Beispiel:

```
Get-VMSwitch * | Format-Table Name
```

4. Verwenden Sie das Cmdlet [New-VM](#), um den virtuellen Computer zu erstellen. Weitere Informationen finden Sie in den folgenden Beispielen.

NOTE

Wenn Sie diese virtuelle Maschine auf einen Hyper-V-Host mit Windows Server 2012 R2 verschieben können, verwenden Sie den Parameter-Version mit [New-VM](#) , um die Konfigurations Version der virtuellen Maschine auf 5 festzulegen. Die standardmäßige VM-Konfigurations Version für Windows Server 2016 wird von Windows Server 2012 R2 oder früheren Versionen nicht unterstützt. Nachdem der virtuelle Computer erstellt wurde, können Sie die Konfigurations Version des virtuellen Computers nicht mehr ändern. Weitere Informationen finden Sie [unter Unterstützte Konfigurations Versionen für virtuelle Computer](#).

- **Vorhandene virtuelle Festplatte** : um einen virtuellen Computer mit einer vorhandenen virtuellen Festplatte zu erstellen, können Sie den folgenden Befehl verwenden:
 - **-Name** ist der Name, den Sie für den virtuellen Computer angeben, den Sie erstellen.
 - **-MemoryStartupBytes** ist die Menge an Arbeitsspeicher, die dem virtuellen Computer beim Start zur Verfügung steht.
 - **-BootDevice** ist das Gerät, mit dem der virtuelle Computer gestartet wird, wenn er mit dem Netzwerkadapter (Network Adapter) oder der virtuellen Festplatte (VHD) gestartet wird.
 - **-VhdpPath** ist der Pfad zu dem virtuellen Computer Datenträger, den Sie verwenden möchten.
 - **-Path** ist der Pfad zum Speichern der Konfigurationsdateien der virtuellen Maschine.
 - **-Generierung** ist die Generation der virtuellen Maschine. Verwenden Sie Generation 1 für VHD und Generation 2 für vhdx. Weitere Informationen finden Sie [unter sollte ich einen virtuellen Computer der Generation 1 oder 2 in Hyper-V erstellen?](#).
 - **-"Switch "** ist der Name des virtuellen Switches, den der virtuelle Computer für die Verbindung mit anderen virtuellen Computern oder dem Netzwerk verwenden soll. Weitere Informationen finden Sie unter [Erstellen eines virtuellen Switches für virtuelle Hyper-V-Computer](#).

```
New-VM -Name <Name> -MemoryStartupBytes <Memory> -BootDevice <BootDevice> -VHDPATH  
<VHDPATH> -Path <Path> -Generation <Generation> -Switch <SwitchName>
```

Beispiel:

```
New-VM -Name Win10VM -MemoryStartupBytes 4GB -BootDevice VHD -VHDPATH .\VMs\Win10.vhdx -  
Path .\VMData -Generation 2 -Switch ExternalSwitch
```

Dadurch wird ein virtueller Computer der Generation 2 mit dem Namen Win10VM und 4 GB Arbeitsspeicher erstellt. Er startet aus dem Ordner "vms\win10.vhdx" im aktuellen Verzeichnis und verwendet den virtuellen Switch "externalswitch". Die Konfigurationsdateien der virtuellen Maschine werden im Ordner vmdata gespeichert.

- **Neue virtuelle Festplatte** : um einen virtuellen Computer mit einer neuen virtuellen Festplatte zu erstellen, ersetzen Sie den Parameter **"-vhdpPath"** aus dem obigen Beispiel durch **"-newvhdpPath"** , und fügen Sie den Parameter **"-newvhdsizesizebytes"** hinzu. Beispiel:

```
New-VM -Name Win10VM -MemoryStartupBytes 4GB -BootDevice VHD -NewVHDPATH .\VMs\Win10.vhdx -Path  
.\VMData -NewVHDSizesizeBytes 20GB -Generation 2 -Switch ExternalSwitch
```

- **Neue virtuelle Festplatte, die mit dem Betriebssystem Abbild gestartet wird**: um einen virtuellen Computer mit einem neuen virtuellen Datenträger zu erstellen, der zu einem

Betriebssystem Abbild gestartet wird, finden Sie weitere Informationen im PowerShell-Beispiel unter Exemplarische Vorgehensweise: Erstellen eines virtuellen Computers unter [Windows 10](#).

5. Starten Sie den virtuellen Computer mithilfe des Cmdlets [Start-VM](#) . Führen Sie das folgende Cmdlet aus, wobei Name der Name des virtuellen Computers ist, den Sie erstellt haben.

```
Start-VM -Name <Name>
```

Beispiel:

```
Start-VM -Name Win10VM
```

6. Stellen Sie mithilfe der Verbindung mit virtuellen Computern (VMConnect) eine Verbindung mit dem virtuellen Computer her.

```
VMConnect.exe
```

Optionen im Assistenten für neue virtuelle Computer im Hyper-V-Manager

In der folgenden Tabelle sind die Optionen aufgeführt, die Sie auswählen können, wenn Sie einen virtuellen Computer im Hyper-V-Manager erstellen, und die Standardeinstellungen.

SEITE	STANDARD FÜR WINDOWS SERVER 2016 UND WINDOWS 10	WEITERE OPTIONEN
Name und Pfad angeben	Name: neuer virtueller Computer. Speicherort: c:\ProgramData\Microsoft\Windows\Hyper-v\ .	Sie können auch einen eigenen Namen eingeben und einen anderen Speicherort für den virtuellen Computer auswählen. Hier werden die Konfigurationsdateien für den virtuellen Computer gespeichert.
Generation angeben	Erste Generation	Sie können auch einen virtuellen Computer der Generation 2 erstellen. Weitere Informationen finden Sie unter sollte ich einen virtuellen Computer der Generation 1 oder 2 in Hyper-V erstellen? .
Speicher zuweisen	Start Speicher: 1024 MB Dynamischer Arbeitsspeicher: nicht ausgewählt	Sie können den Start Speicher von 32 MB auf 5902mb festlegen. Sie können auch dynamischer Arbeitsspeicher verwenden. Weitere Informationen finden Sie unter Übersicht über Hyper-V-dynamischer Arbeitsspeicher .

SEITE	STANDARD FÜR WINDOWS SERVER 2016 UND WINDOWS 10	WEITERE OPTIONEN
Netzwerk konfigurieren	Nicht verbunden	Sie können eine Netzwerkverbindung für die virtuelle Maschine aus einer Liste vorhandener virtueller Switches auswählen. Weitere Informationen finden Sie unter Erstellen eines virtuellen Switches für virtuelle Hyper-V-Computer .
Virtuelle Festplatte verbinden	Virtuelle Festplatte erstellen Name: <VMName>.vhdx Speicherort: c:\Users\Public\Documents\Hyper-v\virtuelle Festplatten\ Größe: 127 GB	Sie können auch eine vorhandene virtuelle Festplatte verwenden oder warten und eine virtuelle Festplatte später anfügen.
Installationsoptionen	Betriebssystem später installieren	Mit diesen Optionen wird die Start Reihenfolge des virtuellen Computers geändert, sodass Sie die Installation über eine ISO-Datei, eine startbare Diskette oder einen netzwerkinstallationsdienst wie die Windows-Bereitstellungs Dienste (WDS) Durchführung können.
Zusammenfassung	Zeigt die Optionen an, die Sie ausgewählt haben, damit Sie sicherstellen können, dass Sie korrekt sind. -Name -Generierung -Arbeitsspeicher -Netzwerk -Festplatte -Betriebs System	Tipp: Sie können die Zusammenfassung von der Seite kopieren und in e-Mail oder an einer anderen Stelle einfügen, um die Nachverfolgung der virtuellen Computer zu unterstützen.

Siehe auch

- [New-VM](#)
- [Unterstützte Konfigurations Versionen für virtuelle Computer](#)
- [Soll ich in Hyper-V einen virtuellen Computer der 1. oder der 2. Generation erstellen?](#)
- [Erstellen eines virtuellen Switches für Hyper-V-VMs](#)

Planen von Hyper-V unter Windows Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows Server 2019

Verwenden Sie diese Ressourcen, um Ihre Hyper-V-Bereitstellung zu planen.

- [Hyper-V-Skalierbarkeit in Windows Server](#)
- [Hyper-V-Sicherheit in Windows Server](#)
- [Netzwerke in Windows Server](#)
- [Sollte ich einen virtuellen Computer der Generation 1 oder 2 erstellen?](#)
- [Planen der GPU-Beschleunigung in Windows Server](#)
- [Planen der Bereitstellung von Geräten mit diskreter Geräte Zuweisung](#)

Sollte ich einen virtuellen Computer der Generation 1 oder 2 in Hyper-V erstellen?

09.04.2020 • 19 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

NOTE

Wenn Sie virtuelle Windows-Computer (VMS) aus einer lokalen Umgebung in Microsoft Azure hochladen möchten, werden VMS der Generation 1 und der Generation 2 im VHD-Dateiformat unterstützt, die einen Datenträger mit fester Größe aufweisen. Weitere Informationen zu den in Azure unterstützten Funktionen der Generation 2 finden Sie unter [VMS der Generation 2](#) in Azure. Weitere Informationen zum Hochladen einer Windows-VHD- oder vhdx-Datei finden Sie unter [Vorbereiten einer Windows-VHD oder vhdx zum Hochladen in Azure](#).

Die Entscheidung, einen virtuellen Computer der Generation 1 oder 2 zu erstellen, hängt von dem Gast Betriebssystem ab, das Sie installieren möchten, und von der Start Methode, die Sie zum Bereitstellen der virtuellen Maschine verwenden möchten. Es wird empfohlen, einen virtuellen Computer der Generation 2 zu erstellen, um Funktionen wie den sicheren Start zu nutzen, es sei denn, eine der folgenden Anweisungen ist true:

- Die VHD, die Sie starten möchten, ist nicht [UEFI-kompatibel](#).
- Generation 2 unterstützt nicht das Betriebssystem, das Sie auf dem virtuellen Computer ausführen möchten.
- Generation 2 unterstützt die gewünschte Start Methode nicht.

Weitere Informationen zu den Features, die mit virtuellen Computern der Generation 2 verfügbar sind, finden Sie unter [Hyper-V-Funktions Kompatibilität nach Generierung und Gast](#).

Die Generierung eines virtuellen Computers kann nach dem Erstellen nicht mehr geändert werden. Daher wird empfohlen, dass Sie die Überlegungen hier überprüfen und das Betriebssystem, die Start Methode und die Features auswählen, die Sie verwenden möchten, bevor Sie eine Generation auswählen.

Welche Gast Betriebssysteme werden unterstützt?

Virtuelle Computer der Generation 1 unterstützen die meisten Gast Betriebssysteme. Virtuelle Computer der Generation 2 unterstützen die meisten 64-Bit-Versionen von Windows und höhere Versionen von Linux- und FreeBSD-Betriebssystemen. Verwenden Sie die folgenden Abschnitte, um zu sehen, welche Generation des virtuellen Computers das Gast Betriebssystem unterstützt, das Sie installieren möchten.

- [Unterstützung für Windows-Gast Betriebssysteme](#)
- [Unterstützung von CentOS und Red Hat Enterprise Linux Gastbetriebssystemen](#)
- [Unterstützung für Debian-Gast Betriebssystem](#)
- [Unterstützung für FreeBSD-Gast Betriebssysteme](#)
- [Unterstützung für Oracle Linux Gast Betriebssystem](#)
- [Unterstützung für SUSE-Gast Betriebssysteme](#)
- [Unterstützung für Ubuntu-Gast Betriebssysteme](#)

Unterstützung für Windows-Gast Betriebssysteme

In der folgenden Tabelle wird gezeigt, welche 64-Bit-Versionen von Windows als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwendet werden können.

64-BIT-VERSIONEN VON WINDOWS	ERSTE GENERATION	ZWEITE GENERATION
Windows Server 2019	✓	✓
Windows Server 2016	✓	✓
Windows Server 2012 R2	✓	✓
Windows Server 2012	✓	✓
Windows Server 2008 R2	✓	✗
WindowsServer 2008	✓	✗
Windows 10	✓	✓
Windows 8.1	✓	✓
Windows 8	✓	✓
Windows 7	✓	✗

In der folgenden Tabelle wird gezeigt, welche 32-Bit-Versionen von Windows als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwendet werden können.

32-BIT-VERSIONEN VON WINDOWS	ERSTE GENERATION	ZWEITE GENERATION
Windows 10	✓	✗
Windows 8.1	✓	✗
Windows 8	✓	✗
Windows 7	✓	✗

Unterstützung von CentOS und Red Hat Enterprise Linux Gastbetriebssystemen

Die folgende Tabelle zeigt, welche Versionen von Red Hat Enterprise Linux (RHEL) und CentOS als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwendet werden können.

BETRIEBSSYSTEMVERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
RHEL/CentOS 7. x-Serie	✓	✓
RHEL/CentOS 6. x-Reihe	✓	✓ Hinweis: Wird nur unter Windows Server 2016 und höher unterstützt.
RHEL/CentOS 5. x-Reihe	✓	✗

Weitere Informationen finden Sie unter [CentOS und Red Hat Enterprise Linux von virtuellen Computern auf Hyper-V](#).

Unterstützung für Debian-Gast Betriebssystem

Die folgende Tabelle zeigt, welche Versionen von Debian als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwendet werden können.

BETRIEBSSYSTEMVERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
Debian 7. x-Reihe	✓	✗
Debian 8. x-Reihe	✓	✓

Weitere Informationen finden Sie unter [virtuelle Debian-Computer auf Hyper-V](#).

Unterstützung für FreeBSD-Gast Betriebssysteme

In der folgenden Tabelle sind die Versionen von FreeBSD aufgeführt, die Sie als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwenden können.

BETRIEBSSYSTEMVERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
FreeBSD 10 und 10,1	✓	✗
FreeBSD 9,1 und 9,3	✓	✗
FreeBSD 8,4	✓	✗

Weitere Informationen finden Sie unter [FreeBSD Virtual Machines on Hyper-V](#).

Unterstützung für Oracle Linux Gast Betriebssystem

In der folgenden Tabelle ist aufgeführt, welche Versionen der red hat-kompatiblen Kernel Serie Sie als Gast Betriebssystem für virtuelle Computer der Generation 1 und Generation 2 verwenden können.

RED HAT-KOMPATIBLE KERNEL REIHEN VERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
Oracle Linux 7. x-Serie	✓	✓
Oracle Linux 6. x-Reihe	✓	✗

Die folgende Tabelle zeigt, welche Versionen von nicht breakable Enterprise Kernel Sie als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwenden können.

NICHT BREAKABLE ENTERPRISE KERNEL (UEK)-VERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
Oracle Linux UEK R3 QU3	✓	✗
Oracle Linux UEK R3 QU2	✓	✗
Oracle Linux UEK R3 QU1	✓	✗

Weitere Informationen finden Sie unter [Oracle Linux Virtual Machines on Hyper-V](#).

Unterstützung für SUSE-Gast Betriebssysteme

Die folgende Tabelle zeigt, welche SUSE-Versionen Sie als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwenden können.

BETRIEBSSYSTEMVERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
SUSE Linux Enterprise Server 12-Serie	✓	✓
SUSE Linux Enterprise Server 11-Serie	✓	✗
Öffnen Sie SuSE 12,3.	✓	✗

Weitere Informationen finden Sie unter [SUSE Virtual Machines on Hyper-V](#).

Unterstützung für Ubuntu-Gast Betriebssysteme

Die folgende Tabelle zeigt, welche Versionen von Ubuntu Sie als Gast Betriebssystem für virtuelle Maschinen der Generation 1 und Generation 2 verwenden können.

BETRIEBSSYSTEMVERSIONEN	ERSTE GENERATION	ZWEITE GENERATION
Ubuntu 14,04 und höhere Versionen	✓	✓
Ubuntu 12.04	✓	✗

Weitere Informationen finden Sie unter [Ubuntu Virtual Machines on Hyper-V](#).

Wie kann ich den virtuellen Computer starten?

Die folgende Tabelle zeigt, welche Startmethoden von virtuellen Maschinen der Generation 1 und der Generation 2 unterstützt werden.

START METHODE	ERSTE GENERATION	ZWEITE GENERATION
PXE-Start mithilfe einer standardmäßigen Netzwerkkarte	✗	✓
PXE-Start mithilfe eines Legacy-Netzwerkkadapters	✓	✗
Starten von einer virtuellen SCSI-Festplatte (. Vhdx) oder virtuelle DVD (. ISO)	✗	✓
Starten von der virtuellen Festplatte des IDE-Controllers (. VHD) oder virtuelle DVD (. ISO)	✓	✗
Start von Diskette (. VFD)	✓	✗

Was sind die Vorteile der Verwendung von virtuellen Computern der Generation 2?

Im folgenden finden Sie einige der Vorteile, die Sie bei der Verwendung eines virtuellen Computers der Generation 2 erhalten:

- **Sicherer Start** Dies ist ein Feature, mit dem überprüft wird, ob das Start Lade Paket von einer vertrauenswürdigen Zertifizierungsstelle in der UEFI-Datenbank signiert ist, um zu verhindern, dass nicht autorisierte Firmware, Betriebssysteme oder UEFI-Treiber zur Startzeit ausgeführt werden. Der sichere Start ist standardmäßig bei virtuellen Computern der Generation 2 aktiviert. Wenn Sie ein Gast Betriebssystem ausführen müssen, das vom sicheren Start nicht unterstützt wird, können Sie es nach der Erstellung des virtuellen Computers deaktivieren. Weitere Informationen finden Sie unter [Sicherer Start](#).

Zum Sichern von virtuellen Linux-Computern der Start Generation müssen Sie die Vorlage für den sicheren Start der UEFI-Zertifizierungsstelle auswählen, wenn Sie den virtuellen Computer erstellen.

- **Größeres Start Volume** Das maximale Start Volume für virtuelle Maschinen der Generation 2 beträgt 64 TB. Dies ist die maximale Datenträger Größe, die von einem unterstützt wird. VHDX. Bei virtuellen Computern der Generation 1 beträgt das maximale Start Volume 2 TB für ein. Vhdx und 2040gb für ein. VHD. Weitere Informationen finden Sie unter [Übersicht über die Hyper-V-Format für virtuelle Festplatten](#).

Sie können auch eine geringfügige Verbesserung der Start-und Installationszeiten virtueller Maschinen mit virtuellen Computern der Generation 2 festzustellen.

Worin besteht der Unterschied bei der Geräte Unterstützung?

In der folgenden Tabelle werden die verfügbaren Geräte zwischen virtuellen Maschinen der Generation 1 und der Generation 2 verglichen.

GERÄT DER GENERATION 1	ERSATZ DER GENERATION 2	ERWEITERUNGEN DER GENERATION 2
IDE-Controller	Virtueller SCSI-Controller	Start über .vhdx (max. Größe 64 TB und Onlinegrößenänderungs-Funktionalität).
IDE-CD-ROM	Virtuelle SCSI-CD-ROM	Unterstützung für bis zu 64 SCSI-DVD-Geräte pro SCSI-Controller.
Legacy-BIOS	UEFI-Firmware	Sicherer Start
Ältere Netzwerkkarte	Synthetischer Netzwerkadapter	Netzwerkstart mit IPv4 und IPv6
Disketten- und DMA-Controller	Keine Diskettencontrollerunterstützung	N/V
UART (Universal Asynchronous Receiver/Transmitter, universeller asynchroner Empfänger/Übermittler) für COM-Ports	Optionaler UART zwecks Debugging	Schneller und zuverlässiger
i8042-Tastaturcontroller	Softwarebasierte Eingabe	Beansprucht aufgrund der nicht vorhandenen Emulation weniger Ressourcen. Verkleinert zudem die Angriffsfläche vom Gastbetriebssystem.
PS/2-Tastatur	Softwarebasierte Tastatur	Beansprucht aufgrund der nicht vorhandenen Emulation weniger Ressourcen. Verkleinert zudem die Angriffsfläche vom Gastbetriebssystem.

GERÄT DER GENERATION 1	ERSATZ DER GENERATION 2	ERWEITERUNGEN DER GENERATION 2
PS/2-Maus	Softwarebasierte Maus	Beansprucht aufgrund der nicht vorhandenen Emulation weniger Ressourcen. Verkleinert zudem die Angriffsfläche vom Gastbetriebssystem.
S3-Video	Softwarebasiertes Video	Beansprucht aufgrund der nicht vorhandenen Emulation weniger Ressourcen. Verkleinert zudem die Angriffsfläche vom Gastbetriebssystem.
PCI-Bus	Nicht mehr erforderlich	N/V
Programmierbarer Interruptcontroller (Programmable interrupt controller, PIC)	Nicht mehr erforderlich	N/V
Programmierbarer Intervallzeitgeber (Programmable interval timer, PIT)	Nicht mehr erforderlich	N/V
Super-E/A-Gerät	Nicht mehr erforderlich	N/V

Weitere Informationen zu virtuellen Maschinen der Generation 2

Hier finden Sie einige zusätzliche Tipps zur Verwendung virtueller Computer der Generation 2.

Anfügen oder Hinzufügen eines DVD-Laufwerks

- Sie können ein physisches CD-oder DVD-Laufwerk nicht an einen virtuellen Computer der Generation 2 anfügen. Das virtuelle DVD-Laufwerk in virtuellen Computern der Generation 2 unterstützt nur ISO-Imagedateien. Zum Erstellen einer ISO-Imagedatei einer Windows-Umgebung können Sie das Befehlszeilentool `Oscdimg` verwenden. Weitere Informationen finden Sie unter [Befehlszeilenoptionen von Oscdimg](#).
- Wenn Sie einen neuen virtuellen Computer mit dem Windows PowerShell-Cmdlet "New-VM" erstellen, verfügt der virtuelle Computer der Generation 2 über kein DVD-Laufwerk. Sie können ein DVD-Laufwerk hinzufügen, während der virtuelle Computer ausgeführt wird.

UEFI-Firmware verwenden

- Der sichere Start oder UEFI-Firmware ist auf dem physischen Hyper-V-Host nicht erforderlich. Hyper-v stellt virtuelle Maschinen für virtuelle Maschinen bereit, die unabhängig von den auf dem Hyper-v-Host sind.
- UEFI-Firmware auf einem virtuellen Computer der Generation 2 unterstützt den Setup Modus für den sicheren Start nicht.
- Das Ausführen einer UEFI-Shell oder anderer UEFI-Anwendungen auf einem virtuellen Computer der Generation 2 wird nicht unterstützt. Die Verwendung einer Microsoft-fremden UEFI-Shell oder von UEFI-Anwendungen ist technisch zwar möglich, wenn sie direkt von den Quellen kompiliert werden. Wenn diese Anwendungen nicht ordnungs entsprechend digital signiert sind, müssen Sie den sicheren Start für den virtuellen Computer deaktivieren.

Arbeiten mit vhdx-Dateien

- Sie können die Größe einer vhdx-Datei ändern, die das Start Volume für einen virtuellen Computer der Generation 2 enthält, während der virtuelle Computer ausgeführt wird.
- Die Erstellung einer vhdx-Datei, die auf virtuellen Computern der Generation 1 und der Generation 2 gestartet werden kann, wird nicht unterstützt oder empfohlen.
- Die Generation des virtuellen Computers ist eine Eigenschaft des virtuellen Computers und keine Eigenschaft

der virtuellen Festplatte. Daher können Sie nicht feststellen, ob eine vhdx-Datei von einem virtuellen Computer der Generation 1 oder der Generation 2 erstellt wurde.

- Eine mit einem virtuellen Computer der Generation 2 erstellte vhdx-Datei kann an den IDE-Controller oder den SCSI-Controller eines virtuellen Computers der Generation 1 angefügt werden. Wenn es sich jedoch um eine startbare vhdx-Datei handelt, wird der virtuelle Computer der Generation 1 nicht gestartet.

Verwenden von IPv6 anstelle von IPv4

Virtuelle Computer der Generation 2 verwenden standardmäßig IPv4. Um stattdessen IPv6 zu verwenden, führen Sie das Windows PowerShell-Cmdlet [Set-vmfirmware](#) aus. Mit dem folgenden Befehl wird beispielsweise das bevorzugte Protokoll für einen virtuellen Computer namens "testvm" auf IPv6 festgelegt:

```
Set-VMFirmware -VMName TestVM -IPProtocolPreference IPv6
```

Hinzufügen eines COM-Ports für das Kernel Debugging

COM-Ports sind auf virtuellen Computern der Generation 2 nicht verfügbar, bis Sie sie hinzufügen. Hierfür können Sie Windows PowerShell oder Windows-Verwaltungsinstrumentation (WMI) verwenden. Diese Schritte zeigen, wie Sie dies mit Windows PowerShell durchführen können.

So fügen Sie einen COM-Port hinzu:

1. Deaktivieren Sie den sicheren Start. Das Kernel Debugging ist mit dem sicheren Start nicht kompatibel. Stellen Sie sicher, dass der virtuelle Computer ausgeschaltet ist, und verwenden Sie dann das Cmdlet [Set-vmfirmware](#). Beispielsweise deaktiviert der folgende Befehl den sicheren Start auf dem virtuellen Computer "testvm":

```
Set-VMFirmware -Vmname TestVM -EnableSecureBoot Off
```

2. Fügen Sie einen COM-Port hinzu. Verwenden Sie hierfür das Cmdlet [Set-vmcomport](#). Mit dem folgenden Befehl wird z. B. der erste com-Port auf dem virtuellen Computer "testvm" konfiguriert, um eine Verbindung mit dem Named Pipe "testpipe" auf dem lokalen Computer herzustellen:

```
Set-VMComPort -VMName TestVM 1 \\.\pipe\TestPipe
```

NOTE

Konfigurierte COM-Ports sind nicht in den Einstellungen eines virtuellen Computers im Hyper-V-Manager aufgeführt.

Weitere Informationen

- [Virtuelle Linux- und FreeBSD Computer unter Hyper-V](#)
- [Verwenden von lokalen Ressourcen auf einem virtuellen Hyper-V-Computer mit VMConnect](#)
- [Planen der Hyper-V-Skalierbarkeit in Windows Server 2016](#)

Planen der Hyper-V-Netzwerke in Windows Server

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Microsoft Hyper-V Server 2016, Windows Server 2016, Microsoft Hyper-V Server 2019, Windows Server 2019

Ein grundlegendes Verständnis von Netzwerken in Hyper-V hilft Ihnen beim Planen von Netzwerken für virtuelle Computer. Außerdem werden in diesem Artikel einige Netzwerk Aspekte bei der Verwendung der Live Migration und bei Verwendung von Hyper-V mit anderen Serverfunktionen und-Rollen behandelt.

Grundlagen zum Hyper-V-Netzwerk

Grundlegende Netzwerke in Hyper-V sind recht einfach. Es verwendet zwei Teile: einen virtuellen Switch und einen virtuellen Netzwerkadapter. Sie benötigen mindestens eine von jedem, um Netzwerke für einen virtuellen Computer einzurichten. Der virtuelle Switch stellt eine Verbindung mit einem beliebigen Ethernet-basierten Netzwerk her. Der virtuelle Netzwerkadapter stellt eine Verbindung mit einem Port auf dem virtuellen Switch her, sodass ein virtueller Computer ein Netzwerk verwenden kann.

Die einfachste Möglichkeit zum Einrichten von grundlegenden Netzwerken besteht darin, einen virtuellen Switch zu erstellen, wenn Sie Hyper-V installieren. Wenn Sie dann einen virtuellen Computer erstellen, können Sie ihn mit dem Switch verbinden. Beim Herstellen einer Verbindung mit dem Switch wird dem virtuellen Computer automatisch ein virtueller Netzwerkadapter hinzugefügt. Anweisungen hierzu finden Sie unter [Erstellen eines virtuellen Switches für virtuelle Hyper-V-Computer](#).

Um unterschiedliche Netzwerktypen zu verarbeiten, können Sie virtuelle Switches und virtuelle Netzwerkadapter hinzufügen. Alle Switches sind Teil des Hyper-V-Hosts, aber jeder virtuelle Netzwerkadapter gehört nur einem virtuellen Computer an.

Bei dem virtuellen Switch handelt es sich um einen softwarebasierten Schicht-2-Ethernet-Netzwerk Switch. Es bietet integrierte Funktionen zum überwachen, Steuern und Segmentieren von Datenverkehr sowie zur Sicherheit und Diagnose. Sie können dem Satz integrierter Funktionen hinzufügen, indem Sie Plug-ins installieren, die auch als *Erweiterungen* bezeichnet werden. Diese sind für unabhängige Softwarehersteller verfügbar. Weitere Informationen zu Switch und Erweiterungen finden Sie unter [virtueller Hyper-V-Switch](#).

Optionen für Switch und Netzwerkadapter

Hyper-V bietet drei Arten von virtuellen Switches und zwei Arten von virtuellen Netzwerkadaptern. Wählen Sie aus, welche der beiden Optionen bei der Erstellung ausgewählt werden sollen. Sie können Hyper-v-Manager oder das Hyper-v-Modul für Windows PowerShell verwenden, um virtuelle Switches und virtuelle Netzwerkadapter zu erstellen und zu verwalten. Einige erweiterte Netzwerkfunktionen wie erweiterte Port-Zugriffs Steuerungs Listen (Access Control Lists, ACLs) können nur mithilfe von Cmdlets im Hyper-V-Modul verwaltet werden.

Sie können einige Änderungen an einem virtuellen Switch oder virtuellen Netzwerkadapter vornehmen, nachdem Sie ihn erstellt haben. Beispielsweise ist es möglich, einen vorhandenen Switch in einen anderen Typ zu ändern, dies wirkt sich jedoch auf die Netzwerkfunktionen aller virtuellen Computer aus, die mit diesem Switch verbunden sind. Dies geschieht wahrscheinlich nicht, es sei denn, Sie haben einen Fehler gemacht oder müssen etwas testen. Ein weiteres Beispiel: Sie können einen virtuellen Netzwerkadapter mit einem anderen Switch verbinden, was Sie möglicherweise tun, wenn Sie eine Verbindung mit einem anderen Netzwerk herstellen möchten. Es ist jedoch nicht möglich, einen virtuellen Netzwerkadapter von einem Typ in einen anderen zu ändern. Anstatt den Typ zu ändern, fügen Sie einen weiteren virtuellen Netzwerkadapter hinzu, und wählen Sie den entsprechenden Typ aus.

Die Typen virtueller Switches lauten:

- **Externer virtueller Switch** : stellt eine Verbindung mit einem verkabelten, physischen Netzwerk her, indem es an einen physischen Netzwerkkadapter gebunden wird.
- **Interner virtueller Switch** : stellt eine Verbindung mit einem Netzwerk her, das nur von den virtuellen Maschinen auf dem Host mit dem virtuellen Switch und zwischen dem Host und den virtuellen Maschinen verwendet werden kann.
- **Privater virtueller Switch** : stellt eine Verbindung mit einem Netzwerk her, das nur von den virtuellen Maschinen verwendet werden kann, die auf dem Host ausgeführt werden und über den virtuellen Switch verfügen, aber keine Netzwerkverbindungen zwischen dem Host und den virtuellen Maschinen bereitstellen.

Typen von virtuellen Netzwerkkadaptern:

- **Hyper-V-spezifischer Netzwerkkadapter** : verfügbar für virtuelle Computer der Generation 1 und der Generation 2. Sie wurde speziell für Hyper-v entwickelt und erfordert einen Treiber, der in Hyper-v-Integrationsdiensten enthalten ist. Diese Art von Netzwerkkadapter ist schneller und wird empfohlen, es sei denn, Sie müssen im Netzwerk starten oder ein nicht unterstütztes Gast Betriebssystem ausführen. Der erforderliche Treiber wird nur für unterstützte Gast Betriebssysteme bereitgestellt. Beachten Sie, dass dieser Typ im Hyper-V-Manager und in den Netzwerk-Cmdlets nur als Netzwerkkadapter bezeichnet wird.
- **Legacy-Netzwerkkadapter** : nur in virtuellen Computern der Generation 1 verfügbar. Emuliert einen Intel 21140-basierten PCI-Fast-Ethernet-Adapter und kann verwendet werden, um in einem Netzwerk zu starten, sodass Sie ein Betriebssystem von einem Dienst wie Windows-Bereitstellungs Dienste installieren können.

Hyper-V-Netzwerke und zugehörige Technologien

Die neuesten Versionen von Windows Server enthalten Verbesserungen, die Ihnen weitere Optionen zum Konfigurieren des Netzwerks für Hyper-V zur Verfügung stehen. Windows Server 2012 führte z. B. Unterstützung für konvergierte Netzwerke ein. Auf diese Weise können Sie Netzwerk Datenverkehr über einen externen virtuellen Switch weiterleiten. Windows Server 2016 baut darauf auf, indem der Remote Zugriff auf den direkten Speicher (RDMA) auf Netzwerkkadaptern zugelassen wird, die an einen virtuellen Hyper-V-Switch gebunden sind. Sie können diese Konfiguration entweder mit oder ohne Switch Embedded Teaming (Set) verwenden. Weitere Informationen finden Sie [unter Remote Direct Memory \(Access\) RDMA und Switch Embedded Teaming \(Set\)](#) .

Einige Features basieren auf bestimmten Netzwerkkonfigurationen oder unter bestimmten Konfigurationen besser. Beachten Sie diese Punkte beim Planen oder Aktualisieren der Netzwerkinfrastruktur.

Failoverclustering : Es empfiehlt sich, den Cluster Datenverkehr zu isolieren und Hyper-V-Quality of Service (QoS) auf dem virtuellen Switch zu verwenden. Weitere Informationen finden Sie unter [Netzwerk Empfehlungen für einen Hyper-V-Cluster](#) .

Live Migration : Verwenden Sie Leistungsoptionen, um die Netzwerk- und CPU-Auslastung zu reduzieren und die Zeit, die zum Durchführen einer Live Migration benötigt wird. Anweisungen finden Sie unter [Einrichten von Hosts für die Live Migration ohne Failoverclustering](#).

Direkte Speicherplätze : dieses Feature basiert auf dem SMB 3.0-Netzwerkprotokoll und RDMA. Weitere Informationen finden Sie unter [direkte Speicherplätze in Windows Server 2016](#).

Planen der Hyper-V-Skalierbarkeit in Windows Server 2016 und Windows Server 2019

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows Server 2019

Dieser Artikel enthält Details zur maximalen Konfiguration für Komponenten, die Sie auf einem Hyper-V-Host oder seinen virtuellen Maschinen hinzufügen und entfernen können, z. b. virtuelle Prozessoren oder Prüfpunkte. Berücksichtigen Sie beim Planen der Bereitstellung die Höchstwerte, die für die einzelnen virtuellen Computer gelten, sowie die für den Hyper-V-Host geltenden Höchstwerte.

Maximums für Arbeitsspeicher und logische Prozessoren sind die größten Steigerungen von Windows Server 2012 als Reaktion auf Anforderungen zur Unterstützung von neueren Szenarien wie Machine Learning und Datenanalyse. Der Windows Server-Blog veröffentlichte vor kurzem die Leistungsergebnisse eines virtuellen Computers mit 5,5 Terabyte Arbeitsspeicher und 128 virtuellen Prozessoren mit einer in-Memory Database von 4 TB. Die Leistung war größer als 95% der Leistung eines physischen Servers. Weitere Informationen finden Sie unter [Windows Server 2016 Hyper-V-VM-Leistung in großem Maßstab für die Verarbeitung im Arbeitsspeicher](#). Andere Zahlen ähneln denen für Windows Server 2012. (Maximums für Windows Server 2012 R2 waren identisch mit Windows Server 2012.)

NOTE

Weitere Informationen zu System Center Virtual Machine Manager (VMM) finden Sie unter [Virtual Machine Manager](#). VMM ist ein Microsoft-Produkt zur Verwaltung virtualisierter Datacenter, das separat verkauft wird.

Maximums für virtuelle Maschinen

Diese Höchstwerte gelten für jeden virtuellen Computer. Nicht alle Komponenten sind in beiden Generationen virtueller Computer verfügbar. Einen Vergleich der Generationen finden Sie unter [sollte ich einen virtuellen Computer der Generation 1 oder 2 in Hyper-V erstellen?](#)

KOMPONENTE	MAXIMUM	HINWEISE
Prüfpunkte	50	Der tatsächliche Wert kann in Abhängigkeit vom verfügbaren Speicher niedriger sein. Jeder Prüfpunkt wird als AVHD-Datei gespeichert, die physischen Speicher verwendet.
Arbeitsspeicher	12 TB für Generation 2; 1 TB für Generation 1	Überprüfen Sie die Anforderungen für das jeweilige Betriebssystem, um den Mindestwert und den empfohlenen Wert zu bestimmen.
Serielle (COM-) Anschlüsse	2	None.
Größe von direkt an einen virtuellen Computer angeschlossenen physischen Datenträgern	Variiert	Die maximale Größe hängt vom Gastbetriebssystem ab.

KOMPONENTE	MAXIMUM	HINWEISE
Virtuelle Fibre Channel-Adapter	4	Es empfiehlt sich, jeden Fibre Channel-Adapter mit einem unterschiedlichen virtuellen SAN zu verbinden.
Virtuelle Diskettenlaufwerke	1 virtuelles Diskettenlaufwerk	None.
Kapazität virtueller Festplatten	64 TB für vhdx-Format; 2040 GB für VHD-Format	Jede virtuelle Festplatte wird auf physischen Medien in Abhängigkeit des durch die virtuelle Festplatte verwendeten Formats als VHDX- oder VHD-Datei unterstützt.
Virtuelle IDE-Datenträger	4	Der Start Datenträger (manchmal als Start Datenträger bezeichnet) muss an eines der IDE-Geräte angeschlossen werden. Beim Startdatenträger kann es sich entweder um eine virtuelle Festplatte oder um einen physischen Datenträger, der an einen virtuellen Computer angeschlossen ist, handeln.
Virtuelle Prozessoren	240 für Generation 2; 64 für Generation 1; 320 verfügbar für das Host Betriebssystem (Stamm Partition)	Die Anzahl der von einem Gastbetriebssystem unterstützten virtuellen Prozessoren kann niedriger sein. Weitere Informationen finden Sie in den Informationen, die für das jeweilige Betriebssystem veröffentlicht wurden.
Virtuelle SCSI-Controller	4	Die Verwendung von virtuellen SCSI-Geräten erfordert Integration Services, die für unterstützte Gast Betriebssysteme verfügbar sind. Ausführliche Informationen dazu, welche Betriebssysteme unterstützt werden, finden Sie unter Unterstützte virtuelle Linux-und FreeBSD -Computer und unterstützte Windows-Gast Betriebssysteme .
Virtuelle SCSI-Datenträger	256	Jeder SCSI-Controller unterstützt maximal 64 Datenträger. Das heißt, für jeden virtuellen Computer können bis zu 256 virtuelle SCSI-Datenträger konfiguriert werden. (4 Controller x 64 Datenträger pro Controller)
Virtuelle Netzwerkkarten	Windows Server 2016 unterstützt 12 gesamt: -8 Hyper-V-spezifische Netzwerkadapter -4 Legacy-Netzwerkadapter Windows Server 2019 unterstützt 68 gesamt: -64 Hyper-V-spezifische Netzwerkadapter -4 Legacy-Netzwerkadapter	Der Hyper-V-spezifische Netzwerkadapter bietet eine bessere Leistung und erfordert einen Treiber, der in Integration Services enthalten ist. Weitere Informationen finden Sie unter Planen von Hyper-V-Netzwerken in Windows Server .

Maximums für Hyper-V-Hosts

Diese Höchstwerte gelten für jeden Hyper-V-Host.

KOMPONENTE	MAXIMUM	HINWEISE	
Logische Prozessoren	512	Beide müssen in der Firmware aktiviert werden: -Hardware gestützte Virtualisierung -Hardware erzwungene Daten Ausführungs Verhinderung (Data Execution Prevention, DEP) Für das Host Betriebssystem (Stamm Partition) werden nur die maximalen 320 logischen Prozessoren angezeigt.	
Arbeitsspeicher	24 TB	None.	
Netzwerkkartenbegriffe (NIC-Teamvorgang)	Keine Begrenzung durch Hyper-V.	Weitere Informationen finden Sie unter NIC-Team Vorgang .	
Physische Netzwerkkarten	Keine Begrenzung durch Hyper-V.	None.	
Virtuelle Computer pro Server	1024	None.	
Speicher	Begrenzt durch das, was vom Host Betriebssystem unterstützt wird. Keine Begrenzung durch Hyper-V.	Hinweis: Bei Verwendung von SMB 3,0 unterstützt Microsoft Network Attached Storage (NAS). Die NFS-basierte Speicherung wird nicht unterstützt.	
Virtuelle Netzwerk-Switchports pro Server	Unterschiedlich; keine Begrenzung durch Hyper-V.	Der Grenzwert hängt in der Praxis von den verfügbaren Computerressourcen ab.	
Virtuelle Prozessoren pro logischem Prozessor	Kein Verhältnis durch Hyper-V vorgegeben.	None.	
Virtuelle Prozessoren pro Server	2.048	None.	
Virtuelle SANs (Storage Area Networks).	Keine Begrenzung durch Hyper-V.	None.	
Virtuelle Switches	Unterschiedlich; keine Begrenzung durch Hyper-V.	Der Grenzwert hängt in der Praxis von den verfügbaren Computerressourcen ab.	

Failovercluster und Hyper-V

In dieser Tabelle werden die Höchstwerte aufgelistet, die bei der Verwendung von Hyper-V und Failoverclustering gelten. Es ist wichtig, dass Sie eine Kapazitätsplanung durchführen, um sicherzustellen, dass ausreichend Hardware Ressourcen vorhanden sind, um alle virtuellen Computer in einer Cluster Umgebung auszuführen.

Weitere Informationen zu Updates für das Failoverclustering, einschließlich neuer Features für virtuelle Computer, finden Sie unter [Neues beim Failoverclustering unter Windows Server 2016](#).

KOMPONENTE	MAXIMUM	HINWEISE
Knoten pro Cluster	64	Berücksichtigen Sie die Anzahl von Knoten, die Sie für das Failover reservieren möchten, sowie Wartungsaufgaben wie etwa das Anwenden von Updates. Es wird empfohlen, ausreichend Ressourcen einzuplanen, damit 1 Knoten für das Failover reserviert werden kann. Dies bedeutet, dass dieser Knoten sich so lange im Leerlauf befindet, bis das Failover zu einem anderen Knoten erfolgt ist. (Dies wird mitunter auch als passiver Knoten bezeichnet.) Sie können diese Anzahl erhöhen, wenn Sie zusätzliche Knoten reservieren möchten. Es gibt kein empfohlenes Verhältnis oder einen Multiplikator reservierter Knoten für aktive Knoten. die einzige Voraussetzung besteht darin, dass die Gesamtanzahl der Knoten in einem Cluster nicht den maximalen Wert von 64 überschreiten kann.
Ausführen virtueller Computer pro Cluster und pro Knoten	8.000 pro Cluster	Mehrere Faktoren können sich auf die tatsächliche Anzahl von virtuellen Computern auswirken, die Sie gleichzeitig auf einem Knoten ausführen können, wie z. b.: <ul style="list-style-type: none">-Menge des physischen Speichers, der von den einzelnen virtuellen Computern verwendet wird.-Netzwerk- und Speicherbandbreite.-Anzahl der Datenträger Spindeln, die sich auf die Datenträger-e/a-Leistung auswirken.

Planen der Hyper-V-Sicherheit in Windows Server

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Sichern Sie das Hyper-V-Host Betriebssystem, die virtuellen Computer, die Konfigurationsdateien und die Daten des virtuellen Computers. Verwenden Sie die folgende Liste der empfohlenen Vorgehensweisen als Checkliste, die Sie beim Schutz Ihrer Hyper-V-Umgebung unterstützt.

Sichern des Hyper-V-Hosts

- **Halten Sie das Host Betriebssystem als sicher.**
 - Minimieren Sie die Angriffsfläche mithilfe der mindestens erforderlichen Windows Server-Installationsoption, die Sie für das Verwaltungs Betriebssystem benötigen. Weitere Informationen finden Sie im [Abschnitt Installationsoptionen](#) der technischen Inhalts Bibliothek für Windows Server. Es wird nicht empfohlen, produktionsworkloads auf Hyper-V unter Windows 10 auszuführen.
 - Halten Sie das Betriebssystem, die Firmware und die Gerätetreiber für das Hyper-V-Host mit den neuesten Sicherheitsupdates auf dem neuesten Stand. Überprüfen Sie die Empfehlungen Ihres Herstellers, um Firmware und Treiber zu aktualisieren.
 - Verwenden Sie den Hyper-V-Host nicht als Arbeitsstation, oder installieren Sie keine unnötige Software.
 - Verwalten Sie den Hyper-V-Host Remote. Wenn Sie den Hyper-V-Host lokal verwalten müssen, verwenden Sie Credential Guard. Weitere Informationen finden Sie unter [Schützen abgeleiteter Domänenanmeldeinformationen mit Credential Guard](#).
 - Aktivieren von Code Integritäts Richtlinien Verwenden Sie virtualisierungsbasierte, Sicherheits geschützte Code Integritäts Dienste. Weitere Informationen finden Sie im [Device Guard-Bereitstellungs Handbuch](#).

- **Verwenden Sie ein sicheres Netzwerk.**
 - Verwenden Sie ein separates Netzwerk mit einem dedizierten Netzwerkadapter für den physischen Hyper-V-Computer.
 - Verwenden Sie ein privates oder sicheres Netzwerk für den Zugriff auf VM-Konfigurationen und virtuelle Festplatten Dateien.
 - Verwenden Sie ein privates/dediziertes Netzwerk für den Live Migrations Datenverkehr. Aktivieren Sie IPSec in diesem Netzwerk, um die Verschlüsselung zu verwenden und die Daten Ihrer VM während der Migration zu schützen. Weitere Informationen finden Sie unter [Einrichten von Hosts für die Live Migration ohne Failoverclustering](#).

- **Sicherer Speicher Migrations Datenverkehr.**

Verwenden Sie SMB 3,0 für die End-to-End-Verschlüsselung von SMB-Daten und Datenschutz Manipulationen bzw. das Löschen von nicht vertrauenswürdigen Netzwerken. Verwenden Sie ein privates Netzwerk für den Zugriff auf den SMB-Freigabe Inhalt, um man-in-the-Middle-Angriffe zu verhindern. Weitere Informationen finden Sie unter [SMB-Sicherheitsverbesserungen](#).

- **Konfigurieren Sie Hosts als Teil eines geschützten Fabrics.**

Weitere Informationen finden Sie unter geschütztes [Fabric](#).

- **Sichere Geräte.**

Sichern Sie die Speichergeräte, auf denen die Ressourcen Dateien des virtuellen Computers aufbewahrt werden.

- **Sichern Sie die Festplatte.**

Verwenden Sie BitLocker-Laufwerkverschlüsselung, um Ressourcen zu schützen.

- **Sichern Sie das Hyper-V-Host Betriebssystem.**

Verwenden Sie die in der [Windows Server-Sicherheitsbasis Linie](#) beschriebenen grundlegenden Sicherheitseinstellungen.

- **Erteilen Sie entsprechende Berechtigungen.**

- Fügen Sie Benutzer hinzu, die den Hyper-v-Host für die Hyper-v-Administratoren Gruppe verwalten müssen.
- Erteilen Sie keine Berechtigungen für Administratoren für virtuelle Computer auf dem Hyper-V-Host Betriebssystem.

- **Konfigurieren Sie antivirenausschlüsse und Optionen für Hyper-V.**

Für Windows Defender sind bereits [Automatische Ausschlüsse](#) konfiguriert. Weitere Informationen zu Ausschlüssen finden Sie unter [Empfohlene antivirenausschlüsse für Hyper-V-Hosts](#).

- **Fügen Sie keine unbekannten VHDs ein.** Dadurch kann der Host Angriffe auf Dateisystem Ebene verfügbar machen.

- **Aktivieren Sie die Schachtelung in Ihrer Produktionsumgebung nur, wenn dies erforderlich ist.**

Wenn Sie die Schachtelung aktivieren, führen Sie keine nicht unterstützten Hypervisoren auf einem virtuellen Computer aus.

Für sicherere Umgebungen:

- **Verwenden Sie Hardware mit einem Trusted Platform Module-Chip (TPM) 2,0, um ein geschütztes Fabric einzurichten.**

Weitere Informationen finden Sie unter [System Anforderungen für Hyper-V auf Windows Server 2016](#).

Sichern virtueller Computer

- **Erstellen Sie virtuelle Computer der Generation 2 für unterstützte Gast Betriebssysteme.**

Weitere Informationen finden Sie unter [Sicherheitseinstellungen der Generation 2](#).

- **Aktivieren Sie den sicheren Start.**

Weitere Informationen finden Sie unter [Sicherheitseinstellungen der Generation 2](#).

- **Halten Sie das Gast Betriebssystem sicher.**

- Installieren Sie die neuesten Sicherheitsupdates, bevor Sie einen virtuellen Computer in einer Produktionsumgebung einschalten.
- Installieren Sie Integration Services für die unterstützten Gast Betriebssysteme, die diese benötigen, und halten Sie Sie auf dem neuesten Stand. Integration Services-Updates für Gäste, die unterstützte Windows-Versionen ausführen, sind über Windows Update verfügbar.
- Härtung des Betriebssystems, das auf den einzelnen virtuellen Computern ausgeführt wird, basierend auf der Rolle, die es ausführt. Verwenden Sie die grundlegenden Sicherheits Einstellungs Empfehlungen, die in der [Windows-Sicherheitsbaseline](#) beschrieben werden.

- **Verwenden Sie ein sicheres Netzwerk.**

Stellen Sie sicher, dass virtuelle Netzwerkadapter eine Verbindung mit dem richtigen virtuellen Switch herstellen und die entsprechenden Sicherheitseinstellungen und Einschränkungen angewendet werden.

- **Speichern von virtuellen Festplatten und Momentaufnahme Dateien an einem sicheren Ort.**
- **Sichere Geräte.**

Konfigurieren Sie nur erforderliche Geräte für eine virtuelle Maschine. Aktivieren Sie keine diskrete Geräte Zuweisung in Ihrer Produktionsumgebung, es sei denn, Sie benötigen Sie für ein bestimmtes Szenario. Wenn Sie diese Option aktivieren, stellen Sie sicher, dass Sie nur Geräte von vertrauenswürdigen Anbietern verfügbar machen.

- **Konfigurieren Sie die Software für Antivirus-, Firewall-und Eindring Versuche auf virtuellen Computern entsprechend der Rolle des virtuellen Computers entsprechend.**
- **Aktivieren Sie die virtualisierungsbasierte Sicherheit für Gäste, auf denen Windows 10 oder Windows Server 2016 oder höher ausgeführt wird.**

Weitere Informationen finden Sie im [Device Guard-Bereitstellungs Handbuch](#).

- **Aktivieren Sie nur diskrete Geräte Zuweisungen, wenn dies für eine bestimmte Arbeitsauslastung erforderlich ist.**

Aufgrund der Art der Übergabe eines physischen Geräts sollten Sie mit dem Gerätehersteller zusammenarbeiten, um zu verstehen, ob er in einer sicheren Umgebung verwendet werden sollte.

Für sicherere Umgebungen:

- **Stellen Sie virtuelle Computer mit aktiviertem Schutz bereit, und stellen Sie Sie in einem geschützten Fabric bereit.**

Weitere Informationen finden Sie unter [Sicherheitseinstellungen der Generation 2](#) und geschütztes [Fabric](#).

Planen der GPU-Beschleunigung in Windows Server

27.03.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

In diesem Artikel werden die in Windows Server verfügbaren Funktionen für die Grafikvirtualisierung vorgestellt.

Verwendung der GPU-Beschleunigung

Abhängig von der Arbeitsauslastung sollten Sie die GPU-Beschleunigung in Erwägung gezogen. Vor der Auswahl von GPU-Beschleunigung sollten Sie Folgendes berücksichtigen:

- **App-und desktopremoting-Workloads (VDI/daas)** : Wenn Sie einen app-oder desktopremotingdienst mit Windows Server entwickeln, sollten Sie den Katalog der apps in Erwägung gezogen haben, die Ihre Benutzer erwarten. Einige Arten von apps, wie z. b. CAD/CAM-apps, Simulations-apps, Spiele und Render/Visualisierungs-apps, basieren stark auf 3D-Rendering, um eine reibungslose und reaktionsfähige Interaktivität zu ermöglichen. Die meisten Kunden werden GPUs in Erwägung gezogen, dass Sie mit diesen Arten von apps eine angemessene Benutzer Leistung haben.
- **Remoterendering-, Codierungs-und Visualisierungs Arbeits Auslastungen**: Diese Grafik orientierten Workloads basieren tendenziell stark auf den spezialisierten Funktionen von GPU, wie z. b. effizientes 3D-Rendering und Frame Codierung/Decodierung, um Kosten Effektivität und Durchsatz Ziele zu erreichen. Für diese Art der Arbeitsauslastung kann ein einzelner GPU-fähiger virtueller Computer in der Lage sein, den Durchsatz von vielen virtuellen CPU-Computern abzugleichen.
- **HPC-und ml-Arbeits Auslastungen**: für hoch Daten parallele Compute-Workloads, wie z. b. Hochleistungsmodelle für Compute-und Machine Learning-Modelle, können GPUs die Zeit bis zum Ergebnis, die Zeit bis zum Rückschluss und die Trainingszeit drastisch verkürzen. Alternativ bieten Sie möglicherweise eine bessere Kosteneffizienz als eine reine CPU-Architektur auf einer vergleichbaren Leistungs Ebene. Viele HPC-und Machine Learning-Frameworks haben eine Option zum Aktivieren der GPU-Beschleunigung. Stellen Sie sich vor, ob dies für die jeweilige Arbeitsauslastung von Vorteil

GPU-Virtualisierung in Windows Server

GPU-Virtualisierungstechnologien ermöglichen eine GPU-Beschleunigung in einer virtualisierten Umgebung, in der Regel auf virtuellen Computern. Wenn Ihre Arbeitsauslastung mit Hyper-V virtualisiert ist, müssen Sie die Grafikvirtualisierung verwenden, um eine GPU-Beschleunigung von der physischen GPU zu Ihren virtualisierten Apps oder Diensten bereitzustellen. Wenn Ihre Arbeitsauslastung jedoch direkt auf physischen Windows Server-Hosts ausgeführt wird, ist keine Grafik Virtualisierung erforderlich. Ihre apps und Dienste haben bereits Zugriff auf die GPU-Funktionen und APIs, die in Windows Server System intern unterstützt werden.

Die folgenden Technologien zur Grafik Virtualisierung sind für Hyper-V-VMs in Windows Server verfügbar:

- [Diskrete Geräte Zuweisung \(DDA\)](#)
- [RemoteFX vGPU](#)

Zusätzlich zu VM-Workloads unterstützt Windows Server auch die GPU-Beschleunigung von containerisierten Workloads innerhalb von Windows-Containern. Weitere Informationen finden Sie unter [GPU-Beschleunigung in Windows-Containern](#).

Diskrete Geräte Zuweisung (DDA)

Bei der diskreten Geräte Zuweisung (DDA), auch als GPU-Pass-Through bezeichnet, können Sie einen oder mehrere physische GPUs für einen virtuellen Computer verwenden. In einer DDA-Bereitstellung werden virtualisierte Arbeits Auslastungen auf dem systemeigenen Treiber ausgeführt und verfügen in der Regel über vollständigen Zugriff auf die GPU-Funktionalität. DDA bietet die höchste Ebene der APP-Kompatibilität und der möglichen Leistung. DDA kann auch eine GPU-Beschleunigung für Linux-VMs bereitstellen, die unterstützt werden.

Eine DDA-Bereitstellung kann nur eine begrenzte Anzahl von virtuellen Computern beschleunigen, da jede physische GPU eine Beschleunigung für höchstens eine VM bereitstellen kann. Wenn Sie einen Dienst entwickeln, dessen Architektur freigegebene virtuelle Computer unterstützt, sollten Sie mehrere beschleunigte Workloads pro VM verwenden. Wenn Sie z. b. einen Desktop Remoting-Dienst mit RDS entwickeln, können Sie die Benutzer Skalierung verbessern, indem Sie die Multi-Session-Funktionen von Windows Server verwenden, um auf jedem virtuellen Computer mehrere Benutzer Desktops zu hosten. Diese Benutzer haben die Vorteile der GPU-Beschleunigung gemeinsam.

Weitere Informationen finden Sie in folgenden Themen:

- [Planen der Bereitstellung einer diskreten Geräte Zuweisung](#)
- [Bereitstellen von Grafik Geräten mithilfe der diskreten Geräte Zuweisung](#)

RemoteFX vGPU

NOTE

Remotefx vgpu wird in Windows Server 2016 vollständig unterstützt, wird aber in Windows Server 2019 nicht unterstützt.

Remotefx vgpu ist eine Grafik-Virtualisierungstechnologie, die die gemeinsame Nutzung einer einzelnen physischen GPU zwischen mehreren virtuellen Computern ermöglicht. In einer remotefx-vgpu-Bereitstellung werden virtualisierte Arbeits Auslastungen auf dem remotefx 3D-Adapter von Microsoft ausgeführt, mit dem GPU-Verarbeitungsanforderungen zwischen dem Host und den Gästen koordiniert werden. Remotefx vgpu eignet sich am besten für Wissensarbeiter und hochleistungsfähige Workloads, bei denen keine dedizierten GPU-Ressourcen erforderlich sind. Remotefx vgpu kann nur GPU-Beschleunigung für Windows-VMS bereitstellen.

Weitere Informationen finden Sie in folgenden Themen:

- [Bereitstellen von Grafikgeräten mit RemoteFX vGPU](#)
- [Unterstützung von remotefx 3D-Video Adaptern \(vgpu\)](#)

Vergleichen von DDA und remotefx vgpu

Beachten Sie bei der Planung der Bereitstellung die folgenden Funktionen, und unterstützen Sie die Unterschiede zwischen den Technologien für die

	REMOTEFX VGPU	DISKRETE GERÄTEZUWEISUNG
GPU-Ressourcenmodell	Dediziert oder freigegeben	Nur dediziert
VM-Dichte	Hoch (mindestens ein GPUs zu vielen VMS)	Niedrig (mindestens ein GPUs zu einer VM)
Anwendungskompatibilität	DX 11.1, OpenGL 4.4, OpenCL 1.1	Alle GPU-Funktionen werden vom Hersteller bereitgestellt (DX 12, OpenGL, CUDA)

	REMOTEFX VGPU	DISKRETE GERÄTEZUWEISUNG
AVC444	Standardmäßig aktiviert	Verfügbar über Gruppenrichtlinie
GPU VRAM	Bis zu 1 GB dediziertes VRAM	Bis zur Menge des von der GPU unterstützen VRAMs
Bildfrequenz	Bis zu 30 Bilder pro Sekunde	Bis zu 60 Bilder pro Sekunde
GPU-Treiber im Gastbetriebssystem	Anzeigetreiber für RemoteFX 3D-Adapter (Microsoft)	GPU-Anbieter Treiber (nVidia, AMD, Intel)
Host Betriebssystem	Windows Server 2016	Windows Server 2016; Windows Server 2019
Unterstützung des Gastbetriebssystems	Windows Server 2012 R2; Windows Server 2016; Windows 7 SP1; Windows 8.1; Windows 10	Windows Server 2012 R2; Windows Server 2016; Windows Server 2019; Windows 10; Linux
Hypervisor	Microsoft Hyper-V	Microsoft Hyper-V
GPU-Hardware	Enterprise-GPUs (z. B. Nvidia Quadro/GRID oder AMD FirePro)	Enterprise-GPUs (z. B. Nvidia Quadro/GRID oder AMD FirePro)
Serverhardware	Keine speziellen Anforderungen	Moderner Server, stellt IOMMU dem Betriebssystem zur Verfügung (meist SR-IOV-kompatible Hardware)

Planen der Bereitstellung von Geräten mit diskreter Geräte Zuweisung

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Microsoft Hyper-V Server 2016, Windows Server 2016, Microsoft Hyper-V Server 2019, Windows Server 2019

Durch die diskrete Geräte Zuweisung kann auf physische PCIe-Hardware direkt von einem virtuellen Computer aus zugegriffen werden. In diesem Leitfaden werden die Arten von Geräten erläutert, die diskrete Geräte Zuweisungen, Host Systemanforderungen, Einschränkungen der virtuellen Computer sowie Sicherheitsauswirkungen der diskreten Geräte Zuweisung verwenden können.

Bei der erstmaligen Veröffentlichung einer diskreten Geräte Zuweisung haben wir uns auf zwei Geräteklassen konzentriert, die von Microsoft formal unterstützt werden: Grafikadapter und nvme-Speichergeräte. Andere Geräte sind wahrscheinlich funktionsfähig, und Hardware Anbieter können Unterstützung für diese Geräte anbieten. Wenden Sie sich für diese anderen Geräte an diese Hardware Anbieter, um Unterstützung zu erhalten.

Weitere Informationen zu anderen Methoden der GPU-Virtualisierung finden Sie unter [Planen der GPU-Beschleunigung in Windows Server](#). Wenn Sie zum Testen der diskreten Geräte Zuweisung bereit sind, können Sie zum Einstieg zum Bereitstellen von [Grafik Geräten mithilfe der diskreten Geräte Zuweisung](#) oder Bereitstellen von [Speichergeräten mithilfe der diskreten Geräte Zuweisung](#) wechseln.

Unterstützte Virtual Machines und Gast Betriebssysteme

Für VMS der Generation 1 oder 2 wird eine diskrete Geräte Zuweisung unterstützt. Zu den unterstützten Gästen zählen zusätzlich Windows 10, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 mit angewendetem [KB 3133690](#) und verschiedene Verteilungen des [Linux-Betriebssystems](#).

Systemanforderungen

Zusätzlich zu den [Systemanforderungen für Windows Server](#) und den [Systemanforderungen für Hyper-V](#) erfordert die diskrete Geräte Zuweisung Server Klassen Hardware, die dem Betriebs System die Steuerung der Konfiguration des PCIe-Fabrics (System eigenes PCI Express-Steuerelement) gewähren kann. Außerdem muss das komplexe PCIe-Stammverzeichnis "Access Control Services (ACS)" unterstützen, mit dem Hyper-V den gesamten PCIe-Datenverkehr über die e/a-MMU erzwingen kann.

Diese Funktionen werden in der Regel nicht direkt im BIOS des Servers verfügbar gemacht und sind häufig hinter anderen Einstellungen verborgen. Beispielsweise sind die gleichen Funktionen für die SR-IOV-Unterstützung erforderlich, und im BIOS müssen Sie möglicherweise "SR-IOV aktivieren" festlegen. Wenden Sie sich an Ihren Systemhersteller, wenn Sie die richtige Einstellung in Ihrem BIOS nicht identifizieren können.

Um sicherzustellen, dass Hardware für die Hardware eine diskrete Geräte Zuweisung ermöglicht, haben unsere Techniker ein [Machine profile-Skript](#) eingefügt, das Sie auf einem Hyper-V-fähigen Host ausführen können, um zu testen, ob der Server ordnungsgemäß eingerichtet ist und welche Geräte eine diskrete Geräte Zuweisung unterstützen.

Geräteanforderungen

Nicht jedes PCIe-Gerät kann mit diskreter Geräte Zuweisung verwendet werden. Beispielsweise werden ältere Geräte, die Legacy-PCI-Interrupts (intX) nutzen, nicht unterstützt. Die [Blogbeiträge](#) von Jake Oshin werden

ausführlicher behandelt, aber für den Consumer wird bei der Ausführung des [Machine profile-Skripts](#) angezeigt, welche Geräte für die diskrete Geräte Zuweisung eingesetzt werden können.

Gerätehersteller können sich an Ihren Microsoft-Vertreter wenden, um weitere Informationen zu erhalten.

Gerätetreiber

Da die diskrete Geräte Zuweisung das gesamte PCIe-Gerät an die Gast-VM übergibt, muss vor dem Bereitstellen des Geräts innerhalb des virtuellen Computers kein Host Treiber installiert werden. Die einzige Voraussetzung für den Host ist, dass der [PCIe-Speicherort Pfad](#) des Geräts bestimmt werden kann. Der Treiber des Geräts kann optional installiert werden, wenn dies zur Identifizierung des Geräts beiträgt. Beispielsweise wird eine GPU, auf der der Gerätetreiber auf dem Host installiert ist, möglicherweise als Microsoft Basic-Rendering-Gerät angezeigt. Wenn der Gerätetreiber installiert ist, werden der Hersteller und das Modell wahrscheinlich angezeigt.

Nachdem das Gerät innerhalb des Gast Betriebssystems bereitgestellt wurde, kann der Gerätetreiber des Herstellers jetzt wie üblich innerhalb des virtuellen Gast Computers installiert werden.

Einschränkungen für virtuelle Computer

Aufgrund der Art, wie die diskrete Geräte Zuweisung implementiert ist, werden einige Features eines virtuellen Computers eingeschränkt, während ein Gerät angefügt wird. Die folgenden Funktionen sind nicht verfügbar:

- Speichern/Wiederherstellen virtueller Computer
- Live Migration eines virtuellen Computers
- Die Verwendung von dynamischem Arbeitsspeicher
- Hinzufügen des virtuellen Computers zu einem hoch Verfügbarkeits Cluster (ha)

Sicherheit

Die diskrete Geräte Zuweisung übergibt das gesamte Gerät an den virtuellen Computer. Dies bedeutet, dass alle Funktionen dieses Geräts über das Gast Betriebssystem zugänglich sind. Einige Funktionen, wie z. b. Firmwareupdates, können sich negativ auf die Stabilität des Systems auswirken. Daher werden dem Administrator beim Aufheben der Einbindung des Geräts vom Host zahlreiche Warnungen angezeigt. Es wird dringend empfohlen, die diskrete Geräte Zuweisung nur dann zu verwenden, wenn die Mandanten der VMS vertrauenswürdig sind.

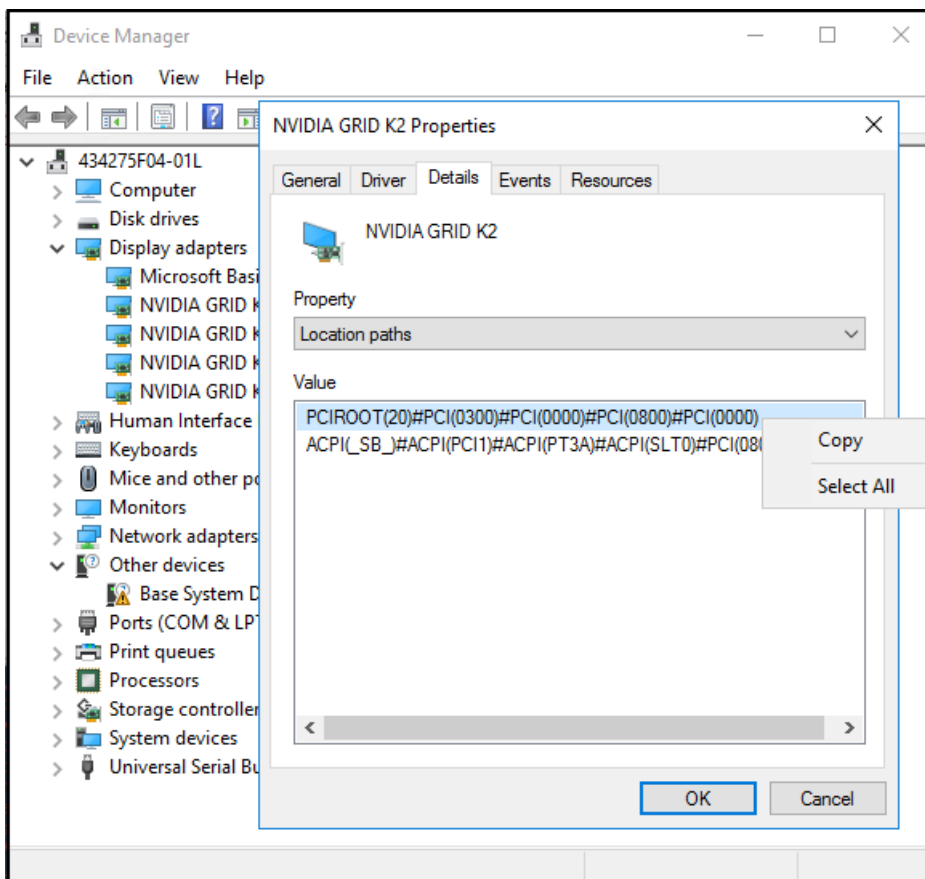
Wenn der Administrator ein Gerät mit einem nicht vertrauenswürdigen Mandanten verwenden möchte, haben wir Geräteherstellern die Möglichkeit gegeben, einen geräteentschärfungs-Treiber zu erstellen, der auf dem Host installiert werden kann. Wenden Sie sich an den Gerätehersteller, um zu erfahren, ob er einen Geräte Entschärfungs Treiber bereitstellt.

Wenn Sie die Sicherheitsüberprüfungen für ein Gerät umgehen möchten, das keinen Treiber für die Geräte Entschärfung hat, müssen Sie den `-Force` Parameter an das `Dismount-VMHostAssignableDevice` -Cmdlet übergeben. Dabei haben Sie sich bewusst, dass Sie das Sicherheitsprofil des Systems geändert haben und dies nur während der Erstellung von Prototypen oder vertrauenswürdigen Umgebungen empfohlen wird.

PCIe-Speicherort Pfad

Der Pfad für den PCIe-Speicherort ist erforderlich, um das Gerät vom Host zu entfernen und zu binden. Ein Beispiel für einen Speicherort Pfad sieht wie folgt aus: `"PCIROOT(20)#PCI(0300)#PCI(0000)#PCI(0800)#PCI(0000)"`. Das [Computer Profil Skript](#) gibt auch den Speicherort Pfad des PCIe-Geräts zurück.

Der Speicherort Pfad wird mithilfe Geräte-Manager



- Öffnen Sie Geräte-Manager, und suchen Sie nach dem Gerät.
- Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie "Eigenschaften"
- Navigieren Sie zur Registerkarte Details, und wählen Sie in der Dropdown-Eigenschaft die Option "Location Path" aus.
- Klicken Sie mit der rechten Maustaste auf den Eintrag, der mit pciroot beginnt, und wählen Sie "Kopieren". Sie verfügen nun über den Speicherort Pfad für das Gerät.

MMIO-Speicherplatz

Einige Geräte, insbesondere GPUs, erfordern zusätzlichen MMIO-Speicherplatz, der dem virtuellen Computer zugeordnet werden muss, damit der Arbeitsspeicher des Geräts zugänglich ist. Standardmäßig beginnt jede VM mit 128 MB geringem MMIO-Speicherplatz und 512 MB hohem MMIO-Speicherplatz. Ein Gerät benötigt jedoch möglicherweise mehr MMIO-Speicherplatz, oder es können mehrere Geräte durchlaufen werden, sodass die kombinierten Anforderungen diese Werte überschreiten. Das Ändern des MMIO-Speicherplatzes erfolgt direkt und kann in PowerShell mithilfe der folgenden Befehle ausgeführt werden:

```
Set-VM -LowMemoryMappedIoSpace 3Gb -VMName $vm
Set-VM -HighMemoryMappedIoSpace 33280Mb -VMName $vm
```

Die einfachste Möglichkeit, um zu bestimmen, wie viel MMIO-Speicherplatz belegt werden soll, ist die Verwendung des [Computer Profil Skripts](#). Führen Sie die folgenden Befehle in einer PowerShell-Konsole aus, um das Computer Profil Skript herunterzuladen und auszuführen:

```
curl -o SurveyDDA.ps1 https://raw.githubusercontent.com/MicrosoftDocs/Virtualization-Documentation/live/hyperv-tools/DiscreteDeviceAssignment/SurveyDDA.ps1
.\SurveyDDA.ps1
```

Bei Geräten, die zugewiesen werden können, zeigt das Skript die MMIO-Anforderungen eines bestimmten Geräts wie im folgenden Beispiel an:

```
NVIDIA GRID K520
Express Endpoint -- more secure.
...
And it requires at least: 176 MB of MMIO gap space
...
```

Der niedrige MMIO-Speicherplatz wird nur von 32-Bit-Betriebssystemen und Geräten verwendet, die 32-Bit-Adressen verwenden. In den meisten Fällen reicht das Festlegen des hohen MMIO-Speicherplatzes eines virtuellen Computers aus, da 32-Bit-Konfigurationen nicht sehr häufig verwendet werden.

IMPORTANT

Beim Zuweisen von MMIO-Speicherplatz zu einem virtuellen Computer muss der Benutzer sicherstellen, dass der MMIO-Speicherplatz auf die Summe des angeforderten MMIO-Speicherplatzes für alle gewünschten zugewiesenen Geräte zuzüglich eines zusätzlichen Puffers festgelegt wird, wenn es andere virtuelle Geräte gibt, die einige MB MMIO-Speicherplatz erfordern. Verwenden Sie die oben beschriebenen MMIO-Standardwerte als Puffer für niedriges und hohes MMIO (128 MB bzw. 512 MB).

Wenn ein Benutzer eine einzelne K520-GPU wie im obigen Beispiel zuweisen würde, muss er den MMIO-Speicherplatz der VM auf den Wert festlegen, der vom Computer Profil Skript und einem Puffer--176 MB + 512 MB ausgegeben wird. Wenn ein Benutzer drei K520-GPUs zuweisen würde, muss er den MMIO-Speicherplatz auf drei Mal 176 MB plus einen Puffer oder 528 MB + 512 MB festlegen.

Eine ausführlichere Betrachtung von MMIO Space finden Sie im techcommunity [-Blog unter diskrete Geräte Zuweisung-GPUs](#) .

Skript für Computer Profil

Um zu vereinfachen, ob der Server ordnungsgemäß konfiguriert ist und welche Geräte durch diskrete Geräte Zuweisung übermittelt werden können, stellt einer unserer Techniker das folgende PowerShell-Skript bereit: [surveydda.ps1](#).

Stellen Sie vor der Verwendung des Skripts sicher, dass die Hyper-V-Rolle installiert ist, und führen Sie das Skript in einem PowerShell-Befehlsfenster aus, das über Administrator Rechte verfügt.

Wenn das System nicht ordnungsgemäß für die Unterstützung der diskreten Geräte Zuweisung konfiguriert ist, zeigt das Tool eine Fehlermeldung an, die falsch ist. Wenn das Tool feststellt, dass das System ordnungsgemäß konfiguriert ist, werden alle Geräte aufgelistet, die auf dem PCIe-Bus gefunden werden können.

Das Tool zeigt für jedes gefundene Gerät an, ob es mit diskreter Geräte Zuweisung verwendet werden kann. Wenn ein Gerät als kompatibel mit der diskreten Geräte Zuweisung identifiziert wird, stellt das Skript einen Grund dar. Wenn ein Gerät erfolgreich als kompatibel identifiziert wurde, wird der Speicherort Pfad des Geräts angezeigt. Wenn dieses Gerät außerdem [MMIO-Speicherplatz](#)erfordert, wird es ebenfalls angezeigt.

Intel(R) C600/X79 series chipset USB2 Enhanced Host Controller #1 - 1D26
Old-style PCI device, switch port, etc. Not assignable.

Intel(R) Xeon(R) A E7 v2/Xeon(R) E5 v2/Core i7 IOAPIC - 0E2C
Embedded Endpoint -- less secure.
And it has no interrupts at all -- assignment can work.
And it requires at least: 1 MB of MMIO gap space
PCIR00T(0)#PCI(0504)

NVIDIA GRID K520
Express Endpoint -- more secure.
And its interrupts are message-based, assignment can work.
And it requires at least: 176 MB of MMIO gap space
PCIR00T(20)#PCI(0200)#PCI(0000)#PCI(0800)#PCI(0000)

Intel(R) Xeon(R) A E7 v2/Xeon(R) E5 v2/Core i7 Crystal Beach DMA Channel 0 - 0E20
Embedded Endpoint -- less secure.
All of the interrupts are line-based, no assignment can work.

Bereitstellen von Hyper-V unter Windows Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Diese Ressourcen helfen Ihnen bei der Bereitstellung von Hyper-V auf Windows Server 2016.

- [Konfigurieren von virtuellen lokalen Netzwerken für Hyper-V](#)
- [Einrichten von Hosts für die Live Migration ohne Failoverclustering](#)
- [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#)
- [Bereitstellen von Grafik Geräten mithilfe der diskreten Geräte Zuweisung](#)
- [Bereitstellen von Grafikgeräten mit RemoteFX vGPU](#)
- [Bereitstellen von Speichergeräten mit diskreter Geräte Zuweisung](#)

Exportieren und Importieren virtueller Computer

13.05.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

In diesem Artikel erfahren Sie, wie Sie einen virtuellen Computer exportieren und importieren. Dies ist eine schnelle Möglichkeit, Sie zu verschieben oder zu kopieren. In diesem Artikel werden auch einige der Optionen erläutert, die Sie beim Exportieren oder importieren treffen müssen.

Exportieren eines virtuellen Computers

Bei einem Export werden alle erforderlichen Dateien in einer Einheit gesammelt: virtuelle Festplatten Dateien, Konfigurationsdateien für virtuelle Computer und alle Prüf Punkt Dateien. Dies können Sie auf einem virtuellen Computer durchführen, der sich im Zustand "gestartet" oder "beendet" befindet.

Verwenden des Hyper-V-Managers

So erstellen Sie einen Export eines virtuellen Computers

1. In Hyper-V-Manager mit der rechten Maustaste in den virtuellen Computer, und wählen Sie **exportieren**.
2. Wählen Sie den Speicherort der exportierten Dateien aus, und klicken Sie auf **exportieren**.

Wenn der Export abgeschlossen ist, werden alle exportierten Dateien am Export Speicherort angezeigt.

PowerShell

Öffnen Sie eine Sitzung als Administrator, und führen Sie einen Befehl wie den folgenden aus, nachdem Sie den < Namen und Pfad der VM ersetzt haben > < > :

```
Export-VM -Name \<vm name\> -Path \<path\>
```

Weitere Informationen finden Sie unter [Export-VM](#).

Importieren eines virtuellen Computers

Beim Importieren wird der virtuelle Computer beim Hyper-V-Host registriert. Sie können zurück in den Host oder einen neuen Host importieren. Wenn Sie auf denselben Host importieren, müssen Sie den virtuellen Computer nicht zuerst exportieren, da Hyper-V versucht, den virtuellen Computer aus den verfügbaren Dateien neu zu erstellen. Wenn Sie einen virtuellen Computer importieren, wird er registriert, damit er auf dem Hyper-V-Host verwendet werden kann.

Mit dem Assistenten zum Importieren virtueller Computer können Sie auch Inkompatibilitäten beheben, die beim Wechsel von einem Host zu einem anderen vorhanden sein können. Dies sind häufig Unterschiede bei physischer Hardware, z. b. Arbeitsspeicher, virtuelle Switches und virtuelle Prozessoren.

Importieren mit dem Hyper-V-Manager

So importieren Sie einen virtuellen Computer:

1. Klicken Sie im Hyper-V-Manager im Menü **Aktionen** auf **virtuellen Computer importieren**.
2. Klicken Sie auf **Weiter**.

3. Wählen Sie den Ordner aus, der die exportierten Dateien enthält, und klicken Sie auf **weiter**.
4. Wählen Sie den zu importierenden virtuellen Computer aus.
5. Wählen Sie den Importtyp aus, und klicken Sie auf **weiter**. (Beschreibungen finden Sie unten unter [Importieren von Typen](#).)
6. Klicken Sie auf **Fertig stellen**.

Importieren mithilfe von PowerShell

Verwenden Sie das Cmdlet **Import-VM**, und befolgen Sie dabei das Beispiel für den gewünschten Importtyp. Beschreibungen der Typen finden Sie unten unter [Importieren von Typen](#).

Direkt registrieren

Bei dieser Art von Import werden die Dateien verwendet, in denen Sie zum Zeitpunkt des Imports gespeichert sind, und die ID der virtuellen Maschine wird beibehalten. Der folgende Befehl zeigt ein Beispiel für eine Import Datei. Führen Sie einen ähnlichen Befehl mit ihren eigenen Werten aus.

```
Import-VM -Path 'C:\vm export path>\2B91FEB3-F1E0-4FFF-B8BE-29CED892A95A.vmcx'
```

Restore

Um den virtuellen Computer mit einem eigenen Pfad für die Dateien des virtuellen Computers zu importieren, führen Sie einen Befehl wie diesen aus, und ersetzen Sie die Beispiele durch ihre Werte:

```
Import-VM -Path 'C:\vm export path>\2B91FEB3-F1E0-4FFF-B8BE-29CED892A95A.vmcx' -Copy -VhdDestinationPath 'D:\Virtual Machines\WIN10DOC' -VirtualMachinePath 'D:\Virtual Machines\WIN10DOC'
```

Als Kopie importieren

Um einen Kopier Import abzuschließen und die Dateien des virtuellen Computers an den Hyper-V-Standard Speicherort zu verschieben, führen Sie einen Befehl wie diesen aus, und ersetzen Sie die Beispiele durch ihre Werte:

```
Import-VM -Path 'C:\vm export path>\2B91FEB3-F1E0-4FFF-B8BE-29CED892A95A.vmcx' -Copy -GenerateNewId
```

Weitere Informationen finden Sie unter [Import-VM](#).

Typen importieren

Hyper-V bietet drei Import Typen:

- **Direkt registrieren** – bei diesem Typ wird davon ausgegangen, dass sich die Export Dateien an dem Speicherort befinden, an dem Sie den virtuellen Computer speichern und ausführen. Der importierte virtuelle Computer hat die gleiche ID wie beim Export. Wenn der virtuelle Computer bereits bei Hyper-V registriert ist, muss er daher gelöscht werden, bevor der Import Vorgang funktioniert. Wenn der Import abgeschlossen ist, werden die Export Dateien zu den Dateien mit dem Status "wird ausgeführt" und können nicht entfernt werden.
- **Wiederherstellen der virtuellen Maschine** – stellen Sie die virtuelle Maschine an einem von Ihnen ausgewählten Speicherort wieder her, oder verwenden Sie die Standardeinstellung für Hyper-V. Mit diesem Importtyp wird eine Kopie der exportierten Dateien erstellt und an den ausgewählten Speicherort verschoben. Nach dem Importieren hat der virtuelle Computer dieselbe ID wie zum Zeitpunkt des Exports. Wenn der virtuelle Computer bereits in Hyper-V ausgeführt wird, muss er daher gelöscht werden, bevor der Import abgeschlossen werden kann. Wenn der Import abgeschlossen ist, bleiben die exportierten Dateien intakt und können entfernt oder importiert werden.
- **Kopieren Sie den virtuellen Computer** – Dies ähnelt dem wiederherungstyp, in dem Sie einen Speicherort für die Dateien auswählen. Der Unterschied besteht darin, dass der importierte virtuelle

Computer über eine neue eindeutige ID verfügt. Dies bedeutet, dass der virtuelle Computer mehrmals auf denselben Host importiert werden kann.

Einrichten von Hosts für die Live Migration ohne Failoverclustering

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

In diesem Artikel erfahren Sie, wie Sie Hosts einrichten, die nicht gruppiert sind, damit Sie Live Migrationen zwischen Ihnen ausführen können. Verwenden Sie diese Anweisungen, wenn Sie bei der Installation von Hyper-V keine Live Migration eingerichtet haben, oder wenn Sie die Einstellungen ändern möchten. Verwenden Sie zum Einrichten von gruppierten Hosts die Tools für Failoverclustering.

Anforderungen für die Einrichtung einer Live Migration

Um nicht gruppierte Hosts für die Live Migration einzurichten, benötigen Sie Folgendes:

- Ein Benutzerkonto mit der Berechtigung zum Ausführen der verschiedenen Schritte. Die Mitgliedschaft in der lokalen Hyper-V-Administrator Gruppe oder der Gruppe "Administratoren" auf dem Quell- und dem Zielcomputer erfüllt diese Anforderung, es sei denn, Sie konfigurieren die eingeschränkte Delegation. Die Mitgliedschaft in der Gruppe Domänen Administratoren ist erforderlich, um die eingeschränkte Delegation zu konfigurieren.
- Die Hyper-V-Rolle in Windows Server 2016 oder Windows Server 2012 R2, die auf dem Quell- und dem Zielsystem installiert ist. Sie können eine Live Migration zwischen Hosts ausführen, auf denen Windows Server 2016 und Windows Server 2012 R2 ausgeführt wird, wenn der virtuelle Computer mindestens Version 5 ist.
Anweisungen zur Versionsaktualisierung finden Sie unter [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#). Installationsanweisungen finden Sie unter [Installieren der Hyper-V-Rolle unter Windows Server](#).
- Quell- und Zielcomputer, die entweder zur gleichen Active Directory Domäne gehören oder zu Domänen gehören, die einander vertrauen.
- Die Hyper-V-Verwaltungs Tools, die auf einem Computer installiert sind, auf dem Windows Server 2016 oder Windows 10 ausgeführt wird, es sei denn, die Tools sind auf dem Quell- oder Ziel Server installiert, und Sie führen die Tools vom Server aus.

Optionen für Authentifizierung und Netzwerk

Beachten Sie, wie Sie Folgendes einrichten möchten:

- **Authentifizierung:** welches Protokoll wird verwendet, um den Datenverkehr für die Live Migration zwischen den Quell- und Ziel Servern zu authentifizieren? Die Auswahl bestimmt, ob Sie sich beim Quell Server anmelden müssen, bevor Sie eine Live Migration starten:
 - Mithilfe von Kerberos können Sie sich nicht beim Server anmelden, sondern müssen die eingeschränkte Delegation einrichten. Weitere Informationen finden Sie weiter unten.
 - Mit "kredssp" können Sie die Konfiguration der eingeschränkten Delegation vermeiden. Sie müssen sich jedoch beim Quell Server anmelden. Hierzu können Sie eine lokale Konsolen Sitzung, eine Remotedesktop Sitzung oder eine Windows PowerShell-Remote Sitzung verwenden.

Für "kredssp" ist eine Anmeldung in Situationen erforderlich, die möglicherweise nicht offensichtlich sind. Wenn Sie sich beispielsweise bei TestServer01 anmelden, um eine virtuelle Maschine zu Bezeichnung testserver02 zu verschieben, und die virtuelle Maschine anschließend wieder in TestServer01 verschieben möchten, müssen Sie sich bei Bezeichnung testserver02 anmelden, bevor Sie versuchen, die virtuelle Maschine zurück auf TestServer01 zu verschieben. Wenn Sie dies nicht tun, schlägt der Authentifizierungs Versuch fehl, es tritt ein Fehler auf, und die folgende Meldung wird angezeigt:

"Fehler beim Migrations Vorgang für den virtuellen Computer bei der Migrations Quelle. Fehler beim Herstellen einer Verbindung mit dem Host *Computernamen*: im Sicherheitspaket 0x8009030E sind keine Anmelde Informationen verfügbar. "

- **Leistung:** ist es sinnvoll, Leistungsoptionen zu konfigurieren? Diese Optionen können die Netzwerk-und CPU-Auslastung reduzieren und die Live Migrationen schneller machen. Stellen Sie Ihre Anforderungen und ihre Infrastruktur in Erwägung, und testen Sie verschiedene Konfigurationen, um Ihnen die Entscheidung zu erleichtern. Die Optionen werden am Ende von Schritt 2 beschrieben.
- **Netzwerk Präferenz:** lässt Sie Live Migration-Datenverkehr über ein beliebiges verfügbares Netzwerk zu, oder isolieren Sie den Datenverkehr für bestimmte Netzwerke? Als bewährte Sicherheitsmethode wird empfohlen, den Datenverkehr auf vertrauenswürdige, private Netzwerken zu isolieren, da der Datenverkehr für die Livemigration beim Senden über das Netzwerk nicht verschlüsselt wird. Die Netzwerkisolation kann über ein physisch isoliertes Netzwerk oder über eine andere vertrauenswürdige Netzwerktechnologie, z. B. VLANs, erreicht werden.

Schritt 1: Konfigurieren der eingeschränkten Delegation (optional)

Wenn Sie sich für die Verwendung von Kerberos zum Authentifizieren des Datenverkehrs für die Live Migration entschieden haben, konfigurieren Sie die eingeschränkte Delegation mithilfe eines Kontos, das Mitglied der Gruppe Domänen Administratoren ist.

Verwenden des Snap-Ins "Benutzer und Computer" zum Konfigurieren der eingeschränkten Delegation

1. Öffnen Sie das Snap-In **"Active Directory-Benutzer und -Computer"**. (Wählen Sie unter Server-Manager den Server aus, wenn er nicht ausgewählt ist, **klicken Sie auf Extras >> Active Directory Benutzer und Computer**).
2. Wählen Sie im Navigationsbereich von **Active Directory Benutzer und Computer** die Domäne aus, und doppelklicken Sie auf den Ordner **Computer**.
3. Klicken Sie im Ordner **Computer** mit der rechten Maustaste auf das Computer Konto des Quell Servers, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie in **Eigenschaften** auf die Registerkarte **Delegation**.
5. Wählen Sie auf der Registerkarte Delegation die Option **Computer nur bei Delegationen angegebener Dienste vertrauen aus**, und wählen Sie dann **beliebiges Authentifizierungsprotokoll verwenden** aus.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie unter **Dienste hinzufügen** auf **Benutzer oder Computer**.
8. Geben Sie in **Benutzer oder Computer auswählen** den Namen des Zielservers ein. Klicken Sie auf **Namen überprüfen**, um Sie zu überprüfen, und klicken Sie auf **OK**.
9. Führen Sie in der Liste der verfügbaren Dienste unter **Dienste hinzufügen** die folgenden Schritte aus, und klicken Sie dann auf **OK**:
 - Wenn Sie den Speicher des virtuellen Computers entfernen möchten, wählen Sie **cifs** aus. Dies ist

erforderlich, wenn Sie den Speicher zusammen mit dem virtuellen Computer verschieben möchten, und wenn Sie nur den Speicher eines virtuellen Computers verschieben möchten. Wenn der Server für die Verwendung des SMB-Speichers für Hyper-V konfiguriert ist, wurde diese Auswahl bereits getroffen.

- Wenn Sie virtuelle Computer verschieben möchten, wählen Sie den **Migrationsdienst für virtuelles System von Microsoft** aus.
10. Stellen Sie auf der Registerkarte **Delegierung** des Dialogfelds **„Eigenschaften“** sicher, dass die von Ihnen im vorherigen Schritt ausgewählten Dienste als Dienste aufgelistet sind, für die der Zielcomputer delegierte Anmeldeinformationen bereitstellen kann. Klicken Sie auf **OK**.
 11. Wählen Sie im Ordner **Computers** das Computerkonto des Zielservers aus, und wiederholen Sie den Prozess. Vergewissern Sie sich, dass Sie im Dialogfeld **Benutzer oder Computer auswählen** den Namen des Quellservers angegeben haben.

Die Konfigurationsänderungen treten in Kraft, nachdem die beiden folgenden Aktionen durchgeführt wurden:

- Die Änderungen werden auf die Domänen Controller repliziert, bei denen die Server, auf denen Hyper-V ausgeführt wird, angemeldet sind.
- Der Domänen Controller gibt ein neues Kerberos-Ticket aus.

Schritt 2: Einrichten der Quell-und Zielcomputer für die Live Migration

Dieser Schritt umfasst die Auswahl von Optionen für die Authentifizierung und das Netzwerk. Als bewährte Sicherheitsmaßnahme empfiehlt es sich, bestimmte Netzwerke auszuwählen, die für den Datenverkehr für die Live Migration verwendet werden sollen, wie oben erläutert. Außerdem wird in diesem Schritt gezeigt, wie Sie die Option Leistung auswählen.

Verwenden des Hyper-V-Managers zum Einrichten der Quell-und Zielcomputer für die Live Migration

1. Öffnen Sie den Hyper-V-Manager. (**Klicken Sie** in Server-Manager auf Extras >> **Hyper-V-Manager**.)
2. Wählen Sie im Navigationsbereich einen der Server aus. (Falls nicht aufgeführt, klicken Sie mit der rechten Maustaste auf **Hyper-V-Manager**, klicken Sie auf **Verbindung mit Server herstellen**, geben Sie den Servernamen ein, und klicken Sie auf **OK** Wiederholen Sie den Vorgang, um weitere Server hinzuzufügen.
3. Klicken Sie im Bereich **Aktion** auf **Hyper-V-Einstellungen** >> **Live Migrationen**.
4. Aktivieren Sie im Bereich **Livemigrationen** die Option **Ein- und ausgehende Livemigrationen ermöglichen**.
5. Geben Sie unter **gleichzeitige Live Migrationen** eine andere Zahl an, wenn Sie nicht den Standardwert von 2 verwenden möchten.
6. Wenn spezielle Netzwerkverbindungen den Datenverkehr für die Livemigration akzeptieren sollen, klicken Sie unter **Eingehende Livemigrationen** auf **Hinzufügen**, um die IP-Adressinformationen einzugeben. Klicken Sie anderenfalls auf **Beliebiges Netzwerk für Livemigration verwenden**. Klicken Sie auf **OK**.
7. Um die Kerberos-und Leistungsoptionen auszuwählen, erweitern Sie **Live Migrationen**, und wählen Sie dann **Erweiterte Funktionen** aus.
 - Wenn Sie die eingeschränkte Delegierung konfiguriert haben, wählen Sie unter **Authentifizierungsprotokoll** die Option **Kerberos** aus.
 - Überprüfen Sie unter **Leistungsoptionen** die Details, und wählen Sie eine andere Option aus, wenn Sie für Ihre Umgebung geeignet ist.
8. Klicken Sie auf **OK**.
9. Wählen Sie im Hyper-V-Manager den anderen Server aus, und wiederholen Sie die Schritte.

Verwenden von Windows PowerShell zum Einrichten der Quell- und Zielcomputer für die Live Migration

Zum Konfigurieren der Live Migration auf nicht gruppierten Hosts sind drei Cmdlets verfügbar: "[enable-vmmigration](#)", "[Set-vmmigrationnetwork](#)" und "[Set-VMHost](#)". In diesem Beispiel werden alle drei verwendet und folgende Aktionen durchgeführt:

- Hiermit wird die Live Migration auf dem lokalen Host konfiguriert.
- Ermöglicht eingehenden Migrations Datenverkehr nur in einem bestimmten Netzwerk.
- Wählt Kerberos als Authentifizierungsprotokoll aus.

Jede Zeile entspricht einem separaten Befehl.

```
PS C:\> Enable-VMMigration

PS C:\> Set-VMMigrationNetwork 192.168.10.1

PS C:\> Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos
```

Mit "Set-VMHost" können Sie auch eine Leistungs Option (und viele andere Host Einstellungen) auswählen. Wenn Sie z. B. SMB auswählen, aber das Authentifizierungsprotokoll auf den Standardwert von "kredssp" festlegen, geben Sie Folgendes ein:

```
PS C:\> Set-VMHost -VirtualMachineMigrationPerformanceOption SMB
```

In dieser Tabelle wird beschrieben, wie die Leistungsoptionen funktionieren.

OPTION	BESCHREIBUNG
TCP/IP	Der Arbeitsspeicher des virtuellen Computers wird über eine TCP/IP-Verbindung auf den Zielservers kopiert.
Komprimierung	Komprimiert den Speicherinhalt der virtuellen Maschine, bevor Sie über eine TCP/IP-Verbindung auf den Zielservers kopiert wird. Hinweis: Dies ist die Standard Einstellung.
SMB	<p>Der Arbeitsspeicher des virtuellen Computers wird über eine SMB 3,0-Verbindung auf den Zielservers kopiert.</p> <p>-SMB Direct wird verwendet, wenn für die Netzwerkadapter auf den Quell- und Ziel Servern RDMA (Remote Direct Memory Access)-Funktionen aktiviert sind.</p> <p>-SMB Multichannel erkennt und verwendet automatisch mehrere Verbindungen, wenn eine entsprechende SMB Multichannel-Konfiguration identifiziert wird.</p> <p>Weitere Informationen finden Sie unter Optimieren der Leistung von Dateiservern mit "SMB Direct".</p>

Nächste Schritte

Nachdem Sie die Hosts eingerichtet haben, sind Sie bereit, eine Live Migration durchzuführen. Anweisungen hierzu finden [Sie unter Verwenden der Live Migration ohne Failoverclustering zum Verschieben einer virtuellen Maschine](#).

Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2019, Windows Server 2016, Windows Server (halbjährlicher Kanal)

Machen Sie die neuesten Hyper-V-Features auf Ihren virtuellen Computern verfügbar, indem Sie die Konfigurations Version aktualisieren. Gehen Sie dazu erst wie folgt vor:

- Sie aktualisieren Ihre Hyper-V-Hosts auf die neueste Version von Windows oder Windows Server.
- Sie aktualisieren die Cluster Funktionsebene.
- Sie müssen den virtuellen Computer nicht auf einen Hyper-V-Host verschieben, auf dem eine frühere Version von Windows oder Windows Server ausgeführt wird.

Weitere Informationen finden Sie unter [Cluster Operating System Rolling Upgrade](#) und [Durchführen eines parallelen Upgrades eines Hyper-V-Host Clusters in VMM](#).

Schritt 1: Überprüfen der Konfigurations Versionen des virtuellen Computers

1. Klicken Sie auf dem Windows-Desktop auf die Schaltfläche „Start“, und geben Sie einen beliebigen Teil des Namens **Windows PowerShell** ein.
2. Klicken Sie mit der rechten Maustaste auf Windows PowerShell, und wählen Sie **als Administrator ausführen**.
3. Verwenden Sie das Cmdlet [Get-VM](#). Führen Sie den folgenden Befehl aus, um die Versionen Ihrer virtuellen Computer zu erhalten.

```
Get-VM * | Format-Table Name, Version
```

Sie können die Konfigurations Version auch im Hyper-V-Manager anzeigen, indem Sie den virtuellen Computer auswählen und sich die Registerkarte **Zusammenfassung** ansehen.

Schritt 2: Aktualisieren der Konfigurations Version des virtuellen Computers

1. Fahren Sie den virtuellen Computer im Hyper-V-Manager herunter.
2. Wählen Sie Aktion > upgradekonfigurationsversion aus. Wenn diese Option für den virtuellen Computer nicht verfügbar ist, befindet er sich bereits in der höchsten Konfigurations Version, die vom Hyper-V-Host unterstützt wird.

Um die Konfigurations Version des virtuellen Computers mithilfe von Windows PowerShell zu aktualisieren, verwenden Sie das Cmdlet [Update-VMVersion](#) . Führen Sie den folgenden Befehl aus, wobei "VMName" der Name des virtuellen Computers ist.

```
Update-VMVersion <vmname>
```

Unterstützte Konfigurations Versionen für virtuelle Computer

Führen Sie das PowerShell-Cmdlet [Get-vmhostsupportedversion](#) aus, um die vom Hyper-V-Host unterstützten VM-Konfigurations Versionen anzuzeigen. Wenn Sie einen virtuellen Computer erstellen, wird er mit der Standard Konfigurations Version erstellt. Führen Sie den folgenden Befehl aus, um zu sehen, was der Standardwert ist.

```
Get-VMHostSupportedVersion -Default
```

Wenn Sie einen virtuellen Computer erstellen müssen, der zu einem Hyper-V-Host verschoben werden kann, auf dem eine ältere Version von Windows ausgeführt wird, verwenden Sie das Cmdlet [New-VM](#) mit dem Parameter-Version. Um beispielsweise einen virtuellen Computer zu erstellen, den Sie auf einen Hyper-V-Host mit Windows Server 2012 R2 verschieben können, führen Sie den folgenden Befehl aus. Mit diesem Befehl wird ein virtueller Computer namens "WindowsCV5" mit der Konfigurations Version 5,0 erstellt.

```
New-VM -Name "WindowsCV5" -Version 5.0
```

NOTE

Sie können virtuelle Maschinen importieren, die für einen Hyper-V-Host erstellt wurden, auf dem eine ältere Version von Windows ausgeführt wird, oder Sie aus einer Sicherung wiederherstellen. Wenn die Konfigurations Version des virtuellen Computers nicht als unterstützt für das Hyper-V-Host Betriebssystem in der folgenden Tabelle aufgeführt ist, müssen Sie die VM-Konfigurations Version aktualisieren, bevor Sie den virtuellen Computer starten können.

Unterstützte VM-Konfigurations Versionen für lang Zeit Wartungs Hosts

In der folgenden Tabelle sind die VM-Konfigurations Versionen aufgelistet, die auf Hosts unterstützt werden, auf denen eine langfristige Wartungsversion von Windows ausgeführt wird.

WIND OWS- VERSI ON DES HYPER -V- HOSTS	9,1	9,0	8.3	8.2	8.1	8.0	7.1	7.0	6.2	5.0
Windo ws Server 2019	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws 10 Enterp rise LTSC 2019	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws Server 2016	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓

WIND OWS- VERSI ON DES HYPER -V- HOSTS	9,1	9,0	8.3	8.2	8.1	8.0	7.1	7.0	6.2	5.0
Windo ws Server, Versio n 1903	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws Server, Versio n 1809	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws 10- Updat e vom Oktob er 2018 (Versio n 1809)	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws Server, Versio n 1803	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws 10 April 2018- Updat e (Versio n 1803)	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Windo ws 10 Fall Creato rs Updat e (Versio n 1709)	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓

WIND OWS- VERSI ON DES HYPER -V- HOSTS	9,1	9,0	8.3	8.2	8.1	8.0	7.1	7.0	6.2	5.0
Windo ws 10 Creato rs Updat e (Versio n 1703)	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓
Windo ws 10 Annive rsary Updat e (Versio n 1607)	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓

Warum sollte ich die VM-Konfigurations Version aktualisieren?

Beim Verschieben oder Importieren einer virtuellen Maschine auf einen Computer, auf dem Hyper-V unter Windows Server 2019, Windows Server 2016 oder Windows 10 ausgeführt wird, wird die Konfiguration der virtuellen Maschine nicht automatisch aktualisiert. Dies bedeutet, dass Sie den virtuellen Computer zurück auf einen Hyper-V-Host verschieben können, auf dem eine frühere Version von Windows oder Windows Server ausgeführt wird. Dies bedeutet jedoch auch, dass Sie einige der neuen Features für virtuelle Computer erst verwenden können, wenn Sie die Konfigurations Version manuell aktualisieren. Nachdem Sie das Upgrade ausgeführt haben, können Sie die Konfigurations Version des virtuellen Computers nicht herabstufen.

Die Konfigurations Version des virtuellen Computers stellt die Kompatibilität der Konfiguration der virtuellen Maschine, des gespeicherten Zustands und der Momentaufnahme Dateien mit der Hyper-V-Version dar. Wenn Sie die Konfigurations Version aktualisieren, ändern Sie die Dateistruktur, die zum Speichern der Konfiguration der virtuellen Maschinen und der Prüf Punkt Dateien verwendet wird. Außerdem aktualisieren Sie die Konfigurations Version auf die aktuelle Version, die von diesem Hyper-V-Host unterstützt wird. Aktualisierte virtuelle Computer verwenden ein neues Konfigurationsdateiformat, das entworfen wurde, um die Effizienz beim Lesen und Schreiben von VM-Konfigurationsdaten zu steigern. Das Upgrade verringert auch das Potenzial von Datenbeschädigungen bei einem Speicherausfall.

In der folgenden Tabelle sind Beschreibungen, Dateinamen Erweiterungen und Standard Speicherorte für die einzelnen Dateitypen aufgeführt, die für neue oder aktualisierte virtuelle Maschinen verwendet werden.

DATEITYPEN VIRTUELLER COMPUTER	BESCHREIBUNG
Konfiguration	Konfigurationsinformationen für virtuelle Computer, die im Binärdatei Format gespeichert werden. Dateinamenerweiterung: vmcx Standard Speicherort: c:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines

DATEITYPEN VIRTUELLER COMPUTER	BESCHREIBUNG
Lauf Zeit Status	Lauf Zeit Zustandsinformationen des virtuellen Computers, die im Binärdatei Format gespeichert werden. Dateinamenerweiterung: VMRS und. vmgs Standard Speicherort: c:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines
Virtuelle Festplatte	Speichert virtuelle Festplatten für die virtuelle Maschine. Dateinamenerweiterung: VHD-oder vhdx-Datei Standard Speicherort: c:\ProgramData\Microsoft\Windows\Hyper-v\virtuelle Festplatten
Automatische virtuelle Festplatte	Differenzierende Datenträger Dateien, die für Prüfpunkte virtueller Maschinen verwendet werden. Dateinamenerweiterung: avhdx Standard Speicherort: c:\ProgramData\Microsoft\Windows\Hyper-v\virtuelle Festplatten
Prüfpunkt	Prüfpunkte werden in mehreren Prüfpunktdateien gespeichert. Jeder Prüfpunkt erstellt eine Konfigurationsdatei und eine Datei mit dem Laufzeitzustand. Dateinamen Erweiterungen: VMRS und. vmcx Standard Speicherort: c:\programdata\microsoft\windows\momentaufnahmen

Was geschieht, wenn ich die Konfigurations Version des virtuellen Computers nicht Aktualisierungsver?

Wenn Sie über virtuelle Computer verfügen, die Sie mit einer früheren Version von Hyper-V erstellt haben, funktionieren einige Features, die auf dem neueren Host Betriebssystem verfügbar sind, möglicherweise erst dann für diese virtuellen Maschinen, wenn Sie die Konfigurations Version aktualisieren.

Als allgemeine Richtlinie wird empfohlen, die Konfigurations Version zu aktualisieren, nachdem Sie die Virtualisierungshosts erfolgreich auf eine neuere Version von Windows aktualisiert haben, und Sie können sicher sein, dass kein Rollback erforderlich ist. Wenn Sie das Feature für parallele [Upgrades des Cluster](#) Betriebssystems verwenden, liegt dies in der Regel nach dem Aktualisieren der Cluster Funktionsebene. Auf diese Weise profitieren Sie auch von neuen Features, internen Änderungen und Optimierungen.

NOTE

Nachdem die VM-Konfigurations Version aktualisiert wurde, kann der virtuelle Computer nicht auf Hosts gestartet werden, die die aktualisierte Konfigurations Version nicht unterstützen.

In der folgenden Tabelle ist die Mindestversion der VM-Konfiguration aufgeführt, die für die Verwendung einiger Hyper-V-Features erforderlich ist.

FEATURE	MINDESTVERSION DER VM-KONFIGURATION
Speicher bei laufendem Systembetrieb hinzufügen/entfernen	6.2

FEATURE	MINDESTVERSION DER VM-KONFIGURATION
Sicherer Start für Linux-VMs	6.2
Produktionsprüfpunkte	6.2
PowerShell Direct	6.2
VM-Gruppierung	6.2
Virtual Trusted Platform Module (vTPM)	7.0
Mehrere Warteschlangen für virtuelle Computer (vmmq)	7.1
XSAVE-Unterstützung	8.0
Schlüsselspeicher Laufwerk	8.0
Virtualisierungsbasierte Sicherheitsunterstützung (VSB)	8.0
Netzwerkvirtualisierung	8.0
Anzahl virtueller Prozessoren	8.0
Große Arbeitsspeicher-VMS	8.0
Erhöhen Sie die standardmäßige maximale Anzahl von virtuellen Geräten auf 64 pro Gerät (z. b. Netzwerk und zugewiesene Geräte).	8.3
Zusätzliche Prozessor Features für Perfmon zulassen	9,0
Automatisches Bereitstellen der Multithreading - Konfiguration für VMS, die auf Hosts mit dem Kern Planer ausgeführt werden	9,0
Ruhe Zustands Unterstützung	9,0

Weitere Informationen zu diesen Features finden Sie unter [Neues in Hyper-V unter Windows Server](#).

Bereitstellen von Grafik Geräten mithilfe der diskreten Geräte Zuweisung

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Microsoft Hyper-V Server 2016, Windows Server 2016, Windows Server 2019 Microsoft Hyper-V Server 2019

Ab Windows Server 2016 können Sie eine diskrete Geräte Zuweisung oder DDA verwenden, um ein gesamtes PCIe-Gerät an eine VM zu übergeben. Dadurch wird ein hoher Leistungs Zugriff auf Geräte wie [nvme-Speicher](#) oder Grafikkarten innerhalb eines virtuellen Computers ermöglicht, während die Gerätesystem eigene Treiber genutzt werden können. Weitere Informationen zu den einzelnen Geräten, zu den möglichen Auswirkungen auf die Sicherheit usw. finden Sie unter Planen der Bereitstellung von [Geräten mit diskreter Geräte Zuweisung](#).

Die Verwendung eines Geräts mit diskreter Geräte Zuweisung umfasst drei Schritte:

- Konfigurieren der VM für die diskrete Geräte Zuweisung
- Aufheben der Einbindung des Geräts von der Host Partition
- Zuweisen des Geräts zum virtuellen Gastcomputer

Der Befehl "alle" kann auf dem Host in einer Windows PowerShell-Konsole als Administrator ausgeführt werden.

Konfigurieren des virtuellen Computers für DDA

Bei der diskreten Geräte Zuweisung gelten einige Einschränkungen für die VMs, und der folgende Schritt muss ausgeführt werden.

1. Konfigurieren Sie die Aktion "automatisches Abbrechen" eines virtuellen Computers, um durch Ausführen von

```
Set-VM -Name VMName -AutomaticStopAction TurnOff
```

Für Grafikgeräte sind einige zusätzliche VM-Vorbereitung erforderlich.

Einige Hardware Leistung ist besser, wenn der virtuelle Computer auf eine bestimmte Art und Weise konfiguriert ist. Weitere Informationen dazu, ob Sie die folgenden Konfigurationen für Ihre Hardware benötigen, wenden Sie sich an den Hardwarehersteller. Weitere Informationen finden Sie unter Planen der Bereitstellung [von Geräten mithilfe der diskreten Geräte Zuweisung](#) und in diesem [Blogbeitrag](#).

1. Aktivieren der Schreibweise auf der CPU

```
Set-VM -GuestControlledCacheTypes $true -VMName VMName
```

2. Konfigurieren des 32-Bit-MMIO-Speicherplatzes

```
Set-VM -LowMemoryMappedIoSpace 3Gb -VMName VMName
```

3. Mehr als 32-Bit-MMIO-Speicherplatz konfigurieren

```
Set-VM -HighMemoryMappedIoSpace 33280Mb -VMName VMName
```


TIP

Die obigen MMIO-Speicherplatz Werte sind sinnvolle Werte, die für das Experimentieren mit einem einzelnen GPU festgelegt werden. Wenn nach dem Starten des virtuellen Computers ein Fehler im Zusammenhang mit nicht ausreichenden Ressourcen gemeldet wird, müssen Sie diese Werte wahrscheinlich ändern. Weitere Informationen zur genauen Berechnung von MMIO-Anforderungen finden Sie unter Planen der Bereitstellung [von Geräten mit diskreter Geräte Zuweisung](#).

Aufheben der Einbindung des Geräts von der Host Partition

Optional: Installieren des Partitionierungs Treibers

Die diskrete Geräte Zuweisung bietet Hardware-Hersteller die Möglichkeit, einen Sicherheits Entschärfungs Treiber für Ihre Geräte bereitzustellen. Beachten Sie, dass dieser Treiber nicht mit dem Gerätetreiber identisch ist, der auf der Gast-VM installiert wird. Es liegt an dem Ermessen des Hardware Anbieters, diesen Treiber bereitzustellen. Wenn Sie ihn jedoch bereitstellen, installieren Sie ihn, bevor Sie das Gerät von der Host Partition trennen. Wenden Sie sich an den Hardwarehersteller, um weitere Informationen darüber zu erhalten, ob ein Entschärfungs Treiber vorhanden ist.

Wenn kein Partitionierungs Treiber bereitgestellt wird, müssen Sie während der Aufhebung der Bereitstellung die `-force` Option verwenden, um die Sicherheitswarnung zu umgehen. Weitere Informationen zu den Sicherheits Implikationen finden Sie unter Planen der Bereitstellung von [Geräten mit diskreter Geräte Zuweisung](#).

Suchen des Speicher Orts des Geräts

Der PCI-Speicherort Pfad ist erforderlich, um das Gerät vom Host zu entfernen und zu binden. Ein Beispiel für einen Speicherort Pfad sieht wie folgt aus: `"PCIROOT(20)#PCI(0300)#PCI(0000)#PCI(0800)#PCI(0000)"`. Weitere Informationen zum Speicherort Pfad finden Sie hier: Planen der Bereitstellung [von Geräten mit diskreter Geräte Zuweisung](#).

Deaktivieren des Geräts

Stellen Sie mithilfe von Geräte-Manager oder PowerShell sicher, dass das Gerät "deaktiviert" ist.

Aufheben der Einbindung des Geräts

Abhängig davon, ob der Anbieter einen Entschärfungs Treiber bereitgestellt hat, müssen Sie entweder die Option "-Force" verwenden oder nicht.

- Bei Installation eines Entschärfungs Treibers

```
Dismount-VMHostAssignableDevice -LocationPath $locationPath
```

- Wenn ein Entschärfungs Treiber nicht installiert wurde

```
Dismount-VMHostAssignableDevice -force -LocationPath $locationPath
```

Zuweisen des Geräts zum virtuellen Gastcomputer

Der letzte Schritt besteht darin, Hyper-V mitzuteilen, dass ein virtueller Computer Zugriff auf das Gerät haben soll. Zusätzlich zu dem oben gefundenen Speicherort Pfad müssen Sie den Namen des virtuellen Computers kennen.

```
Add-VMAssignableDevice -LocationPath $locationPath -VMName VMName
```

Wie geht es weiter?

Nachdem ein Gerät erfolgreich auf einem virtuellen Computer bereitgestellt wurde, können Sie diesen virtuellen Computer starten und mit dem Gerät interagieren, wie Sie es normalerweise bei einem Bare-Metal-System ausführen würden. Dies bedeutet, dass Sie jetzt die Treiber des Hardware Anbieters auf dem virtuellen Computer installieren können und Anwendungen sehen können, dass die Hardware vorhanden ist. Sie können dies überprüfen, indem Sie in der Gast-VM den Geräte-Manager öffnen und sehen, dass die Hardware jetzt angezeigt wird.

Entfernen eines Geräts und Zurückgeben des Geräts an den Host

Wenn Sie das Gerät wieder in den ursprünglichen Zustand zurücksetzen möchten, müssen Sie den virtuellen Computer unterbinden und folgendes ausgeben:

```
#Remove the device from the VM
Remove-VMAssignableDevice -LocationPath $locationPath -VMName VMName
#Mount the device back in the host
Mount-VMHostAssignableDevice -LocationPath $locationPath
```

Anschließend können Sie das Gerät im Geräte-Manager erneut aktivieren, und das Host Betriebssystem kann erneut mit dem Gerät interagieren.

Beispiel

Einbinden einer GPU an einen virtuellen Computer

In diesem Beispiel verwenden wir PowerShell, um einen virtuellen Computer mit dem Namen "ddatest1" zu konfigurieren, mit dem die erste von der Hersteller-NVIDIA verfügbare GPU übernommen und der VM zugewiesen wird.

```
#Configure the VM for a Discrete Device Assignment
$vm = "ddatest1"
#Set automatic stop action to TurnOff
Set-VM -Name $vm -AutomaticStopAction TurnOff
#Enable Write-Combining on the CPU
Set-VM -GuestControlledCacheTypes $true -VMName $vm
#Configure 32 bit MMIO space
Set-VM -LowMemoryMappedIoSpace 3Gb -VMName $vm
#Configure Greater than 32 bit MMIO space
Set-VM -HighMemoryMappedIoSpace 33280Mb -VMName $vm

#Find the Location Path and disable the Device
#Enumerate all PNP Devices on the system
$pnpdevs = Get-PnpDevice -presentOnly
#Select only those devices that are Display devices manufactured by NVIDIA
$gpudev = $pnpdevs | where-object {$_.Class -like "Display" -and $_.Manufacturer -like "NVIDIA"}
#Select the location path of the first device that's available to be dismounted by the host.
$locationPath = ($gpudev | Get-PnpDeviceProperty DEVPKY_Device_LocationPaths).data[0]
#Disable the PNP Device
Disable-PnpDevice -InstanceId $gpudev[0].InstanceId

#Dismount the Device from the Host
Dismount-VMHostAssignableDevice -force -LocationPath $locationPath

#Assign the device to the guest VM.
Add-VMAssignableDevice -LocationPath $locationPath -VMName $vm
```

Problembehandlung

Wenn Sie eine GPU an eine VM übermitteln haben, Remotedesktop oder eine Anwendung die GPU nicht erkennt, überprüfen Sie die folgenden häufigen Probleme:

- Stellen Sie sicher, dass Sie die neueste Version des unterstützten Treibers des GPU-Anbieters installiert haben und dass der Treiber keine Fehler meldet, indem Sie den Gerätestatus in Geräte-Manager überprüfen.
- Stellen Sie sicher, dass auf Ihrem Gerät ausreichend MMIO-Speicherplatz innerhalb der VM zugeordnet ist. Weitere Informationen finden Sie unter [MMIO-Speicherplatz](#).
- Stellen Sie sicher, dass Sie eine GPU verwenden, die der Anbieter unterstützt, die in dieser Konfiguration verwendet wird. Beispielsweise verhindern einige Anbieter, dass Ihre verbraucherkarten funktionieren, wenn Sie an einen virtuellen Computer übermittelt werden.
- Stellen Sie sicher, dass die Anwendung, die ausgeführt wird, auf einem virtuellen Computer ausgeführt wird und dass sowohl die GPU als auch die zugehörigen Treiber von der Anwendung unterstützt werden. Einige Anwendungen verfügen über Zulassungs Listen mit GPUs und Umgebungen.
- Wenn Sie die Remotedesktop-Sitzungshost-Rolle oder Windows MultiPoint Services auf dem Gast verwenden, müssen Sie sicherstellen, dass ein bestimmter Gruppenrichtlinie Eintrag festgelegt ist, um die Verwendung der Standard-GPU zuzulassen. Wenn Sie ein Gruppenrichtlinie Objekt verwenden, das auf den Gast angewendet wird (oder die Editor für lokale Gruppenrichtlinien auf dem Gast), navigieren Sie zu folgendem Gruppenrichtlinie Element: **Computer Konfiguration > Administrator Vorlagen > Windows-Komponenten ** > Remotedesktopdienste** ** > Remotedesktop-Sitzungshost** > Remote Sitzungs Umgebung > den Hardware-Standard Grafikadapter für alle Remotedesktopdienste Sitzungen verwenden**. Legen Sie diesen Wert auf aktiviert fest, und starten Sie den virtuellen Computer neu, sobald die Richtlinie angewendet wurde.

Bereitstellen von Grafik Geräten mithilfe von remotefx vgpu

27.03.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016

Die vgpu-Funktion für remotefx ermöglicht es mehreren virtuellen Computern, eine physische GPU gemeinsam zu nutzen. Rendering- und computeressourcen werden dynamisch zwischen virtuellen Computern gemeinsam genutzt, sodass remotefx vgpu für hochleistungsfähige Workloads geeignet ist, bei denen keine dedizierten GPU-Ressourcen erforderlich sind. Beispielsweise kann in einem VDI-Dienst remotefx vgpu zum Auslagern von App-renderingkosten an die GPU verwendet werden, wobei die CPU-Auslastung verringert und die Dienst Skalierbarkeit verbessert wird.

Anforderungen für RemoteFX vGPU

Systemanforderungen für den Host:

- Windows Server 2016
- Eine DirectX 11,0-kompatible GPU mit einem WDDM 1,2-kompatiblen Treiber
- Eine CPU mit slat-Unterstützung (Second Level Address Translation)

Anforderungen an die Gast-VM:

- Unterstützte Gast Betriebssysteme. Weitere Informationen finden Sie [unter Unterstützung von remotefx 3D-Video Adaptern \(vgpu\)](#).

Weitere Überlegungen zu Gast-VMs:

- Die Funktionen OpenGL und OpenCL sind nur in Gästen verfügbar, auf denen Windows 10 oder Windows Server 2016 ausgeführt wird.
- DirectX 11,0 ist nur für Gäste verfügbar, auf denen Windows 8 oder höher ausgeführt wird.

Remotefx-vgpu aktivieren

So konfigurieren Sie remotefx vgpu auf dem Windows Server 2016-Host:

1. Installieren Sie die von Ihrem GPU-Anbieter empfohlenen Grafiktreiber für Windows Server 2016.
2. Erstellen eines virtuellen Computers, auf dem ein von remotefx vgpu unterstütztes Gast Betriebssystem ausgeführt wird. Weitere Informationen finden Sie [unter Unterstützung von remotefx 3D-Video Adaptern \(vgpu\)](#).
3. Fügen Sie den remotefx 3D-Grafikadapter der VM hinzu. Weitere Informationen finden Sie unter [Konfigurieren des remotefx-vgpu-3D-Adapters](#).

Standardmäßig verwendet remotefx vgpu alle verfügbaren und unterstützten GPUs. Führen Sie die folgenden Schritte aus, um die von remotefx vgpu verwendeten GPUs einzuschränken:

1. Navigieren Sie zu den Hyper-V-Einstellungen in Hyper-V-Manager.
2. Wählen Sie **physische GPUs** in den Hyper-V-Einstellungen aus.
3. Wählen Sie die nicht zu verwendende GPU aus, und deaktivieren Sie die Option **Diese GPU mit RemoteFX verwenden**.

Konfigurieren des RemoteFX vGPU 3D-Adapters

Sie können entweder die Hyper-V-Manager-Benutzeroberfläche oder die PowerShell-Cmdlets verwenden, um die RemoteFX vGPU 3D-Grafikkarte zu konfigurieren.

Konfigurieren von remotefx vgpu mit dem Hyper-V-Manager

1. Beendet den virtuellen Computer, wenn er gerade ausgeführt wird.
2. Öffnen Sie den Hyper-V-Manager, navigieren Sie zu **VM-Einstellungen**, und wählen Sie dann **Hardware hinzufügen**.
3. Wählen Sie **remotefx 3D-Grafik Adapter** und dann **Hinzufügen** aus.
4. Legen Sie die maximale Anzahl der Monitore, die maximale Monitorauflösung und den dedizierten Videospeicher fest oder übernehmen Sie die Standardwerte.

NOTE

- Wenn Sie höhere Werte für eine dieser Optionen festlegen, wirkt sich dies auf die Dienst Skalierung aus, daher sollten Sie nur die erforderlichen Werte festlegen.
- Wenn Sie 1 GB dedizierten VRAM verwenden müssen, verwenden Sie eine 64-Bit-Gast-VM anstelle von 32-Bit (x86), um optimale Ergebnisse zu erzielen.

5. Wählen Sie **OK** aus, um die Konfiguration abzuschließen.

Konfigurieren von remotefx vgpu mit PowerShell-Cmdlets

Verwenden Sie die folgenden PowerShell-Cmdlets, um den Adapter hinzuzufügen, zu überprüfen und zu konfigurieren:

- [Add-VMRemoteFx3dVideoAdapter](#)
- [Get-VMRemoteFx3dVideoAdapter](#)
- [Set-VMRemoteFx3dVideoAdapter](#)
- [Get-vmremotefxphysicalvideoadapter](#)

Überwachen der Leistung

Die Leistung und Skalierbarkeit eines remotefx-vgpu-fähigen dienstangs werden durch eine Vielzahl von Faktoren festgelegt, wie z. b. die Anzahl von GPUs auf Ihrem System, den gesamten GPU-Arbeitsspeicher, die Menge an System Arbeitsspeicher und die Arbeitsspeicher Geschwindigkeit, die Anzahl der CPU-Kerne und die CPU-Taktfrequenz Ausführungs.

Host System Arbeitsspeicher

Für jede mit einer vgpu aktivierte VM verwendet remotefx den System Arbeitsspeicher sowohl im Gast Betriebssystem als auch auf dem Host Server. Der Hypervisor gewährleistet die Verfügbarkeit von System Arbeitsspeicher für ein Gast Betriebssystem. Auf dem Host muss jeder vgpu-fähige virtuelle Desktop seine Systemspeicher Anforderung für den Hypervisor ankündigen. Beim Starten des vgpu-fähigen virtuellen Desktops reserviert der Hypervisor zusätzlichen System Arbeitsspeicher auf dem Host.

Die Arbeitsspeicher Anforderung für den remotefx-fähigen Server ist dynamisch, weil der auf dem remotefx-fähigen Server belegte Arbeitsspeicher von der Anzahl der Monitore abhängig ist, die den vgpu-fähigen virtuellen Desktops zugeordnet sind, und der maximalen Auflösung für Diese Monitore.

Host-GPU-Videospeicher

Jeder für vgpu aktivierte virtuelle Desktop verwendet den GPU-Hardware Videospeicher auf dem Host Server zum Rendering des Desktops. Außerdem verwendet ein Codec den Videospeicher, um den gerenderten Bildschirm zu komprimieren. Der erforderliche Arbeitsspeicher für das Rendering und die Komprimierung basiert direkt auf der

Anzahl der Monitore, die für den virtuellen Computer bereitgestellt werden. Die Menge des reservierten Grafik Speichers variiert abhängig von der System Bildschirmauflösung und der Anzahl der Monitore, die vorhanden sind. Für einige Benutzer ist eine höhere Bildschirmauflösung für bestimmte Aufgaben erforderlich, aber es gibt eine größere Skalierbarkeit mit Einstellungen mit niedrigerer Auflösung, wenn alle anderen Einstellungen konstant bleiben.

Host-CPU

Der Hypervisor plant den Host und die VMs auf der CPU. Der mehr Aufwand wird auf einem remotefx-fähigen Host gesteigert, da das System einen zusätzlichen Prozess (rdvgm.exe) pro vgpu-aktiviertem virtuellen Desktop ausführt. Dieser Prozess verwendet den Grafikgeräte Treiber zum Ausführen von Befehlen auf der GPU. Der Codec verwendet die CPU auch zum Komprimieren von Bildschirm Daten, die an den Client zurückgesendet werden müssen.

Mehr virtuelle Prozessoren bedeuten eine bessere Benutzer Leistung. Es wird empfohlen, mindestens zwei virtuelle CPUs pro vgpu-aktiviertem virtuellen Desktop zuzuordnen. Außerdem wird die Verwendung der x64-Architektur für vgpu-fähige virtuelle Desktops empfohlen, da die Leistung auf virtuellen x64-Computern besser als x86 Virtual Machines ist.

GPU-Verarbeitungsleistung

Jeder für vgpu aktivierte virtuelle Desktop verfügt über einen entsprechenden DirectX-Prozess, der auf dem Host Server ausgeführt wird. Dieser Prozess gibt alle Grafikbefehle wieder, die er vom virtuellen remotefx-Desktop empfängt, auf die physische GPU. Dies ist vergleichbar mit der gleichzeitig Ausführung mehrerer DirectX-Anwendungen auf derselben physischen GPU.

Normalerweise sind Grafikgeräte und Treiber darauf abgestimmt, nur einige Anwendungen auf dem Desktop auszuführen, aber remotefx dehnt die GPUs noch weiter aus. vgpus enthalten Leistungsindikatoren, die die GPU-Antwort auf remotefx-Anforderungen messen und Sie dabei unterstützen, sicherzustellen, dass die GPUs nicht zu weit gestreckt werden.

Wenn eine GPU wenig Ressourcen hat, dauert die Ausführung von Lese-und Schreibvorgängen lange. Administratoren können mithilfe von Leistungsindikatoren erkennen, wann Ressourcen angepasst und Ausfallzeiten für Benutzer verhindert werden sollen.

Weitere Informationen zu Leistungsindikatoren zum Überwachen von remotefx vgpu-Verhalten finden Sie unter [Diagnostizieren von Problemen mit der Grafikleistung in Remotedesktop](#).

Bereitstellen von nvme-Speichergeräten mithilfe der diskreten Geräte Zuweisung

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Microsoft Hyper-V Server 2016, Windows Server 2016

Ab Windows Server 2016 können Sie eine diskrete Geräte Zuweisung oder DDA verwenden, um ein gesamtes PCIe-Gerät an eine VM zu übergeben. Dadurch wird ein hoher Leistungs Zugriff auf Geräte wie nvme-Speicher oder Grafikkarten innerhalb eines virtuellen Computers ermöglicht, während die Gerätesystem eigene Treiber genutzt werden können. Weitere Informationen zu den einzelnen Geräten, zu den möglichen Auswirkungen auf die Sicherheit usw. finden Sie unter Planen der Bereitstellung von [Geräten mit diskreter Geräte Zuweisung](#). Die Verwendung eines Geräts mit DDA umfasst drei Schritte:

- Konfigurieren des virtuellen Computers für DDA
- Aufheben der Einbindung des Geräts von der Host Partition
- Zuweisen des Geräts zum virtuellen Gastcomputer

Der Befehl "alle" kann auf dem Host in einer Windows PowerShell-Konsole als Administrator ausgeführt werden.

Konfigurieren des virtuellen Computers für DDA

Bei der diskreten Geräte Zuweisung gelten einige Einschränkungen für die VMs, und der folgende Schritt muss ausgeführt werden.

1. Konfigurieren Sie die Aktion "automatisches Abbrechen" eines virtuellen Computers, um durch Ausführen von

```
Set-VM -Name VMName -AutomaticStopAction TurnOff
```

Aufheben der Einbindung des Geräts von der Host Partition

Suchen des Speicher Orts des Geräts

Der PCI-Speicherort Pfad ist erforderlich, um das Gerät vom Host zu entfernen und zu binden. Ein Beispiel für einen Speicherort Pfad sieht wie folgt aus: `"PCIROOT(20)#PCI(0300)#PCI(0000)#PCI(0800)#PCI(0000)"`. Weitere Informationen zum Speicherort Pfad finden Sie hier: Planen der Bereitstellung [von Geräten mit diskreter Geräte Zuweisung](#).

Deaktivieren des Geräts

Stellen Sie mithilfe von Geräte-Manager oder PowerShell sicher, dass das Gerät "deaktiviert" ist.

Aufheben der Einbindung des Geräts

```
Dismount-VMHostAssignableDevice -LocationPath $locationPath
```

Zuweisen des Geräts zum virtuellen Gastcomputer

Der letzte Schritt besteht darin, Hyper-V mitzuteilen, dass ein virtueller Computer Zugriff auf das Gerät haben soll. Zusätzlich zu dem oben gefundenen Speicherort Pfad müssen Sie den Namen des virtuellen Computers kennen.

```
Add-VMAssignableDevice -LocationPath $locationPath -VMName VMName
```

Wie geht es weiter?

Nachdem ein Gerät erfolgreich auf einem virtuellen Computer bereitgestellt wurde, können Sie diesen virtuellen Computer starten und mit dem Gerät interagieren, wie Sie es normalerweise bei einem Bare-Metal-System ausführen würden. Sie können dies überprüfen, indem Sie in der Gast-VM den Geräte-Manager öffnen und sehen, dass die Hardware jetzt angezeigt wird.

Entfernen eines Geräts und Zurückgeben des Geräts an den Host

Wenn Sie das Gerät wieder in den ursprünglichen Zustand zurücksetzen möchten, müssen Sie den virtuellen Computer unterbinden und folgendes ausgeben:

```
#Remove the device from the VM
Remove-VMAssignableDevice -LocationPath $locationPath -VMName VMName
#Mount the device back in the host
Mount-VMHostAssignableDevice -LocationPath $locationPath
```

Anschließend können Sie das Gerät im Geräte-Manager erneut aktivieren, und das Host Betriebssystem kann erneut mit dem Gerät interagieren.

Verwalten von Hyper-V unter Windows Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows Server 2019

Verwenden Sie die Ressourcen in diesem Abschnitt, um Hyper-V unter Windows Server zu verwalten:

- [Konfigurieren von beständigen Speichergeräten für Hyper-V-VMs](#)
- [Wählen zwischen Standard- oder Produktionsprüfpunkten](#)
- [Erstellen eines VHD-Satzes](#)
- [Aktivieren oder Deaktivieren von Prüfpunkten](#)
- [Verwalten des Hosts mit Hyper-V-Manager](#)
- [Verwalten von Host-CPU Ressourcensteuerungen](#)
- [Verwenden von VM-CPU-Gruppen](#)
- [Verwalten von Hypervisor Scheduler-Typen](#)
- [Informationen zur Hyper-V Scheduler-Auswahl](#)
- [Verwalten von Integrationsdiensten](#)
- [Verwalten von Windows-VMs mit PowerShell Direct](#)
- [Einrichten von Hyper-V-Replikaten](#)
- [Aktivieren der Intel Performance Monitoring-Hardware](#)
- [Verschieben von VMs mit Livemigration](#)

Cmdlets zum Konfigurieren von persistenten Speichergeräten für Hyper-V-VMS

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

Dieser Artikel bietet Systemadministratoren und IT-Experten Informationen zum Konfigurieren von Hyper-V-VMS mit persistentem Speicher (Speicher Klassen Speicher oder nvdimms). Jdec-kompatible nvdimms persistente Speichergeräte werden in Windows Server 2016 und Windows 10 unterstützt und ermöglichen den Zugriff auf byteebene auf nicht flüchtige Geräte mit sehr geringer Latenzzeit. Persistente VM-Speichergeräte werden in Windows Server 2019 unterstützt.

Erstellen eines persistenten Speichergeräts für eine VM

Verwenden Sie das Cmdlet **New-VHD**, um ein dauerhaftes Speichergerät für einen virtuellen Computer zu erstellen. Das Gerät muss auf einem vorhandenen NTFS-DAX-Volumen erstellt werden. Die neue Dateinamenerweiterung (vhdpmem) wird verwendet, um anzugeben, dass es sich bei dem Gerät um ein dauerhaftes Speichergerät handelt. Nur das festgelegte VHD-Dateiformat wird unterstützt.

Beispiel: `New-VHD d:\VMPMEMDevice1.vhdpmem -Fixed -SizeBytes 4GB`

Erstellen eines virtuellen Computers mit einem permanenten Speichercontroller

Verwenden Sie das Cmdlet **New-VM**, um einen virtuellen Computer der Generation 2 mit der angegebenen Speichergröße und dem Pfad zu einem vhdx-Image zu erstellen. Verwenden Sie dann **Add-vmppmemcontroller**, um einem virtuellen Computer einen persistenten Speichercontroller hinzuzufügen.

Beispiel:

```
New-VM -Name "ProductionVM1" -MemoryStartupBytes 1GB -VHDPATH c:\vhd\BaseImage.vhdx  
  
Add-VMppmemController ProductionVM1x
```

Anfügen eines permanenten Speichergeräts an einen virtuellen Computer

Verwenden Sie **Add-vmhardddiskdrive**, um ein dauerhaftes Speichergerät an eine VM anzufügen.

Beispiel: `Add-VMHardDiskDrive ProductionVM1 PMEM -ControllerLocation 1 -Path D:\VPMEMDevice1.vhdpmem`

Persistente Speichergeräte in einem virtuellen Hyper-V-Computer werden als persistentes Speichergerät angezeigt, das vom Gast Betriebssystem genutzt und verwaltet werden muss. Gast Betriebssysteme können das Gerät als Block- oder DAX-Volumen verwenden. Wenn persistente Speichergeräte innerhalb eines virtuellen Computers als DAX-Volumen verwendet werden, profitieren Sie von einer geringen Wartezeit für die Adressfähigkeit des Host Geräts (keine e/a-Virtualisierung im Codepfad).

NOTE

Persistenter Speicher wird nur für Hyper-V Gen2-VMS unterstützt. Livemigration-und Speicher Migration werden für virtuelle Computer mit persistentem Arbeitsspeicher nicht unterstützt. Produktions Prüfpunkte von VMS enthalten keinen permanenten Speicherstatus.

Auswählen zwischen Standard-oder Produktions Prüfpunkten in Hyper-V

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Ab Windows Server 2016 und Windows 10 können Sie zwischen Standard-und Produktions Prüfpunkten für jeden virtuellen Computer wählen. Produktions Prüfpunkte sind die Standardeinstellungen für neue virtuelle Computer.

- Produktions Prüfpunkte sind "Zeitpunkt"-Images einer virtuellen Maschine, die später auf eine Weise wieder hergestellt werden können, die für alle produktionsworkloads vollständig unterstützt wird. Dies erfolgt mithilfe von Sicherungstechnologie innerhalb des Gastbetriebssystems zum Erstellen des Prüfpunkts anstatt mit Technologie zum Speichern des Zustands.
- Standard Prüfpunkte erfassen den Zustand, die Daten und die Hardwarekonfiguration eines ausgelaufenen virtuellen Computers und sind für die Verwendung in Entwicklungs-und Testszenarien vorgesehen. Standard Prüfpunkte können nützlich sein, wenn Sie einen bestimmten Zustand oder eine bestimmte Bedingung eines ausgelaufenen virtuellen Computers neu erstellen müssen, damit Sie ein Problem beheben können.

Ändern von Prüfpunkten in Produktions-oder Standard Prüfpunkte

1. Klicken Sie im **Hyper-V-Manager** mit der rechten Maustaste auf den virtuellen Computer, und klicken Sie auf **Einstellungen**.
2. Wählen Sie im Abschnitt **Verwaltung** die Option **Prüfpunkte** aus.
3. Wählen Sie entweder „Produktionsprüfpunkte“ oder „Standardprüfpunkte“ aus.

Wenn Sie Produktions Prüfpunkte auswählen, können Sie auch angeben, ob der Host einen Standard Prüf Punkt akzeptieren soll, wenn ein Produktions Prüf Punkt nicht verwendet werden kann. Wenn Sie dieses Kontrollkästchen deaktivieren und kein Produktions Prüf Punkt erstellt werden kann, wird kein Prüfpunkt erstellt.

4. Wenn Sie die Prüf Punkt Konfigurationsdateien an einem anderen Ort speichern möchten, ändern Sie Sie im Abschnitt **Speicherort** der Prüf Punkt Datei.
5. Klicken Sie auf **über** nehmen, um die Änderungen zu speichern. Wenn Sie fertig sind, klicken Sie auf **OK** , um das Dialogfeld zu schließen.

NOTE

Nur **Produktions Prüfpunkte** werden auf Gast Computern unterstützt, auf denen Active Directory Domain Services Rolle (Domänen Controller) oder Active Directory Lightweight Directory Services Rolle ausgeführt wird.

Siehe auch

- [Produktionsprüfpunkte](#)

- Aktivieren oder Deaktivieren von Prüfpunkten

Erstellen von Hyper-V-VHD-Satz Dateien

01.05.2020 • 3 minutes to read • [Edit Online](#)

VHD-Set-Dateien sind ein neues frei gegebenes virtuelles Datenträger Modell für Gast Cluster in Windows Server 2016. VHD-Set-Dateien unterstützen die Online Größe von freigegebenen virtuellen Datenträgern, unterstützen das Hyper-V-Replikat und können in Anwendungen konsistente Prüfpunkte eingeschlossen werden.

VHD-Satz Dateien verwenden den neuen VHD-Dateityp. VHDs. VHD-Set-Dateien speichern Prüf Punkt Informationen über den virtuellen Gruppen Datenträger, der in Gast Clustern verwendet wird, in Form von Metadaten.

Hyper-V übernimmt alle Aspekte der Verwaltung der Prüf Punkt Ketten und das Zusammenführen des freigegebenen VHD-Satzes. Verwaltungssoftware kann Datenträger Vorgänge wie die Online Änderung der Größe von VHD-Dateien auf die gleiche Weise wie für ausführen. Vhdx-Dateien. Dies bedeutet, dass Verwaltungssoftware nicht über das VHD-Dateiformat informiert werden muss.

NOTE

Es ist wichtig, die Auswirkungen von VHD-Dateien vor der Bereitstellung in der Produktion auszuwerten. Stellen Sie sicher, dass Ihre Umgebung keine Leistungs-oder Funktions Verschlechterung hat, wie z. b. die Datenträger Latenz.

Erstellen einer VHD-Datei im Hyper-V-Manager

1. Öffnen Sie den Hyper-V-Manager. Klicken Sie auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie dann auf **Hyper-V-Manager**.
2. Klicken Sie im Aktionsbereich auf **Neu**, und klicken Sie dann auf **Festplatte**.
3. Wählen Sie auf der Seite Datenträger **Format auswählen** die Option **VHD-Satz** als Format der virtuellen Festplatte aus.
4. Gehen Sie auf den Seiten des Assistenten, um die virtuelle Festplatte anzupassen. Sie können auf **Weiter** klicken, um alle Seiten des Assistenten nacheinander zu bearbeiten. Sie können aber auch im linken Bereich auf den Namen einer Seite klicken, um direkt zu einer Seite zu wechseln.
5. Wenn Sie mit dem Konfigurieren der virtuellen Festplatte fertig sind, klicken Sie auf **Fertig stellen**.

Erstellen einer VHD-Satz Datei aus Windows PowerShell

Verwenden Sie das Cmdlet **New-VHD** mit dem Dateityp. VHDs im Dateipfad. In diesem Beispiel wird eine VHD-Datei mit dem Namen base. VHDs erstellt, die 10 Gigabyte groß ist.

```
PS c:\>New-VHD -Path c:\base.vhds -SizeBytes 10GB
```

Migrieren einer freigegebenen vhdx-Datei in eine VHD-Datei

Zum Migrieren einer vorhandenen freigegebenen vhdx-Datei zu VHDs muss der virtuelle Computer offline geschaltet werden. Dies ist der empfohlene Prozess mithilfe von Windows PowerShell:

1. Entfernen Sie das vhdx von der VM. Führen Sie zum Beispiel aus:

```
PS c:\>Remove-VMHardDiskDrive existing.vhdx
```

2. Konvertieren Sie die vhdx-Datei in eine VHDs. Führen Sie zum Beispiel aus:

```
PS c:\>Convert-VHD existing.vhdx new.vhds
```

3. Fügen Sie die VHDs der VM hinzu. Führen Sie zum Beispiel aus:

```
PS c:\>Add-VMHardDiskDrive new.vhds
```

Aktivieren oder Deaktivieren von Prüfpunkten in Hyper-V

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

Sie können Prüfpunkte für jeden virtuellen Computer aktivieren oder deaktivieren.

1. Klicken Sie im **Hyper-V-Manager** mit der rechten Maustaste auf den virtuellen Computer, und klicken Sie auf **Einstellungen**.
2. Wählen Sie im Abschnitt **Verwaltung** die Option **Prüfpunkte** aus.
3. Vergewissern Sie sich, dass **Prüfpunkte aktivieren** ausgewählt ist, damit dieser virtuelle Computer Prüfpunkte erstellen kann. Zum Deaktivieren von Prüfpunkten deaktivieren Sie das Kontrollkästchen **Prüfpunkte aktivieren**.
4. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern. Wenn Sie fertig sind, klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Siehe auch

[Auswählen zwischen Standard-oder Produktions Prüfpunkten in Hyper-V](#)

Remote Verwaltung von Hyper-v-Hosts mit dem Hyper-v-Manager

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Windows Server 2012 R2, Windows 10, Windows 8.1

In diesem Artikel werden die unterstützten Kombinationen von Hyper-v-Hosts und Hyper-v-Manager-Versionen aufgelistet, und es wird beschrieben, wie Sie eine Verbindung mit Remote- und lokalen Hyper-v-Hosts herstellen, um

Mit dem Hyper-v-Manager können Sie eine kleine Anzahl von Hyper-v-Hosts sowohl Remote als auch lokal verwalten. Die Installation wird bei der Installation der Hyper-v-Verwaltungs Tools installiert, die Sie entweder über eine vollständige Hyper-v-Installation oder eine reine Tools-Installation durchführen können. Wenn Sie eine nur-Tools-Installation durchführen, können Sie die Tools auf Computern verwenden, die die Hardwareanforderungen zum Hosten von Hyper-V nicht erfüllen. Weitere Informationen zu Hardware für Hyper-V-Hosts finden Sie unter [System Anforderungen](#).

Wenn Hyper-V-Manager nicht installiert ist, lesen Sie die [Anweisungen](#) unten.

Unterstützte Kombinationen aus Hyper-v-Manager und Hyper-v-Host Versionen

In einigen Fällen können Sie eine andere Version von Hyper-v-Manager verwenden als die Hyper-v-Version auf dem Host, wie in der Tabelle dargestellt. Wenn Sie dies tun, stellt der Hyper-v-Manager die verfügbaren Funktionen für die Hyper-v-Version auf dem Host bereit, den Sie verwalten. Wenn Sie z. B. die Version von Hyper-v-Manager in Windows Server 2012 R2 verwenden, um einen Host, auf dem Hyper-v unter Windows Server 2012 ausgeführt wird, Remote zu verwalten, können Sie in Windows Server 2012 R2 auf diesem Hyper-v-Host verfügbare Funktionen nicht verwenden.

In der folgenden Tabelle ist aufgeführt, welche Versionen eines Hyper-v-Hosts von einer bestimmten Version von Hyper-v-Manager verwaltet werden können. Es werden nur unterstützte Betriebssystemversionen aufgelistet. Ausführliche Informationen zum Support Status einer bestimmten Betriebssystemversion finden Sie auf der Seite [Microsoft Lifecycle Policy](#) auf der Schaltfläche **Product Lebenszyklus suchen**. Im Allgemeinen können ältere Versionen von Hyper-v-Manager nur einen Hyper-v-Host verwalten, auf dem dieselbe Version oder die vergleichbare Version von Windows Server ausgeführt wird.

HYPER-V-MANAGER-VERSION	HYPER-V-HOST VERSION
Windows 2016, Windows 10	<ul style="list-style-type: none">-Windows Server 2016 – alle Editionen und Installationsoptionen, einschließlich nano Server, und die entsprechende Version von Hyper-V Server-Windows Server 2012 R2 – alle Editionen und Installationsoptionen sowie die entsprechende Version von Hyper-V Server-Windows Server 2012 – alle Editionen und Installationsoptionen und die entsprechende Version von Hyper-V Server-Windows 10-Windows 8.1

HYPER-V-MANAGER-VERSION	HYPER-V-HOST VERSION
Windows Server 2012 R2, Windows 8.1	-Windows Server 2012 R2 – alle Editionen und Installationsoptionen sowie die entsprechende Version von Hyper-V Server -Windows Server 2012 – alle Editionen und Installationsoptionen und die entsprechende Version von Hyper-V Server -Windows 8.1
Windows Server 2012	-Windows Server 2012 – alle Editionen und Installationsoptionen und die entsprechende Version von Hyper-V Server
Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1	-Windows Server 2008 R2 – alle Editionen und Installationsoptionen sowie die entsprechende Version von Hyper-V Server
Windows Server 2008, Windows Vista Service Pack 2	-Windows Server 2008 – alle Editionen und Installationsoptionen und die entsprechende Version von Hyper-V Server

NOTE

Die Service Pack-Unterstützung wurde für Windows 8 am 12. Januar 2016 beendet. Weitere Informationen finden Sie in den [Windows 8.1 FAQ](#).

Herstellen einer Verbindung mit einem Hyper-V-Host

Zum Herstellen einer Verbindung mit einem Hyper-v-Host über den Hyper-v-Manager klicken Sie im linken Bereich mit der rechten Maustaste auf **Hyper-v-Manager** , und klicken Sie dann auf **Verbindung mit Server herstellen**.

Verwalten von Hyper-V auf einem lokalen Computer

Mit dem Hyper-v-Manager werden keine Computer aufgelistet, auf denen Hyper-v gehostet wird, bis Sie den Computer einschließlich eines lokalen Computers hinzufügen. Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Hyper-V-Manager**.
2. Klicken Sie auf **Verbindung mit Server herstellen**.
3. Klicken Sie unter **Computer auswählen** auf **lokaler Computer** , und klicken Sie dann auf **OK**.

Wenn keine Verbindung hergestellt werden kann:

- Es ist möglich, dass nur die Hyper-V-Tools installiert werden. Suchen Sie nach dem Verwaltungsdienst für virtuelle Computer, um zu überprüfen, ob die Hyper-V-Plattform installiert ist. /(Öffnen Sie die Desktop-App für Dienste: Klicken Sie auf **Start**, klicken Sie auf **Start**, geben Sie **Services. ms** ein, und drücken Sie dann die **Eingabe**-Taste. Wenn der Verwaltungsdienst für virtuelle Computer nicht aufgeführt ist, installieren Sie die Hyper-v-Plattform, indem Sie die Anweisungen unter [Installieren von Hyper-v](#) befolgen.
- Überprüfen Sie, ob Ihre Hardware die Anforderungen erfüllt. Siehe [System Anforderungen](#).
- Überprüfen Sie, ob Ihr Benutzerkonto der Gruppe "Administratoren" oder der Gruppe "Hyper-V-Administratoren" angehört.

Remote Verwaltung von Hyper-V-Hosts

Zum Verwalten von Hyper-V-Remote Hosts aktivieren Sie die Remote Verwaltung auf dem lokalen Computer und Remote Host.

Öffnen Sie unter Windows Server Server-Manager >**lokalen Server** >**Remote Verwaltung** , und klicken Sie dann auf **Remote Verbindungen mit diesem Computer zulassen**.

Oder öffnen Sie Windows PowerShell von einem der beiden Betriebssysteme als Administrator, und führen Sie Folgendes aus:

```
Enable-PSRemoting
```

Herstellen einer Verbindung mit Hosts in derselben Domäne

Bei Windows 8.1 und früheren Versionen funktioniert die Remote Verwaltung nur, wenn sich der Host in derselben Domäne befindet und das lokale Benutzerkonto auch auf dem Remote Host ausgeführt wird.

Wählen Sie zum Hinzufügen eines Hyper-v-Remote Hosts zu Hyper-v-Manager **einen anderen Computer** im Dialogfeld **Computer auswählen** aus, und geben Sie den Hostnamen des Remote Hosts, den NetBIOS-Namen oder den voll qualifizierten Domänen Namen (FQDN) ein.

Der Hyper-V-Manager in Windows Server 2016 und Windows 10 bietet mehr Typen von Remote Verbindungen als vorherige Versionen, die in den folgenden Abschnitten beschrieben werden.

Herstellen einer Verbindung mit einem Windows 2016-oder Windows 10-Remote Host als anderer Benutzer

Auf diese Weise können Sie eine Verbindung mit dem Hyper-v-Host herstellen, wenn Sie nicht auf dem lokalen Computer als Benutzer ausgeführt werden, der Mitglied der Gruppe "Hyper-v-Administratoren" oder der Gruppe "Administratoren" auf dem Hyper-v-Host ist. Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Hyper-V-Manager**.
2. Klicken Sie auf **Verbindung mit Server herstellen**.
3. Wählen Sie im Dialogfeld **Computer auswählen** die Option **als anderer Benutzer verbinden** aus.
4. Wählen Sie **Benutzer festlegen** aus.

NOTE

Dies funktioniert nur für Windows Server 2016-oder Windows 10- Remote Hosts.

Herstellen einer Verbindung mit einem Windows 2016-oder Windows 10-Remote Host über die IP-Adresse

Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Hyper-V-Manager**.
2. Klicken Sie auf **Verbindung mit Server herstellen**.
3. Geben Sie die IP-Adresse in das Textfeld **anderer Computer** ein .

NOTE

Dies funktioniert nur für Windows Server 2016-oder Windows 10- Remote Hosts.

Herstellen einer Verbindung mit einem Windows 2016-oder Windows 10-Remote Host außerhalb Ihrer Domäne oder ohne Domäne

Dazu gehen Sie folgendermaßen vor:

1. Öffnen Sie auf dem zu verwaltenden Hyper-V-Host eine Windows PowerShell-Sitzung als Administrator.
2. Erstellen Sie die erforderlichen Firewallregeln für private Netzwerk Zonen:

```
Enable-PSRemoting
```

3. Um den Remote Zugriff auf Öffentliche Zonen zuzulassen, aktivieren Sie Firewallregeln für "kredssp" und "WinRM":

```
Enable-WSManCredSSP -Role server
```

Weitere Informationen finden Sie unter [enable-psremoting](#) und [enable-wsmankredssp](#).

Konfigurieren Sie als nächstes den Computer, den Sie zum Verwalten des Hyper-V-Hosts verwenden.

1. Öffnen Sie eine Windows PowerShell-Sitzung als Administrator.
2. Führen Sie die folgenden Befehle aus:

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value "fqdn-of-hyper-v-host"
```

```
Enable-WSManCredSSP -Role client -DelegateComputer "fqdn-of-hyper-v-host"
```

3. Möglicherweise müssen Sie auch die folgende Gruppenrichtlinie konfigurieren:
 - **Computer Konfiguration > Administrative Vorlagen > Delegierung von Anmelde Informationen für den System > > Zulassen der Delegierung von neuen Anmelde Informationen mit nur NTLM-Server Authentifizierung**
 - Klicken Sie auf **aktivieren** , und fügen Sie *WSMAN/sqdn-of-Hyper-v-Host* hinzu.
4. Öffnen Sie den **Hyper-V-Manager**.
5. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Hyper-V-Manager**.
6. Klicken Sie auf **Verbindung mit Server herstellen**.

NOTE

Dies funktioniert nur für Windows Server 2016-oder Windows 10- **Remote** Hosts.

Informationen zu Cmdlets finden Sie unter [Set-Item](#) und [enable-wsmankredssp](#).

Installieren von Hyper-V-Manager

Wenn Sie ein UI-Tool verwenden möchten, wählen Sie das geeignete für das Betriebssystem auf dem Computer aus, auf dem Sie Hyper-V-Manager ausführen möchten:

Öffnen Sie unter Windows Server Server-Manager > **Verwalten Sie > Rollen und Features hinzufügen**. Wechseln Sie zur Seite " **Features** ", und erweitern Sie **Remote Server-Verwaltungs Tools > Rollen Verwaltungs Tools > Hyper-V-Verwaltungs Tools**.

Unter Windows ist Hyper-v-Manager auf [jedem Windows-Betriebssystem verfügbar, das Hyper-v umfasst](#).

1. Klicken Sie auf dem Windows-Desktop auf die Schaltfläche Start, und geben Sie **Programme und Funktionen** ein.
2. Klicken Sie in den Suchergebnissen auf **Programme und Funktionen**.
3. Klicken Sie im linken **Bereich auf Windows-Funktionen ein-oder ausschalten**.
4. Erweitern Sie den Hyper-v-Ordner, und **Klicken Sie auf Hyper-v-Verwaltungs Tools**.

5. Klicken Sie zum Installieren von Hyper-v-Manager auf **Hyper-v-Verwaltungs Tools**. Wenn Sie auch das Hyper-V-Modul installieren möchten, klicken Sie auf diese Option.

Um Windows PowerShell zu verwenden, führen Sie den folgenden Befehl als Administrator aus:

```
add-windowsfeature rsat-hyper-v-tools
```

Siehe auch

[Installieren von Hyper-V](#)

Verwaltung von CPU-Ressourcen für Hyper-V-Hosts

09.04.2020 • 8 minutes to read • [Edit Online](#)

Die in Windows Server 2016 oder höher eingeführten CPU-Ressourcen Steuerungen für Hyper-v-Hosts ermöglichen Hyper-v-Administratoren, die CPU-Ressourcen des Host Servers zwischen dem Stammverzeichnis, der Verwaltungs Partition und den Gast-VMS besser zu verwalten und zuzuordnen. Mithilfe dieser Steuerelemente können Administratoren eine Teilmenge der Prozessoren eines Host Systems für die Stamm Partition festlegen. Dies kann die von einem Hyper-V-Host ausgeführte Arbeit von den Arbeits Auslastungen, die auf virtuellen Gast Computern ausgeführt werden, trennen, indem Sie Sie in separaten Teilmengen der System Prozessoren ausführen.

Ausführliche Informationen zu Hardware für Hyper-v-Hosts finden Sie unter [System Anforderungen für Windows 10 Hyper-v](#).

Hintergrund

Vor dem Festlegen von Steuerelementen für die CPU-Ressourcen von Hyper-v-Hosts ist es hilfreich, die Grundlagen der Hyper-v-Architektur zu überprüfen.

Eine allgemeine Zusammenfassung finden Sie im Abschnitt "[Hyper-V-Architektur](#)". Dies sind wichtige Konzepte für diesen Artikel:

- Hyper-V erstellt und verwaltet virtuelle Computer Partitionen, für die Compute-Ressourcen zugeordnet und freigegeben werden, unter Kontrolle über den Hypervisor. Partitionen bieten starke Isolations Grenzen zwischen allen virtuellen Gast Computern und zwischen Gast-VMS und der Stamm Partition.
- Die Stamm Partition ist selbst eine virtuelle Computer Partition, obwohl Sie über eindeutige Eigenschaften und weitaus größere Berechtigungen als virtuelle Gastcomputer verfügt. Die Stamm Partition stellt die Verwaltungsdienste zur Verfügung, die alle virtuellen Gastcomputer steuern, Unterstützung für virtuelle Geräte für Gäste bereitstellen und alle Geräte-e/a für virtuelle Gast Maschinen verwalten. Microsoft empfiehlt dringend, keine anwendungsworkloads in einer Host Partition auszuführen.
- Jeder virtuelle Prozessor (VP) der Stamm Partition ist 1:1 einem zugrunde liegenden logischen Prozessor (LP) zugeordnet. Ein Host-VP wird immer auf der gleichen zugrunde liegenden LP ausgeführt – es gibt keine Migration der VPS der Stamm Partition.
- Standardmäßig können die LPs, auf denen Host-VPS ausgeführt wird, auch Gast-VPS ausführen.
- Ein Gast-VP kann vom Hypervisor geplant werden, damit er auf allen verfügbaren logischen Prozessoren ausgeführt werden kann. Der Hypervisor-Planer kümmert sich um die zeitliche Cache Lokalität, die NUMA-Topologie und viele andere Faktoren beim Planen eines Gast-VP-Diensts. letztlich könnte der VP auf jeder Host-LP geplant werden.

Die minimale Stamm-oder minroot-Konfiguration

Für frühe Versionen von Hyper-V gab es eine Obergrenze von 64 VPS pro Partition. Dies gilt sowohl für die Stamm- als auch für die Gast Partitionen. Da Systeme mit mehr als 64 logischen Prozessoren auf High-End-Servern auftraten, hat Hyper-V auch seine Host Skalierungs Grenzwerte entwickelt, um diese größeren Systeme zu unterstützen. zu einem Punkt, der einen Host mit bis zu 320 LPS unterstützt. Allerdings hat das Limit von 64 VP pro Partition zu diesem Zeitpunkt eine Reihe von Herausforderungen und die Komplexität eingeführt, die die Unterstützung von mehr als 64 VPS pro Partition beeinträchtigen. Um dies zu beheben, beschränkte Hyper-V die Anzahl der VPS, die auf die Stamm Partition festgestellt wurden, auf 64, auch wenn auf dem zugrunde liegenden

Computer Viele logische Prozessoren verfügbar waren. Der Hypervisor verwendet weiterhin alle verfügbaren LPs für das Ausführen von Gast-VPS, aber die Stamm Partition wird bei 64 künstlich gekappt. Diese Konfiguration wurde als "minimale Stamm"-oder "minroot"-Konfiguration bezeichnet. Leistungstests bestätigten, dass der Stamm selbst bei großen Systemen mit mehr als 64 LPs nicht mehr als 64 Stamm-VPS benötigt, um eine ausreichende Unterstützung für eine große Anzahl von Gast-VMS und Gast-VPS zu bieten – tatsächlich waren viel weniger als 64 Stamm-VPS häufig ausreichend, abhängig von der Anzahl und Größe der Gast-VMS. , die jeweils ausgeführter Workloads usw.

Dieses "minroot"-Konzept wird heute weiterhin verwendet. Auch wenn Windows Server 2016 Hyper-V seine maximale Architekturunterstützung für Host LPs auf 512 LPs erweitert hat, ist die Stamm Partition weiterhin auf maximal 320 LPs beschränkt.

Verwenden von minroot zum einschränken und Isolieren von hostcomputerressourcen

Mit dem hohen Standard Schwellenwert von 320 LPs in Windows Server 2016 Hyper-V wird die minroot-Konfiguration nur auf den größten Server Systemen verwendet. Diese Funktion kann jedoch vom Hyper-V-Host Administrator auf einen wesentlich niedrigeren Schwellenwert festgelegt werden. Dadurch wird die Menge der verfügbaren Host-CPU-Ressourcen für die Stamm Partition stark eingeschränkt. Die genaue Anzahl der zu verwendenden Stamm-LPs muss natürlich sorgfältig ausgewählt werden, um die maximalen Anforderungen der virtuellen Computer und Arbeits Auslastungen zu unterstützen, die dem Host zugeordnet sind. Allerdings können angemessene Werte für die Anzahl der Host LPs durch sorgfältige Bewertung und Überwachung von produktionsworkloads ermittelt und in nicht produktiven Umgebungen vor umfassender Bereitstellung überprüft werden.

Aktivieren und Konfigurieren von minroot

Die minroot-Konfiguration wird über Hypervisor-BCD-Einträge gesteuert. So aktivieren Sie minroot von einer cmd-Eingabeaufforderung mit Administratorrechten:

```
bcdedit /set hypervisorrootproc n
```

Dabei steht n für die Anzahl der Stamm-VPS.

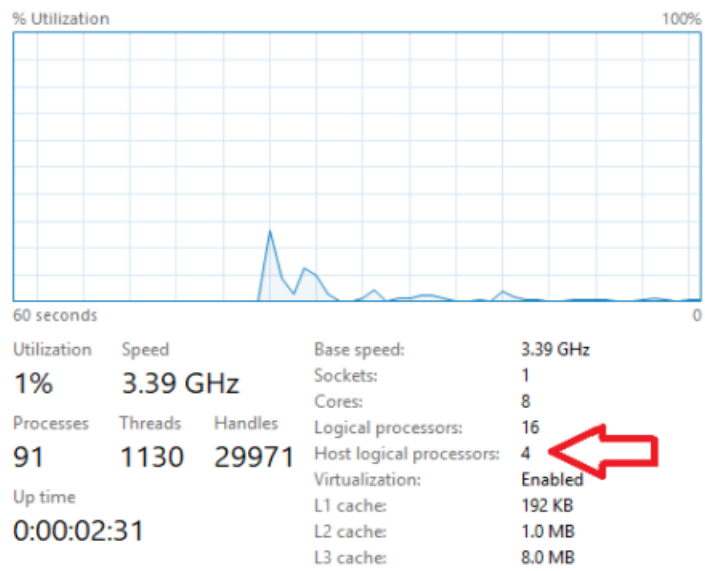
Das System muss neu gestartet werden, und die neue Anzahl der Stamm Prozessoren bleibt für die Lebensdauer des Betriebssystems erhalten. Die minroot-Konfiguration kann zur Laufzeit nicht dynamisch geändert werden.

Wenn mehrere NUMA-Knoten vorhanden sind, erhält jeder Knoten `n/NumaNodeCount` Prozessoren.

Beachten Sie, dass Sie bei mehreren NUMA-Knoten sicherstellen müssen, dass die Topologie der VM so hoch ist, dass auf jedem NUMA-Knoten ausreichend freie LPs (d.h. LPs ohne Stamm-VPS) vorhanden sind, um die entsprechenden NUMA-Knoten-VPS des virtuellen Computers auszuführen.

Die minroot-Konfiguration wird überprüft.

Sie können die minroot-Konfiguration des Hosts mit dem Task-Manager überprüfen, wie unten gezeigt.



Wenn minroot aktiv ist, zeigt der Task-Manager zusätzlich zur Gesamtanzahl der logischen Prozessoren im System die Anzahl der logischen Prozessoren an, die dem Host derzeit zugewiesen sind.

Ressourcen Steuerelemente für virtuelle Maschinen

13.05.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

In diesem Artikel werden die Hyper-V-Ressourcen- und Isolations Steuerelemente für virtuelle Computer beschrieben. Diese Funktionen, die wir als VM-CPU-Gruppen oder einfach "CPU-Gruppen" bezeichnen, wurden in Windows Server 2016 eingeführt. Mit CPU-Gruppen können Hyper-V-Administratoren die CPU-Ressourcen des Hosts auf virtuellen Gast Computern besser verwalten und zuordnen. Mithilfe von CPU-Gruppen können Hyper-V-Administratoren folgende Aktionen ausführen:

- Erstellen Sie Gruppen von virtuellen Computern, wobei jede Gruppe über unterschiedliche Belegungen der gesamten CPU-Ressourcen des Virtualisierungshosts verfügt, die für die gesamte Gruppe freigegeben sind. Dadurch kann der Host Administrator Dienst Klassen für verschiedene Typen von VMS implementieren.
- Legen Sie CPU-Ressourcen Limits auf bestimmte Gruppen fest. Diese "Gruppen Abdeckung" legt die obere Grenze für die Host-CPU-Ressourcen fest, die von der gesamten Gruppe genutzt werden können, und erzwingt effektiv die gewünschte Dienstklasse für diese Gruppe.
- Beschränken Sie eine CPU-Gruppe so, dass Sie nur auf einem bestimmten Satz der Prozessoren des Host Systems ausgeführt wird. Dies kann verwendet werden, um VMS zu isolieren, die zu verschiedenen CPU-Gruppen gehören.

Verwalten von CPU-Gruppen

CPU-Gruppen werden über den Hyper-V-hostcomputedienst oder HCS verwaltet. Im Blog des Microsoft-Virtualisierungsteams finden Sie eine gute Beschreibung der HCS, der dazugehörigen Informationen, Links zu den HCS-APIs und weitere Informationen zum Microsoft-virtualisierungsteamblog im Beitrag [Introducing the Host Compute Service \(HCS\)](#).

NOTE

Nur die HCS können zum Erstellen und Verwalten von CPU-Gruppen verwendet werden. Die WMI- und PowerShell-Verwaltungs Schnittstellen von Hyper-V-Manager unterstützen keine CPU-Gruppen.

Microsoft stellt ein Befehlszeilen-Hilfsprogramm `cpugroups.exe` im [Microsoft Download Center](#) zur Verfügung, das die HCS-Schnittstelle zum Verwalten von CPU-Gruppen verwendet. Dieses Hilfsprogramm kann auch die CPU-Topologie eines Hosts anzeigen.

Funktionsweise von CPU-Gruppen

Die Zuordnung von hostcomputerressourcen über CPU-Gruppen hinweg wird durch den Hyper-V-Hypervisor erzwungen, indem eine berechnete CPU-Gruppe verwendet wird. Die CPU-Gruppen Abdeckung ist ein Bruchteil der CPU-Gesamtkapazität für eine CPU-Gruppe. Der Wert der Gruppen Abdeckung hängt von der Gruppenklasse bzw. der zugewiesenen Prioritätsstufe ab. Das Ende der berechneten Gruppe kann als "Zahl der CPU-Zeit in LP" betrachtet werden. Dieses Gruppen Budget ist freigegeben, wenn nur ein einzelner virtueller Computer aktiv war, könnte die CPU-Belegung der gesamten Gruppe für sich selbst verwendet werden.

Das Limit für die CPU-Gruppe wird als $G = n \times C$ berechnet, wobei Folgendes gilt:

G is the amount of host LP we'd like to assign to the group
n is the total number of logical processors (LPs) in the group
C is the maximum CPU allocation – that is, the class of service desired for the group, expressed as a percentage of the system's total compute capacity

Nehmen Sie beispielsweise eine CPU-Gruppe, die mit 4 logischen Prozessoren (LPs) konfiguriert ist, und eine Obergrenze von 50%.

$G = n * C$
 $G = 4 * 50\%$
 $G = 2 \text{ LP's worth of CPU time for the entire group}$

In diesem Beispiel wird der CPU-Zeit von 2 LP die CPU-Zeit von 2 LP zugewiesen.

Beachten Sie, dass das Gruppen Limit unabhängig von der Anzahl von virtuellen Computern oder virtuellen Prozessoren, die an die Gruppe gebunden sind, und unabhängig vom Zustand (z. b. Herunterfahren oder starten) der virtuellen Computer, die der CPU-Gruppe zugewiesen sind, gilt. Daher erhält jeder an die gleiche CPU-Gruppe gebundene virtuelle Computer einen Bruchteil der Gesamt-CPU-Belegung der Gruppe. Dies ändert sich mit der Anzahl der VMS, die an die CPU-Gruppe gebunden sind. Daher muss bei virtuellen Computern, die an eine CPU-Gruppe gebunden oder ungebunden sind, das Gesamtlimit für die CPU-Gruppe umgelesen und so festgelegt werden, dass die gewünschte Obergrenze pro VM beibehalten wird. Die Software Schicht des VM-Host Administrators oder der Virtualisierungsverwaltung ist für die Verwaltung von Gruppen Limits nach Bedarf zuständig, um die gewünschte CPU-Ressourcen Zuordnung pro VM zu erzielen.

Beispiele für Dienst Klassen

Sehen wir uns einige einfache Beispiele an. Angenommen, der Hyper-V-Host Administrator möchte zwei Dienst Ebenen für Gast-VMS unterstützen:

1. Eine Low-End-Ebene "C". Wir legen dieser Ebene 10% der Compute-Ressourcen des gesamten Hosts zu.
2. Eine mittlere "B"-Ebene. Dieser Ebene werden 50% der Compute-Ressourcen des gesamten Hosts zugeordnet.

An dieser Stelle in unserem Beispiel wird bestätigt, dass keine anderen CPU-Ressourcen Steuerungen verwendet werden, wie z. b. einzelne VM-Caps, Gewichtungen und Reserven. Einzelne VM-Caps sind jedoch wichtig, da wir später etwas später sehen werden.

Der Einfachheit halber gehen wir davon aus, dass jeder virtuelle Computer über 1 VP verfügt und dass der Host über 8 LPs verfügt. Wir beginnen mit einem leeren Host.

Zum Erstellen der Ebene "B" legt der Host-adminstartor die Gruppen Abdeckung auf 50% fest:

$G = n * C$
 $G = 8 * 50\%$
 $G = 4 \text{ LP's worth of CPU time for the entire group}$

Der Host Administrator fügt einen einzelnen virtuellen Computer der Ebene "B" hinzu. An diesem Punkt kann der VM "B" der Ebene "B" höchstens 50% der CPU des Hosts oder das Äquivalent von 4 LPs in unserem Beispiel System verwenden.

Nun fügt der Administrator einen zweiten virtuellen Computer der Ebene "Ebene B" hinzu. Die Zuordnung der CPU-Gruppe – wird gleichmäßig auf alle virtuellen Computer aufgeteilt. Wir haben insgesamt 2 virtuelle Computer in Gruppe b, sodass jeder virtuelle Computer nun die Hälfte der Gruppe b insgesamt 50%, 25% oder die Entsprechung von 2 LPs der COMPUTE-Zeit erhält.

Festlegen von CPU-Caps auf einzelnen VMS

Zusätzlich zum Gruppen Limit kann jede VM auch eine einzelne "VM-Obergrenze" aufweisen. Die CPU-Ressourcenkontrolle pro VM, einschließlich einer CPU-Abdeckung, Gewichtung und Reserve, ist seit der Einführung Teil von Hyper-V. In Kombination mit einer Gruppen Abdeckung gibt eine VM-Obergrenze die maximale CPU-Kapazität an, die jeder VP erhalten kann. Dies gilt auch, wenn für die Gruppe CPU-Ressourcen verfügbar sind.

Beispielsweise kann es vorkommen, dass der Host Administrator eine VM-Obergrenze von 10% auf "C"-VMS platzieren möchte. Dies ist auch der Fall, wenn sich die meisten VPS "C" im Leerlauf befinden, kann jeder VP nie mehr als 10% erhalten. Ohne eine VM-Obergrenze könnten "C"-VMS die Leistung auf der Basis der durch ihre Ebene zulässigen Stufen erreichen.

Isolieren von VM-Gruppen für bestimmte Host Prozessoren

Hyper-V-Host Administratoren können auch die Möglichkeit haben, Compute-Ressourcen für einen virtuellen Computer zu verwenden. Stellen Sie sich z. b. vor, dass der Administrator eine Premium-VM mit einer Klasse von 100% anbieten möchte. Diese Premium-VMS erfordern außerdem die niedrigste Zeit für Zeitplanung und Jitter. Das heißt, Sie werden möglicherweise nicht von einem anderen virtuellen Computer aufgehoben. Um diese Trennung zu erreichen, kann eine CPU-Gruppe auch mit einer bestimmten LP-Affinitäts Zuordnung konfiguriert werden.

Um z. b. in unserem Beispiel eine "A"-VM auf dem Host zu integrieren, erstellt der Administrator eine neue CPU-Gruppe und legt die Prozessor Affinität der Gruppe auf eine Teilmenge der LPs des Hosts fest. Die Gruppen B und C werden den verbleibenden LPs zugeordnet. Der Administrator könnte einen einzelnen virtuellen Computer in Gruppe a erstellen, der dann exklusiven Zugriff auf alle LPs in Gruppe a hätte, während die Gruppen B und C der niedrigeren Ebene die verbleibenden LPs freigeben würden.

Trennen von Stamm-VPS von Gast-VPS

Standardmäßig wird in Hyper-V auf jeder zugrunde liegenden physischen LP eine Stamm-VP erstellt. Diese Stamm-VPS sind der System LPs strikt 1:1 zugeordnet und werden nicht migriert – das heißt, dass jeder Stamm-VP immer auf derselben physischen LP ausgeführt wird. Gast-VPS können auf jeder verfügbaren LP ausgeführt werden und werden die Ausführung mit Stamm-VPS freigeben.

Es kann jedoch wünschenswert sein, die Stamm-VP-Aktivität von Gast-VPS vollständig zu trennen. Sehen Sie sich unser Beispiel oben an, in dem wir einen virtuellen Premium-Tarif "a" implementieren. Um sicherzustellen, dass die VPS der "A"-VM die geringstmögliche Latenz und "Jitter" oder die Zeitplanung aufweisen, möchten wir Sie auf einem dedizierten Satz von LPs ausführen und sicherstellen, dass der Stamm nicht auf diesen LPs ausgeführt wird.

Dies kann mithilfe einer Kombination aus der "minroot"-Konfiguration erreicht werden, wodurch die Host-Betriebssystem Partition auf eine Teilmenge der logischen Gesamt Systemprozessoren und mindestens eine affinisierte CPU-Gruppe beschränkt wird.

Der Virtualisierungshost kann so konfiguriert werden, dass die Host Partition auf bestimmte LPs beschränkt wird, wobei eine oder mehrere CPU-Gruppen den verbleibenden LPs zugeordnet werden. Auf diese Weise können die Stamm- und Gast Partitionen auf dedizierten CPU-Ressourcen und vollständig isoliert und ohne CPU-Freigabe ausgeführt werden.

Weitere Informationen zur Konfiguration von "minroot" finden Sie unter [Hyper-V-Host-CPU-Ressourcenverwaltung](#).

Verwenden des cpugroups-Tools

Sehen wir uns nun einige Beispiele für die Verwendung des cpugroups-Tools an.

NOTE

Befehlszeilenparameter für das cpugroups-Tool werden nur mithilfe von Leerzeichen als Trennzeichen übergeben. Keine Zeichen "/" oder "-" sollten den gewünschten Befehls Zeilenschalter fortsetzen.

Ermitteln der CPU-Topologie

Das Ausführen von cpugroups mit der getcpuproperty-Funktion gibt Informationen zum aktuellen System zurück, wie unten dargestellt, einschließlich des LP-Indexes, des NUMA-Knotens, zu dem die LP gehört, der Paket- und Kern-IDs und des Stamm-VP-Index.

Das folgende Beispiel zeigt ein System mit 2 CPU-Sockets und NUMA-Knoten, insgesamt 32 LPs und Multithreading aktiviert und so konfiguriert, dass minroot mit 8 Stamm-VPS und 4 von jedem NUMA-Knoten aktiviert wird. Die LPs mit Stamm-VPS haben einen rootvpindex >= 0; LPs mit einem rootvpindex von "-1" sind für die Stamm Partition nicht verfügbar, werden jedoch weiterhin vom Hypervisor verwaltet und führen Gast-VPS wie von anderen Konfigurationseinstellungen zugelassen aus.

```
C:\vm\tools>CpuGroups.exe GetCpuTopology
```

LpIndex	NodeNumber	PackageId	CoreId	RootVpIndex
0	0	0	0	0
1	0	0	0	1
2	0	0	1	2
3	0	0	1	3
4	0	0	2	-1
5	0	0	2	-1
6	0	0	3	-1
7	0	0	3	-1
8	0	0	4	-1
9	0	0	4	-1
10	0	0	5	-1
11	0	0	5	-1
12	0	0	6	-1
13	0	0	6	-1
14	0	0	7	-1
15	0	0	7	-1
16	1	1	16	4
17	1	1	16	5
18	1	1	17	6
19	1	1	17	7
20	1	1	18	-1
21	1	1	18	-1
22	1	1	19	-1
23	1	1	19	-1
24	1	1	20	-1
25	1	1	20	-1
26	1	1	21	-1
27	1	1	21	-1
28	1	1	22	-1
29	1	1	22	-1
30	1	1	23	-1
31	1	1	23	-1

Beispiel 2 – Drucken aller CPU-Gruppen auf dem Host

Hier werden alle CPU-Gruppen auf dem aktuellen Host, die groupID, die CPU-Abdeckung der Gruppe und die der Gruppe zugewiesenen LPs aufgelistet.

Beachten Sie, dass gültige Werte für die CPU-Abdeckung im Bereich [0, 65536] liegen und dass diese Werte die Gruppen Abdeckung in Prozent (z. b. 32768 = 50%) Ausdrücken.

```
C:\vm\tools>CpuGroups.exe GetGroups
```

CpuGroupId	CpuCap	LpIndexes
36AB08CB-3A76-4B38-992E-000000000002	32768	4,5,6,7,8,9,10,11,20,21,22,23
36AB08CB-3A76-4B38-992E-000000000003	65536	12,13,14,15
36AB08CB-3A76-4B38-992E-000000000004	65536	24,25,26,27,28,29,30,31

Beispiel 3 – Drucken einer einzelnen CPU-Gruppe

In diesem Beispiel fragen wir eine einzelne CPU-Gruppe mithilfe der groupid als Filter ab.

```
C:\vm\tools>CpuGroups.exe GetGroups /GroupId:36AB08CB-3A76-4B38-992E-000000000003
```

CpuGroupId	CpuCap	LpIndexes
36AB08CB-3A76-4B38-992E-000000000003	65536	12,13,14,15

Beispiel 4 – Erstellen einer neuen CPU-Gruppe

Hier erstellen wir eine neue CPU-Gruppe, die die Gruppen-ID und den Satz von LPs angibt, der der Gruppe zugewiesen werden soll.

```
C:\vm\tools>CpuGroups.exe CreateGroup /GroupId:36AB08CB-3A76-4B38-992E-000000000001 /GroupAffinity:0,1,16,17
```

Zeigen Sie jetzt die neu hinzugefügte Gruppe an.

```
C:\vm\tools>CpuGroups.exe GetGroups
```

CpuGroupId	CpuCap	LpIndexes
36AB08CB-3A76-4B38-992E-000000000001	65536	0,1,16,17
36AB08CB-3A76-4B38-992E-000000000002	32768	4,5,6,7,8,9,10,11,20,21,22,23
36AB08CB-3A76-4B38-992E-000000000003	65536	12,13,14,15
36AB08CB-3A76-4B38-992E-000000000004	65536	24,25,26,27,28,29,30,31

Beispiel 5 – Festlegen der CPU-Gruppen Abdeckung auf 50%

Hier legen wir das Limit für die CPU-Gruppe auf 50% fest.

```
C:\vm\tools>CpuGroups.exe SetGroupProperty /GroupId:36AB08CB-3A76-4B38-992E-000000000001 /CpuCap:32768
```

Nun bestätigen wir unsere Einstellung, indem wir die soeben aktualisierte Gruppe anzeigen.

```
C:\vm\tools>CpuGroups.exe GetGroups /GroupId:36AB08CB-3A76-4B38-992E-000000000001
```

CpuGroupId	CpuCap	LpIndexes
36AB08CB-3A76-4B38-992E-000000000001	32768	0,1,16,17

Beispiel 6 – Drucken von CPU-Gruppen-IDs für alle virtuellen Computer auf dem Host

```
C:\vm\tools>CpuGroups.exe GetVmGroup
```

VmName	VmId	CpuGroupId
G2 4ABCFC2F-6C22-498C-BB38-7151CE678758	36ab08cb-3a76-4b38-992e-000000000002	
P1 973B9426-0711-4742-AD3B-D8C39D6A0DEC	36ab08cb-3a76-4b38-992e-000000000003	
P2 A593D93A-3A5F-48AB-8862-A4350E3459E8	36ab08cb-3a76-4b38-992e-000000000004	
G3 B0F3FCD5-FECF-4A21-A4A2-DE4102787200	36ab08cb-3a76-4b38-992e-000000000002	
G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC	36ab08cb-3a76-4b38-992e-000000000002	

Beispiel 7 – Aufheben der Bindung eines virtuellen Computers an die CPU-Gruppe

Wenn Sie einen virtuellen Computer aus einer CPU-Gruppe entfernen möchten, legen Sie die cpugroupid der VM auf die GUID NULL fest. Dadurch wird die Bindung der VM an die CPU-Gruppe entbindet.

```
C:\vm\tools>CpuGroups.exe SetVmGroup /VmName:g1 /GroupId:00000000-0000-0000-0000-000000000000
```

```
C:\vm\tools>CpuGroups.exe GetVmGroup
```

VmName	VmId	CpuGroupId
G2 4ABCFC2F-6C22-498C-BB38-7151CE678758	36ab08cb-3a76-4b38-992e-000000000002	
P1 973B9426-0711-4742-AD3B-D8C39D6A0DEC	36ab08cb-3a76-4b38-992e-000000000003	
P2 A593D93A-3A5F-48AB-8862-A4350E3459E8	36ab08cb-3a76-4b38-992e-000000000004	
G3 B0F3FCD5-FECF-4A21-A4A2-DE4102787200	36ab08cb-3a76-4b38-992e-000000000002	
G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC	00000000-0000-0000-0000-000000000000	

Beispiel 8 – Binden eines virtuellen Computers an eine vorhandene CPU-Gruppe

Hier fügen wir eine VM zu einer vorhandenen CPU-Gruppe hinzu. Beachten Sie, dass der virtuelle Computer nicht an eine vorhandene CPU-Gruppe gebunden werden darf, oder das Festlegen der CPU-Gruppen-ID schlägt fehl.

```
C:\vm\tools>CpuGroups.exe SetVmGroup /VmName:g1 /GroupId:36AB08CB-3A76-4B38-992E-000000000001
```

Vergewissern Sie sich nun, dass der virtuelle Computer in der gewünschten CPU-Gruppe ist.

```
C:\vm\tools>CpuGroups.exe GetVmGroup
```

VmName	VmId	CpuGroupId
G2 4ABCFC2F-6C22-498C-BB38-7151CE678758	36ab08cb-3a76-4b38-992e-000000000002	
P1 973B9426-0711-4742-AD3B-D8C39D6A0DEC	36ab08cb-3a76-4b38-992e-000000000003	
P2 A593D93A-3A5F-48AB-8862-A4350E3459E8	36ab08cb-3a76-4b38-992e-000000000004	
G3 B0F3FCD5-FECF-4A21-A4A2-DE4102787200	36ab08cb-3a76-4b38-992e-000000000002	
G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC	36AB08CB-3A76-4B38-992E-000000000001	

Beispiel 9 – Drucken aller VMS gruppiert nach CPU-Gruppen-ID

```
C:\vm\tools>CpuGroups.exe GetGroupVms
```

CpuGroupId	VmName	VmId
36AB08CB-3A76-4B38-992E-000000000001	G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC	
36ab08cb-3a76-4b38-992e-000000000002	G2 4ABCFC2F-6C22-498C-BB38-7151CE678758	
36ab08cb-3a76-4b38-992e-000000000002	G3 B0F3FCD5-FECF-4A21-A4A2-DE4102787200	
36ab08cb-3a76-4b38-992e-000000000003	P1 973B9426-0711-4742-AD3B-D8C39D6A0DEC	
36ab08cb-3a76-4b38-992e-000000000004	P2 A593D93A-3A5F-48AB-8862-A4350E3459E8	

Beispiel 10 – Drucken aller VMs für eine einzelne CPU-Gruppe

```
C:\vm\tools>CpuGroups.exe GetGroupVms /GroupId:36ab08cb-3a76-4b38-992e-000000000002
```

CpuGroupId	VmName	VmId
36ab08cb-3a76-4b38-992e-000000000002	G2 4ABCFC2F-6C22-498C-BB38-7151CE678758	
36ab08cb-3a76-4b38-992e-000000000002	G3 B0F3FCD5-FECF-4A21-A4A2-DE4102787200	

Beispiel 11 – Versuch, eine nicht leere CPU-Gruppe zu löschen

Nur leere CPU-Gruppen – d. h. CPU-Gruppen ohne gebundene VMs – können gelöscht werden. Beim Versuch, eine nicht leere CPU-Gruppe zu löschen, tritt ein Fehler auf.

```
C:\vm\tools>CpuGroups.exe DeleteGroup /GroupId:36ab08cb-3a76-4b38-992e-000000000001
(null)
Failed with error 0xc0350070
```

Beispiel 12 – Aufheben der Bindung des einzigen virtuellen Computers an eine CPU-Gruppe und Löschen der Gruppe

In diesem Beispiel verwenden wir mehrere Befehle zum Überprüfen einer CPU-Gruppe, zum Entfernen der einzelnen VM, die zu dieser Gruppe gehört, und zum Löschen der Gruppe.

Zuerst zählen wir die VMs in unserer Gruppe.

```
C:\vm\tools>CpuGroups.exe GetGroupVms /GroupId:36AB08CB-3A76-4B38-992E-000000000001
CpuGroupId          VmName          VmId
-----
36AB08CB-3A76-4B38-992E-000000000001  G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC
```

Wir sehen, dass nur eine einzelne VM mit dem Namen "G1" zu dieser Gruppe gehört. Entfernen Sie den virtuellen Computer mit dem Namen "G1" aus unserer Gruppe, indem Sie die Gruppen-ID der VM auf NULL festlegen.

```
C:\vm\tools>CpuGroups.exe SetVmGroup /VmName:g1 /GroupId:00000000-0000-0000-0000-000000000000
```

Und überprüfen Sie unsere Änderung...

```
C:\vm\tools>CpuGroups.exe GetVmGroup /VmName:g1
VmName          VmId          CpuGroupId
-----
G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC 00000000-0000-0000-0000-000000000000
```

Nachdem die Gruppe nun leer ist, können wir Sie problemlos löschen.

```
C:\vm\tools>CpuGroups.exe DeleteGroup /GroupId:36ab08cb-3a76-4b38-992e-000000000001
```

Vergewissern Sie sich, dass die Gruppe nicht mehr vorhanden ist.

```
C:\vm\tools>CpuGroups.exe GetGroups
CpuGroupId          CpuCap          LpIndexes
-----
36AB08CB-3A76-4B38-992E-000000000002 32768 4,5,6,7,8,9,10,11,20,21,22,23
36AB08CB-3A76-4B38-992E-000000000003 65536 12,13,14,15
36AB08CB-3A76-4B38-992E-000000000004 65536 24,25,26,27,28,29,30,31
```

Beispiel 13 – Binden eines virtuellen Computers an seine ursprüngliche CPU-Gruppe

```
C:\vm\tools>CpuGroups.exe SetVmGroup /VmName:g1 /GroupId:36AB08CB-3A76-4B38-992E-000000000002
```

```
C:\vm\tools>CpuGroups.exe GetGroupVms
```

```
CpuGroupId VmName VmId
```

```
-----  
36ab08cb-3a76-4b38-992e-000000000002 G2 4ABCF2F-6C22-498C-BB38-7151CE678758  
36ab08cb-3a76-4b38-992e-000000000002 G3 B0F3FCD5-FECF-4A21-A4A2-DE4102787200  
36AB08CB-3A76-4B38-992E-000000000002 G1 F699B50F-86F2-4E48-8BA5-EB06883C1FDC  
36ab08cb-3a76-4b38-992e-000000000003 P1 973B9426-0711-4742-AD3B-D8C39D6A0DEC  
36ab08cb-3a76-4b38-992e-000000000004 P2 A593D93A-3A5F-48AB-8862-A4350E3459E8
```


Verwalten von Hyper-V-Hypervisor-Scheduler-Typen

21.05.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Windows Server, Version 1709, Windows Server, Version 1803, Windows Server 2019

In diesem Artikel werden neue Modi der Logik für die Planung virtueller Prozessoren beschrieben, die zuerst in Windows Server 2016 eingeführt wurden. Diese Modi oder Scheduler-Typen bestimmen, wie der Hyper-V-Hypervisor die Arbeit über virtuelle Gast Prozessoren hinweg ordnet und verwaltet. Ein Hyper-V-Host Administrator kann Hypervisor-planertypen auswählen, die am besten für die virtuellen Gastcomputer (Virtual Machines, VMS) geeignet sind, und die VMs so konfigurieren, dass Sie von der Planungslogik profitieren.

NOTE

Updates sind erforderlich, um die in diesem Dokument beschriebenen Features für den Hypervisor-Scheduler zu verwenden. Weitere Informationen finden Sie unter [erforderliche Updates](#).

Hintergrund

Vor der Erörterung der Logik und der Kontrollen hinter der virtuellen Hyper-V-Prozessor Planung ist es hilfreich, die grundlegenden Konzepte in diesem Artikel zu überprüfen.

Informationen zu SMT

Gleichzeitiges Multithreading (oder SMT) ist ein Verfahren, das in modernen Prozessor Entwürfen genutzt wird, mit dem die Ressourcen des Prozessors von separaten, unabhängigen Ausführungsthreads gemeinsam genutzt werden können. SMT bietet im Allgemeinen eine geringfügige Leistungssteigerung für die meisten Arbeits Auslastungen, indem Berechnungen nach Möglichkeit parallelisiert werden, um den Anweisungs Durchsatz zu erhöhen, obwohl keine Leistungssteigerung oder sogar ein geringfügiger Leistungsverlust auftreten kann, wenn Konflikte zwischen Threads für freigegebene Prozessorressourcen auftreten. Prozessoren, die SMT unterstützen, sind sowohl bei Intel als auch bei AMD verfügbar Intel bezieht sich auf die SMT-Angebote als Intel Hyperthreading-Technologie oder Intel HT.

Für den Zweck dieses Artikels gelten die Beschreibungen von SMT und deren Verwendung durch Hyper-V gleichermaßen für Intel-und AMD-Systeme.

- Weitere Informationen zur Intel HT-Technologie finden Sie in der [Intel Hyper-Threading-Technologie](#) .
- Weitere Informationen zu AMD SMT finden Sie in [der Kernarchitektur "Zen"](#) .

Grundlegendes zur Virtualisierung von Prozessoren durch Hyper-V

Vor der Betrachtung der Hypervisor-planertypen ist es auch hilfreich, die Hyper-V-Architektur zu verstehen. Eine allgemeine Zusammenfassung finden Sie in der [Übersicht über die Hyper-V-Technologie](#). Dies sind wichtige Konzepte für diesen Artikel:

- Hyper-V erstellt und verwaltet virtuelle Computer Partitionen, für die Compute-Ressourcen zugeordnet und freigegeben werden, unter Kontrolle über den Hypervisor. Partitionen bieten starke Isolations Grenzen zwischen allen virtuellen Gast Computern und zwischen Gast-VMS und der Stamm Partition.
- Die Stamm Partition ist selbst eine virtuelle Computer Partition, obwohl Sie über eindeutige Eigenschaften und weitaus größere Berechtigungen als virtuelle Gastcomputer verfügt. Die Stamm Partition stellt die

Verwaltungsdienste zur Verfügung, die alle virtuellen Gastcomputer steuern, Unterstützung für virtuelle Geräte für Gäste bereitstellen und alle Geräte-e/a für virtuelle Gast Maschinen verwalten. Microsoft empfiehlt dringend, keine anwendungsworkloads in der Stamm Partition auszuführen.

- Jeder virtuelle Prozessor (VP) der Stamm Partition ist 1:1 einem zugrunde liegenden logischen Prozessor (LP) zugeordnet. Ein Host-VP läuft immer auf der gleichen zugrunde liegenden LP – es gibt keine Migration der VPS der Stamm Partition.
- Standardmäßig können die LPs, auf denen Host-VPS ausgeführt wird, auch Gast-VPS ausführen.
- Ein Gast-VP kann vom Hypervisor geplant werden, damit er auf allen verfügbaren logischen Prozessoren ausgeführt werden kann. Der Hypervisor-Planer kümmert sich um die zeitliche Cache Lokalität, die NUMA-Topologie und viele andere Faktoren beim Planen eines Gast-VP-Diensts. letztlich könnte der VP auf jeder Host-LP geplant werden.

Typen von Hypervisor-Scheduler

Ab Windows Server 2016 unterstützt der Hyper-V-Hypervisor verschiedene Modi der planerlogik, die bestimmen, wie der Hypervisor virtuelle Prozessoren auf den zugrunde liegenden logischen Prozessoren plant. Diese Scheduler-Typen lauten wie folgt:

Der klassische Scheduler

Der klassische Scheduler war seit seiner Inbetriebnahme der Standardwert für alle Versionen des Windows Hyper-v-Hypervisors, einschließlich Windows Server 2016 Hyper-v. Der klassische Scheduler bietet eine faire Freigabe, präemptives Roundrobin-Planungsmodell für virtuelle Gast Prozessoren.

Der klassische scheduler typ ist die am besten geeignete Option für die große Mehrheit herkömmlicher Hyper-V-Verwendungen – für Private Clouds, Hostinganbieter usw. Die Leistungsmerkmale sind gut verständlich und am besten optimiert, um eine Vielzahl von Virtualisierungsszenarien zu unterstützen, wie z. b. das über-Abonnement von VPS zu LPs, das gleichzeitige Ausführen von vielen heterogenen virtuellen Computern und Workloads, die Ausführung größerer Hochleistungs-VMS mit hoher Leistung und die Unterstützung der gesamten Features von Hyper-V ohne Einschränkungen.

Der Kern Planer

Der Hypervisor Core Scheduler ist eine neue Alternative zur klassischen Scheduler-Logik, die in Windows Server 2016 und Windows 10, Version 1607, eingeführt wurde. Der Kern Planer bietet eine starke Sicherheitsgrenze für die workloadworkloadisolation und reduzierte Leistungsschwankungen für Workloads innerhalb von VMS, die auf einem SMT-fähigen Virtualisierungshost ausgeführt werden. Der Kern Planer ermöglicht das gleichzeitige Ausführen von virtuellen SMT- und nicht-SMT-Computern auf dem gleichen SMT-aktivierten Virtualisierungshost.

Der Kern Planer nutzt die SMT-Topologie des Virtualisierungshosts und macht optional SMT-Paare für Gast-VMS verfügbar, und es werden Gruppen von virtuellen Gast Prozessoren von demselben virtuellen Computer auf Gruppen von SMT-logischen Prozessoren geplant. Dies erfolgt symmetrisch, sodass VPS in Gruppen von zwei Gruppen geplant werden, und ein Kern wird nie von virtuellen Computern gemeinsam genutzt, wenn LPs in Gruppen von zwei Gruppen verwendet werden. Wenn der VP für einen virtuellen Computer ohne aktivierte SMT geplant ist, beansprucht dieser VP den gesamten Kern, wenn er ausgeführt wird.

Das Gesamtergebnis des Kern Planers ist Folgendes:

- Gast-VPS sind so eingeschränkt, dass Sie auf zugrunde liegenden physischen Kern Paaren ausgeführt werden, indem Sie einen virtuellen Computer auf die Kern Grenzen des Prozessors isolieren und dadurch die Sicherheits Anfälligkeit für Angriffe durch böswillige virtuelle Computer verringern.
- Die Varianz im Durchsatz ist erheblich reduziert.
- Die Leistung wird möglicherweise reduziert, denn wenn nur eine Gruppe von VPS ausgeführt werden kann, wird nur einer der Anweisungs Datenströme im Kern ausgeführt, während der andere in den Leerlauf

versetzt wird.

- Das Betriebssystem und die Anwendungen, die auf dem virtuellen Gastcomputer ausgeführt werden, können SMT-Verhaltens- und Programmierschnittstellen (APIs) verwenden, um die Arbeit über SMT-Threads zu steuern und zu verteilen, genauso wie bei der Ausführung nicht virtualisierter Anwendungen.
- Eine starke Sicherheitsgrenze für die Isolation von Gast Arbeitslasten (Gast-VPS) ist darauf beschränkt, auf zugrunde liegenden physischen Kern Paaren ausgeführt zu werden

Der Kern Planer wird standardmäßig ab Windows Server 2019 verwendet. Unter Windows Server 2016 ist der Kern Planer optional und muss vom Hyper-V-Host Administrator explizit aktiviert werden, und der klassische Scheduler ist die Standardeinstellung.

Kern Planer-Verhalten mit deaktiviertem Host SMT

Wenn der Hypervisor für die Verwendung des Core Scheduler-Typs konfiguriert ist, aber die SMT-Funktion auf dem Virtualisierungshost deaktiviert oder nicht vorhanden ist, verwendet der Hypervisor das klassische schedulerverhalten, unabhängig von der Einstellung für den hypervisorschedulertyp.

Der Stamm Planer

Der Stamm Planer wurde mit Windows 10, Version 1803, eingeführt. Wenn der stammschedulertyp aktiviert ist, steuert der Hypervisor die Arbeitsplanung der Stamm Partition. Der NT-Scheduler in der Betriebssystem Instanz der Stamm Partition verwaltet alle Aspekte der Planungsarbeit an System LPs.

Der Stamm Planer erfüllt die besonderen Anforderungen, die bei der Unterstützung einer hilfsprogrammpartition bestehen, um eine starke workloadisolation bereitzustellen, wie Sie mit Windows Defender Application Guard (WDAG) verwendet wird. In diesem Szenario bietet das belassen von Planungsaufgaben für das Stamm Betriebssystem mehrere Vorteile. Beispielsweise können CPU-Ressourcen Steuerungen, die auf Container Szenarien anwendbar sind, mit der hilfsprogrammpartition verwendet werden, um die Verwaltung und Bereitstellung zu vereinfachen. Außerdem kann der Stamm Betriebssystem-Scheduler im Container problemlos Metriken zur CPU-Auslastung der Arbeitsauslastung erfassen und diese Daten als Eingabe für dieselbe Planungsrichtlinie verwenden, die für alle anderen Arbeits Auslastungen im System gilt. Diese Metriken helfen Ihnen auch, eine eindeutige Attribut Arbeit in einem Anwendungs Container für das Host System durchzuführen. Die Nachverfolgung dieser Metriken ist mit herkömmlichen VM-Workloads schwieriger, bei denen einige Arbeiten an allen laufenden virtuellen Computern in der Stamm Partition stattfinden.

Verwendung von root Scheduler auf Client Systemen

Ab Windows 10, Version 1803, wird der Stamm Planer standardmäßig nur auf Client Systemen verwendet, wobei der Hypervisor Unterstützung für virtualisierungsbasierte Sicherheit und WDAG-workloadisolation und für den ordnungsgemäßen Betrieb zukünftiger Systeme mit heterogenen Kern Architekturen aktiviert werden kann. Dies ist die einzige unterstützte Konfiguration für den Hypervisor-Scheduler für Client Systeme. Administratoren sollten nicht versuchen, den standardmäßigen Hypervisor-Planertyp auf Windows 10-Client Systemen zu überschreiben.

CPU-Ressourcen Steuerelemente für virtuelle Computer und der Stamm Planer

Die von Hyper-V bereitgestellten Prozessorressourcen-Steuerelemente für virtuelle Computer werden nicht unterstützt, wenn der Hypervisor-Stamm Planer aktiviert ist, da die Scheduler-Logik des Stamm Betriebssystems Host Ressourcen auf globaler Basis verwaltet und nicht über die spezifischen Konfigurationseinstellungen eines virtuellen Computers verfügt. Die Hyper-V-Prozessorressourcen Kontrolle, wie z. b. Caps, Gewichtungen und Reserven, sind nur anwendbar, wenn der Hypervisor die VP-Planung direkt steuert, z. b. mit den klassischen und den wichtigsten Scheduler-Typen.

Verwendung von root Scheduler auf Serversystemen

Der Stamm Planer wird zurzeit nicht für die Verwendung mit Hyper-V auf Servern empfohlen, da seine Leistungsmerkmale noch nicht vollständig charakterisiert und optimiert wurden, um die breite Palette von Workloads zu erfüllen, die für viele servervirtualisierungsbereitstellungen typisch sind.

Aktivieren von SMT auf virtuellen Gast Computern

Sobald der Hypervisor des Virtualisierungshosts für die Verwendung des kernplanertyps konfiguriert ist, können virtuelle Gastcomputer für die Verwendung von SMT konfiguriert werden, wenn gewünscht. Das verfügbar machen der Tatsache, dass VPS mit einem virtuellen Gastcomputer Hyperthread werden, ermöglicht dem Planer im Gast Betriebssystem und den Arbeits Auslastungen, die auf der VM ausgeführt werden, die SMT-Topologie in ihrer eigenen Arbeitsplanung zu erkennen und zu nutzen. Auf Windows Server 2016 ist Gast SMT nicht standardmäßig konfiguriert und muss vom Hyper-V-Host Administrator explizit aktiviert werden. Ab Windows Server 2019 erbt neue virtuelle Computer, die auf dem Host erstellt werden, standardmäßig die SMT-Topologie des Hosts. Das heißt, eine VM der Version 9,0, die auf einem Host mit 2 SMT-Threads pro Kern erstellt wurde, würde ebenfalls 2 SMT-Threads pro Kern sehen.

PowerShell muss zum Aktivieren von SMT auf einem virtuellen Gastcomputer verwendet werden. im Hyper-V-Manager wird keine Benutzeroberfläche bereitgestellt. Um SMT auf einem virtuellen Gastcomputer zu aktivieren, öffnen Sie ein PowerShell-Fenster mit ausreichenden Berechtigungen, und geben Sie Folgendes ein:

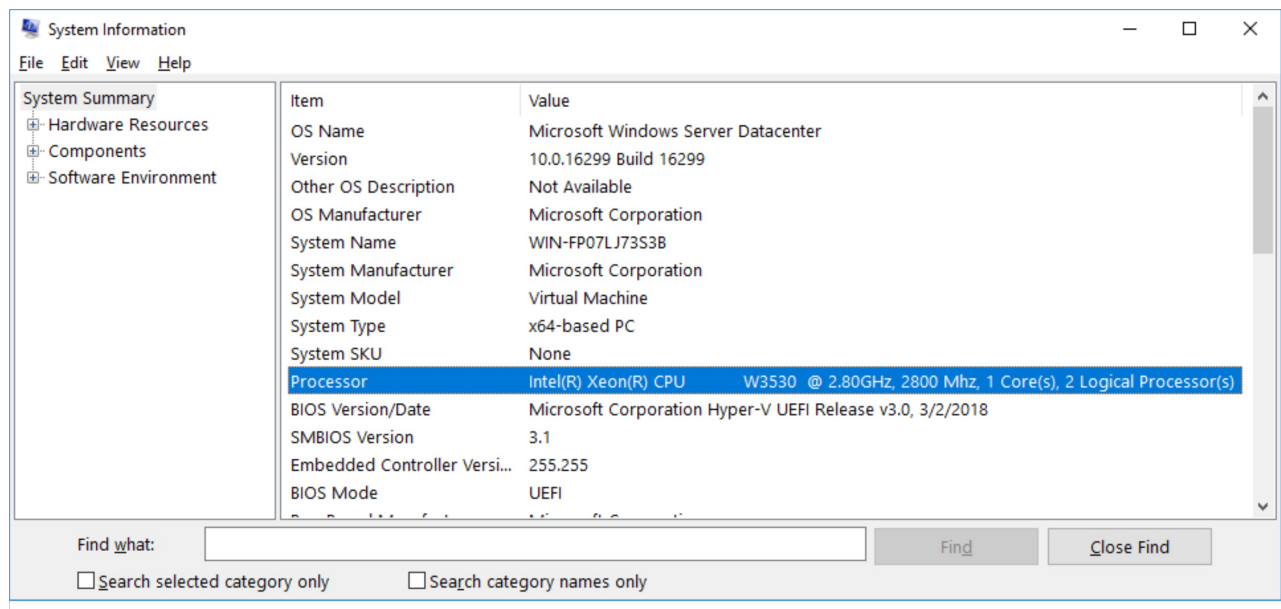
```
Set-VMProcessor -VMName <VMName> -HwThreadCountPerCore <n>
```

Dabei ist die Anzahl der SMT-Threads pro Kern, die der Gast-VM sieht. Beachten Sie, dass = 0 den hwthreadzähltpcore-Wert so festlegt, dass er mit der SMT-Thread Anzahl des Hosts pro Kernwert identisch ist.

NOTE

Das Festlegen von hwthreadzähltpcore = 0 wird ab Windows Server 2019 unterstützt.

Im folgenden finden Sie ein Beispiel für System Informationen, die vom Gast Betriebssystem auf einem virtuellen Computer mit zwei virtuellen Prozessoren und SMT aktiviert wurden. Das Gast Betriebssystem erkennt zwei logische Prozessoren, die zu demselben Kern gehören.



Konfigurieren des Hypervisor-Scheduler-Typs auf Windows Server 2016 Hyper-V

Windows Server 2016 Hyper-V verwendet standardmäßig das klassische Hypervisor-Scheduler-Modell. Der Hypervisor kann optional für die Verwendung des Kern Planers konfiguriert werden, um die Sicherheit zu erhöhen, indem Gast-VPS für die Ausführung auf entsprechenden physischen SMT-Paaren eingeschränkt werden und die Verwendung von virtuellen Computern mit SMT-Zeitplanung für Ihre Gast-VPS unterstützt wird.

NOTE

Microsoft empfiehlt, dass alle Kunden, die Windows Server 2016 Hyper-V ausführen, den Kern Planer auswählen, um sicherzustellen, dass Ihre Virtualisierungshosts optimal vor potenziell schädlichen Gast-VMS geschützt werden.

Windows Server 2019 Hyper-V verwendet standardmäßig den Kern Planer

Um sicherzustellen, dass Hyper-v-Hosts in der optimalen Sicherheitskonfiguration bereitgestellt werden, verwendet Windows Server 2019 Hyper-v jetzt standardmäßig das Core-Hypervisor-Scheduler-Modell. Der Host Administrator kann optional den Host so konfigurieren, dass er den klassischen Legacy Planer verwendet. Administratoren sollten vor dem Überschreiben der Standardeinstellungen für den Scheduler die Auswirkungen der einzelnen schedulertypen auf die Sicherheit und Leistung von Virtualisierungshosts sorgfältig lesen, verstehen und berücksichtigen. Weitere Informationen finden Sie Untergrund Legendes zur [Hyper-V-Scheduler-Typauswahl](#).

Erforderliche Updates

NOTE

Die folgenden Updates sind erforderlich, um die in diesem Dokument beschriebenen Features für den Hypervisor-Scheduler zu verwenden. Diese Updates enthalten Änderungen zur Unterstützung der neuen `hypervisorschedulertype` BCD-Option, die für die Host Konfiguration erforderlich ist.

VERSION	FREIGABE	UPDATE ERFORDERLICH	KB ARTICLE
Windows Server 2016	1607	2018,07 C	KB4338822
Windows Server 2016	1703	2018,07 C	KB4338827
Windows Server 2016	1709	2018,07 C	KB4338817
Windows Server 2019	1804	Keine	Keine

Auswählen des Hypervisor-planertyps unter Windows Server

Die Konfiguration des Hypervisor-Planers wird über den BCD-Eintrag `hypervisorschedulertype` gesteuert.

Um einen Planertyp auszuwählen, öffnen Sie eine Eingabeaufforderung mit Administratorrechten:

```
bcdedit /set hypervisorschedulertype type
```

Dabei `type` ist einer der folgenden:

- Klassisch
- Core
- Root

Das System muss neu gestartet werden, damit Änderungen am Typ des Hypervisor-Planers wirksam werden.

NOTE

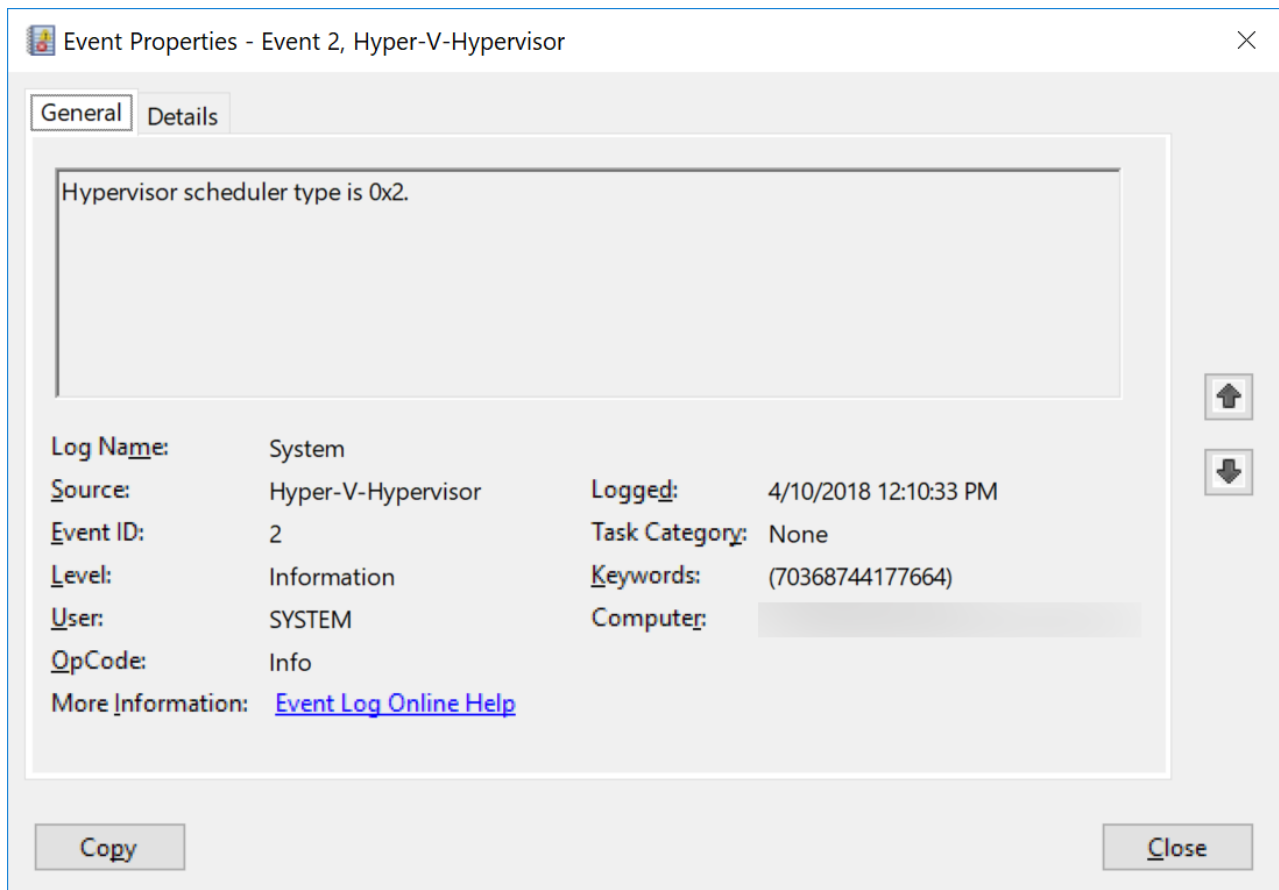
Der Hypervisor-Stamm Planer wird zurzeit nicht unter Windows Server Hyper-V unterstützt. Hyper-V-Administratoren sollten nicht versuchen, den Stamm Planer für die Verwendung mit servervirtualisierungsszenarien zu konfigurieren.

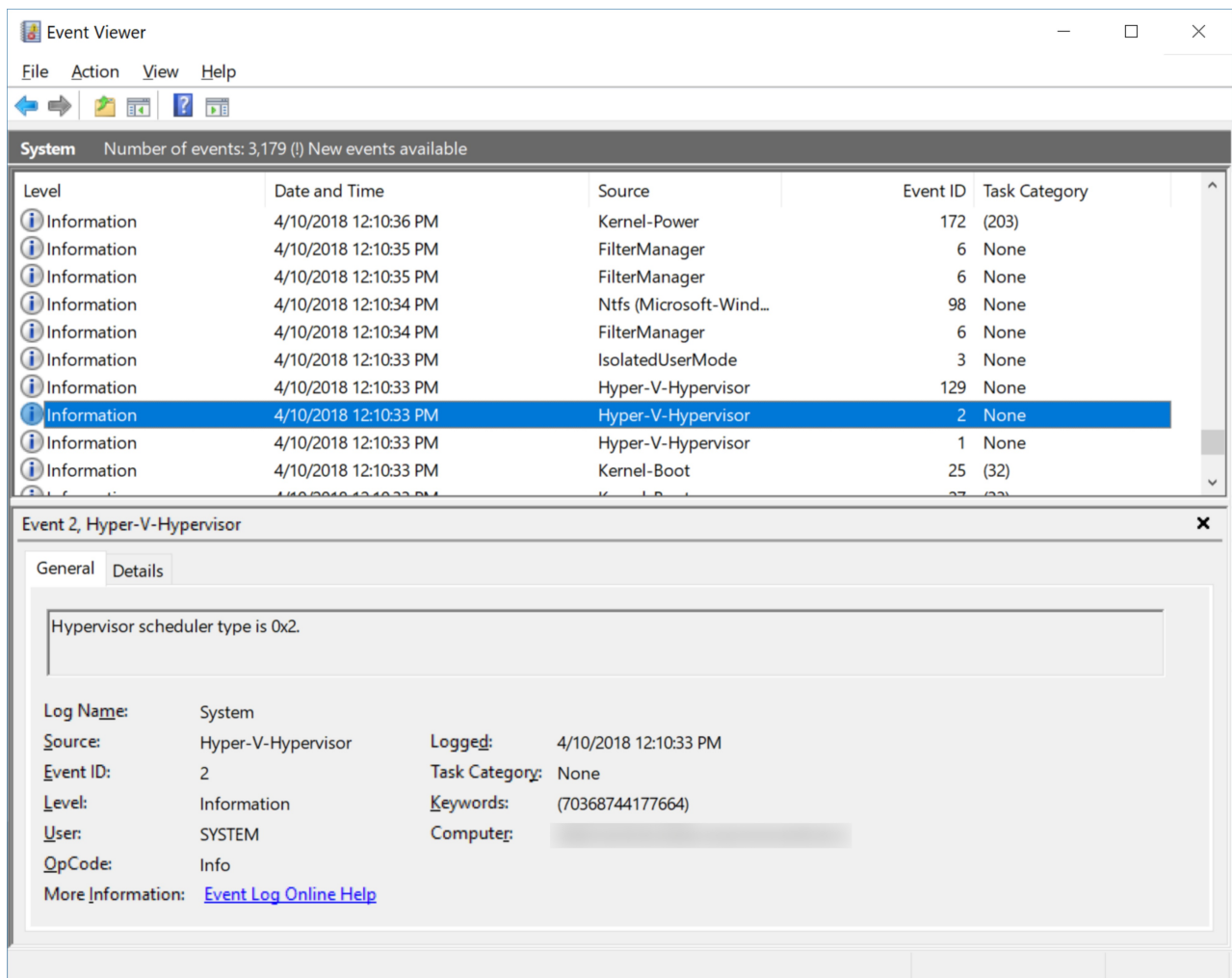
Bestimmen des aktuellen planertyps

Sie können den aktuell verwendeten Hypervisor-Planertyp ermitteln, indem Sie das System Protokoll in Ereignisanzeige auf die aktuelle Hypervisor-Start Ereignis-ID 2 untersuchen, die den beim Hypervisor Launch konfigurierten Hypervisor-Planertyp meldet. Hypervisor-Start Ereignisse können vom Windows-Ereignisanzeige oder über PowerShell abgerufen werden.

Die Hypervisor-Start Ereignis-ID 2 gibt den Hypervisor-Planertyp an, wobei Folgendes gilt:

- 1 = klassisches Scheduler, SMT deaktiviert
- 2 = klassisches Scheduler
- 3 = Core Scheduler
- 4 = root Scheduler

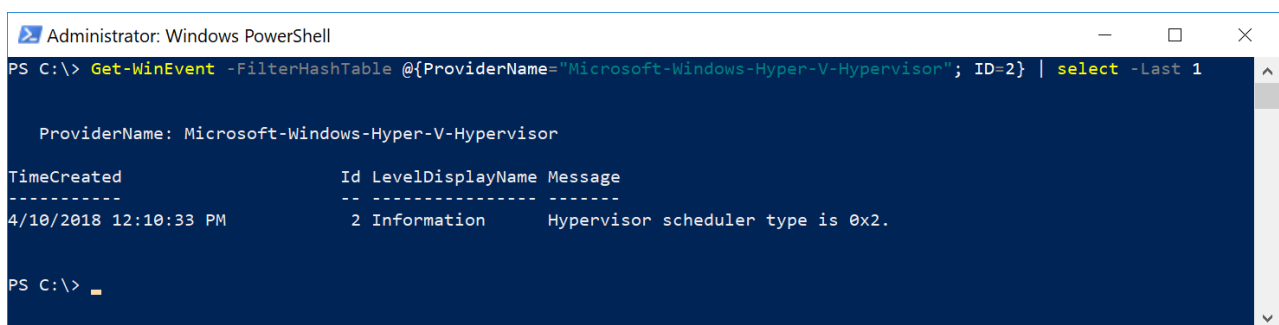




Abfragen des Start Ereignisses für den Hyper-V-Hypervisor-Scheduler mithilfe von PowerShell

Geben Sie die folgenden Befehle von einer PowerShell-Eingabeaufforderung ein, um die Hypervisor-Ereignis-ID 2 mithilfe von PowerShell abzufragen.

```
Get-WinEvent -FilterHashTable @{ProviderName="Microsoft-Windows-Hyper-V-Hypervisor"; ID=2} -MaxEvents 1
```



Informationen zu Hyper-V Hypervisor Scheduler Type Selection

02.12.2019 • 26 minutes to read • [Edit Online](#)

Gilt für:

- Windows Server 2016
- Windows Server, Version 1709
- Windows Server, Version 1803
- Windows Server 2019

In diesem Dokument werden wichtige Änderungen an der standardmäßigen und empfohlenen Verwendung von Hypervisor-Scheduler-Typen für Hyper-V beschrieben. Diese Änderungen wirken sich auf die Systemsicherheit und Virtualisierungsleistung aus. Administratoren von Virtualisierungshosts sollten die in diesem Dokument beschriebenen Änderungen und Implikationen überprüfen und verstehen und die Auswirkungen, den empfohlenen Bereitstellungs Leit Faden und Risikofaktoren sorgfältig auswerten, um die Bereitstellung und Verwaltung zu verstehen. Hyper-V-Hosts in der Oberfläche der schnell veränderlichen Sicherheit.

IMPORTANT

Die derzeit in mehreren Prozessorarchitekturen aussehenden Sicherheitsrisiken für die neben Kanal Sicherheit können von einem böswilligen Gast-VM durch das Planungs Verhalten des herkömmlichen Hypervisor Classic Scheduler-Typs ausgenutzt werden, wenn auf Hosts mit gleichzeitiger Ausführung ausgeführt wird. Multithreading (SMT) aktiviert. Wenn Sie erfolgreich ausgenutzt werden, könnte eine schädliche Arbeitsauslastung Daten außerhalb ihrer Partitions Grenze beobachten. Diese Angriffs Klasse kann verringert werden, indem Sie den Hyper-V-Hypervisor so konfigurieren, dass der Hypervisor Core Scheduler-Typ verwendet und Gast-VMS neu konfiguriert werden. Mit dem Kern Planer schränkt der Hypervisor die VPS eines Gast-VMS auf den gleichen physischen Prozessorkern ein. Dadurch wird die Fähigkeit des virtuellen Computers, auf die Grenzen des physischen Kerns zuzugreifen, auf dem es ausgeführt wird, stark isoliert. Dies ist eine äußerst effektive Entschärfung gegen diese Seitenkanalangriffe, wodurch verhindert wird, dass der virtuelle Computer Artefakte von anderen Partitionen beobachtet, egal ob es sich um den Stamm oder eine andere Gast Partition handelt. Daher ändert Microsoft die standardmäßigen und empfohlenen Konfigurationseinstellungen für Virtualisierungshosts und Gast-VMS.

Hintergrund

Ab Windows Server 2016 unterstützt Hyper-V verschiedene Methoden zum Planen und Verwalten virtueller Prozessoren, die als Hypervisor-planertypen bezeichnet werden. Eine ausführliche Beschreibung aller Hypervisor-planertypen finden Sie Untergrund Legendes zu [und Verwendung von Hyper-V-Hypervisor-Scheduler-Typen](#).

NOTE

Neue Hypervisor-Scheduler-Typen wurden erstmals mit Windows Server 2016 eingeführt und sind in früheren Versionen nicht verfügbar. Alle Versionen von Hyper-V vor Windows Server 2016 unterstützen nur den klassischen Scheduler. Die Unterstützung für den Kern Planer wurde erst kürzlich veröffentlicht.

Informationen zu Hypervisor-Scheduler-Typen

Der Schwerpunkt dieses Artikels liegt auf der Verwendung des neuen Hypervisor-kernplanertyps im Vergleich zum Legacy-Scheduler "klassisch" und der Schnittmenge dieser Scheduler-Typen mit symmetrischem Multithreading

oder SMT. Es ist wichtig, die Unterschiede zwischen den Kern- und klassischen Zeit Planungs Modulen zu verstehen und zu erfahren, wie die einzelnen Orte von Gast-VMS auf den zugrunde liegenden System Prozessoren funktionieren.

Der klassische Scheduler

Der klassische Scheduler bezieht sich auf die Methode "Fair-Share", "Roundrobin" für die Planung von Arbeitsaufgaben an virtuellen Prozessoren (VPS) im gesamten System, einschließlich Stamm-VPS und VPS, die zu Gast-VMS gehören. Der klassische Scheduler ist der standardmäßige Scheduler-Typ, der für alle Versionen von Hyper-V verwendet wird (bis Windows Server 2019, wie in diesem Dokument beschrieben). Die Leistungsmerkmale des klassischen Zeit Planungs Moduls sind gut zu verstehen, und der klassische Scheduler wird demonstriert, dass er das Abonnement von Workloads unterstützt, d. h. über Abonnement des VP: LP-Verhältnis des Hosts um einen angemessenen Rand (abhängig vom Typen von Workloads, die virtualisiert werden, Gesamtressourcen Nutzung usw.).

Bei der Ausführung auf einem Virtualisierungshost mit aktiviertem SMT plant der klassische Scheduler Gast-VPS von einem beliebigen virtuellen Computer in jedem SMT-Thread, der zu einem Kern gehört. Daher können unterschiedliche VMS gleichzeitig auf demselben Kern ausgeführt werden (eine VM, die auf einem Thread eines Kerns ausgeführt wird, während eine andere VM auf dem anderen Thread ausgeführt wird).

Der Kern Planer

Der Kern Planer nutzt die Eigenschaften von SMT, um die Isolation von Gast Arbeits Auslastungen zu ermöglichen, was sich auf die Sicherheit und die Systemleistung auswirkt. Der zentrale Scheduler stellt sicher, dass VPS von einem virtuellen Computer auf gleich geordneten SMT-Threads geplant sind. Dies erfolgt symmetrisch, sodass VPS in Gruppen von zwei Gruppen geplant werden, und ein System-CPU-Kern wird nie von virtuellen Computern gemeinsam genutzt, wenn LPs in Gruppen von zwei Gruppen verwendet werden.

Wenn Sie Gast-VPS für zugrunde liegende SMT-Paare planen, bietet der Kern Planer eine starke Sicherheitsgrenze für die workloadisolation und kann auch verwendet werden, um die Leistungs Variabilität für Latenz abhängige Workloads zu verringern.

Beachten Sie Folgendes: Wenn für einen virtuellen Computer, auf dem kein SMT aktiviert ist, der VP geplant ist, nutzt dieser VP den gesamten Kern, wenn er ausgeführt wird, und der gleich geordnete SMT-Thread des Kerns bleibt im Leerlauf. Dies ist erforderlich, um die richtige workloadisolation bereitzustellen, wirkt sich jedoch auf die Gesamtleistung des Systems aus, insbesondere wenn die System LPs überschrieben werden, d. h., wenn das Gesamtverhältnis von VP: LP 1:1 überschreitet. Aus diesem Grund ist das Ausführen von virtuellen Gast Computern, die ohne mehrere Threads pro Kern konfiguriert wurden, eine suboptimale Konfiguration.

Vorteile der mit dem Kern Planer

Der zentrale Scheduler bietet die folgenden Vorteile:

- Eine starke Sicherheitsgrenze für die Isolation von Gast Arbeitslasten (Gast-VPS) ist darauf beschränkt, auf zugrunde liegenden physischen Kern Paaren ausgeführt zu werden
- Reduzierte workloadvarianz: die Variabilität der workloadarbeitsauslastung ist erheblich reduziert und bietet eine höhere Arbeitsauslastung
- Verwendung von SMT in Gast-VMS: das Betriebssystem und die Anwendungen, die auf dem virtuellen Gastcomputer ausgeführt werden, können SMT-Verhaltens- und Programmierschnittstellen (APIs) verwenden, um die Arbeit über SMT-Threads zu steuern und zu verteilen, genauso wie bei der Ausführung nicht virtualisierter Anwendungen.

Der zentrale Scheduler wird derzeit auf Azure-Virtualisierungshosts verwendet, insbesondere, um die starke Sicherheitsgrenze und eine geringe Arbeitsauslastung zu nutzen. Microsoft ist der Meinung, dass der kernplanertyp sein sollte und weiterhin der standardmäßige Hypervisor-Zeit Plantyp für die Mehrzahl der Virtualisierungsszenarien ist. Um sicherzustellen, dass unsere Kunden standardmäßig sicher sind, nimmt Microsoft diese Änderung jetzt für Windows Server 2019 vor.

Grundlegende Auswirkungen der Leistung von Scheduler auf Gast Arbeits Auslastungen

Obwohl es erforderlich ist, bestimmte Sicherheitsrisiken effektiv zu mindern, kann der Kern Planer möglicherweise auch die Leistung beeinträchtigen. Kunden haben möglicherweise einen Unterschied in den Leistungsmerkmalen mit ihren VMS und Auswirkungen auf die Gesamtauslastung der Arbeitsauslastung ihrer Virtualisierungshosts. In Fällen, in denen der Kern Planer einen nicht-SMT-VP ausführen muss, wird nur einer der Anweisungen Datenströme im zugrunde liegenden logischen Kern ausgeführt, während der andere im Leerlauf bleiben muss. Dadurch wird die gesamte Host Kapazität für Gast Arbeits Auslastungen eingeschränkt.

Diese Auswirkungen auf die Leistung können minimiert werden, indem die Bereitstellungs Anleitung in diesem Dokument erläutert wird. Host Administratoren müssen Ihre spezifischen Szenarien für die Virtualisierungssoftware sorgfältig berücksichtigen und deren Toleranz für das Sicherheitsrisiko gegen den Bedarf an maximaler Arbeits Auslastungs Dichte, die Konsolidierung von Virtualisierungshosts usw. abwägen.

Änderungen an den Standardkonfigurationen und empfohlenen Konfigurationen für Windows Server 2016 und Windows Server 2019

Zum Bereitstellen von Hyper-V-Hosts mit dem maximalen Sicherheitsstatus ist die Verwendung des Typs "Hypervisor Core Scheduler" erforderlich. Um sicherzustellen, dass unsere Kunden standardmäßig sicher sind, ändert Microsoft die folgenden Standardeinstellungen und empfohlenen Einstellungen.

NOTE

Obwohl die interne Unterstützung der Scheduler-Typen in der ersten Version von Windows Server 2016, Windows Server 1709 und Windows Server 1803 enthalten war, sind Updates erforderlich, um auf die Konfigurations Steuerung zuzugreifen, die die Auswahl des Typ des Hypervisor-Planers. Ausführliche Informationen zu diesen Updates finden Sie unter [verstehen und Verwenden von Hyper-V-Hypervisor-planertypen](#).

Änderungen am Virtualisierungshost

- Der Hypervisor verwendet standardmäßig den Kern Planer ab Windows Server 2019.
- Microsoft startet die Konfiguration des Kern Planers auf Windows Server 2016. Der Typ "Hypervisor Core Scheduler" wird in Windows Server 2016 unterstützt, aber der Standardwert ist der klassische Scheduler. Der Kern Planer ist optional und muss vom Hyper-V-Host Administrator explizit aktiviert werden.

Änderungen an der Konfiguration der virtuellen Maschine

- Unter Windows Server 2019 erben neue virtuelle Computer, die mit der Standard-VM-Version 9,0 erstellt wurden, automatisch die SMT-Eigenschaften (aktiviert oder deaktiviert) des Virtualisierungshosts. Das heißt, wenn SMT auf dem physischen Host aktiviert ist, wird für neu erstellte VMS auch die SMT-Funktion aktiviert, und die SMT-Topologie des Hosts wird standardmäßig geerbt, wobei die VM die gleiche Anzahl von Hardwarethreads pro Kern wie das zugrunde liegende System aufweist. Dies wird in der VM-Konfiguration mit `hwthreadzahlpercore = 0` übernommen, wobei 0 angibt, dass der virtuelle Computer die SMT-Einstellungen des Hosts erben soll.
- Vorhandene virtuelle Computer mit einer VM-Version von 8,2 oder früher behalten ihre ursprüngliche VM-Prozessor Einstellung für `hwthreadzahlpercore` bei, und die Standardeinstellung für 8,2-VM-Versionen Gäste lautet `hwthreadzahlpercore = 1`. Wenn diese Gäste auf einem Windows Server 2019-Host ausgeführt werden, werden Sie wie folgt behandelt:
 1. Wenn die VM eine VP-Anzahl hat, die kleiner oder gleich der Anzahl der LP-Kerne ist, wird der virtuelle Computer vom Kern Planer als nicht-SMT-VM behandelt. Wenn der Gast-VP in einem einzelnen SMT-Thread ausgeführt wird, wird der gleich geordnete SMT-Thread des Kerns als `idle` verwendet. Dies ist nicht optimal, was zu einem Gesamtverlust der Leistung führt.
 2. Wenn die VM mehr VPS als LP-Kerne aufweist, wird der virtuelle Computer vom Kern Planer als

SMT-VM behandelt. Der virtuelle Computer hat jedoch keine anderen Anzeichen dafür, dass es sich um eine SMT-VM handelt. Beispielsweise weist die Verwendung der CPUID-Anweisung oder der Windows-APIs zum Abfragen der CPU-Topologie durch das Betriebssystem oder die Anwendung nicht darauf hin, dass SMT aktiviert ist.

- Wenn eine vorhandene VM durch den Vorgang "Update-VM" explizit von der VM-Version des virtuellen Computers auf die Version 9,0 aktualisiert wird, behält der virtuelle Computer seinen aktuellen Wert für `hwthreadzahlpercore` bei. Für den virtuellen Computer ist die SMT-aktivierte Funktion nicht aktiviert.
- Unter Windows Server 2016 empfiehlt Microsoft, SMT für Gast-VMS zu aktivieren. Standardmäßig ist für virtuelle Computer, die unter Windows Server 2016 erstellt werden, die SMT-Deaktivierung aktiviert, d. h. `hwthreadzahlwert` ist auf 1 festgelegt, sofern nicht explizit geändert.

NOTE

Windows Server 2016 bietet keine Unterstützung für das Festlegen von `hwthreadzahlpercore` auf 0.

Verwalten der SMT-Konfiguration für virtuelle Computer

Die SMT-Konfiguration des Gast-virtuellen Computers wird pro VM-Basis festgelegt. Der Host Administrator kann die SMT-Konfiguration eines virtuellen Computers überprüfen und konfigurieren, um eine der folgenden Optionen auszuwählen:

1. `Konfigurieren von virtuellen Computern für die ausführen als SMT-fähig, wobei optional die Host-SMT-Topologie automatisch geerbt wirdConfigure VMs to run as SMT-enabled, optionally inheriting the host SMT topology automatically`
2. `Konfigurieren von virtuellen Computern, die als nicht-SMT ausgeführt werdenConfigure VMs to run as non-SMT`

Die SMT-Konfiguration für einen virtuellen Computer wird in den Übersichts Bereichen der Hyper-V-Manager-Konsole angezeigt. Die Konfiguration der SMT-Einstellungen eines virtuellen Computers kann mithilfe der VM-Einstellungen oder PowerShell erfolgen.

Konfigurieren von VM-SMT-Einstellungen mithilfe von PowerShell

Um die SMT-Einstellungen für einen virtuellen Gastcomputer zu konfigurieren, öffnen Sie ein PowerShell-Fenster mit ausreichenden Berechtigungen, und geben Sie Folgendes ein:

```
Set-VMProcessor -VMName <VMName> -HwThreadCountPerCore <0, 1, 2>
```

Erläuterungen:

0 = Inherit SMT topology from the host (this setting of `HwThreadCountPerCore=0` is not supported on Windows Server 2016)

1 = Non-SMT

Values > 1 = the desired number of SMT threads per core. May not exceed the number of physical SMT threads per core.

Um die SMT-Einstellungen für einen virtuellen Gastcomputer zu lesen, öffnen Sie ein PowerShell-Fenster mit ausreichenden Berechtigungen, und geben Sie Folgendes ein:

```
(Get-VMProcessor -VMName <VMName>).HwThreadCountPerCore
```

Beachten Sie, dass Gast-VMS, die mit `hwthreadzahlpercore = 0` konfiguriert werden, angeben, dass SMT für den Gast aktiviert ist, und dass die gleiche Anzahl von SMT-Threads für den Gast verfügbar ist wie auf dem zugrunde liegenden Virtualisierungshost, in der Regel 2.

Gast-VMs können Änderungen an der CPU-Topologie über VM-Mobilitäts Szenarien hinweg beobachten

Das Betriebssystem und die Anwendungen auf einem virtuellen Computer können vor und nach dem Lebenszyklus von virtuellen Computern (z. B. Live Migration oder Speicher- und Wiederherstellungs Vorgänge) Änderungen an den Einstellungen für Host und VM Während eines Vorgangs, bei dem der Zustand des virtuellen Computers gespeichert und wieder hergestellt wird, werden sowohl die `hwthreadzahlpercore`-Einstellung der VM als auch der erkannte Wert (d. h. die berechnete Kombination aus der Einstellung des virtuellen Computers und der Konfiguration des Quell Hosts) migriert. Der virtuelle Computer wird mit diesen Einstellungen auf dem Zielhost weiter ausgeführt. Zu dem Zeitpunkt, an dem der virtuelle Computer heruntergefahren und neu gestartet wird, wird möglicherweise der von der VM beobachtete erkannte Wert geändert. Dies sollte nicht ausreichen, da Betriebssystem- und anwendungsebenensoftware im Rahmen ihrer normalen Start- und Initialisierungs Code Flüsse nach CPU-Topologieinformationen suchen soll. Da diese Start Zeit-Initialisierungs Sequenzen bei Live Migrationen oder Speicher-/Wiederherstellungs Vorgängen übersprungen werden, können virtuelle Computer, die diese Zustandsübergänge durchlaufen, den ursprünglich berechneten erkannten Wert beobachten, bis Sie heruntergefahren und neu gestartet werden.

Warnungen bezüglich nicht optimaler VM-Konfigurationen

Virtuelle Computer, die mit mehr VPS konfiguriert sind als physische Kerne auf dem Host vorhanden sind, führen zu einer nicht optimalen Konfiguration. Der Hypervisor-Planer behandelt diese VMS so, als ob Sie SMT-fähig sind. Betriebssystem- und Anwendungssoftware auf dem virtuellen Computer wird jedoch eine CPU-Topologie angezeigt, die anzeigt, dass SMT deaktiviert ist. Wenn diese Bedingung erkannt wird, protokolliert der Hyper-V-Arbeitsprozess ein Ereignis auf dem Virtualisierungshost, und der Host Administrator wird darauf gewarnt, dass die VM-Konfiguration nicht optimal ist und dass für den virtuellen Computer SMT empfohlen wird.

Identifizieren von nicht optimal konfigurierten VMS

Sie können nicht-SMT-VMS ermitteln, indem Sie das System Protokoll in Ereignisanzeige für die Hyper-V-Arbeitsprozess Ereignis-ID 3498 überprüfen, die für einen virtuellen Computer ausgelöst wird, wenn die Anzahl der VPS in der VM größer als die Anzahl der physischen Kerne ist. Arbeitsprozess Ereignisse können von Ereignisanzeige oder über PowerShell abgerufen werden.

Abfragen des Hyper-V-Arbeitsprozess-VM-Ereignisses mithilfe von PowerShell

Geben Sie die folgenden Befehle von einer PowerShell-Eingabeaufforderung ein, um die Ereignis-ID 3498 für den Hyper-V-Arbeitsprozess mit PowerShell abzufragen.

```
Get-WinEvent -FilterHashTable @{ProviderName="Microsoft-Windows-Hyper-V-Worker"; ID=3498}
```

Auswirkungen der Gast-SMT-Konfiguration auf die Verwendung von Hypervisor-Erleuchtungen für Gast Betriebssysteme

Der Microsoft-Hypervisor bietet mehrere-oder-Hinweise, die vom Betriebssystem, das auf einer Gast-VM ausgeführt wird, möglicherweise abgefragt und verwendet werden, um Optimierungen zu initiieren, z. B. solche, die die Leistung verbessern oder die Behandlung verschiedener Bedingungen bei der Ausführung virtualisierten. Eine vor kurzem eingeführte Erleuchtung bezieht sich auf die Behandlung von virtuellen Prozessorzeit Plänen und die Verwendung von Betriebs systementschärfungen für Seitenkanalangriffe, die SMT ausnutzen.

NOTE

Microsoft empfiehlt, dass Host Administratoren SMT für Gast-VMS aktivieren, um die workloadleistung zu optimieren.

Die Details dieser Gast Aufklärung werden unten bereitgestellt, aber der Hauptgrund für die Virtualisierungshost-Administratoren besteht darin, dass für virtuelle Computer hwhthreadzähltpcore entsprechend der physischen SMT-Konfiguration des Hosts konfiguriert werden muss. Dadurch kann der Hypervisor melden, dass keine nicht architektonische Kern Freigabe vorhanden ist. Daher können alle Gast Betriebssysteme, die Optimierungen unterstützen, die die Aufklärung erfordern, aktiviert werden. Erstellen Sie unter Windows Server 2019 neue VMs, und belassen Sie den Standardwert hwhthreadzähltpcore (0). Ältere VMS, die von Windows Server 2016-Hosts migriert wurden, können auf die Windows Server 2019-Konfigurations Version aktualisiert werden. Danach empfiehlt Microsoft, hwhthreadzähltpcore = 0 festzulegen. Unter Windows Server 2016 empfiehlt Microsoft, hwhthreadzähltpcore entsprechend der Host Konfiguration (in der Regel 2) festzulegen.

Details zu "nononarchitekturalcoresharung"

Ab Windows Server 2016 definiert der Hypervisor eine neue Erleuchtung, um die Verarbeitung der VP-Planung und-Platzierung für das Gast Betriebssystem zu beschreiben. Diese Aufklärung wird in der [Funktionsspezifikation der obersten Ebene von Hypervisor v 5.0](#) cdefiniert.

Synthetisches CPUID-Blatt "Hypervisor" CPUID. 0x40000004. EAX: 18 [nononarchitekturalcoreshareing = 1] gibt an, dass ein virtueller Prozessor nie einen physischen Kern mit einem anderen virtuellen Prozessor gemeinsam nutzt, mit Ausnahme von virtuellen Prozessoren, die als gleich geordnetes SMT-Element gemeldet werden. Threads. Beispielsweise wird ein Gast-VP nie in einem SMT-Thread parallel zu einem Stamm-VP ausgeführt, der gleichzeitig auf einem gleich geordneten SMT-Thread desselben Prozessorkerns ausgeführt wird. Diese Bedingung ist nur bei der virtualisierten Ausführung möglich und stellt ein nicht architektonisches SMT-Verhalten dar, das auch schwerwiegende Auswirkungen auf die Sicherheit hat. Das Gast Betriebssystem kann nononarchitekturalcoreshareing = 1 verwenden, um zu verhindern, dass Optimierungen sicher aktiviert werden können. Dies kann dazu beitragen, den Leistungs Aufwand bei der Festlegung von stibp zu vermeiden.

In bestimmten Konfigurationen weist der Hypervisor nicht darauf hin, dass nononarchitekturalcoreshareing = 1 ist. Wenn ein Host beispielsweise SMT aktiviert hat und für die Verwendung des klassischen Hypervisor-Schedulers konfiguriert ist, wird nononarchitekturalcoreshareing auf 0 festgelegt. Dadurch wird möglicherweise verhindert, dass aktivierte Gäste bestimmte Optimierungen aktivieren. Daher empfiehlt Microsoft, dass Host Administratoren, die SMT verwenden, den Hypervisor-Kern Planer verwenden und sicherstellen, dass virtuelle Computer so konfiguriert sind, dass die SMT-Konfiguration vom Host geerbt wird, um eine optimale workloadleistung sicherzustellen.

Zusammenfassung

Die Sicherheits Bedrohungslandschaft wird weiterentwickelt. Um sicherzustellen, dass unsere Kunden standardmäßig sicher sind, ändert Microsoft die Standardkonfiguration für den Hypervisor und die virtuellen Computer ab Windows Server 2019 Hyper-V und bietet aktualisierte Anleitungen und Empfehlungen für Kunden, die Windows ausführen. Server 2016 Hyper-V. Administratoren von Virtualisierungshosts sollten:

- Lesen und verstehen Sie die Anweisungen in diesem Dokument.
- Evaluieren und Anpassen der Virtualisierungsbereitstellungen, um sicherzustellen, dass Sie die Anforderungen an Sicherheit, Leistung, Virtualisierungsdichte und Arbeits Auslastungen für die Reaktionsfähigkeit ihrer individuellen Anforderungen erfüllen
- Sie sollten vorhandene Windows Server 2016 Hyper-V-Hosts neu konfigurieren, um die starken Sicherheitsvorteile des Hypervisor-Kern Planers zu nutzen.
- Aktualisieren vorhandener nicht-SMT-VMS, um die Leistung zu verringern, die durch die Planung von Einschränkungen durch die VP-Isolation auferlegt werden

Verwalten von Hyper-V-Integration Services

13.05.2020 • 18 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2012, Windows Server 2012r2, Windows Server 2016, Windows Server 2019

Mithilfe der bidirektionalen Kommunikation mit dem Hyper-v-Host können Sie Hyper-V Integration Services die Leistung virtueller Computer verbessern und bequeme Features bereitstellen. Viele dieser Dienste sind Bequemlichkeiten, wie z. b. das Kopieren von Gast Dateien, während andere für die Funktionalität des virtuellen Computers, z. b. synthetische Gerätetreiber, wichtig sind. Diese Dienste und Treiber werden manchmal als "Integrations Komponenten" bezeichnet. Sie können steuern, ob einzelne bequeme Dienste für einen bestimmten virtuellen Computer ausgeführt werden. Die Treiber Komponenten sind nicht für die manuelle Wartung vorgesehen.

Ausführliche Informationen zu den einzelnen Integrationsdiensten finden Sie unter [Hyper-V-Integration Services](#).

IMPORTANT

Jeder Dienst, den Sie verwenden möchten, muss sowohl auf dem Host als auch auf dem Gast aktiviert sein, damit er funktioniert. Alle Integrationsdienste mit Ausnahme von "Hyper-V-Gastschnittstellendienst" sind unter Windows-Gastbetriebssystemen standardmäßig aktiviert. Die Dienste können einzeln aktiviert und deaktiviert werden. In den nächsten Abschnitten wird erläutert, wie Sie.

Aktivieren oder Deaktivieren eines Integrations Dienstanbieter mit dem Hyper-V-Manager

1. Klicken Sie im mittleren Bereich mit der rechten Maustaste auf den virtuellen Computer, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im linken Bereich des Fensters **Einstellungen** unter **Verwaltung** auf **Integration Services**.

Im Integration Services Bereich werden alle Integrationsdienste aufgelistet, die auf dem Hyper-V-Host verfügbar sind, und ob der Host die virtuelle Maschine für die Verwendung aktiviert hat.

Aktivieren oder Deaktivieren eines Integrations Dienstanbieter mithilfe von PowerShell

Verwenden Sie hierzu " [enable-vmintegrationservice](#) " und "Enable [-vmintegrationservice](#)", um dies in PowerShell zu tun.

In den folgenden Beispielen wird veranschaulicht, wie Sie den Integrations Dienst für Gast Dateien kopieren für einen virtuellen Computer namens "demovm" aktivieren und deaktivieren.

1. Hier erhalten Sie eine Liste der laufenden Integrationsdienste:

```
Get-VMIntegrationService -VMName "DemoVM"
```

2. Die Ausgabe sollte wie folgt aussehen:

VMName	Name	Enabled	PrimaryStatusDescription	SecondaryStatusDescription
-----	----	-----	-----	-----
DemoVM	Guest Service Interface	False	OK	
DemoVM	Heartbeat	True	OK	OK
DemoVM	Key-Value Pair Exchange	True	OK	
DemoVM	Shutdown	True	OK	
DemoVM	Time Synchronization	True	OK	
DemoVM	VSS	True	OK	

3. Gast Dienst Schnittstelle aktivieren:

```
Enable-VMIntegrationService -VMName "DemoVM" -Name "Guest Service Interface"
```

4. Überprüfen Sie, ob die Gast Dienst Schnittstelle aktiviert ist:

```
Get-VMIntegrationService -VMName "DemoVM"
```

5. Gast Dienst Schnittstelle ausschalten:

```
Disable-VMIntegrationService -VMName "DemoVM" -Name "Guest Service Interface"
```

Überprüfen der Integration Services-Version des Gasts

Einige Features funktionieren möglicherweise nicht ordnungsgemäß oder überhaupt nicht, wenn die Integrationsdienste des Gasts nicht aktuell sind. Um die Versionsinformationen für ein Fenster zu erhalten, melden Sie sich beim Gast Betriebssystem an, öffnen Sie eine Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

```
REG QUERY "HKLM\Software\Microsoft\Virtual Machine\Auto" /v IntegrationServicesVersion
```

Ältere Gast Betriebssysteme haben nicht alle verfügbaren Dienste. Beispielsweise können Windows Server 2008 R2-Gäste nicht über das "Hyper-V-Gastschnittstellendienst" verfügen.

Starten und Beenden eines Integrations Diensts von einem Windows-Gast

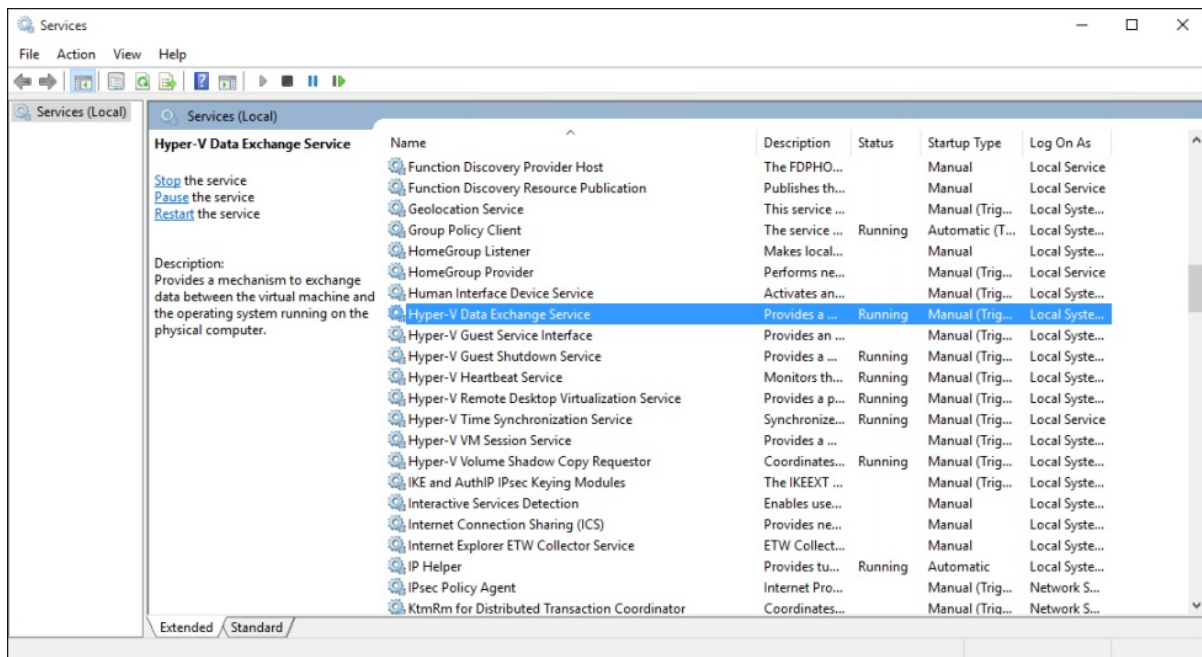
Damit ein Integrations Dienst voll funktionsfähig ist, muss der zugehörige Dienst innerhalb des Gast Betriebssystems zusätzlich zur Aktivierung auf dem Host ausgeführt werden. In Windows-Gastbetriebssystemen wird jeder Integrations Dienst als standardmäßiger Windows-Dienst aufgeführt. Sie können das Applet "Dienste" in der Systemsteuerung oder PowerShell verwenden, um diese Dienste zu starten und zu starten.

IMPORTANT

Das Beenden eines Integrations Diensts kann die Fähigkeit des Hosts, den virtuellen Computer zu verwalten, stark beeinträchtigen. Um ordnungsgemäß zu funktionieren, muss jeder Integrations Dienst, den Sie verwenden möchten, sowohl auf dem Host als auch auf dem Gast aktiviert sein. Als bewährte Vorgehensweise sollten Sie die Integrationsdienste von Hyper-V nur mithilfe der oben aufgeführten Anweisungen steuern. Der übereinstimmende Dienst im Gast Betriebssystem wird automatisch beendet oder gestartet, wenn Sie seinen Status in Hyper-V ändern. Wenn Sie einen Dienst im Gast Betriebssystem starten, aber in Hyper-V deaktiviert ist, wird der Dienst angehalten. Wenn Sie einen Dienst im Gast Betriebssystem, der in Hyper-v aktiviert ist, beendet haben, startet Hyper-v ihn schließlich erneut. Wenn Sie den Dienst im Gast deaktivieren, kann er von Hyper-V nicht gestartet werden.

Verwenden von Windows-Diensten zum Starten oder Beenden eines Integrations Diensts innerhalb eines Windows-Gast Diensts

1. Öffnen Sie den Dienst-Manager, indem Sie `services.msc` als Administrator ausführen oder indem Sie in der Systemsteuerung auf das Symbol "Dienste" doppelklicken.



2. Suchen Sie die Dienste, die mit "Hyper-V" beginnen.
3. Klicken Sie mit der rechten Maustaste auf den Dienst, der gestartet oder beendet werden soll. Klicken Sie auf die gewünschte Aktion.

Verwenden von Windows PowerShell zum Starten oder Beenden eines Integrations Diensts innerhalb eines Windows-Gast Betriebssystems

1. Führen Sie Folgendes aus, um eine Liste der Integrationsdienste zu erhalten:

```
Get-Service -Name vm*
```

2. Die Ausgabe sollte etwa so aussehen:

```
Status   Name                DisplayName
-----
Running  vmicguestinterface  Hyper-V Guest Service Interface
Running  vmicheartbeat       Hyper-V Heartbeat Service
Running  vmickvpexchange     Hyper-V Data Exchange Service
Running  vmicrdv             Hyper-V Remote Desktop Virtualizati...
Running  vmicshutdown        Hyper-V Guest Shutdown Service
Running  vmictimesync        Hyper-V Time Synchronization Service
Stopped  vmicvm session      Hyper-V VM Session Service
Running  vmicvss             Hyper-V Volume Shadow Copy Requestor
```

3. Ausführen von " [Start-Service](#) " oder "Start -[Service](#)". Um beispielsweise Windows PowerShell Direct zu deaktivieren, führen Sie Folgendes aus:

```
Stop-Service -Name vmicvm session
```

Starten und Beenden eines Integrations Diensts von einem Linux-Gast

Linux-Integrationsdienste werden in der Regel über den Linux-Kernel bereitgestellt. Der Treiber für Linux-

Integrationsdienste hat den Namen **hv_utils**.

1. Um herauszufinden, ob **hv_utils** geladen ist, verwenden Sie den folgenden Befehl:

```
lsmod | grep hv_utils
```

2. Die Ausgabe sollte etwa so aussehen:

Module	Size	Used by
hv_utils	20480	0
hv_vmbus	61440	8
hv_balloon, hyperv_keyboard, hv_netvsc, hid_hyperv, hv_utils, hyperv_fb, hv_storvsc		

3. Wenn Sie herausfinden möchten, ob die erforderlichen Daemons ausgeführt werden, verwenden Sie diesen Befehl.

```
ps -ef | grep hv
```

4. Die Ausgabe sollte etwa so aussehen:

root	236	2	0	Jul11	?	00:00:00	[hv_vmbus_con]
root	237	2	0	Jul11	?	00:00:00	[hv_vmbus_ctl]
...							
root	252	2	0	Jul11	?	00:00:00	[hv_vmbus_ctl]
root	1286	1	0	Jul11	?	00:01:11	/usr/lib/linux-tools/3.13.0-32-generic/hv_kvp_daemon
root	9333	1	0	Oct12	?	00:00:00	/usr/lib/linux-tools/3.13.0-32-generic/hv_kvp_daemon
root	9365	1	0	Oct12	?	00:00:00	/usr/lib/linux-tools/3.13.0-32-generic/hv_vss_daemon
scooley	43774	43755	0	21:20	pts/0	00:00:00	grep --color=auto hv

5. Führen Sie Folgendes aus, um festzustellen, welche Daemons verfügbar sind:

```
compgen -c hv_
```

6. Die Ausgabe sollte etwa so aussehen:

```
hv_vss_daemon
hv_get_dhcp_info
hv_get_dns_info
hv_set_ifconfig
hv_kvp_daemon
hv_fcopy_daemon
```

Zu den unter Umständen aufgelisteten Integrations Dienst-Daemons zählen die folgenden. Wenn fehlende vorhanden sind, werden Sie möglicherweise auf Ihrem System nicht unterstützt, oder Sie sind möglicherweise nicht installiert. Weitere Informationen finden Sie [unter Unterstützte virtuelle Linux-und FreeBSD-Computer für Hyper-V unter Windows](#).

- **hv_vss_daemon**: Dieser Daemon ist zum Erstellen von Sicherungen virtueller Linux-Computer erforderlich.
- **hv_kvp_daemon**: Dieser Daemon ermöglicht das Festlegen und Abfragen von systeminternen und extrinsischen Schlüssel-Wert-Paaren.
- **hv_fcopy_daemon**: Dieser Daemon implementiert einen Datei Kopier Dienst zwischen Host und Gast.

Beispiele

Diese Beispiele veranschaulichen das Beenden und Starten des KVP-Daemons mit dem Namen `hv_kvp_daemon` .

1. Verwenden Sie die Prozess-ID () -PID, um den Prozess des Daemons zu verhindern. Um die PID zu finden, sehen Sie sich die zweite Spalte der Ausgabe an, oder verwenden Sie `pidof` . Hyper-V-Daemons werden als root-Vorgänge ausgeführt, sodass Sie Root-Berechtigungen benötigen.

```
sudo kill -15 `pidof hv_kvp_daemon`
```

2. Führen Sie folgende Schritte aus, um zu überprüfen, ob der gesamte `hv_kvp_daemon` Prozess

```
ps -ef | hv
```

3. Um den Daemon erneut zu starten, führen Sie den Daemon als root-Vorgang aus:

```
sudo hv_kvp_daemon
```

4. Führen Sie Folgendes aus, um zu überprüfen, ob der `hv_kvp_daemon` Prozess mit einer neuen Prozess-ID aufgelistet ist:

```
ps -ef | hv
```

Integration Services auf dem neuesten Stand halten

Es wird empfohlen, Integration Services auf dem neuesten Stand zu halten, um die bestmögliche Leistung und die neuesten Features für Ihre virtuellen Computer zu erhalten. Dies ist für die meisten Windows-Gäste standardmäßig der Fall, wenn Sie so eingerichtet sind, dass wichtige Updates von Windows Update erhalten werden. Linux-Gäste, die aktuelle Kernel verwenden, erhalten beim Aktualisieren des Kernels die neuesten Integrations Komponenten.

Für virtuelle Maschinen, die auf Windows 10-/Windows Server 2016/2019-Hosts ausgeführt werden:

NOTE

Die Image Datei "vmguest. ISO" ist nicht in Hyper-V unter Windows 10/Windows Server 2016/2019 enthalten, da Sie nicht mehr benötigt wird.

GAST	UPDATEMECHANISMUS	NOTIZEN
Windows 10	Windows Update	
Windows 8.1	Windows Update	
Windows 8	Windows Update	Benötigt den Integrationsdienst „Datenaustausch“.*
Windows 7	Windows Update	Benötigt den Integrationsdienst „Datenaustausch“.*
Windows Vista (SP 2)	Windows Update	Benötigt den Integrationsdienst „Datenaustausch“.*
-		

GAST	UPDATEMECHANISMUS	NOTIZEN
Windows Server 2016	Windows Update	
Windows Server (halbjährlicher Kanal)	Windows Update	
Windows Server 2012 R2	Windows Update	
Windows Server 2012	Windows Update	Benötigt den Integrationsdienst „Datenaustausch“.*
Windows Server 2008 R2 (SP 1)	Windows Update	Benötigt den Integrationsdienst „Datenaustausch“.*
Windows Server 2008 (SP 2)	Windows Update	Erweiterte Unterstützung nur in Windows Server 2016 (Weitere Informationen).
Windows Home Server 2011	Windows Update	Wird in Windows Server 2016 (Weitere Informationen) nicht unterstützt.
Windows Small Business Server 2011	Windows Update	Nicht im grundlegenden Support enthalten (Weitere Informationen).
-		
Linux-Gastbetriebssysteme	Paket-Manager	Integration Services für Linux sind in die Distribution integriert, es können jedoch optionale Updates verfügbar sein. *****

*Wenn der Datenaustausch-Integrations Dienst nicht aktiviert werden kann, stehen die Integrationsdienste für diese Gäste im [Download Center](#) als CAB-Datei (CAB-Datei) zur Verfügung. Anweisungen zum Anwenden eines CAB finden Sie in diesem [Blogbeitrag](#).

Für virtuelle Maschinen, die auf Windows 8.1/Windows Server 2012r2-Hosts ausgeführt werden:

GAST	UPDATEMECHANISMUS	NOTIZEN
Windows 10	Windows Update	
Windows 8.1	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows 8	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows 7	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Vista (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows XP (SP 2, SP 3)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.

GAST	UPDATEMECHANISMUS	NOTIZEN
-		
Windows Server 2016	Windows Update	
Windows Server (halbjährlicher Kanal)	Windows Update	
Windows Server 2012 R2	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2012	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2008 R2	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2008 (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Home Server 2011	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Small Business Server 2011	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2003 R2 (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2003 (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
-		
Linux-Gastbetriebssysteme	Paket-Manager	Integration Services für Linux sind in die Distribution integriert, es können jedoch optionale Updates verfügbar sein. **

Für virtuelle Computer, die auf Windows 8/Windows Server 2012-Hosts ausgeführt werden:

GAST	UPDATEMECHANISMUS	NOTIZEN
Windows 8.1	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows 8	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows 7	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Vista (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.

GAST	UPDATEMECHANISMUS	NOTIZEN
Windows XP (SP 2, SP 3)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
-		
Windows Server 2012 R2	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2012	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2008 R2	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2008 (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Home Server 2011	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Small Business Server 2011	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2003 R2 (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
Windows Server 2003 (SP 2)	Integrationsdienste-Datenträger	Weitere Informationen finden Sie unten unter.
-		
Linux-Gastbetriebssysteme	Paket-Manager	Integration Services für Linux sind in die Distribution integriert, es können jedoch optionale Updates verfügbar sein. **

Weitere Informationen zu Linux-Gastbetriebssystemen finden Sie [unter Unterstützte virtuelle Linux-und FreeBSD-Computer für Hyper-V unter Windows](#).

Installieren oder Aktualisieren von Integrationsdiensten

NOTE

Bei Hosts, die älter als Windows Server 2016 und Windows 10 sind, müssen Sie die Integrationsdienste in den Gastbetriebssystemen **manuell installieren oder aktualisieren**.

Verfahren zum manuellen Installieren oder Aktualisieren der Integrationsdienste:

1. Öffnen Sie den Hyper-V-Manager. Klicken Sie im Menü Extras von Server-Manager auf **Hyper-V-Manager**.
2. Stellen Sie eine Verbindung mit dem virtuellen Computer her. Klicken Sie mit der rechten Maustaste auf den virtuellen Computer und dann auf **verbinden**.
3. Klicken Sie im Menü **Aktion** von **Verbindung mit virtuellen**

Computern%%amp;quot; auf **Installationsdatenträger für Integrationsdienste einlegen**. Dadurch wird der Installationsdatenträger im virtuellen DVD-Laufwerk geladen. Abhängig vom Gast Betriebssystem müssen Sie die Installation möglicherweise manuell starten.

4. Nach Abschluss der Installation sind alle Integrationsdienste verfügbar.

NOTE

Diese Schritte **können nicht automatisiert** oder innerhalb einer Windows PowerShell-Sitzung für virtuelle **Online** Computer ausgeführt werden. Sie können Sie auf vhdx- **Offline** Images anwenden. Weitere Informationen finden [Sie unter Installieren von Integration Services, wenn der virtuelle Computer nicht ausgeführt wird](#). Sie können die Bereitstellung der Integrationsdienste auch über **Configuration Manager** mit den VMS **Online** automatisieren, aber Sie müssen die VMs am Ende der Installation neu starten. Weitere Informationen finden [Sie unter Bereitstellen von Hyper-V-Integration Services auf VMS mithilfe von config Manager](#)

Verwalten von virtuellen Windows-Computern mit PowerShell Direct

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016, Windows Server 2019

Mit PowerShell Direct können Sie einen virtuellen Computer unter Windows 10, Windows Server 2016 oder Windows Server 2019 über einen Hyper-V-Host unter Windows 10, Windows Server 2016 oder Windows 2019 Server remote verwalten. PowerShell Direct ermöglicht die Windows PowerShell-Verwaltung innerhalb eines virtuellen Computers unabhängig von der Netzwerkkonfiguration oder den Remote Verwaltungs Einstellungen auf dem Hyper-V-Host oder dem virtuellen Computer. Dies erleichtert Hyper-V-Administratoren die Automatisierung und Erstellung von Skripts zur Verwaltung und Konfiguration virtueller Computer.

Es gibt zwei Möglichkeiten, PowerShell Direct auszuführen:

- Erstellen und Beenden einer PowerShell Direct-Sitzung mit PSSession-cmdlets
- Ausführen von Skripts oder Befehls mit dem Invoke-Command-cmdlet

Wenn Sie ältere virtuelle Computer verwalten, verwenden Sie die Verbindung mit virtuellen Computern (VMConnect) oder [Konfigurieren Sie ein virtuelles Netzwerk für den virtuellen Computer](#).

Erstellen und Beenden einer PowerShell Direct-Sitzung mit PSSession-cmdlets

1. Öffnen Sie Windows PowerShell auf dem Hyper-V-Host als Administrator.
2. Verwenden [Sie das Enter-PSSession-](#) Cmdlet, um eine Verbindung mit dem virtuellen Computer herzustellen. Führen Sie einen der folgenden Befehle aus, um eine Sitzung mit dem Namen oder der GUID des virtuellen Computers zu erstellen:

```
Enter-PSSession -VMName <VMName>
```

```
Enter-PSSession -VMGUID <VMGUID>
```

3. Geben Sie Ihre Anmelde Informationen für den virtuellen Computer ein.
4. Führen Sie alle erforderlichen Befehle aus. Diese Befehle werden auf dem virtuellen Computer ausgeführt, auf dem Sie die Sitzung erstellt haben.
5. Wenn Sie fertig sind, verwenden Sie [Exit-PSSession](#) , um die Sitzung zu schließen.

```
Exit-PSSession
```

Ausführen von Skripts oder Befehls mit dem Cmdlet "Invoke-Command"

Sie können mithilfe des Cmdlets [Invoke-Command](#) einen vordefinierten Satz von Befehlen auf dem virtuellen

Computer ausführen. Es folgt ein Beispiel der Nutzung des Cmdlets „Invoke-Command“, wobei „PSTest“ der Name des virtuellen Computers ist und sich das auszuführende Skript (foo.ps1) im Skriptordner auf Laufwerk C:/ befindet:

```
Invoke-Command -VMName PSTest -FilePath C:\script\foo.ps1
```

Zum Ausführen eines einzelnen Befehls verwenden Sie den Parameter **-ScriptBlock**:

```
Invoke-Command -VMName PSTest -ScriptBlock { cmdlet }
```

Was ist erforderlich, um PowerShell direkt zu verwenden?

So richten Sie eine PowerShell Direct-Sitzung auf einem virtuellen Computer ein

- Der virtuelle Computer muss lokal auf dem Host ausgeführt und gestartet werden.
- Sie müssen am Hostcomputer als Hyper-V-Administrator angemeldet sein.
- Sie müssen gültige Anmeldeinformationen für den virtuellen Computer angeben.
- Auf dem Host Betriebssystem muss mindestens Windows 10 oder Windows Server 2016 ausgeführt werden.
- Auf dem virtuellen Computer muss mindestens Windows 10 oder Windows Server 2016 ausgeführt werden.

Mithilfe des Cmdlets [Get-VM](#) können Sie überprüfen, ob die von Ihnen verwendeten Anmelde Informationen die Rolle "Hyper-V-Administrator" aufweisen und eine Liste der virtuellen Computer, die lokal auf dem Host ausgeführt werden, und gestartet wird.

Weitere Informationen

[Enter-PSSession](#)

[Exit-PSSession](#)

[Befehl "aufrufen"](#)

Einrichten von Hyper-V-Replikaten

09.04.2020 • 22 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Hyper-V-Replikat ist ein wesentlicher Bestandteil der Hyper-V-Rolle. Es trägt zu ihrer Strategie für die Notfall Wiederherstellung bei, indem virtuelle Computer von einem Hyper-V-Host Server auf einen anderen replizieren werden, um Ihre Workloads verfügbar zu halten. Das Hyper-V-Replikat erstellt eine Kopie eines virtuellen Live Computers auf einem virtuellen Replikat Computer, der offline ist. Beachten Sie Folgendes:

- **Hyper-V-Hosts:** primäre und sekundäre Host Server können sich physisch nebeneinander befinden oder sich an verschiedenen geografischen Standorten mit Replikation über eine WAN-Verbindung befinden. Hyper-V-Hosts können eigenständig, gruppiert oder eine Kombination aus beidem sein. Es gibt keine Active Directory Abhängigkeit zwischen den Servern, und Sie müssen keine Domänen Mitglieder sein.
- **Replikation und Änderungs Nachverfolgung:** Wenn Sie das Hyper-V-Replikat für eine bestimmte virtuelle Maschine aktivieren, wird bei der ersten Replikation ein identischer virtueller Replikat Computer auf einem sekundären Host. Danach erstellt und verwaltet die Hyper-V-Replikat-Änderungs Nachverfolgung eine Protokolldatei, mit der Änderungen auf der VHD einer virtuellen Maschine erfasst werden. Die Protokolldatei wird auf der Grundlage der Replikations Häufigkeits Einstellungen in umgekehrter Reihenfolge an die Replikat-VHD. Dies bedeutet, dass die neuesten Änderungen gespeichert und asynchron repliziert werden. Die Replikation kann über HTTP oder HTTPS erfolgen.
- **Erweiterte (verkettete) Replikation:** auf diese Weise können Sie eine virtuelle Maschine von einem primären Host auf einen sekundären Host replizieren und dann den sekundären Host auf einen dritten Host replizieren. Beachten Sie, dass Sie nicht vom primären Host direkt auf den zweiten und den dritten replizieren können.

Mit diesem Feature ist das Hyper-V-Replikat für die Notfall Wiederherstellung stabiler, denn wenn ein Ausfall auftritt, können Sie das primäre und das erweiterte Replikat wiederherstellen. Sie können ein Failover zum erweiterten Replikat ausführen, wenn der primäre und der sekundäre Standort ausfällt. Beachten Sie, dass das erweiterte Replikat keine Anwendungs konsistente Replikation unterstützt und die gleichen VHDs verwenden muss, die vom sekundären Replikat verwendet werden.

- **Failover:** Wenn ein Ausfall in Ihrem primären (oder sekundären) Standort auftritt, können Sie manuell ein Test-, geplantes oder ungeplantes Failover initiieren.

	TEST	GEPLANT	UNPLANNED
Wann sollte ich ausgeführt werden?	Überprüfen, ob für einen virtuellen Computer ein Failover und Start am sekundären Standort möglich ist Nützlich für Tests und Schulungen	Während geplanter Ausfallzeiten und Ausfällen	Bei unerwarteten Ereignissen
Wird ein doppelter virtueller Computer erstellt?	Ja	Nein	Nein

	TEST	GEPLANT	UNPLANNED
Wo wird Sie initiiert?	Auf dem virtuellen Replikat Computer	Initiiert auf dem primären und abgeschlossen auf dem sekundären Computer	Auf dem virtuellen Replikat Computer
Wie oft sollte ich ausgeführt werden?	Wir empfehlen, einmal pro Monat zu testen.	Einmal alle sechs Monate oder gemäß den Konformitätsanforderungen	Nur im Notfall, wenn der primäre virtuelle Computer nicht verfügbar ist
Wird der primäre virtuelle Computer weiterhin repliziert?	Ja	Ja. Wenn der Ausfall gelöst wird, repliziert die umgekehrte Replikation die Änderungen zurück zum primären Standort, sodass die primäre und die sekundäre Datenbank synchronisiert werden.	Nein
Gibt es Datenverluste?	Keine	None. Nach dem Failover repliziert das Hyper-V-Replikat den letzten Satz an nach verfolgten Änderungen zurück zum primären Replikat, um den Verlust von Daten zu	Hängt vom Ereignis und den Wiederherstellungspunkten ab
Gibt es Ausfallzeiten?	None. Dies wirkt sich nicht auf Ihre Produktionsumgebung aus. Während des Failovers wird ein doppelter virtueller Testcomputer erstellt. Nachdem das Failover abgeschlossen ist, wählen Sie ein Failover auf dem virtuellen Replikat Computer aus, das automatisch bereinigt und gelöscht wird.	Die Dauer des geplanten Ausfalls.	Die Dauer des ungeplanten Ausfalls.

- **Wiederherstellungspunkte:** beim Konfigurieren der Replikationseinstellungen für einen virtuellen Computer geben Sie die Wiederherstellungspunkte an, die Sie aus dem virtuellen Computer speichern möchten. Wiederherstellungspunkte stellen eine Momentaufnahme dar, von der aus Sie einen virtuellen Computer wiederherstellen können. Wenn Sie einen letzten Wiederherstellungspunkt wiederherstellen, gehen offensichtlich weniger Daten verloren. Sie können vor bis zu 24 Stunden auf Wiederherstellungspunkte zugreifen.

Bereitstellungsvoraussetzungen

Bevor Sie beginnen, sollten Sie Folgendes überprüfen:

- **Ermitteln Sie, welche VHDs repliziert werden müssen.** Insbesondere VHDs, die Daten enthalten, die sich schnell ändern und nach einem Failover nicht vom Replikat Server verwendet werden (z. B. Auslagerungs Datenträger), sollten von der Replikation ausgeschlossen werden, um Netzwerkbandbreite. Notieren Sie sich, welche VHDs ausgeschlossen werden können.

- **Entscheiden Sie, wie oft Daten synchronisiert werden müssen:** die Synchronisierung der Daten auf dem Replikat Server erfolgt entsprechend der von Ihnen konfigurierten Replikations Häufigkeit (30 Sekunden, 5 Minuten oder 15 Minuten). Die Häufigkeit, die Sie auswählen, sollte Folgendes berücksichtigen: sind die virtuellen Computer mit einem niedrigen RPO-Wert auf dem Computer ausgeführt? Was sind ihre Bandbreiten Aspekte? Ihre äußerst kritischen virtuellen Computer benötigen offensichtlich häufigere Replikationen.
- **Entscheiden, wie Daten wieder hergestellt werden sollen:** Standardmäßig speichert das Hyper-V-Replikat nur einen einzelnen Wiederherstellungspunkt, bei dem es sich um die letzte vom primären Replikat gesendete Replikation Wenn Sie jedoch die Option zum Wiederherstellen von Daten bis zu einem früheren Zeitpunkt möchten, können Sie angeben, dass zusätzliche Wiederherstellungspunkte gespeichert werden sollen (maximal 24 Stunden). Wenn Sie zusätzliche Wiederherstellungspunkte benötigen, sollten Sie beachten, dass dies mehr Aufwand für Verarbeitungs-und Speicherressourcen erfordert.
- **Ermitteln Sie, welche Arbeits Auslastungen Sie replizieren:** bei der Hyper-V-Standard Replikation wird nach einem Failover die Konsistenz des Betriebssystems des virtuellen Computers gewahrt, aber nicht der Status der Anwendungen, die auf dem virtuellen Computer ausgeführt werden. Wenn Sie in der Lage sein möchten, ihren Arbeits Auslastungs Status wiederherzustellen, können Sie App-konsistente Wiederherstellungspunkte erstellen. Beachten Sie, dass die APP-konsistente Wiederherstellung auf dem erweiterten Replikat Standort nicht verfügbar ist, wenn Sie die erweiterte (verkettete) Replikation
- **Legen Sie fest, wie die anfängliche Replikation der Daten virtueller Computer durchzuführenist:** die Replikation beginnt mit dem übertragen der Anforderungen zum Übertragen des aktuellen Zustands der virtuellen Computer. Dieser anfängliche Zustand kann direkt über das vorhandene Netzwerk übermittelt werden – entweder sofort oder zu einem konfigurierbaren späteren Zeitpunkt. Sie können auch einen bereits vorhandenen wiederhergestellten virtuellen Computer verwenden (z. b., wenn Sie eine frühere Sicherung des virtuellen Computers auf dem Replikat Server wieder hergestellt haben) als Erstkopie. Alternativ können Sie Netzwerkbandbreite einsparen, indem Sie die Erstkopie auf externe Medien kopieren und diese physisch an den Replikatstandort senden. Wenn Sie einen bereits vorhandenen virtuellen Computer verwenden möchten, löschen Sie alle vorherigen Momentaufnahmen, die ihm zugeordnet sind.

Bereitstellungsschritte

Schritt 1: Einrichten der Hyper-V-Hosts

Sie benötigen mindestens zwei Hyper-V-Hosts mit einem oder mehreren virtuellen Computern auf jedem Server. [Beginnen Sie mit Hyper-V](#). Der Host Server, auf dem Sie virtuelle Computer replizieren, muss als Replikat Server eingerichtet werden.

1. Wählen Sie in den Hyper-V-Einstellungen für den Server, auf dem Sie virtuelle Computer replizieren, unter **Replikationskonfiguration** die Option **diesen Computer als Replikat Server** aktivieren aus.
2. Sie können über HTTP oder verschlüsselte HTTPS replizieren. Wählen Sie **Kerberos (http) verwenden** oder **Zertifikat basierte Authentifizierung (HTTPS) verwenden**. Standardmäßig sind http 80 und HTTPS 443 als Firewalleausnahmen auf dem Hyper-V-Replikat Server aktiviert. Wenn Sie die Standard Port Einstellungen ändern, müssen Sie auch die Firewalleausnahme ändern. Wenn Sie über HTTPS replizieren, müssen Sie ein Zertifikat auswählen, und Sie sollten die Zertifikat Authentifizierung eingerichtet haben.
3. Aktivieren Sie für die Autorisierung die Option **Replikation von einem beliebigen authentifizierten Server zulassen**, um dem Replikat Server zuzulassen, dass der Replikations Datenverkehr für virtuelle Computer von einem beliebigen primären Server Aktivieren Sie **Replikation von den angegebenen Servern zulassen**, um nur Datenverkehr von den primären Servern zu akzeptieren, die Sie speziell auswählen.

Für beide Optionen können Sie angeben, wo die replizierten VHDs auf dem Hyper-V-Replikat Server gespeichert werden sollen.

4. Klicken Sie auf **OK** oder **Übernehmen**.

Schritt 2: Einrichten der Firewall

Um die Replikation zwischen dem primären und dem sekundären Server zuzulassen, muss der Datenverkehr über die Windows-Firewall (oder andere Firewalls von Drittanbietern) durchlaufen werden. Wenn Sie die Hyper-V-Rolle auf den Servern installiert haben, werden standardmäßig Ausnahmen für http (80) und HTTPS (443) erstellt. Wenn Sie diese Standardports verwenden, müssen Sie nur die Regeln aktivieren:

- So aktivieren Sie die Regeln auf einem eigenständigen Host Server:
 1. Öffnen Sie Windows-Firewall mit Vorlauf Sicherheit, und klicken Sie auf **Eingehende Regeln**
 2. Zum Aktivieren der HTTP-Authentifizierung (Kerberos) klicken Sie mit der rechten Maustaste auf **Hyper-V-Replikat-http-Listener (TCP-in) > Regel aktivieren**. Klicken Sie zum Aktivieren der HTTPS-Zertifikat basierten Authentifizierung mit der rechten Maustaste auf **Hyper-V-Replikat-HTTPS-Listener (TCP-in) > E-able-Regel**.
- Um Regeln für einen Hyper-V-Cluster zu aktivieren, öffnen Sie eine Windows PowerShell-Sitzung mithilfe von **als Administrator ausführen**, und führen Sie dann einen der folgenden Befehle aus:

- Für http:

```
get-clusternode | ForEach-Object {Invoke-command -computername $_.name -scriptblock {Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"}}
```

- Für https:

```
get-clusternode | ForEach-Object {Invoke-command -computername $_.name -scriptblock {Enable-Netfirewallrule -displayname "Hyper-V Replica HTTPS Listener (TCP-In)"}}
```

Aktivieren der Replikation der virtuellen Computer

Führen Sie auf jedem virtuellen Computer, den Sie replizieren möchten, folgende Schritte aus:

1. Wählen Sie im **Detail** Bereich von Hyper-V-Manager einen virtuellen Computer aus, indem Sie darauf klicken.
Klicken Sie mit der rechten Maustaste auf den ausgewählten virtuellen Computer, und klicken Sie auf **Replikation aktivieren**, um den Assistenten zum Aktivieren
2. Klicken Sie auf der Seite **Vorbemerkungen** auf **Weiter**.
3. Geben Sie auf der Seite **Replikat Server angeben** im Feld Replikat Server den NetBIOS-oder FQDN des Replikat Servers ein. Wenn der Replikat Serverteil eines Failoverclusters ist, geben Sie den Namen des Hyper-V-Replikat Brokers ein. Klicken Sie auf **Weiter**.
4. Auf der Seite **Verbindungsparameter angeben** Ruft das Hyper-V-Replikat automatisch die Authentifizierungs- und Port Einstellungen ab, die Sie für den Replikat Server konfiguriert haben. Wenn Werte nicht abgerufen werden, überprüfen Sie, ob der Server als Replikat Server konfiguriert und in DNS registriert ist. Falls erforderlich, müssen Sie die Einstellung manuell eingeben.
5. Vergewissern Sie sich auf der Seite **Replikations-VHDs auswählen**, dass die VHDs, die Sie replizieren möchten, ausgewählt ist, und deaktivieren Sie die Kontrollkästchen für alle virtuellen Festplatten, die Sie von der Replikation ausschließen möchten. Klicken Sie dann auf **Weiter**.
6. Geben Sie auf der Seite **Replikations Häufigkeit konfigurieren** an, wie oft Änderungen vom primären zum sekundären Replikat synchronisiert werden sollen. Klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite **zusätzliche Wiederherstellungspunkte konfigurieren** aus, ob nur der letzte Wiederherstellungspunkt beibehalten oder zusätzliche Punkte erstellt werden sollen. Wenn Sie Anwendungen und Arbeits Auslastungen mit ihren eigenen VSS-Writern konsistent wiederherstellen möchten, sollten Sie **Volumeschattenkopie-Dienst (VSS) frequency** auswählen und angeben, wie oft App-konsistente Momentaufnahmen erstellt werden sollen. Beachten Sie, dass der Hyper-v-VMM-

requestdienst auf den primären und sekundären Hyper-v-Servern ausgeführt werden muss. Klicken Sie dann auf **Weiter**.

- Wählen Sie auf der Seite **erste Replikation auswählen** die zu verwendende anfängliche Replikations Methode aus. Mit der Standardeinstellung zum Senden der ersten Kopie über das Netzwerk werden die Konfigurationsdatei des primären virtuellen Computers (vmcx) und die virtuellen Festplatten Dateien (vhdx und VHD), die Sie über die Netzwerkverbindung ausgewählt haben, kopiert. Überprüfen Sie die Verfügbarkeit der Netzwerkbandbreite, wenn Sie diese Option verwenden möchten. Wenn der primäre virtuelle Computer bereits auf dem sekundären Standort als replizierten virtuellen Computer konfiguriert ist, kann es hilfreich sein, **eine vorhandene virtuelle Maschine auf dem Replikationsserver als erste Kopie zu verwenden**. Sie können den Hyper-V-Export verwenden, um den primären virtuellen Computer zu exportieren und als virtuellen Replikat Computer auf dem sekundären Server zu importieren. Bei größeren virtuellen Computern oder eingeschränkter Bandbreite können Sie entscheiden, ob die erste Replikation über das Netzwerk zu einem späteren Zeitpunkt erfolgen soll, und anschließend außerhalb der Spitzenzeiten konfigurieren oder die Informationen zur ersten Replikation als Offline Medien senden.

Wenn Sie Offline Replikation durchführen, transportieren Sie die anfängliche Kopie mithilfe eines externen Speichermediums (z. B. einer Festplatte oder eines USB-Laufwerks) auf den sekundären Server. Zu diesem Zweck müssen Sie den externen Speicher mit dem primären Server (oder Besitzer Knoten in einem Cluster) verbinden. Wenn Sie dann erste Kopie mithilfe externer Medien senden auswählen, können Sie einen Speicherort lokal oder auf dem externen Medium angeben, auf dem die anfängliche Kopie gespeichert werden kann. Ein Platzhalter für einen virtuellen Computer wird am Replikat Standort erstellt. Nachdem die erste Replikation abgeschlossen ist, kann der externe Speicher an den Replikat Standort ausgeliefert werden. Dort verbinden Sie das externe Medium mit dem sekundären Server oder dem Besitzer Knoten des sekundären Clusters. Anschließend importieren Sie das erste Replikat an einen angegebenen Speicherort und führen es in den virtuellen Platzhalter Computer zusammen.

- Überprüfen Sie auf der Seite Fertigstellen der **Replikation** die Informationen in der Zusammenfassung, und klicken Sie dann auf **Fertigstellen**. Die Daten des virtuellen Computers werden in Übereinstimmung mit den ausgewählten Einstellungen übertragen. Daraufhin wird ein Dialogfeld mit dem Hinweis angezeigt, dass die Replikation erfolgreich aktiviert wurde.
- Wenn Sie die erweiterte (verkettete) Replikation konfigurieren möchten, öffnen Sie den Replikat Server, und klicken Sie mit der rechten Maustaste auf die zu replizierende virtuelle Maschine. Klicken Sie auf **Replikation** > erweitern Sie die **Replikation**, und geben Sie die

Ausführen eines Failovers

Nach Abschluss dieser Bereitstellung Schritte ist Ihre replizierte Umgebung betriebsbereit. Nun können Sie Failover nach Bedarf ausführen.

Test Failover: Wenn Sie ein Test Failover ausführen möchten, klicken Sie mit der rechten Maustaste auf den primären virtuellen Computer, und wählen Sie **Replikation** > **Test Failover** aus. Wählen Sie bei der Konfiguration den neuesten oder einen anderen Wiederherstellungspunkt aus. Auf dem sekundären Standort wird ein neuer virtueller Testcomputer erstellt und gestartet. Nachdem Sie die Tests abgeschlossen haben, wählen Sie **Test Failover** auf dem virtuellen Replikat Computer beenden aus, um den Vorgang zu bereinigen. Beachten Sie, dass Sie für einen virtuellen Computer nur ein Test Failover gleichzeitig ausführen können. [Weitere Informationen](#).

Geplantes Failover: zum Ausführen eines geplanten Failovers klicken Sie mit der rechten Maustaste auf den primären virtuellen Computer, und wählen Sie **Replikation** > **Geplantes Failover**. Beim geplanten Failover werden Voraussetzungs Prüfungen durchgeführt, um einen Datenverlust zu verhindern. Es wird überprüft, ob der primäre virtuelle Computer vor dem Failover heruntergefahren wird. Nach dem Failover des virtuellen Computers werden die Änderungen an den primären Standort replizieren, wenn der virtuelle Computer verfügbar ist. Beachten Sie, dass der primäre Server zu diesem Zweck so konfiguriert werden muss, dass die Replikation vom sekundären Server oder vom Hyper-V-Replikat Broker bei einem primären Cluster empfangen wird. Das geplante

Failover sendet den letzten Satz an nach verfolgten Änderungen. [Weitere Informationen](#).

Ungeplantes Failover: Wenn Sie ein ungeplantes Failover ausführen möchten, klicken Sie mit der rechten Maustaste auf den virtuellen Replikat Computer, und wählen Sie **Replikations** > nicht **Geplantes Failover** vom Hyper-V-Manager oder Failover Wenn diese Option aktiviert ist, können Sie den letzten Wiederherstellungspunkt oder frühere Wiederherstellungspunkte wiederherstellen. Überprüfen Sie nach dem Failover, ob alles erwartungsgemäß auf dem virtuellen Computer ausgeführt wird, und klicken Sie dann auf dem virtuellen Replikat Computer auf **Fertig** stellen. [Weitere Informationen](#).

Aktivieren der Intel Performance Monitoring-Hardware auf einem virtuellen Hyper-V-Computer

09.04.2020 • 4 minutes to read • [Edit Online](#)

Intel-Prozessoren enthalten Features, die als Leistungs Überwachungs Hardware bezeichnet werden (z. b. PMU, ETB, LBR). Diese Features werden von der Leistungs optimierenden Software wie Intel VTune-Verstärker verwendet, um die Softwareleistung zu analysieren. Vor Windows Server 2019 und Windows 10, Version 1809, konnten weder das Host Betriebssystem noch virtuelle Hyper-v-Gastcomputer bei Aktivierung von Hyper-v Hardware zur Leistungsüberwachung verwenden. Ab Windows Server 2019 und Windows 10, Version 1809, hat das Host Betriebssystem standardmäßig Zugriff auf die Leistungs Überwachungs Hardware. Virtuelle Hyper-v-Gastcomputer haben standardmäßig keinen Zugriff, aber Hyper-v-Administratoren können den Zugriff auf mindestens einen virtuellen Gastcomputer gewähren. In diesem Dokument werden die erforderlichen Schritte zum Bereitstellen der Hardware für die Leistungsüberwachung für virtuelle Gastcomputer beschrieben.

Voraussetzungen

Zum Aktivieren der Leistungs Überwachungs Hardware auf einem virtuellen Computer benötigen Sie Folgendes:

- Intel-Prozessor mit Leistungs Überwachungs Hardware (z.b. PMU, Peer-/LBR). In [diesem Dokument](#) von Intel können Sie feststellen, welche Hardware für die Leistungsüberwachung von Ihrem System unterstützt wird.
- Windows Server 2019 oder Windows 10, Version 1809 (Oktober 2018 Update) oder höher
- Ein virtueller Hyper-V-Computer *ohne* eine nicht [Genetzte Virtualisierung](#) , der ebenfalls den Status "beendet" aufweist

Zum Aktivieren der bevorstehenden Hardware für die Leistungsüberwachung von Intel Processor Trace (IPT) auf einem virtuellen Computer benötigen Sie Folgendes:

- Einen Intel-Prozessor, der IPT und die PT2GPA-Funktion unterstützt. In [diesem Dokument](#) von Intel können Sie feststellen, welche Hardware für die Leistungsüberwachung von Ihrem System unterstützt wird.
- Windows Server Version 1903 (SAC) oder Windows 10, Version 1903 (Mai 2019 Update) oder höher
- Ein virtueller Hyper-V-Computer *ohne* eine nicht [Genetzte Virtualisierung](#) , der ebenfalls den Status "beendet" aufweist

Aktivieren von Komponenten für die Leistungsüberwachung in einer virtuellen Maschine

Verwenden Sie das `Set-VMProcessor` PowerShell-Cmdlet, wenn Sie als Administrator ausgeführt werden, um unterschiedliche Komponenten der Leistungsüberwachung für einen bestimmten virtuellen Gastcomputer zu aktivieren:

```
# Enable all components except IPT
Set-VMProcessor MyVMName -Perfmon @("pmu", "lbr", "pebs")
```

```
# Enable a specific component
Set-VMProcessor MyVMName -Perfmon @("pmu")
```

```
# Enable IPT
Set-VMProcessor MyVMName -Perfmon @"ipt")
```

```
# Disable all components
Set-VMProcessor MyVMName -Perfmon @()
```

NOTE

Wenn "pebs" für die Leistungsüberwachung aktiviert wird, müssen "pmu" ebenfalls angegeben werden. "Peer" wird nur auf Hardware unterstützt, die über eine PMU-Version > = 4 verfügt. Das Aktivieren einer Komponente, die von den physischen Prozessoren des Hosts nicht unterstützt wird, führt zu einem Fehler beim Starten der virtuellen Maschine.

Auswirkungen der Aktivierung der Leistungs Überwachungs Hardware bei der Speicherung/Wiederherstellung, beim Export und bei der Live Migration

Microsoft empfiehlt keine Live Migration oder Speicherung/Wiederherstellung von virtuellen Computern mit Leistungs Überwachungs Hardware zwischen Systemen mit unterschiedlicher Intel-Hardware. Das spezifische Verhalten der Leistungs Überwachungs Hardware ist oft nicht Architektur und ändert sich zwischen Intel-Hardwaresystemen. Das Verschieben eines laufenden virtuellen Computers zwischen verschiedenen Systemen kann zu unvorhersehbarem Verhalten der nicht-Architektur Indikatoren führen.

Übersicht über die Livemigration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Die Live Migration ist eine Hyper-V-Funktion in Windows Server. So können Sie die Ausführung Virtual Machines transparent von einem Hyper-V-Host zu einem anderen migrieren, ohne dass Ausfallzeiten auftreten. Der Hauptvorteil der Live Migration ist die Flexibilität. das Ausführen von Virtual Machines ist nicht an einen einzelnen Host Computer gebunden. Dies ermöglicht Aktionen wie das Ableiten eines bestimmten Hosts Virtual Machines vor dem Außerbetriebsetzen oder aktualisieren. In Kombination mit Windows-Failoverclustering ermöglicht die Live Migration die Erstellung von hochverfügbaren und fehlertoleranten Systemen.

Verwandte Technologien und Dokumentationen

Die Live Migration wird häufig in Verbindung mit einigen verwandten Technologien wie Failoverclustering und System Center Virtual Machine Manager verwendet. Wenn Sie Livemigration über diese Technologien verwenden, finden Sie hier folgende Verweise auf die aktuelle Dokumentation:

- [Failoverclustering](#) (Windows Server 2016)
- [System Center Virtual Machine Manager](#) (System Center 2016)

Wenn Sie ältere Versionen von Windows Server verwenden oder Details zu den Funktionen benötigen, die in älteren Versionen von Windows Server eingeführt wurden, finden Sie hier Hinweise auf die historische Dokumentation:

- [Livemigration](#) (Windows Server 2008 R2)
- [Livemigration](#) (Windows Server 2012 R2)
- [Failoverclustering](#) (Windows Server 2012 R2)
- [Failoverclustering](#) (Windows Server 2008 R2)
- [System Center Virtual Machine Manager](#) (System Center 2012 R2)
- [System Center Virtual Machine Manager](#) (System Center 2008 R2)

Livemigration in Windows Server 2016

In Windows Server 2016 gibt es weniger Einschränkungen bei der Bereitstellung von Live Migrationen. Sie funktioniert nun ohne Failoverclustering. Andere Funktionen bleiben gegenüber früheren Versionen von Livemigration unverändert. Weitere Informationen zum Konfigurieren und Verwenden der Live Migration ohne Failoverclustering:

- [Einrichten von Hosts für die Live Migration ohne Failoverclustering](#)
- [Verwenden der Live Migration ohne Failoverclustering zum Verschieben einer virtuellen Maschine](#)

Übersicht über die Livemigration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Die Live Migration ist eine Hyper-V-Funktion in Windows Server. So können Sie die Ausführung Virtual Machines transparent von einem Hyper-V-Host zu einem anderen migrieren, ohne dass Ausfallzeiten auftreten. Der Hauptvorteil der Live Migration ist die Flexibilität. das Ausführen von Virtual Machines ist nicht an einen einzelnen Host Computer gebunden. Dies ermöglicht Aktionen wie das Ableiten eines bestimmten Hosts Virtual Machines vor dem Außerbetriebsetzen oder aktualisieren. In Kombination mit Windows-Failoverclustering ermöglicht die Live Migration die Erstellung von hochverfügbaren und fehlertoleranten Systemen.

Verwandte Technologien und Dokumentationen

Die Live Migration wird häufig in Verbindung mit einigen verwandten Technologien wie Failoverclustering und System Center Virtual Machine Manager verwendet. Wenn Sie Livemigration über diese Technologien verwenden, finden Sie hier folgende Verweise auf die aktuelle Dokumentation:

- [Failoverclustering](#) (Windows Server 2016)
- [System Center Virtual Machine Manager](#) (System Center 2016)

Wenn Sie ältere Versionen von Windows Server verwenden oder Details zu den Funktionen benötigen, die in älteren Versionen von Windows Server eingeführt wurden, finden Sie hier Hinweise auf die historische Dokumentation:

- [Livemigration](#) (Windows Server 2008 R2)
- [Livemigration](#) (Windows Server 2012 R2)
- [Failoverclustering](#) (Windows Server 2012 R2)
- [Failoverclustering](#) (Windows Server 2008 R2)
- [System Center Virtual Machine Manager](#) (System Center 2012 R2)
- [System Center Virtual Machine Manager](#) (System Center 2008 R2)

Livemigration in Windows Server 2016

In Windows Server 2016 gibt es weniger Einschränkungen bei der Bereitstellung von Live Migrationen. Sie funktioniert nun ohne Failoverclustering. Andere Funktionen bleiben gegenüber früheren Versionen von Livemigration unverändert. Weitere Informationen zum Konfigurieren und Verwenden der Live Migration ohne Failoverclustering:

- [Einrichten von Hosts für die Live Migration ohne Failoverclustering](#)
- [Verwenden der Live Migration ohne Failoverclustering zum Verschieben einer virtuellen Maschine](#)

Einrichten von Hosts für die Live Migration ohne Failoverclustering

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016, Microsoft Hyper-V Server 2016, Windows Server 2019, Microsoft Hyper-V Server 2019

In diesem Artikel erfahren Sie, wie Sie Hosts einrichten, die nicht gruppiert sind, damit Sie Live Migrationen zwischen Ihnen ausführen können. Verwenden Sie diese Anweisungen, wenn Sie bei der Installation von Hyper-V keine Live Migration eingerichtet haben, oder wenn Sie die Einstellungen ändern möchten. Verwenden Sie zum Einrichten von gruppierten Hosts die Tools für Failoverclustering.

Anforderungen für die Einrichtung einer Live Migration

Um nicht gruppierte Hosts für die Live Migration einzurichten, benötigen Sie Folgendes:

- Ein Benutzerkonto mit der Berechtigung zum Ausführen der verschiedenen Schritte. Die Mitgliedschaft in der lokalen Hyper-V-Administrator Gruppe oder der Gruppe "Administratoren" auf dem Quell- und dem Zielcomputer erfüllt diese Anforderung, es sei denn, Sie konfigurieren die eingeschränkte Delegation. Die Mitgliedschaft in der Gruppe Domänen Administratoren ist erforderlich, um die eingeschränkte Delegation zu konfigurieren.
- Die Hyper-V-Rolle in Windows Server 2016 oder Windows Server 2012 R2, die auf dem Quell- und dem Zielsystem installiert ist. Sie können eine Live Migration zwischen Hosts ausführen, auf denen Windows Server 2016 und Windows Server 2012 R2 ausgeführt wird, wenn der virtuelle Computer mindestens Version 5 ist.
Anweisungen zur Versionsaktualisierung finden Sie unter [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#). Installationsanweisungen finden Sie unter [Installieren der Hyper-V-Rolle unter Windows Server](#).
- Quell- und Zielcomputer, die entweder zur gleichen Active Directory Domäne gehören oder zu Domänen gehören, die einander vertrauen.
- Die Hyper-V-Verwaltungs Tools, die auf einem Computer installiert sind, auf dem Windows Server 2016 oder Windows 10 ausgeführt wird, es sei denn, die Tools sind auf dem Quell- oder Ziel Server installiert, und Sie führen die Tools vom Server aus.

Optionen für Authentifizierung und Netzwerk

Beachten Sie, wie Sie Folgendes einrichten möchten:

- **Authentifizierung:** welches Protokoll wird verwendet, um den Datenverkehr für die Live Migration zwischen den Quell- und Ziel Servern zu authentifizieren? Die Auswahl bestimmt, ob Sie sich beim Quell Server anmelden müssen, bevor Sie eine Live Migration starten:
 - Mithilfe von Kerberos können Sie sich nicht beim Server anmelden, sondern müssen die eingeschränkte Delegation einrichten. Weitere Informationen finden Sie weiter unten.
 - Mit "kredssp" können Sie die Konfiguration der eingeschränkten Delegation vermeiden. Sie müssen sich jedoch beim Quell Server anmelden. Hierzu können Sie eine lokale Konsolen Sitzung, eine Remotedesktop Sitzung oder eine Windows PowerShell-Remote Sitzung verwenden.

Für "kredssp" ist eine Anmeldung in Situationen erforderlich, die möglicherweise nicht offensichtlich sind. Wenn Sie sich beispielsweise bei TestServer01 anmelden, um eine virtuelle Maschine zu Bezeichnung testserver02 zu verschieben, und die virtuelle Maschine anschließend wieder in TestServer01 verschieben möchten, müssen Sie sich bei Bezeichnung testserver02 anmelden, bevor Sie versuchen, die virtuelle Maschine zurück auf TestServer01 zu verschieben. Wenn Sie dies nicht tun, schlägt der Authentifizierungs Versuch fehl, es tritt ein Fehler auf, und die folgende Meldung wird angezeigt:

"Fehler beim Migrations Vorgang für den virtuellen Computer bei der Migrations Quelle. Fehler beim Herstellen einer Verbindung mit dem Host *Computernamen*: im Sicherheitspaket 0x8009030E sind keine Anmelde Informationen verfügbar. "

- **Leistung:** ist es sinnvoll, Leistungsoptionen zu konfigurieren? Diese Optionen können die Netzwerk-und CPU-Auslastung reduzieren und die Live Migrationen schneller machen. Stellen Sie Ihre Anforderungen und ihre Infrastruktur in Erwägung, und testen Sie verschiedene Konfigurationen, um Ihnen die Entscheidung zu erleichtern. Die Optionen werden am Ende von Schritt 2 beschrieben.
- **Netzwerk Präferenz:** lässt Sie Live Migration-Datenverkehr über ein beliebiges verfügbares Netzwerk zu, oder isolieren Sie den Datenverkehr für bestimmte Netzwerke? Als bewährte Sicherheitsmethode wird empfohlen, den Datenverkehr auf vertrauenswürdige, private Netzwerken zu isolieren, da der Datenverkehr für die Livemigration beim Senden über das Netzwerk nicht verschlüsselt wird. Die Netzwerkisolation kann über ein physisch isoliertes Netzwerk oder über eine andere vertrauenswürdige Netzwerktechnologie, z. B. VLANs, erreicht werden.

Schritt 1: Konfigurieren der eingeschränkten Delegation (optional)

Wenn Sie sich für die Verwendung von Kerberos zum Authentifizieren des Datenverkehrs für die Live Migration entschieden haben, konfigurieren Sie die eingeschränkte Delegation mithilfe eines Kontos, das Mitglied der Gruppe Domänen Administratoren ist.

Verwenden des Snap-Ins "Benutzer und Computer" zum Konfigurieren der eingeschränkten Delegation

1. Öffnen Sie das Snap-In %"Active Directory-Benutzer und -Computer%". (Wählen Sie unter Server-Manager den Server aus, wenn er nicht ausgewählt ist, **klicken Sie auf Extras >> Active Directory Benutzer und Computer**).
2. Wählen Sie im Navigationsbereich von **Active Directory Benutzer und Computer** die Domäne aus, und doppelklicken Sie auf den Ordner **Computer** .
3. Klicken Sie im Ordner **Computer** mit der rechten Maustaste auf das Computer Konto des Quell Servers, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie in **Eigenschaften** auf die Registerkarte **Delegation** .
5. Wählen Sie auf der Registerkarte Delegation die Option **Computer nur bei Delegationen angegebener Dienste vertrauen aus** , und wählen Sie dann **beliebiges Authentifizierungsprotokoll verwenden** aus.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie unter **Dienste hinzufügen** auf **Benutzer oder Computer** .
8. Geben Sie in **Benutzer oder Computer auswählen** den Namen des Zielservers ein. Klicken Sie auf **Namen überprüfen** , um Sie zu überprüfen, und klicken Sie auf **OK**
9. Führen Sie in der Liste der verfügbaren Dienste unter **Dienste hinzufügen** die folgenden Schritte aus, und klicken Sie dann auf **OK**:
 - Wenn Sie den Speicher des virtuellen Computers entfernen möchten, wählen Sie **cifs** aus. Dies ist

erforderlich, wenn Sie den Speicher zusammen mit dem virtuellen Computer verschieben möchten, und wenn Sie nur den Speicher eines virtuellen Computers verschieben möchten. Wenn der Server für die Verwendung des SMB-Speichers für Hyper-V konfiguriert ist, wurde diese Auswahl bereits getroffen.

- Wenn Sie virtuelle Computer verschieben möchten, wählen Sie den **Migrationsdienst für virtuelles System von Microsoft** aus.
10. Stellen Sie auf der Registerkarte **Delegierung** des Dialogfelds „Eigenschaften“ sicher, dass die von Ihnen im vorherigen Schritt ausgewählten Dienste als Dienste aufgelistet sind, für die der Zielcomputer delegierte Anmeldeinformationen bereitstellen kann. Klicken Sie auf **OK**.
 11. Wählen Sie im Ordner **Computers** das Computerkonto des Zielservers aus, und wiederholen Sie den Prozess. Vergewissern Sie sich, dass Sie im Dialogfeld **Benutzer oder Computer auswählen** den Namen des Quellservers angegeben haben.

Die Konfigurationsänderungen treten in Kraft, nachdem die beiden folgenden Aktionen durchgeführt wurden:

- Die Änderungen werden auf die Domänen Controller repliziert, bei denen die Server, auf denen Hyper-V ausgeführt wird, angemeldet sind.
- Der Domänen Controller gibt ein neues Kerberos-Ticket aus.

Schritt 2: Einrichten der Quell-und Zielcomputer für die Live Migration

Dieser Schritt umfasst die Auswahl von Optionen für die Authentifizierung und das Netzwerk. Als bewährte Sicherheitsmaßnahme empfiehlt es sich, bestimmte Netzwerke auszuwählen, die für den Datenverkehr für die Live Migration verwendet werden sollen, wie oben erläutert. Außerdem wird in diesem Schritt gezeigt, wie Sie die Option Leistung auswählen.

Verwenden des Hyper-V-Managers zum Einrichten der Quell-und Zielcomputer für die Live Migration

1. Öffnen Sie den Hyper-V-Manager. (**Klicken Sie** in Server-Manager auf Extras >> **Hyper-V-Manager**.)
2. Wählen Sie im Navigationsbereich einen der Server aus. (Falls nicht aufgeführt, klicken Sie mit der rechten Maustaste auf **Hyper-V-Manager**, klicken Sie auf **Verbindung mit Server herstellen**, geben Sie den Servernamen ein, und klicken Sie auf **OK** Wiederholen Sie den Vorgang, um weitere Server hinzuzufügen.
3. Klicken Sie im Bereich **Aktion** auf **Hyper-V-Einstellungen >>Live Migrationen**.
4. Aktivieren Sie im Bereich **Livemigrationen** die Option **Ein- und ausgehende Livemigrationen ermöglichen**.
5. Geben Sie unter **gleichzeitige Live Migrationen** eine andere Zahl an, wenn Sie nicht den Standardwert von 2 verwenden möchten.
6. Wenn spezielle Netzwerkverbindungen den Datenverkehr für die Livemigration akzeptieren sollen, klicken Sie unter **Eingehende Livemigrationen** auf **Hinzufügen**, um die IP-Adressinformationen einzugeben. Klicken Sie anderenfalls auf **Beliebiges Netzwerk für Livemigration verwenden**. Klicken Sie auf **OK**.
7. Um die Kerberos-und Leistungsoptionen auszuwählen, erweitern Sie **Live Migrationen** , und wählen Sie dann **Erweiterte Funktionen** aus.
 - Wenn Sie die eingeschränkte Delegierung konfiguriert haben, wählen Sie unter **Authentifizierungsprotokoll** die Option **Kerberos** aus.
 - Überprüfen Sie unter **Leistungsoptionen** die Details, und wählen Sie eine andere Option aus, wenn Sie für Ihre Umgebung geeignet ist.
8. Klicken Sie auf **OK**.
9. Wählen Sie im Hyper-V-Manager den anderen Server aus, und wiederholen Sie die Schritte.

Verwenden von Windows PowerShell zum Einrichten der Quell- und Zielcomputer für die Live Migration

Zum Konfigurieren der Live Migration auf nicht gruppierten Hosts sind drei Cmdlets verfügbar: "[enable-vmmigration](#)", "[Set-vmmigrationnetwork](#)" und "[Set-VMHost](#)". In diesem Beispiel werden alle drei verwendet und folgende Aktionen durchgeführt:

- Hiermit wird die Live Migration auf dem lokalen Host konfiguriert.
- Ermöglicht eingehenden Migrations Datenverkehr nur in einem bestimmten Netzwerk.
- Wählt Kerberos als Authentifizierungsprotokoll aus.

Jede Zeile entspricht einem separaten Befehl.

```
PS C:\> Enable-VMMigration

PS C:\> Set-VMMigrationNetwork 192.168.10.1

PS C:\> Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos
```

Mit "Set-VMHost" können Sie auch eine Leistungs Option (und viele andere Host Einstellungen) auswählen. Wenn Sie z. B. SMB auswählen, aber das Authentifizierungsprotokoll auf den Standardwert von "kredssp" festlegen, geben Sie Folgendes ein:

```
PS C:\> Set-VMHost -VirtualMachineMigrationPerformanceOption SMB
```

In dieser Tabelle wird beschrieben, wie die Leistungsoptionen funktionieren.

OPTION	BESCHREIBUNG
TCP/IP	Der Arbeitsspeicher des virtuellen Computers wird über eine TCP/IP-Verbindung auf den Zielserverserver kopiert.
Komprimierung	Komprimiert den Speicherinhalt der virtuellen Maschine, bevor Sie über eine TCP/IP-Verbindung auf den Zielserverserver kopiert wird. Hinweis: Dies ist die Standard Einstellung.
SMB	<p>Der Arbeitsspeicher des virtuellen Computers wird über eine SMB 3,0-Verbindung auf den Zielserverserver kopiert.</p> <p>-SMB Direct wird verwendet, wenn für die Netzwerkadapter auf den Quell- und Ziel Servern RDMA (Remote Direct Memory Access)-Funktionen aktiviert sind.</p> <p>-SMB Multichannel erkennt und verwendet automatisch mehrere Verbindungen, wenn eine entsprechende SMB Multichannel-Konfiguration identifiziert wird.</p> <p>Weitere Informationen finden Sie unter Optimieren der Leistung von Dateiservern mit "SMB Direct".</p>

Nächste Schritte

Nachdem Sie die Hosts eingerichtet haben, sind Sie bereit, eine Live Migration durchzuführen. Anweisungen hierzu finden Sie unter [Verwenden der Live Migration ohne Failoverclustering zum Verschieben einer virtuellen Maschine](#).

Verwenden der Live Migration ohne Failoverclustering zum Verschieben einer virtuellen Maschine

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

In diesem Artikel erfahren Sie, wie Sie einen virtuellen Computer mithilfe einer Live Migration ohne Failoverclustering verschieben. Bei einer Live Migration werden virtuelle Maschinen ohne erkennbare Ausfallzeiten zwischen Hyper-V-Hosts verschoben.

Um dies zu erreichen, benötigen Sie Folgendes:

- Ein Benutzerkonto, das Mitglied der lokalen Gruppe "Hyper-V-Administratoren" oder der Gruppe "Administratoren" auf dem Quell- und dem Zielcomputer ist.
- Die Hyper-V-Rolle in Windows Server 2016 oder Windows Server 2012 R2, die auf dem Quell- und Zielsystem installiert ist und für Live Migrationen eingerichtet ist. Sie können eine Live Migration zwischen Hosts ausführen, auf denen Windows Server 2016 und Windows Server 2012 R2 ausgeführt wird, wenn der virtuelle Computer mindestens Version 5 ist.

Anweisungen zur Versionsaktualisierung finden Sie unter [Aktualisieren der Version virtueller Computer in Hyper-V unter Windows 10 oder Windows Server 2016](#). Installationsanweisungen finden Sie unter [Einrichten von Hosts für die Live Migration](#).

- Die Hyper-V-Verwaltungs Tools sind auf einem Computer installiert, auf dem Windows Server 2016 oder Windows 10 ausgeführt wird, es sei denn, die Tools sind auf dem Quell- oder Zielserver installiert, und Sie führen Sie von dort aus.

Verwenden des Hyper-V-Managers zum Verschieben eines laufenden virtuellen Computers

1. Öffnen Sie den Hyper-V-Manager. (Klicken Sie in Server-Manager auf Extras >> **Hyper-V-Manager**.)
2. Wählen Sie im Navigationsbereich einen der Server aus. (Falls nicht aufgeführt, klicken Sie mit der rechten Maustaste auf **Hyper-V-Manager**, klicken Sie auf **Verbindung mit Server herstellen**, geben Sie den Servernamen ein, und klicken Sie auf **OK**. Wiederholen Sie den Vorgang, um weitere Server hinzuzufügen.)
3. Klicken Sie im **Virtual Machines** Bereich mit der rechten Maustaste auf den virtuellen Computer, und klicken Sie dann auf **verschieben**. Der Verschiebungs-Assistent wird geöffnet.
4. Verwenden Sie die Seiten des Assistenten, um den Typ der Verschiebung, den Zielsystem und die Optionen auszuwählen.
5. Überprüfen Sie auf der Seite **Zusammenfassung** die von Ihnen ausgewählten Einstellungen, und klicken Sie dann auf **Fertig stellen**.

Verwenden von Windows PowerShell zum Verschieben eines laufenden virtuellen Computers

Im folgenden Beispiel wird das Cmdlet Move-VM verwendet, um eine virtuelle Maschine mit dem Namen *lmtest* auf einen Zielservers mit dem Namen *Bezeichnung testserver02* zu verschieben und die virtuellen Festplatten und andere Dateien, z. B. Prüfpunkte und Smart Paging-Dateien, in das Verzeichnis *d:\lmtest* auf dem Zielservers zu verschieben.

```
PS C:\> Move-VM LMTTest TestServer02 -IncludeStorage -DestinationStoragePath D:\LMTTest
```

Problembehandlung

Fehler beim Herstellen einer Verbindung.

Wenn Sie die eingeschränkte Delegierung noch nicht eingerichtet haben, müssen Sie sich beim Quell Server anmelden, bevor Sie einen virtuellen Computer verschieben können. Wenn Sie dies nicht tun, schlägt der Authentifizierungs Versuch fehl, es tritt ein Fehler auf, und die Meldung wird angezeigt:

"Fehler beim Migrations Vorgang für den virtuellen Computer bei der Migrations Quelle.

Fehler beim Herstellen einer Verbindung mit dem Host *Computernamen*: im Sicherheitspaket 0x8009030E sind keine Anmelde Informationen verfügbar. "

Um dieses Problem zu beheben, melden Sie sich beim Quell Server an, und wiederholen Sie den Vorgang. Um zu vermeiden, dass Sie sich vor einer Live Migration bei einem Quell Server anmelden müssen, richten Sie die eingeschränkte Delegierung ein. Zum Einrichten der eingeschränkten Delegierung benötigen Sie Domänen Administrator-Anmelde Informationen. Anweisungen hierzu finden [Sie unter Einrichten von Hosts für die Live Migration](#).

Fehler, weil die Host Hardware nicht kompatibel ist.

Wenn für einen virtuellen Computer die Prozessor Kompatibilität nicht aktiviert ist und eine oder mehrere Momentaufnahmen vorhanden sind, schlägt der Verschiebe Vorgang fehl, wenn die Hosts über unterschiedliche Prozessor Versionen verfügen. Es tritt ein Fehler auf, und diese Meldung wird angezeigt:

Der virtuelle Computer kann nicht auf den Zielcomputer verschoben werden. Die Hardware auf dem Zielcomputer ist mit den Hardwareanforderungen dieser virtuellen Maschine nicht kompatibel.

Um dieses Problem zu beheben, fahren Sie den virtuellen Computer herunter, und aktivieren Sie die Einstellung für die Prozessor Kompatibilität.

1. Klicken Sie im Hyper-V-Manager im **Virtual Machines** Bereich mit der rechten Maustaste auf den virtuellen Computer, und klicken Sie dann auf Einstellungen.
2. Erweitern Sie im Navigationsbereich die Option **Prozessoren** , und klicken Sie auf **Kompatibilität**.
3. Überprüfen Sie die **Migration zu einem Computer mit einer anderen Prozessor Version**.
4. Klicken Sie auf **OK**.

Verwenden Sie zum Verwenden von Windows PowerShell das Cmdlet [Set-vmprocessor](#) :

```
PS C:\> Set-VMProcessor TestVM -CompatibilityForMigrationEnabled $true
```


Leistungsoptimierung für Hyper-V-Server

24.04.2020 • 2 minutes to read • [Edit Online](#)

Hyper-V ist die Virtualisierungserverrolle in Windows Server 2016. Virtualisierungsserver können mehrere virtuelle Computer hosten, die voneinander isoliert sind, aber die zugrunde liegenden Hardwareressourcen gemeinsam nutzen, indem sie die Prozessoren, den Arbeitsspeicher und die E/A-Geräte virtualisieren. Durch die Konsolidierung von Servern auf einem einzigen Computer kann die Virtualisierung den Ressourcenverbrauch und die Energieeffizienz verbessern und die Betriebs- und Wartungskosten von Servern senken. Darüber hinaus bieten virtuelle Computer und die Verwaltungs-APIs mehr Flexibilität bei der Verwaltung von Ressourcen, dem Lastenausgleich und der Bereitstellung von Systemen.

Siehe auch

- [Hyper-V-Terminologie](#)
- [Hyper-V-Architektur](#)
- [Hyper-V-Serverkonfiguration](#)
- [Hyper-V-Prozessorleistung](#)
- [Hyper-V-Arbeitsspeicherleistung](#)
- [E/A-Leistung für Hyper-V-Speicher](#)
- [E/A-Leistung für Hyper-V-Netzwerk](#)
- [Erkennen von Engpässen in einer virtualisierten Umgebung](#)
- [Virtuelle Linux-Computer](#)

Virtueller Hyper-V-Switch

27.03.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält eine Übersicht über den virtuellen Hyper-V-Switch, der Ihnen die Möglichkeit bietet, virtuelle Computer (VMS) mit Netzwerken zu verbinden, die sich außerhalb des Hyper-V-Hosts befinden, einschließlich Intranet und Internet der Organisation.

Sie können auch eine Verbindung mit virtuellen Netzwerken auf dem Server herstellen, auf dem Hyper-V ausgeführt wird, wenn Sie Software-Defined Networking (Sdn-)bereitstellen.

NOTE

Zusätzlich zu diesem Thema ist die folgende Dokumentation zum virtuellen Hyper-V-Switch verfügbar.

- [Verwalten virtueller Hyper-V-Switches](#)
- [Remotezugriff auf den direkten Speicher \(RDMA\) und Switch Embedded Teaming \(SET\)](#)
- [Cmdlets für Netzwerk Switch-Team in Windows PowerShell](#)
- [Neues in VMM 2016](#)
- [Einrichten des VMM-netzwerkfabrics](#)
- [Erstellen von Netzwerken mit VMM 2012](#)
- [Hyper-V: Konfigurieren von VLANs und VLAN-Tagging](#)
- [Hyper-V: die WFP-Erweiterung für virtuelle Switches sollte aktiviert werden, wenn Sie für Erweiterungen von Drittanbietern erforderlich ist.](#)

Weitere Informationen zu anderen Netzwerktechnologien finden Sie unter [Netzwerk in Windows Server 2016](#).

Beim virtuellen Hyper-v-Switch handelt es sich um einen softwarebasierten Schicht-2-Ethernet-Netzwerk Switch, der im Hyper-v-Manager verfügbar ist, wenn Sie die Hyper-v-Server Rolle installieren.

Der virtuelle Hyper-V-Switch umfasst Programm gesteuert verwaltete und erweiterbare Funktionen zum Verbinden virtueller Computer mit virtuellen Netzwerken und dem physischen Netzwerk. Außerdem bietet der virtuelle Hyper-V-Switch Richtlinien erzwingung für Sicherheits-, Isolations- und Dienststufen.

NOTE

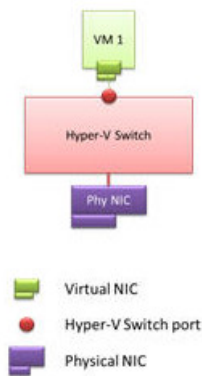
Der virtuelle Hyper-V-Switch unterstützt nur Ethernet und keine anderen drahtgebundenen lokalen Netzwerk (LAN)-Technologien, wie z. B. Infiniband und Fibre Channel.

Der virtuelle Hyper-V-Switch umfasst Mandanten Isolations Funktionen, Datenverkehrs Strukturierung, Schutz vor böswilligen virtuellen Computern und vereinfachte Problembehandlung.

Mit der integrierten Unterstützung für die netzwerkgeräteschnittstellen Spezifikation (NDIS) Filtertreiber und Windows-Filter Plattform (WFP) Legenden-Treiber ermöglicht der virtuelle Hyper-V-Switch unabhängigen Softwareanbietern (ISVs), erweiterbare Plug-ins zu erstellen, die als Erweiterungen für virtuelle Switches bezeichnet werden, die erweiterte Netzwerk- und Sicherheitsfunktionen bieten können. Erweiterungen für virtuelle Switches, die Sie dem virtuellen Hyper-V-Switch hinzufügen, werden im Manager für virtuelle Switches des Hyper-V-Managers angezeigt.

In der folgenden Abbildung verfügt ein virtueller Computer über eine virtuelle NIC, die über einen Switchport mit

dem virtuellen Hyper-V-Switch verbunden ist.



Die Funktionen des virtuellen Hyper-V-Switches bieten Ihnen weitere Optionen zum Erzwingen der Isolation von Mandanten, zum Strukturieren und Steuern von Netzwerk Datenverkehr und zum Anwenden von Schutzmaßnahmen gegen schädliche virtuelle Computer.

NOTE

In Windows Server 2016 zeigt ein virtueller Computer mit einer virtuellen NIC genau den maximalen Durchsatz für die virtuelle NIC an. Klicken Sie zum Anzeigen der Geschwindigkeit der virtuellen NIC unter **Netzwerkverbindungen** mit der rechten Maustaste auf das gewünschte virtuelle NIC-Symbol, und klicken Sie dann auf **Status**. Das Dialogfeld **Status** der virtuellen NIC wird geöffnet. In **Verbindung** entspricht der Wert der **Geschwindigkeit** der Geschwindigkeit der physischen NIC, die auf dem Server installiert ist.

Verwendung für virtuellen Hyper-V-Switch

Im folgenden finden Sie einige Anwendungsszenarien für den virtuellen Hyper-V-Switch.

Anzeigen von Statistiken: ein Entwickler bei einem gehosteten cloudhersteller implementiert ein Verwaltungspaket, in dem der aktuelle Status des virtuellen Hyper-V-Switches angezeigt wird. Das Verwaltungspaket kann aktuelle Funktionen, Konfigurationseinstellungen und individuelle Portnetzwerkstatistiken mit WMI für den gesamten Switch abfragen. Der Status des Switches wird dann angezeigt, um Administratoren eine kurze Übersicht über den Switch zu geben.

Ressourcen Nachverfolgung: ein Hostingunternehmen verkauft Hostingdienste, die auf der Ebene der Mitgliedschaft abgerechnet werden. Die verschiedenen Mitgliedschaftsebenen umfassen unterschiedliche Netzwerkeleistungsebenen. Der Administrator ordnet die Ressourcen so zu, dass die Netzwerkverfügbarkeit entsprechend den Anforderungen der SLAs gleichmäßig verteilt ist. Der Administrator verfolgt Informationen wie die aktuelle Nutzung der zugewiesenen Bandbreite und die Anzahl zugewiesener VM-Warteschlangen (Virtual Machine Queue, VMQ) oder IOV-Kanäle Programm gesteuert. Dasselbe Programm protokolliert außerdem in regelmäßigen Abständen die verwendeten Ressourcen zusätzlich zu den zugewiesenen Ressourcen pro virtuellem Computer, sodass die Ressourceneinträge doppelt erfasst werden.

Verwalten der Reihenfolge von switcherweiterungen: ein Unternehmen hat Erweiterungen auf seinem Hyper-V-Host installiert, um den Datenverkehr zu überwachen und die Angriffs Erkennung zu melden. Während der Wartung werden möglicherweise einige Erweiterungen aktualisiert, was zu Änderungen in der Reihenfolge der Erweiterungen führt. Ein einfaches Skriptprogramm wird ausgeführt, um die Erweiterungen nach einer Aktualisierung wieder zu ordnen.

Weiterleitungs Erweiterung verwaltet VLAN-ID: ein Haupt switchunternehmen baut eine Weiterleitungs Erweiterung auf, die alle Richtlinien für das Netzwerk anwendet. Ein verwaltetes Element sind IDs für virtuelle lokale Netzwerke (Virtual Local Area Network, VLAN). Der virtuelle Switch übergibt die Kontrolle des VLAN an eine Weiterleitungserweiterung. Die Installation des switchunternehmens ruft Programm gesteuert eine-API (Windows-Verwaltungsinstrumentation (WMI)-Anwendungsprogrammierschnittstelle (Application Programming

Interface, API) auf, die die Transparenz übernimmt und den virtuellen Hyper-V-Switch anteilt, die VLAN-Tags zu übergeben und keine Aktionen auszuführen.

Funktionalität des virtuellen Hyper-V-Switches

Einige der Prinzipalfeatures, die der Hyper-V-Switch umfasst, sind:

- **ARP/ND-Vergiftung (Spoofing)** : bietet Schutz vor böswilligen virtuellen Computern, die das Adressauflösungsprotokoll (ARP) Spoofing verwenden, um IP-Adressen von anderen virtuellen Computern zu stehlen. Bietet Schutz vor Angriffen, die per Nachbarermittlungs-Spoofing (Neighbor Discovery, ND) für IPv6 gestartet werden können.
- **DHCP Guard-Schutz**: schützt vor einem schädlichen virtuellen Computer, der sich als DHCP-Server (Dynamic Host Configuration-Protokoll) für man-in-the-Middle-Angriffe darstellt.
- **Port-ACLs**: ermöglicht das Filtern von Datenverkehr auf der Grundlage von Medien Access Control (Mac) oder IP-Adressen/-Bereichen (Internet Protocol), sodass Sie die Isolation virtueller Netzwerke einrichten können.
- **Trunk Modus zu VM**: ermöglicht Administratoren die Einrichtung eines bestimmten virtuellen Computers als virtuelles Gerät und die anschließende Weiterleitung von Datenverkehr von verschiedenen VLANs an den virtuellen Computer.
- **Überwachung des Netzwerk Datenverkehrs**: ermöglicht Administratoren das Überprüfen von Datenverkehr, der den Netzwerk Switch durchläuft.
- **Isoliertes (privates) VLAN**: ermöglicht Administratoren das Aufteilen von Datenverkehr auf mehrere VLANs, um die Einrichtung isolierter Mandanten Communities zu vereinfachen.

Im Folgenden finden Sie eine Liste der Funktionen, die die Verwendbarkeit des virtuellen Hyper-V-Switches verbessern:

- **Bandbreitenbeschränkung und Burst Unterstützung**: die Mindestbandbreite garantiert die reservierte Bandbreite. Die maximale Bandbreite begrenzt die Bandbreite, die ein virtueller Computer belegen kann.
- **Unterstützung von expliziten Überlastungs Benachrichtigungen (ECN)** : ECN-Kennzeichnung, auch bekannt als Data center tcp (dctcp), ermöglicht dem physischen Switch und dem Betriebssystem, den Daten Verkehrsfluss so zu regulieren, dass die Puffer Ressourcen des Switches nicht überflutet werden. Dies führt zu einem höheren Durchsatz beim Datenverkehr.
- **Diagnose**: die Diagnose ermöglicht die einfache Ablauf Verfolgung und Überwachung von Ereignissen und Paketen über den virtuellen Switch.

Remote Zugriff auf den direkten Speicher (RDMA-) und (Set-Switch Embedded Teaming)

27.03.2020 • 29 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zum Konfigurieren des Remote Zugriffs auf den direkten Speicher (RDMA-) Schnittstellen mit Hyper-V in Windows Server 2016 sowie Informationen zum Switch Embedded Teaming (Set).

NOTE

Zusätzlich zu diesem Thema ist der Inhalt des folgenden Switch Embedded-Teaming verfügbar.

- TechNet-Katalog Download: [Windows Server 2016 NIC und Switch Embedded Teaming-Benutzerhandbuch](#)

Konfigurieren von RDMA-Schnittstellen mit Hyper-V

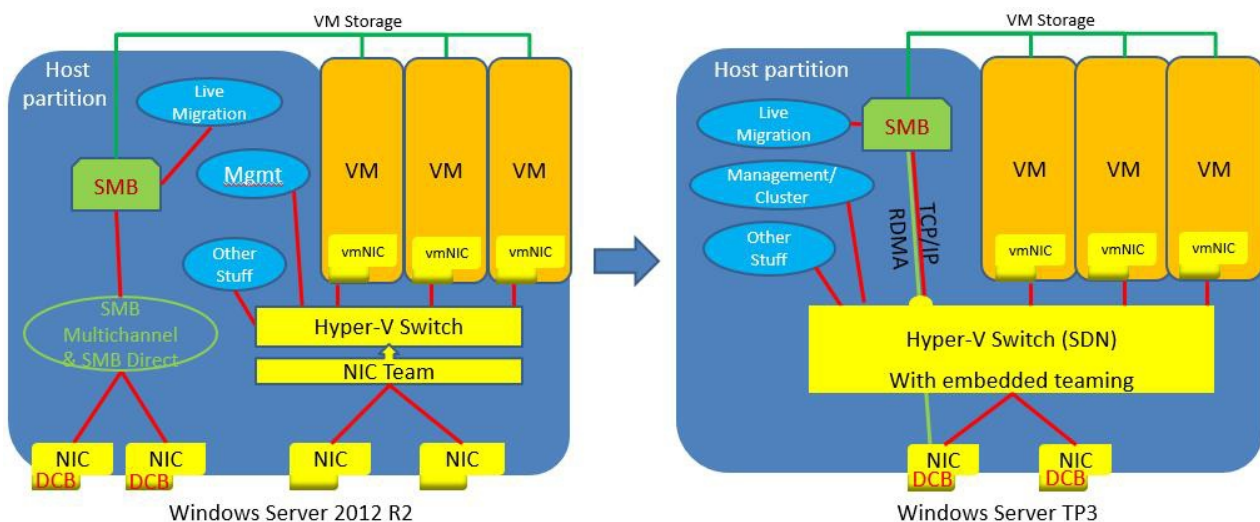
In Windows Server 2012 R2 kann die Verwendung von RDMA und Hyper-V auf demselben Computer wie die Netzwerkkartenerweiterung, die RDMA-Dienste bereitstellen, nicht an einen virtuellen Hyper-V-Switch gebunden werden. Dadurch erhöht sich die Anzahl der physischen Netzwerkkartenerweiterungen, die auf dem Hyper-V-Host installiert werden müssen.

TIP

In Editionen von Windows Server vor Windows Server 2016 ist es nicht möglich, RDMA auf Netzwerkkartenerweiterungen zu konfigurieren, die an ein NIC-Team oder einen virtuellen Hyper-V-Switch gebunden sind. In Windows Server 2016 können Sie RDMA auf Netzwerkkartenerweiterungen aktivieren, die an einen virtuellen Hyper-V-Switch mit oder ohne festgelegt sind.

In Windows Server 2016 können Sie bei Verwendung von RDMA mit oder ohne Festlegung weniger Netzwerkkartenerweiterungen verwenden.

Die folgende Abbildung veranschaulicht die Softwarearchitektur Änderungen zwischen Windows Server 2012 R2 und Windows Server 2016.



Die folgenden Abschnitte enthalten Anweisungen zur Verwendung von Windows PowerShell-Befehlen zum

Aktivieren von Data Center Bridging (DCB), zum Erstellen eines virtuellen Hyper-v-Switches mit einer virtuellen RDMA-NIC (vNIC-)und zum Erstellen eines virtuellen Hyper-v-Switches mit Set-und RDMA-vNICs.

Aktivieren von Data Center Bridging (DCB)

Vor der Verwendung von RDMA-über konvergiertem Ethernet (ROCE) RDMA-Version muss DCB aktiviert werden. Obwohl es für den Internet weiten RDMA-Protokoll (IWarp)-Netzwerken nicht erforderlich ist, wurde durch Tests festgestellt, dass alle Ethernet-basierten RDMA-Technologien mit DCB besser funktionieren. Aus diesem Grund sollten Sie DCB auch für IWarp RDMA-bereit Stellungen verwenden.

Die folgenden Windows PowerShell-Beispiel Befehle veranschaulichen, wie Sie DCB für SMB Direct aktivieren und konfigurieren.

Aktivieren von DCB

```
Install-WindowsFeature Data-Center-Bridging
```

Legen Sie eine Richtlinie für SMB-Direct fest:

```
New-NetQosPolicy "SMB" -NetDirectPortMatchCondition 445 -PriorityValue8021Action 3
```

Aktivieren der Fluss Steuerung für SMB:

```
Enable-NetQosFlowControl -Priority 3
```

Stellen Sie sicher, dass die Fluss Steuerung für anderen Datenverkehr deaktiviert ist:

```
Disable-NetQosFlowControl -Priority 0,1,2,4,5,6,7
```

Anwenden der Richtlinie auf die Ziel Adapter:

```
Enable-NetAdapterQos -Name "SLOT 2"
```

Verschaffen Sie sich eine minimale Bandbreite von SMB Direct:

```
New-NetQosTrafficClass "SMB" -Priority 3 -BandwidthPercentage 30 -Algorithm ETS
```

Wenn Sie einen Kernel Debugger im System installiert haben, müssen Sie den Debugger so konfigurieren, dass QoS durch Ausführen des folgenden Befehls festgelegt werden kann.

Überschreiben des Debuggers: standardmäßig blockiert der Debugger NetQoS:

```
Set-ItemProperty HKLM:"\SYSTEM\CurrentControlSet\Services\NDIS\Parameters" AllowFlowControlUnderDebugger -type DWORD -Value 1 -Force
```

Erstellen eines virtuellen Hyper-V-Switches mit einer RDMA-vNIC

Wenn für die Bereitstellung nicht festgelegt ist, können Sie die folgenden Windows PowerShell-Befehle verwenden, um einen virtuellen Hyper-V-Switch mit einer RDMA-vNIC zu erstellen.

NOTE

Die Verwendung von Set Teams mit RDMA-fähigen physischen NICs bietet weitere RDMA-Ressourcen, die von den vNICs genutzt werden können.

```
New-VMSwitch -Name RDMSwitch -NetAdapterName "SLOT 2"
```

Fügen Sie Host-vNICs hinzu, und machen Sie Sie RDMA-fähig:

```
Add-VMNetworkAdapter -SwitchName RDMSwitch -Name SMB_1  
Enable-NetAdapterRDMA "vEthernet (SMB_1)" "SLOT 2"
```

Überprüfen Sie RDMA-Funktionen:

```
Get-NetAdapterRdma
```

Erstellen eines virtuellen Hyper-V-Switches mit Set- und RDMA-vNICs

Zum Verwenden von RDMA-Unterstützung auf virtuellen Hyper-v-Host Netzwerkadaptern (vNICs) auf einem virtuellen Hyper-v-Switch, der RDMA-Teaming unterstützt, können Sie diese Windows PowerShell-Beispiel Befehle verwenden.

```
New-VMSwitch -Name SETswitch -NetAdapterName "SLOT 2","SLOT 3" -EnableEmbeddedTeaming $true
```

Host-vNICs hinzufügen:

```
Add-VMNetworkAdapter -SwitchName SETswitch -Name SMB_1 -managementOS  
Add-VMNetworkAdapter -SwitchName SETswitch -Name SMB_2 -managementOS
```

Viele Switches übergeben keine Informationen zur Datenverkehrs Klasse für nicht markierten VLAN-Datenverkehr. Stellen Sie daher sicher, dass sich die Host Adapter für RDMA auf VLANs befinden. In diesem Beispiel werden die beiden virtuellen SMB_*-Host Adapter VLAN 42 zugewiesen.

```
Set-VMNetworkAdapterIsolation -ManagementOS -VMNetworkAdapterName SMB_1 -IsolationMode VLAN -  
DefaultIsolationID 42  
Set-VMNetworkAdapterIsolation -ManagementOS -VMNetworkAdapterName SMB_2 -IsolationMode VLAN -  
DefaultIsolationID 42
```

Aktivieren Sie RDMA auf Host-vNICs:

```
Enable-NetAdapterRDMA "vEthernet (SMB_1)","vEthernet (SMB_2)" "SLOT 2", "SLOT 3"
```

RDMA-Funktionen überprüfen; Stellen Sie sicher, dass die Funktionen ungleich NULL sind:

```
Get-NetAdapterRdma | fl *
```

Eingebetteten Teaming wechseln (Set)

Dieser Abschnitt bietet eine Übersicht über Switch Embedded Teaming (Set) in Windows Server 2016 und enthält

die folgenden Abschnitte.

- [Übersicht festlegen](#)
- [Festlegen der Verfügbarkeit](#)
- [Unterstützte und nicht unterstützte NICs für Set](#)
- [Festlegen der Kompatibilität mit Windows Server-Netzwerktechnologien](#)
- [Festlegen von Modi und Einstellungen](#)
- [Set- und Virtual Machine-Warteschlangen \(vmqs\)](#)
- [Set und Hyper-v-Netzwerkvirtualisierung \(HNV\)](#)
- [Festlegen und Livemigration](#)
- [Mac-Adress Verwendung für übertragene Pakete](#)
- [Verwalten eines Set-Teams](#)

Übersicht festlegen

Set ist eine Alternative NIC-Team Vorgangs Lösung, die Sie in Umgebungen mit Hyper-V und dem Software-Defined Networking (Sdn) Stack in Windows Server 2016 verwenden können. Set integriert einige NIC-Team Vorgangs Funktionen in den virtuellen Hyper-V-Switch.

Mit Set können Sie zwischen einem und acht physischen Ethernet-Netzwerkadaptern in einem oder mehreren softwarebasierten virtuellen Netzwerkadaptern gruppieren. Diese virtuellen Netzwerkadapter bieten schnelle Leistung und Fehlertoleranz bei Ausfall eines Netzwerkadapters.

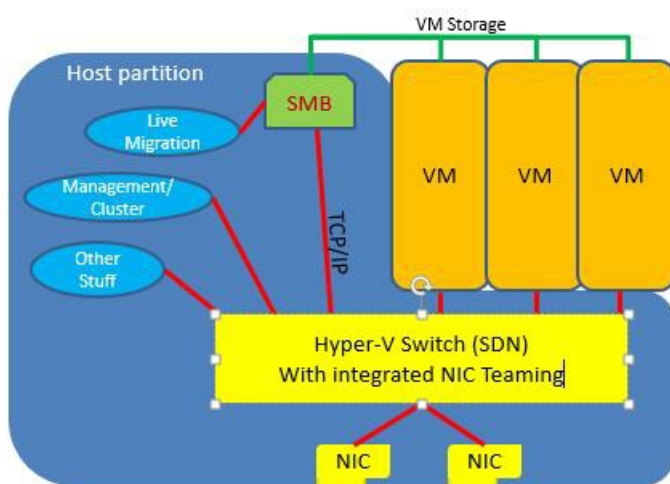
Alle Netzwerkadapter für Mitglieder müssen auf demselben physischen Hyper-V-Host installiert sein, damit Sie in einem Team platziert werden können.

NOTE

Die Verwendung von Set wird nur in einem virtuellen Hyper-V-Switch in Windows Server 2016 unterstützt. In Windows Server 2012 R2 kann Set nicht bereitgestellt werden.

Sie können Ihre Team eigenen NICs mit dem gleichen physischen Switch oder mit unterschiedlichen physischen Switches verbinden. Wenn Sie NICs mit verschiedenen Switches verbinden, müssen sich beide Switches im gleichen Subnetz befinden.

In der folgenden Abbildung wird die festgelegte Architektur dargestellt.



Da Set in den virtuellen Hyper-V-Switch integriert ist, können Sie Set nicht innerhalb eines virtuellen Computers (Virtual Machine, VM) verwenden. Sie können jedoch den NIC-Team Vorgang innerhalb von VMS verwenden.

Weitere Informationen finden Sie unter NIC-Team Vorgang [in Virtual Machines \(VMS\)](#).

Außerdem werden von der Set-Architektur keine Team Schnittstellen verfügbar gemacht. Stattdessen müssen Sie virtuelle Hyper-V-Switchports konfigurieren.

Festlegen der Verfügbarkeit

Set ist in allen Versionen von Windows Server 2016 verfügbar, die Hyper-V und den Sdn-Stapel enthalten. Außerdem können Sie Windows PowerShell-Befehle und Remotedesktop Verbindungen verwenden, um die Gruppe von Remote Computern aus zu verwalten, auf denen ein Client Betriebssystem ausgeführt wird, auf dem die Tools unterstützt werden.

Unterstützte NICs für Set

Sie können eine beliebige Ethernet-NIC verwenden, die die Windows-Hardware Qualifizierung und das Logo (WHQL) Test in einem Set-Team in Windows Server 2016 übermittelt hat. Set erfordert, dass alle Netzwerkadapter, die Mitglieder eines Set-Teams sind, identisch sein müssen (d. h., derselbe Hersteller, dasselbe Modell, dieselbe Firmware und dieser Treiber). Legen Sie Unterstützung zwischen einem und acht Netzwerkadaptern in einem Team fest.

Festlegen der Kompatibilität mit Windows Server-Netzwerktechnologien

Set ist kompatibel mit den folgenden Netzwerktechnologien in Windows Server 2016.

- Datacenter Bridging (DCB)
- Hyper-V-Netzwerkvirtualisierung-NV-GRE und vxlan werden in Windows Server 2016 unterstützt.
- Die Empfangs seitige Prüfsumme verlagert (IPv4-, IPv6-und TCP-). Diese werden unterstützt, wenn Sie von einem der Teammitglieder unterstützt werden.
- Remote Zugriff auf den direkten Speicher (RDMA-)
- Single-root-e/a-Virtualisierung (SR-IOV)
- Die Übertragungs seitige Prüfsumme verlagert (IPv4-, IPv6-und TCP-). Diese werden unterstützt, wenn alle Teammitglieder Sie unterstützen.
- Warteschlangen für virtuelle Computer (VMQ-)
- Virtuelle Empfangs seitige Skalierung (RSS-)

Set ist nicht kompatibel mit den folgenden Netzwerktechnologien in Windows Server 2016.

- 802.1 x-Authentifizierung. Das 802.1 x Extensible Authentication-Protokoll (EAP-) Pakete werden automatisch durch den virtuellen Hyper-V-Switch in festgelegten Szenarien gelöscht.
- IPSec-Task Offload (ipsecto). Dies ist eine Legacy Technologie, die von den meisten Netzwerkadaptern nicht unterstützt wird und wo Sie vorhanden ist. Sie ist standardmäßig deaktiviert.
- Verwenden von QoS (Pacer. exe) auf Host-oder nativen Betriebssystemen. Diese QoS-Szenarien sind keine Hyper-V-Szenarien, sodass sich die Technologien nicht überschneiden. Außerdem ist QoS verfügbar, aber nicht standardmäßig aktiviert. Sie müssen QoS absichtlich aktivieren.
- Empfangs seitige zusammen Fügung (RSC). RSC wird automatisch durch den virtuellen Hyper-V-Switch

deaktiviert.

- Empfangs seitige Skalierung (RSS-). Da Hyper-V die Warteschlangen für VMQ und vmmq verwendet, wird RSS immer deaktiviert, wenn Sie einen virtuellen Switch erstellen.
- TCP-Chimney-Abladung. Diese Technologie ist standardmäßig deaktiviert.
- QoS für virtuelle Computer (VM-QoS-). VM-QoS ist verfügbar, aber standardmäßig deaktiviert. Wenn Sie VM-QoS in einer festgelegten Umgebung konfigurieren, führen die QoS-Einstellungen zu unvorhersehbaren Ergebnissen.

Festlegen von Modi und Einstellungen

Anders als beim NIC-Team Vorgang können Sie einen Teamnamen nicht konfigurieren, wenn Sie ein Set-Team erstellen. Außerdem wird die Verwendung eines Standby-Adapters beim NIC-Team Vorgang unterstützt, wird jedoch in Set nicht unterstützt. Wenn Sie Set bereitstellen, sind alle Netzwerkadapter aktiv und keine im Standbymodus.

Ein weiterer wichtiger Unterschied zwischen dem NIC-Team Vorgang und der Festlegung besteht darin, dass der NIC-Team Vorgang die Auswahl von drei verschiedenen Team Vorgang-Modi ermöglicht, während Set unterstützt nur **Switch Independent** Mode Mit dem Schalter unabhängigen Modus sind die Schalter oder Switches, mit denen die Teammitglieder der Gruppe verbunden sind, nicht mit dem vorhanden sein des Set-Teams in Kenntnis, und es wird nicht festgelegt, wie Netzwerk Datenverkehr an Teammitglieder verteilt wird. stattdessen verteilt das Set-Team eingehende Netzwerke. Datenverkehr über die Gruppe der Teammitglieder.

Wenn Sie ein neues Set-Team erstellen, müssen Sie die folgenden Team Eigenschaften konfigurieren.

- Mitglieds Adapter
- Lasten Ausgleichs Modus

Mitglieds Adapter

Wenn Sie ein Set-Team erstellen, müssen Sie bis zu acht identische Netzwerkadapter angeben, die an den virtuellen Hyper-V-Switch als festgelegte Teammitglieds Adapter gebunden sind.

Lasten Ausgleichs Modus

Die Optionen für den Verteilungsmodus "Team Lastenausgleich festlegen" sind **Hyper-V-Port** und **dynamisch**.

Hyper-V-Port

VMS sind mit einem Port auf dem virtuellen Hyper-V-Switch verbunden. Bei Verwendung des Hyper-v-Port Modus für Set-Teams werden der virtuelle Hyper-v-Switchport und die zugehörige Mac-Adresse verwendet, um den Netzwerk Datenverkehr zwischen den Teammitgliedern festzulegen.

NOTE

Wenn Sie Set in Verbindung mit Packet Direct verwenden, ist der Team Vorgangs Modus **unabhängig** , und der **Hyper-V-Port** des Lasten Ausgleichs Modus ist erforderlich.

Da der angrenzende Switch immer eine bestimmte MAC-Adresse an einem bestimmten Port sieht, verteilt der Switch die Eingangs Last (den Datenverkehr vom Switch an den Host) an den Port, auf dem sich die Mac-Adresse befindet. Dies ist besonders nützlich, wenn virtuelle Computer Warteschlangen (vmqs) verwendet werden, da eine Warteschlange auf der jeweiligen NIC platziert werden kann, an der der Datenverkehr erwartet wird.

Wenn der Host jedoch nur über wenige VMS verfügt, ist dieser Modus möglicherweise nicht genau genug, um eine ausgewogene Verteilung zu erzielen. In diesem Modus wird außerdem immer eine einzelne VM (d. h. der Datenverkehr von einem einzelnen Switchport) auf die Bandbreite beschränkt, die auf einer einzelnen Schnittstelle

verfügbar ist.

Schem

Dieser Lasten Ausgleichs Modus bietet die folgenden Vorteile:

- Ausgehende Lasten werden basierend auf einem Hash der TCP-Ports und IP-Adressen verteilt. Der dynamische Modus gleicht Ladevorgänge auch in Echtzeit neu aus, sodass ein angegebener ausgehender Flow zwischen den festgelegten Teammitgliedern hin und her verschoben werden kann.
- Eingehende Lasten werden auf die gleiche Weise verteilt wie der Hyper-V-portmodus.

Die ausgehenden Lasten in diesem Modus werden basierend auf dem Konzept der flowlets dynamisch ausgeglichen. Ebenso wie bei der menschlichen Sprache an den Enden von Wörtern und Sätzen natürliche Unterbrechungen auftreten, sind TCP-Flows (TCP-Kommunikationsstreams) natürlich auch Unterbrechungen aufgetreten. Der Teil eines TCP-Flows zwischen zwei Unterbrechungen wird als flowlet bezeichnet.

Wenn der Algorithmus für den dynamischen Modus erkennt, dass eine flowlet-Grenze gefunden wurde (z. b. wenn im TCP-Datenfluss eine Unterbrechung der Länge aufgetreten ist), gleicht der Algorithmus den Flow automatisch an ein anderes Teammitglied aus, falls dies erforderlich ist. In einigen seltenen Fällen kann es vorkommen, dass der Algorithmus regelmäßig auch Flows umschließt, die keine flowlets enthalten. Aus diesem Grund kann sich die Affinität zwischen TCP-Fluss und Teammitglied jederzeit ändern, da der dynamische Ausgleichs Algorithmus funktioniert, um die Arbeitsauslastung der Teammitglieder auszugleichen.

Set-und Virtual Machine-Warteschlangen (vmqs)

VMQ und legen eine gute Zusammenarbeit fest. Sie sollten VMQ immer dann aktivieren, wenn Sie Hyper-V verwenden und festlegen.

NOTE

Set zeigt immer die Gesamtzahl der Warteschlangen an, die für alle festgelegten Teammitglieder verfügbar sind. Beim NIC-Team Vorgang wird dies als Sum-of-Queues-Modus bezeichnet.

Die meisten Netzwerkadapter verfügen über Warteschlangen, die für die Empfangs seitige Skalierung (RSS) oder VMQ verwendet werden können, aber nicht beide gleichzeitig.

Einige VMQ-Einstellungen scheinen Einstellungen für RSS-Warteschlangen zu sein, sind aber tatsächlich Einstellungen in den generischen Warteschlangen, die sowohl von RSS als auch von VMQ abhängig davon verwendet werden, welches Feature aktuell verwendet wird. Jede NIC verfügt in ihren erweiterten Eigenschaften über Werte für `*RssBaseProcNumber` und `*MaxRssProcessors`.

Im folgenden finden Sie einige VMQ-Einstellungen, die eine bessere Systemleistung bereitstellen.

- Im Idealfall sollte für jede NIC die `*RssBaseProcNumber` auf eine gerade Zahl größer oder gleich zwei (2) festgelegt werden. Dies liegt daran, dass der erste physische Prozessor, Core 0 (logischen Prozessoren 0 und 1), in der Regel den größten Teil der Systemverarbeitung übernimmt, sodass die Netzwerk Verarbeitung von diesem physischen Prozessor entfernt werden sollte.

NOTE

Einige Computerarchitekturen haben nicht zwei logische Prozessoren pro physischem Prozessor, sodass der Basis Prozessor für solche Computer größer oder gleich 1 sein sollte. Nehmen Sie im Zweifelsfall an, dass der Host einen 2 logischen Prozessor pro physischer Prozessorarchitektur verwendet.

- Die Prozessoren der Teammitglieder sollten so groß sein, dass Sie praktisch und nicht überlappen.

Beispielsweise können Sie in einem 4-Kern-Host (8 logische Prozessoren) mit einem Team von 2 10 Gbit/s-NICs festlegen, dass der erste Wert den Basis Prozessor 2 verwendet und vier Kerne verwendet werden sollen. der zweite Wert wird so festgelegt, dass er den Basis Prozessor 6 verwendet und 2 Kerne verwendet.

Set und Hyper-v-Netzwerkvirtualisierung (HNV)

Der Satz ist vollständig kompatibel mit der Hyper-V-Netzwerkvirtualisierung in Windows Server 2016. Das HNV-Verwaltungssystem stellt Informationen für den Set-Treiber bereit, mit dem die Verteilung des Netzwerk Datenverkehrs auf eine Weise ermöglicht wird, die für den HNV-Datenverkehr optimiert ist.

Festlegen und Livemigration

Livemigration wird in Windows Server 2016 unterstützt.

Mac-Adress Verwendung für übertragene Pakete

Wenn Sie ein Set-Team mit dynamischer Lastenverteilung konfigurieren, werden die Pakete aus einer einzelnen Quelle (z. b. eine einzelne VM-) gleichzeitig auf mehrere Teammitglieder verteilt.

Um zu verhindern, dass die Switches verwirrt werden, und um Mac-Fluktuation-Alarme zu verhindern, wird durch Set die MAC-Quelladresse durch eine andere Mac-Adresse in den Frames ersetzt, die auf andere Teammitglieder als das affinisierte Teammitglied übertragen werden. Aus diesem Grund verwendet jedes Teammitglied eine andere Mac-Adresse, und Mac-Adresskonflikte werden verhindert, wenn ein Fehler auftritt.

Wenn ein Fehler auf der primären NIC erkannt wird, beginnt die festgelegte Team Vorgang-Software mit der Mac-Adresse des virtuellen Computers auf dem Teammitglied, das als temporäres affinisiertes Teammitglied fungieren soll (d. h. dem, das nun als Schnittstelle des virtuellen Computers) angezeigt wird.

Diese Änderung gilt nur für Datenverkehr, der über die zugehörige Mac-Adresse des virtuellen Computers mit der eigenen Mac-Adresse des virtuellen Computers an die zugehörige Mac-Adresse der VM gesendet wird. Der andere Datenverkehr wird weiterhin mit der Quell-MAC-Adresse gesendet, die vor dem Auftreten des Fehlers verwendet wurde.

Im folgenden finden Sie Listen, die das Austausch Verhalten von Mac-Adressen festlegen, basierend auf der Konfiguration des Teams:

- Im Wechsel unabhängigen Modus mit der Hyper-V-Port Verteilung
 - Jeder VMSwitch-Port ist einem Teammitglied zugeordnet.
 - Jedes Paket wird an das Teammitglied gesendet, dem der Port zugeordnet ist.
 - Keine Quell-Mac-Ersetzung durchgeführt
- Im Wechsel unabhängigen Modus mit dynamischer Verteilung
 - Jeder VMSwitch-Port ist einem Teammitglied zugeordnet.
 - Alle ARP/NS-Pakete werden an das Teammitglied gesendet, dem der Port zugeordnet ist.
 - Für Pakete, die für das Teammitglied gesendet werden, dem das affinisierte Teammitglied angehört, ist keine Quell-MAC-Adressen Ersetzung abgeschlossen
 - Für Pakete, die für ein anderes Teammitglied als das affinisierte Teammitglied gesendet werden, wird die Mac-Adresse der Quelle abgeschlossen.

Verwalten eines Set-Teams

Es wird empfohlen, dass Sie System Center Virtual Machine Manager (VMM-) verwenden, um Set-Teams zu

verwalten. Sie können jedoch auch Windows PowerShell verwenden, um die Gruppe zu verwalten. In den folgenden Abschnitten werden die Windows PowerShell-Befehle bereitgestellt, die Sie zum Verwalten von Set verwenden können.

Informationen zum Erstellen eines Set-Teams mithilfe von VMM finden Sie im Abschnitt "Einrichten eines logischen Switches" in der System Center VMM-Bibliothek unter [Erstellen logischer Switches](#).

Erstellen eines Set-Teams

Sie müssen ein Set-Team erstellen, wenn Sie den virtuellen Hyper-V-Switch mit dem Windows PowerShell -Befehl **New-VMSwitch** erstellen.

Wenn Sie den virtuellen Hyper-V-Switch erstellen, müssen Sie den neuen Parameter "**enableembeddedteaming**" in die Befehlssyntax einschließen. Im folgenden Beispiel wird ein Hyper-V-Switch namens **teamedvswitch** mit eingebettetem Team Vorgang und zwei anfängliche Teammitglieder erstellt.

```
New-VMSwitch -Name TeamedvSwitch -NetAdapterName "NIC 1","NIC 2" -EnableEmbeddedTeaming $true
```

Der **enableembeddedteaming** -Parameter wird von Windows PowerShell angenommen, wenn das Argument für **netadaptername** ein Array von NICs anstelle einer einzelnen NIC ist. Daher können Sie den vorherigen Befehl folgendermaßen überarbeiten.

```
New-VMSwitch -Name TeamedvSwitch -NetAdapterName "NIC 1","NIC 2"
```

Wenn Sie einen Set-fähigen Switch mit einem einzelnen Teammitglied erstellen möchten, damit Sie ein Teammitglied zu einem späteren Zeitpunkt hinzufügen können, müssen Sie den **enableembeddteaming**-Parameter verwenden.

```
New-VMSwitch -Name TeamedvSwitch -NetAdapterName "NIC 1" -EnableEmbeddedTeaming $true
```

Hinzufügen oder Entfernen eines Set-Teammitglieds

Der Befehl **Set-vmswitchteam** schließt die Option **netadaptername** ein. Um die Teammitglieder in einem Set-Team zu ändern, geben Sie nach der Option **netadaptername** die gewünschte Liste der Teammitglieder ein. Wenn **teamedvswitch** ursprünglich mit NIC 1 und NIC 2 erstellt wurde, wird mit dem folgenden Beispiel Befehl das Teammitglied "NIC 2" gelöscht und das neue Set-Teammitglied "Nic 3" hinzugefügt.

```
Set-VMSwitchTeam -Name TeamedvSwitch -NetAdapterName "NIC 1","NIC 3"
```

Entfernen eines Set-Teams

Sie können ein Set-Team nur entfernen, indem Sie den virtuellen Hyper-V-Switch entfernen, der das Set-Team enthält. Verwenden Sie das Thema [Remove-VMSwitch](#), um zu erfahren, wie Sie den virtuellen Hyper-V-Switch entfernen. Im folgenden Beispiel wird ein virtueller Switch mit dem Namen **setvswitch** entfernt.

```
Remove-VMSwitch "SETvSwitch"
```

Ändern des Auslastungs Verteilungs Algorithmus für ein Set-Team

Das **Set-vmswitchteam** - Cmdlet verfügt über eine **loadbalancingalgorithmus** -Option. Diese Option nimmt einen von zwei möglichen Werten an: **hypervport** oder **dynamisch**. Verwenden Sie diese Option, um den Lasten Verteilungs Algorithmus für ein Switch-Embedded-Team festzulegen oder zu ändern.

Im folgenden Beispiel verwendet das **vmswitchteam** mit dem Namen **teamedvswitch** den **dynamischen** Lasten Ausgleichs Algorithmus.

```
Set-VMSwitchTeam -Name TeamedvSwitch -LoadBalancingAlgorithm Dynamic
```

Zuordnen virtueller Schnittstellen zu physischen Teammitgliedern

Set ermöglicht Ihnen das Erstellen einer Affinität zwischen einer virtuellen Schnittstelle (d.h., dem Port) des virtuellen Hyper-V-Switches und einer der physischen NICs im Team.

Wenn Sie z. B. zwei Host-vNICs für SMB-Direct erstellen, können Sie wie im Abschnitt [Erstellen eines virtuellen Hyper-V-Switches mit Set-und RDMA-vNICs](#) sicherstellen, dass die beiden vNICs verschiedene Teammitglieder verwenden.

Wenn Sie dem Skript in diesem Abschnitt hinzufügen, können Sie die folgenden Windows PowerShell-Befehle verwenden.

```
Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName SMB_1 -ManagementOS -PhysicalNetAdapterName "SLOT 2"  
Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName SMB_2 -ManagementOS -PhysicalNetAdapterName "SLOT 3"
```

Dieses Thema wird im Abschnitt 4.2.5 des [Windows Server 2016 NIC-und Switch Embedded Teaming-Benutzerhandbuchs](#) ausführlicher erläutert.

Verwalten virtueller Hyper-V-Switches

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Sie können dieses Thema verwenden, um auf den Hyper-V-Verwaltungs Inhalt für virtuelle Switches zuzugreifen.

Dieser Abschnitt enthält die folgenden Themen:

- [Konfigurieren von VLANs auf virtuellen Hyper-V-Switchports](#)
- [Erstellen von Sicherheitsrichtlinien mit erweiterten Port Access Control Listen](#)

Konfigurieren und Anzeigen von VLAN-Einstellungen für virtuelle Hyper-V-Switchports

27.03.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema finden Sie bewährte Methoden zum Konfigurieren und Anzeigen von Einstellungen für virtuelle lokale Netzwerke (VLAN) auf einem virtuellen Hyper-V-Switchport.

Wenn Sie VLAN-Einstellungen auf virtuellen Hyper-v-Switchports konfigurieren möchten, können Sie entweder Windows® Server 2016 Hyper-V-Manager oder System Center Virtual Machine Manager (VMM) verwenden.

Wenn Sie VMM verwenden, verwendet VMM den folgenden Windows PowerShell-Befehl, um den Switchport zu konfigurieren.

```
Set-VMNetworkAdapterIsolation <VM-name|-managementOS> -IsolationMode VLAN -DefaultIsolationID <vlan-value> -AllowUntaggedTraffic $True
```

Wenn Sie VMM nicht verwenden und den Switchport in Windows Server konfigurieren, können Sie die Hyper-V-Manager-Konsole oder den folgenden Windows PowerShell-Befehl verwenden.

```
Set-VMNetworkAdapterVlan <VM-name|-managementOS> -Access -VlanID <vlan-value>
```

Aufgrund dieser zwei Methoden zum Konfigurieren der VLAN-Einstellungen auf virtuellen Hyper-V-Switchports ist es möglich, dass beim Versuch, die Einstellungen für den Switchport anzuzeigen, angezeigt wird, dass die VLAN-Einstellungen nicht konfiguriert sind, auch wenn Sie konfiguriert sind.

Verwenden Sie dieselbe Methode, um Switchport-VLAN-Einstellungen zu konfigurieren und anzuzeigen.

Um sicherzustellen, dass diese Probleme nicht auftreten, müssen Sie die gleiche Methode zum Anzeigen der VLAN-Einstellungen für den Switchport verwenden, die Sie zum Konfigurieren der VLAN-Einstellungen für den Switchport verwendet haben.

Gehen Sie folgendermaßen vor, um die Port Einstellungen für den VLAN-Switch zu konfigurieren und anzuzeigen:

- Wenn Sie VMM oder den Netzwerk Controller zum Einrichten und Verwalten Ihres Netzwerks verwenden und Sie Software-Defined Networking (SDN) bereitgestellt haben, müssen Sie die **vmnetworkadapterisolation** -Cmdlets verwenden.
- Wenn Sie Windows Server 2016 Hyper-V-Manager oder Windows PowerShell-Cmdlets verwenden und keine Software-Defined Networking (SDN) bereitgestellt haben, müssen Sie die **vmnetworkadaptervlan** -Cmdlets verwenden.

Mögliche Probleme

Wenn Sie diese Richtlinien nicht befolgen, stoßen Sie möglicherweise auf die folgenden Probleme.

- In Fällen, in denen Sie Sdn bereitgestellt haben und VMM, Network Controller oder die **vmnetworkadapterisolation** -Cmdlets verwenden, um VLAN-Einstellungen auf einem virtuellen Hyper-v-Switchport zu konfigurieren: Wenn Sie den Hyper-v-Manager verwenden oder **vmnetworkadaptervlan** zum

Anzeigen der Konfigurationseinstellungen verwenden, werden die VLAN-Einstellungen in der Stattdessen müssen Sie das Cmdlet **Get-vmnetworkisolation** verwenden, um die VLAN-Einstellungen anzuzeigen.

- In Fällen, in denen Sie keinen Sdn bereitgestellt haben und stattdessen die VLAN-Einstellungen mithilfe des Hyper-v-Managers oder der **vmnetworkadaptervlan** -Cmdlets auf einem virtuellen Hyper-V-Switchport konfigurieren: Wenn Sie das **Get-vmnetworkisolation** -Cmdlet zum Anzeigen der Konfigurationseinstellungen verwenden, werden die VLAN-Einstellungen in der Befehlsausgabe Stattdessen müssen Sie das Cmdlet **Get vmnetworkadaptervlan** verwenden, um die VLAN-Einstellungen anzuzeigen.

Es ist auch wichtig, nicht zu versuchen, dieselben VLAN-Einstellungen für den Switchport mithilfe beider Konfigurations Methoden zu konfigurieren. Wenn Sie dies tun, ist der Switchport falsch konfiguriert, und das Ergebnis ist möglicherweise ein Fehler bei der Netzwerkkommunikation.

Ressourcen

Weitere Informationen zu den in diesem Thema erwähnten Windows PowerShell-Befehlen finden Sie in den folgenden Themen:

- [Set-vmnetworkadapterisolation](#)
- [Get-vmnetworkadapterisolation](#)
- [Set-vmnetworkadaptervlan](#)
- [Get-vmnetworkadaptervlan](#)

Erstellen von Sicherheitsrichtlinien mit erweiterten Port-Zugriffssteuerungslisten

09.04.2020 • 16 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zu erweiterten Port Access Control Listen (ACLs) in Windows Server 2016. Sie können erweiterte ACLs für den virtuellen Hyper-V-Switch konfigurieren, um Netzwerkdatenverkehr an die und von den virtuellen Computern (VMs), die über virtuelle Netzwerkadapter mit dem Switch verbunden sind, zuzulassen und zu blockieren.

Dieses Thema enthält folgende Abschnitte:

- [Detaillierte ACL-Regeln](#)
- [Zustands behaftete ACL-Regeln](#)

Detaillierte ACL-Regeln

Erweiterte ACLs für den virtuellen Hyper-v-Switch ermöglicht Ihnen das Erstellen detaillierter Regeln, die Sie auf einzelne VM-Netzwerkadapter anwenden können, die mit dem virtuellen Hyper-v-Switch verbunden sind. Durch die Möglichkeit, ausführliche Regeln zu erstellen, können Unternehmen und clouddienstanbieter (Cloud Service Providers, CSPs) netzwerkbasierter Sicherheitsbedrohungen in einer mehrinstanzfähigen freigegebenen Serverumgebung lösen.

Mit erweiterten ACLs müssen Sie nicht allgemeine Regeln erstellen, mit denen der gesamte Datenverkehr über alle Protokolle an einen bzw. von einem virtuellen Computer blockiert oder zugelassen wird. Stattdessen können Sie jetzt den Netzwerkdatenverkehr über einzelne auf den virtuellen Computern ausgeführte Protokolle blockieren oder zulassen. Sie können erweiterte ACL-Regeln in Windows Server 2016 erstellen, die die folgenden 5-Tupel-Parameter enthalten: Quell-IP-Adresse, Ziel-IP-Adresse, Protokoll, Quellport und Zielport. Darüber hinaus kann in jeder Regel die Richtung des Netzwerkdatenverkehrs (ein- oder ausgehend) und die von der Regel unterstützte Aktion (Blockieren oder Zulassen des Datenverkehrs) angegeben werden.

Sie können beispielsweise Port-ACLs für einen virtuellen Computer konfigurieren, um den gesamten ein- und ausgehenden HTTP- und HTTPS-Datenverkehr an Port 80 zuzulassen und gleichzeitig den Netzwerkdatenverkehr aller anderen Protokolle an allen Ports blockieren.

Durch diese Möglichkeit, den Protokolldatenverkehr festzulegen, der von virtuellen Mandantencomputern empfangen werden kann, gewinnen Sie Flexibilität beim Konfigurieren der Sicherheitsrichtlinien.

Konfigurieren von ACL-Regeln mit Windows PowerShell

Zum Konfigurieren einer erweiterten ACL müssen Sie den Windows PowerShell-Befehl **Add-VMNetworkAdapterExtendedAcl** verwenden. Dieser Befehl verfügt über vier verschiedene Syntaxen mit jeweils unterschiedlicher Verwendung:

1. Fügen Sie allen Netzwerkadaptern einer benannten VM, die durch den ersten Parameter (-VMName) angegeben wird, eine erweiterte ACL hinzu. Syntax:

NOTE

Wenn Sie einem Netzwerkadapter anstelle von "alle" eine erweiterte ACL hinzufügen möchten, können Sie den Netzwerkadapter mit dem Parameter "-vmnetworkadaptername" angeben.

```
Add-VMNetworkAdapterExtendedAcl [-VMName] <string[]> [-Action] <VMNetworkAdapterExtendedAclAction>
{Allow | Deny}
    [-Direction] <VMNetworkAdapterExtendedAclDirection> {Inbound | Outbound} [[-LocalIPAddress]
<string>]
    [[-RemoteIPAddress] <string>] [[-LocalPort] <string>] [[-RemotePort] <string>] [[-Protocol]
<string>] [-Weight]
    <int> [-Stateful <bool>] [-IdleSessionTimeout <int>] [-IsolationID <int>] [-Passthru] [-
VMNetworkAdapterName
    <string>] [-ComputerName <string[]>] [-WhatIf] [-Confirm] [<CommonParameters>]
```

2. Hinzufügen einer erweiterten ACL zu einem bestimmten virtuellen Netzwerkadapter auf einem bestimmten virtuellen Computer. Syntax:

```
Add-VMNetworkAdapterExtendedAcl [-VMNetworkAdapter] <VMNetworkAdapterBase[]> [-Action]
<VMNetworkAdapterExtendedAclAction> {Allow | Deny} [-Direction]
<VMNetworkAdapterExtendedAclDirection> {Inbound |
    Outbound} [[-LocalIPAddress] <string>] [[-RemoteIPAddress] <string>] [[-LocalPort] <string>] [[-
RemotePort]
    <string>] [[-Protocol] <string>] [-Weight] <int> [-Stateful <bool>] [-IdleSessionTimeout <int>] [-
IsolationID
    <int>] [-Passthru] [-WhatIf] [-Confirm] [<CommonParameters>]
```

3. Hinzufügen einer erweiterten ACL zu allen virtuellen Netzwerkadaptern, die für die Verwendung durch das Hyper-V-Hostverwaltungs-Betriebssystem reserviert sind.

NOTE

Wenn Sie einem Netzwerkadapter anstelle von "alle" eine erweiterte ACL hinzufügen möchten, können Sie den Netzwerkadapter mit dem Parameter "-vmnetworkadaptername" angeben.

```
Add-VMNetworkAdapterExtendedAcl [-Action] <VMNetworkAdapterExtendedAclAction> {Allow | Deny} [-
Direction]
    <VMNetworkAdapterExtendedAclDirection> {Inbound | Outbound} [[-LocalIPAddress] <string>] [[-
RemoteIPAddress]
    <string>] [[-LocalPort] <string>] [[-RemotePort] <string>] [[-Protocol] <string>] [-Weight] <int> -
ManagementOS
    [-Stateful <bool>] [-IdleSessionTimeout <int>] [-IsolationID <int>] [-Passthru] [-
VMNetworkAdapterName <string>]
    [-ComputerName <string[]>] [-WhatIf] [-Confirm] [<CommonParameters>]
```

4. Hinzufügen einer erweiterten ACL zu einem VM-Objekt, das Sie in Windows PowerShell erstellt haben, z. b. **\$VM = Get-VM "my_vm"**. In der nächsten Codezeile können Sie diesen Befehl mit der folgenden Syntax ausführen, um eine erweiterte ACL zu erstellen:

```
Add-VMNetworkAdapterExtendedAcl [-VM] <VirtualMachine[]> [-Action] <VMNetworkAdapterExtendedAclAction>
{Allow |
    Deny} [-Direction] <VMNetworkAdapterExtendedAclDirection> {Inbound | Outbound} [[-LocalIPAddress]
<string>]
    [[-RemoteIPAddress] <string>] [[-LocalPort] <string>] [[-RemotePort] <string>] [[-Protocol]
<string>] [-Weight]
    <int> [-Stateful <bool>] [-IdleSessionTimeout <int>] [-IsolationID <int>] [-Passthru] [-
VMNetworkAdapterName
    <string>] [-WhatIf] [-Confirm] [<CommonParameters>]
```

Beispiele für detaillierte ACL-Regeln

In den folgenden Beispielen wird gezeigt, wie Sie den Befehl **Add-VMNetworkAdapterExtendedAcl** zum Konfigurieren erweiterter Port-ACLs und zum Erstellen von Sicherheitsrichtlinien für virtuelle Computer verwenden können.

- [Erzwingen der Sicherheit auf Anwendungsebene](#)
- [Erzwingen der Sicherheit auf Benutzer-und Anwendungsebene](#)
- [Bereitstellen von Sicherheitsunterstützung für eine nicht-TCP/UDP-Anwendung](#)

NOTE

Die Werte für den Regelparameter **Richtung** in den folgenden Tabellen basieren auf dem Fluss des Datenverkehrs zu dem bzw. von dem virtuellen Computer, für den Sie die Regel erstellen. Wenn der virtuelle Computer Datenverkehr empfängt, handelt es sich um eingehenden Datenverkehr. Wenn vom virtuellen Computer Datenverkehr gesendet wird, handelt es sich um ausgehenden Datenverkehr. Wenn Sie beispielsweise eine Regel auf einen virtuellen Computer anwenden, mit der eingehender Datenverkehr blockiert wird, verläuft die Richtung des eingehenden Datenverkehrs von externen Ressourcen zum virtuellen Computer. Wenn Sie eine Regel anwenden, mit der ausgehender Datenverkehr blockiert wird, verläuft die Richtung des ausgehenden Datenverkehrs vom lokalen virtuellen Computer zu den externen Ressourcen.

Erzwingen der Sicherheit auf Anwendungsebene

Da von vielen Anwendungsservern für die Kommunikation mit Clientcomputern standardisierte TCP/UDP-Ports verwendet werden, können Sie leicht Regeln erstellen, mit denen der Zugriff auf einen Anwendungsserver blockiert wird, indem der Datenverkehr zu dem bzw. von dem für die Anwendung festgelegten Port gefiltert wird.

Beispielsweise können Sie einem Benutzer die Anmeldung bei einem Anwendungsserver im Datacenter über eine Remotedesktopverbindung (Remote Desktop Connection, RDP) ermöglichen. Da für RDP der TCP-Port 3389 verwendet wird, können Sie schnell die folgende Regel einrichten:

QUELL-IP	ZIEL-IP	PROTOKOLL	QUELLPORT	ZIELPORT	RICHTUNG	AKTION
*	*	TCP	*	3389	Im	Zulassen

In den beiden folgenden Beispielen wird gezeigt, wie Sie mit Windows PowerShell-Befehlen Regeln erstellen können. Die erste Beispiel Regel blockiert den gesamten Datenverkehr an den virtuellen Computer mit dem Namen "ApplicationServer". Die zweite Beispiel Regel, die auf den Netzwerkadapter des virtuellen Computers mit dem Namen "ApplicationServer" angewendet wird, ermöglicht nur eingehenden RDP-Datenverkehr an den virtuellen Computer.

NOTE

Wenn Sie Regeln erstellen, können Sie mit dem Parameter **-Weight** die Reihenfolge bestimmen, in der die Regeln vom virtuellen Hyper-V-Switch verarbeitet werden. Werte für **-Weight** werden als ganze Zahlen ausgedrückt. Regeln mit einer höheren Ganzzahl werden vor Regeln mit niedrigeren Ganzzahlen verarbeitet. Wenn Sie beispielsweise zwei Regeln auf den Netzwerkadapter eines virtuellen Computers angewendet haben (eine mit der Gewichtung 1 und eine mit der Gewichtung 10), wird die Regel mit der Gewichtung 10 zuerst angewendet.

```
Add-VMNetworkAdapterExtendedAcl -VMName "ApplicationServer" -Action "Deny" -Direction "Inbound" -Weight 1
Add-VMNetworkAdapterExtendedAcl -VMName "ApplicationServer" -Action "Allow" -Direction "Inbound" -LocalPort
3389 -Protocol "TCP" -Weight 10
```

Erzwingen der Sicherheit auf Benutzer-und Anwendungsebene

Da mit einer Regel ein 5-Tupel-IP-Paket (Quell-IP, Ziel-IP, Protokoll, Quellport und Zielport) verglichen werden kann, kann mit der Regel eine detailliertere Sicherheitsrichtlinie erzwungen werden als mit einer Port-ACL.

Wenn Sie beispielsweise einen DHCP-Dienst für eine begrenzte Anzahl von Client Computern mithilfe einer bestimmten Gruppe von DHCP-Servern bereitstellen möchten, können Sie auf dem Windows Server 2016-Computer, auf dem Hyper-V ausgeführt wird, auf dem die Benutzer-VMS gehostet werden, die folgenden Regeln konfigurieren:

QUELL-IP	ZIEL-IP	PROTOKOLL	QUELLPORT	ZIELPORT	RICHTUNG	AKTION
*	255.255.255.255	UDP	*	67	Heraus	Zulassen
*	10.175.124.0/25	UDP	*	67	Heraus	Zulassen
10.175.124.0/25	*	UDP	*	68	Im	Zulassen

In den folgenden Beispielen wird gezeigt, wie Sie diese Regeln mit Windows PowerShell-Befehlen erstellen können.

```
Add-VMNetworkAdapterExtendedAcl -VMName "ServerName" -Action "Deny" -Direction "Outbound" -Weight 1
Add-VMNetworkAdapterExtendedAcl -VMName "ServerName" -Action "Allow" -Direction "Outbound" -RemoteIPAddress
255.255.255.255 -RemotePort 67 -Protocol "UDP"-Weight 10
Add-VMNetworkAdapterExtendedAcl -VMName "ServerName" -Action "Allow" -Direction "Outbound" -RemoteIPAddress
10.175.124.0/25 -RemotePort 67 -Protocol "UDP"-Weight 20
Add-VMNetworkAdapterExtendedAcl -VMName "ServerName" -Action "Allow" -Direction "Inbound" -RemoteIPAddress
10.175.124.0/25 -RemotePort 68 -Protocol "UDP"-Weight 20
```

Bereitstellen von Sicherheitsunterstützung für eine nicht-TCP/UDP-Anwendung

Während der größte Teil des Netzwerkdatenverkehrs in einem Datacenter über TCP und UDP erfolgt, werden dennoch für einen Teil des Datenverkehrs andere Protokolle genutzt. Wenn Sie beispielsweise zulassen möchten, dass auf einer Gruppe von Servern eine IP-Multicastanwendung ausgeführt wird, die auf IGMP (Internet Group Management-Protokoll) basiert, können Sie die folgende Regel erstellen.

NOTE

Für IGMP ist die IP-Protokollnummer 0x02 festgelegt.

QUELL-IP	ZIEL-IP	PROTOKOLL	QUELLPORT	ZIELPORT	RICHTUNG	AKTION
*	*	0x02	*	*	Im	Zulassen
*	*	0x02	*	*	Heraus	Zulassen

Im folgenden Beispiel wird gezeigt, wie Sie diese Regeln mit Windows PowerShell-Befehlen erstellen können.

```
Add-VMNetworkAdapterExtendedAcl -VMName "ServerName" -Action "Allow" -Direction "Inbound" -Protocol 2 -Weight 20
Add-VMNetworkAdapterExtendedAcl -VMName "ServerName" -Action "Allow" -Direction "Outbound" -Protocol 2 -Weight 20
```

Zustands behaftete ACL-Regeln

Eine weitere neue Funktion der erweiterten ACLs ermöglicht das Konfigurieren zustandsbehafteter Regeln. Eine Zustands behaftete Regel filtert Pakete basierend auf fünf Attributen in einer Paket Quell-IP, Ziel-IP, Protokoll, Quellport und Zielport.

Zustandsbehaftete Regeln haben die folgenden Funktionen:

- Sie lassen Datenverkehr immer zu und werden nicht zum Blockieren von Datenverkehr verwendet.
- Wenn Sie für den Parameter **Direction** den Wert `"inbound"` angeben und Datenverkehr der Regel entspricht, wird vom virtuellen Hyper-V-Switch eine entsprechende Regel erstellt, mit der das Senden von ausgehendem Datenverkehr durch den virtuellen Computer als Antwort an die externe Ressource zugelassen wird.
- Wenn Sie für den Parameter **Direction** den Wert `"outbound"` angeben und Datenverkehr der Regel entspricht, wird vom virtuellen Hyper-V-Switch dynamisch eine entsprechende Regel erstellt, mit der der Empfang von eingehendem Datenverkehr von der externen Ressource auf dem virtuellen Computer zugelassen wird.
- Dazu gehört ein Timeoutattribut, das in Sekunden gemessen wird. Wenn beim Switch ein Netzwerkpaket eingeht, das einer zustandsbehafteten Regel entspricht, wird vom virtuellen Hyper-V-Switch ein Zustand erstellt, damit alle nachfolgenden Pakete in beiden Richtungen des gleichen Flusses zugelassen werden. Der Zustand läuft ab, wenn in dem durch den Timeoutwert angegebenen Zeitraum kein Datenverkehr in einer der Richtungen auftritt.

Im folgenden Beispiel wird gezeigt, wie Sie zustandsbehaftete Regeln verwenden können.

Zulassen von eingehendem Datenverkehr von einem Remoteserver nur nach einer Kontaktaufnahme durch den lokalen Server

In manchen Fällen muss eine zustandsbehaftete Regel verwendet werden, da nur mit dieser eine bekannte, hergestellte Verbindung nachverfolgt und von anderen Verbindungen unterschieden werden kann.

Wenn Sie beispielsweise zulassen möchten, dass von einem Anwendungsserver für virtuelle Computer an Port 80 Verbindungen mit Webdiensten im Internet initiiert werden und Antworten der Remotewebserver auf den Datenverkehr des virtuellen Computers möglich sein sollen, können Sie eine zustandsbehaftete Regel konfigurieren. In dieser lassen Sie anfänglichen ausgehenden Datenverkehr vom virtuellen Computer zu den Webdiensten zu. Da die Regel zustandsbehaftet ist, wird auch der Antwortdatenverkehr vom virtuellen Computer an die Webserver zugelassen. Aus Sicherheitsgründen können Sie den gesamten eingehenden Netzwerkdatenverkehr an den virtuellen Computer blockieren.

Für diese Regelkonfiguration können Sie die Einstellungen aus der folgenden Tabelle verwenden.

NOTE

Aufgrund von Formatierungseinschränkungen und der Menge der Informationen in der folgenden Tabelle werden die Informationen anders angezeigt als in den vorherigen Tabellen dieses Dokuments.

PARAMETER	REGEL 1	REGEL 2	REGEL 3
Quell-IP	*	*	*
Ziel-IP	*	*	*
Protokoll	*	*	TCP
Quellport	*	*	*
Zielport	*	*	80
Richtung	Im	Heraus	Heraus
Aktion	Verweigern	Verweigern	Zulassen
Zustandsbehaftet	Nein	Nein	Ja
Timeout (in Sekunden)	N/V	N/V	3600

Mit der zustandsbehafteten Regel wird zugelassen, dass über den Anwendungsserver für virtuelle Computer eine Verbindung mit einem Remotewebserver hergestellt wird. Wenn das erste Paket gesendet wird, werden vom virtuellen Hyper-V-Switch dynamisch zwei Flusszustände erstellt, um alle an den Remotewebserver gesendeten und von diesem zurückgesendeten Pakete zuzulassen. Wenn der Fluss der Pakete zwischen den Servern endet, tritt für die Flusszustände ein Timeout gemäß dem festgelegten Timeoutwert von 3600 Sekunden (oder einer Stunde) auf.

Im folgenden Beispiel wird gezeigt, wie Sie diese Regeln mit Windows PowerShell-Befehlen erstellen können.

```
Add-VMNetworkAdapterExtendedAcl -VMName "ApplicationServer" -Action "Deny" -Direction "Inbound" -Weight 1
Add-VMNetworkAdapterExtendedAcl -VMName "ApplicationServer" -Action "Deny" -Direction "Outbound" -Weight 1
Add-VMNetworkAdapterExtendedAcl -VMName "ApplicationServer" -Action "Allow" -Direction "Outbound" 80 "TCP" -
Weight 100 -Stateful -Timeout 3600
```