

Contents

Verwaltung

Verwenden des Windows Admin Centers zur Verwaltung der Umgebung (neu!)

Verwalten von Windows Server-Systemen und -Umgebungen

Verwalten von Windows Server Hybrid Cloud Print

Bereitstellen von Windows Server Hybrid Cloud Print

Was ist die Server Core-Installationsoption?

Was ist in der Server Core-Installationsoption enthalten?

Grundlegende Verwaltungsaufgaben in Server Core

Verwalten von Server Core

Konfigurieren von Speicherabbilddateien

Reparieren der Server Core-Installation

Verwalten von lokalen Systemen mit Server-Manager

Verwalten des lokalen Servers und der Server-Manager-Konsole

Konfigurieren der Remoteverwaltung im Server-Manager

Hinzufügen von Servern zu Server-Manager

Installieren oder Deinstallieren von Rollen, Rollendiensten oder Features

Konfigurieren von „Features bei Bedarf“ unter Windows Server

Anzeigen und Konfigurieren von Leistungs-, Ereignis- und Dienstdaten

Anzeigen von Aufgabendetails und Benachrichtigungen

Ausführen von Best Practices Analyzer-Scans und Verwalten der Scanergebnisse

Erstellen und Verwalten von Servergruppen

Filtern, Sortieren und Abfragen von Daten in Server-Manager-Kacheln

Tastenkombinationen für den Server-Manager

Verwalten von Remoteserver-Verwaltungstools für Server Core- und Remote-Systeme

Verwalten von Windows mit OpenSSH

Erste Schritte mit OpenSSH

Konfigurieren von Windows für OpenSSH

Verwalten von OpenSSH-Schlüsseln

Windows Server Update Services (WSUS) 3.0

Bereitstellen von Windows Server Update Services

Planen der WSUS-Bereitstellung

Schritt 1: Installieren Sie die WSUS-Serverrolle

Schritt 2: Konfigurieren von WSUS

Schritt 3: Genehmigen und Bereitstellen von Updates in WSUS

Schritt 4: Konfigurieren von Gruppenrichtlinien für automatische Updates

Verwalten von Updates mit Windows Server Update Services

Einrichten von Updatesynchronisierungen

Verwalten von WSUS-Clientcomputern und WSUS-Computergruppen

Anzeigen und Verwalten von Updates

WSUS und die Katalogwebsite

Vorgänge für Updates

Assistent für die Serverbereinigung

Ausführen des WSUS-Replikatmodus

WSUS-Nachrichten und Tipps zur Problembehandlung

ISV-Unterstützung für Express-Updatebereitstellung

Monatliche Delta-Update ISV-Unterstützung ohne WSUS

Migrieren der WSUS-Datenbank von der internen Windows-Datenbank (Windows Internal Database, WID) zu SQL

Sammeln von Informationen über Ihre Umgebung und Systeme

Systemdaten

Grundlegendes zu Funktionen

Verwalten von Funktionen

Hinzufügen und Entwickeln von Funktionen

Hinzufügen, Entfernen und Aktualisieren von Funktionen

Auswählen der Funktionsdatenquellen

Häufig gestellte Fragen

Ereignisse mit Ereignissammlung für Setup und Start erfassen

Sammeln von Informationen zur Software Inventory Logging (SIL)

Verwaltung der Protokollierung des Softwarebestands

Aggregator der Protokollierung des Softwarebestands

Sammeln von Informationen für Benutzer mit User Access Logging (UAL)

Verwalten der Benutzerzugriffsprotokollierung
Optimieren der Leistung Ihrer Windows Server
Richtlinien zur Leistungsoptimierung
Microsoft Server Performance Advisor
Server Performance Advisor-Benutzerhandbuch
Server Performance Advisor Pack-Entwicklungsleitfaden
Automatisieren der Windows Server-Verwaltung
Windows PowerShell-Skripting
Windows-Befehle

» 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](#).

Nachdem Sie Windows Server in Ihrer Umgebung bereitgestellt haben, einschließlich der spezifischen Rollen für die benötigten Features und Funktionen, besteht der nächste Schritt darin, diese Server zu verwalten. Windows Server enthält eine Reihe von Tools, mit denen Sie Ihre Windows Server-Umgebung besser verstehen, bestimmte Server verwalten, die Leistung optimieren und viele Verwaltungsaufgaben automatisieren können.

Die Tools, die Sie zum Verwalten von Windows Server-Instanzen verwenden, hängen in hohem Maße von den bereitgestellten Systemtypen (Windows Server mit Desktopdarstellung oder Server Core), physischen und virtuellen Computern sowie dem Standort der Server ab. Verwenden Sie die folgenden Informationen, um grundlegende Verwaltungsaufgaben unter Windows Server auszuführen.

Verwenden Sie die folgende Tabelle, um ermitteln, welche Tools wann zu verwenden sind.

ICH BIN	INSTALLIEREN UND AUSFÜHREN VON WINDOWS ADMIN CENTER	SERVER MANAGER UNTER WINDOWS SERVER AUSFÜHREN	SERVER MANAGER IN RSA1 UNTER WINDOWS 10 AUSFÜHREN
Benutzer an einem Windows 10-PC	X		X
Benutzer an einem Windows Server-System, das mit der Desktopdarstellung arbeitet	X	X	X
Benutzer an einem Windows Server-System, das mit Server Core arbeitet	X (unter Windows 10 installieren, zum Verwalten von Server Core verwenden)		X
Von meinem Windows Server-System weit entfernt	X		X
Von meinem Windows Server-System, das mit der Desktopdarstellung arbeitet, weit entfernt	X	Verwendung von RDS für die Remoteverbindung mit dem Server, dann Verwendung von Server-Manager	X

Zusätzlich zu den unten aufgeführten Tools können Sie auch [Remotedesktopdienste](#) für den Zugriff auf lokale, remote und virtuelle Server verwenden. Dann können Sie mit Server-Manager Verwaltungsaufgaben ausführen.

Verwalten von Windows Server-Systemen und -Umgebungen

Verwalten von lokalen Systemen, Remotesystemen und Systemen ohne Benutzeroberfläche mit Windows Admin Center

Eine browserbasierte Verwaltungs-App, die lokale Verwaltung von Windows-Servers ohne Abhängigkeit von Azure oder der Cloud ermöglicht. Windows Admin Center (früher „Projekt Honolulu“ genannt) ermöglicht Ihnen die vollständige Kontrolle über alle Aspekte Ihrer Serverinfrastruktur und ist besonders nützlich für die Verwaltung in privaten Netzwerken, die nicht mit dem Internet verbunden sind. Sie können Windows Admin Center unter Windows 10, auf einem Gatewayserver oder direkt auf dem Windows Server-System installieren, das Sie verwalten möchten.

Verwalten von lokalen Systemen mit Server-Manager

Eine Verwaltungskonsole, die in der vollständigen Installation von Windows Server enthalten ist. (Es ist nicht verfügbar bei

Installationen ohne Benutzeroberfläche – in Server Core ist Server-Manager nicht enthalten). Verwenden Sie Server-Manager zum Installieren und Entfernen von Serverrollen, Hinzufügen und Entfernen von Remoteservern, Starten und Beenden von Diensten sowie zum Anzeigen von Daten, die über Ihre Umgebung gesammelt wurden.

Verwalten von Remotesystemen und Systemen ohne Benutzeroberfläche mit Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT)

Wenn Ihre Umgebung Installationen von Server Core oder Remoteservern (lokal oder virtuelle Computer) enthält, können Sie diese Systeme mithilfe von RSAT verwalten. RSAT enthält Server-Manager, sodass Sie alle Ihre Server damit verwalten können. Beachten Sie, dass RSAT unter Windows 10 ausgeführt wird. RSAT kann nicht unter Windows Server Core installiert werden. Server Core-Installationen können auch über die Befehlszeile verwaltet werden. Weitere Informationen finden Sie unter [Grundlegende Verwaltungsaufgaben in Server Core](#).

Verwalten von Updates für Windows Server-Systeme

Verwenden Sie Windows Server Update Services (WSUS) zum Verwalten und Bereitstellen von Updates für die Systeme in Ihrer Windows Server-Umgebung.

Sammeln von Informationen über Ihre Umgebung

Ereignissammlung für Setup und Start

Mit „Ereignissammlung für Setup und Start“ können Sie einen Computer zum „Sammeln“ angeben, der eine Vielzahl von wichtigen Ereignissen erfasst, die auf anderen Computern auftreten, wenn sie starten oder den Installationsvorgang durchlaufen. Die erfassten Ereignisse können Sie später mit der Ereignisanzeige, Message Analyzer, Wvtutil oder Windows PowerShell-Cmdlets analysieren.

Protokollierung des Softwarebestands (Software Inventory Logging, SIL)

Die Protokollierung des Softwarebestands in Windows Server ist ein Feature mit einer Reihe einfacher PowerShell-Cmdlets, über die Serveradministratoren eine Liste der auf Servern installierten Microsoft-Software abrufen können. Darüber hinaus bietet sie die Möglichkeit, diese Daten für die Aggregation in regelmäßigen Abständen mithilfe des HTTPS-Protokolls über das Netzwerk zu sammeln und an einen Zielwebserver weiterzuleiten. Zum Verwalten des Features – in erster Linie zum stündlichen Sammeln und Weiterleiten – werden ebenfalls PowerShell-Befehle verwendet.

Benutzerzugriffsprotokollierung (User Access Logging, UAL)

Die Benutzerzugriffsprotokollierung aggregiert eindeutige Ereignisse auf Clientgeräten sowie Benutzeranforderungsereignisse die auf einem Computer unter Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 in einer lokalen Datenbank protokolliert wurden. Diese Datensätze werden dann (über die Abfrage eines Serveradministrators) zur Verfügung gestellt, um Mengen und Instanzen nach Serverrolle, Benutzer, Gerät, lokalem Server und Datum abzurufen. Außerdem bietet UAL auch Nicht-Microsoft-Softwareentwicklern die Möglichkeit, ihre UAL-Ereignisse für die Aggregation zu instrumentieren.

Leistungsoptimierung für die Windows Server-Umgebung

Richtlinien zur Leistungsoptimierung

Überprüfen Sie eine Reihe von Richtlinien, mit denen Sie die Servereinstellungen in Windows Server optimieren und inkrementelle Leistungs- oder Energieeffizienzsteigerungen erzielen können – insbesondere, wenn sich die Art der Arbeitsauslastung im Laufe der Zeit nur wenig ändert.

Microsoft Server Performance Advisor

Mit Microsoft Server Performance Advisor (SPA) können Sie Messdaten sammeln, um Leistungsprobleme auf Windows-Servern unauffällig zu diagnostizieren, ohne Softwareagenten hinzuzufügen oder Produktionsserver neu zu konfigurieren. SPA

generiert umfassende Berichte und historische Diagramme mit Empfehlungen.

Automatisieren der Windows Server-Verwaltung

Windows PowerShell

Windows PowerShell ist eine Befehlszeilen-Shell und -Skriptsprache, die mit der Sie Verwaltungsaufgaben schnell automatisieren können.

Windows-Befehle

Die Windows-Befehlszeilertools dienen zum Ausführen von Verwaltungsaufgaben in Windows. Anhand der Befehlsreferenz können Sie sich mit den Befehlszeilertools vertraut machen, mehr über die Befehlsshell erfahren und Befehlszeilenaufgaben mithilfe von Stapeldateien oder Skripting-Tools automatisieren.

Automatisieren der Windows Server-Verwaltung

Systemdaten

Systemeigene vorhersehbare Analysen analysieren lokal Windows Server-Systemdaten wie Leistungsindikatoren und ETW-Ereignisse und helfen IT-Administratoren proaktiv, problematisches Verhalten in ihren Bereitstellungen zu erkennen und zu beheben.

Windows Admin Center

27.05.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Admin Center, Windows Admin Center-Vorschau

Windows Admin Center ist eine lokal bereitgestellte, browserbasierte App zum Verwalten von Windows-Servern, Clustern, hyperkonvergenter Infrastruktur und Windows 10-PCs. Sie ist ohne über Windows hinausgehende Kosten erhältlich und für den Einsatz in Produktionsumgebungen bereit.

Weitere Informationen zu den Neuerungen finden Sie unter [Versionsverlauf](#).

Jetzt herunterladen

Laden Sie [Windows Admin Center](#) aus dem Microsoft Evaluation Center herunter. Obwohl dort steht „Bewertung beginnen“, handelt es sich um die allgemein verfügbare Version für den Einsatz in der Produktion, die als Teil Ihrer Windows- oder Windows Server-Lizenz enthalten ist.

Hilfe zur Installation finden Sie unter [Installieren](#). Tipps zu den ersten Schritten mit dem Windows Admin Center finden Sie unter [Erste Schritte](#).

Nicht als Vorschau bereitgestellte Versionen von Windows Admin Center können mithilfe von Microsoft Update oder durch manuelles Herunterladen und Installieren von Windows Admin Center aktualisiert werden. Für jede nicht als Vorschauversion bereitgestellte Version von Windows Admin Center wird nach der Veröffentlichung der nächsten nicht als Vorschau bereitgestellten Version 30 Tage lang Support geleistet. Weitere Informationen finden Sie in unserer [Supportrichtlinie](#).

Windows Admin Center-Szenarien

Für die folgenden Aufgaben können Sie das Windows Admin Center verwenden:

	<p>Vereinfachen der Serververwaltung Verwalten Sie Ihre Server und Cluster mit modernisierten Versionen vertrauter Tools wie Server-Manager. Sie können die Installation in weniger als 5 Minuten ausführen und sofort mit der Verwaltung beginnen, es ist keine zusätzliche Konfiguration erforderlich. Weitere Informationen finden Sie unter Was ist Windows Admin Center?</p>
	<p>Arbeiten mit Hybridlösungen Die Integration in Azure unterstützt Sie beim optionalen Verbinden ihrer lokalen Server mit relevanten Clouddiensten. Weitere Informationen finden Sie unter Azure-Hybriddienste.</p>



Optimieren der hyperkonvergenten Verwaltung
Optimieren Sie die Verwaltung von Azure Stack HCI oder hyperkonvergenten Windows Server-Clustern. Verwenden Sie vereinfachte Workloads, um virtuelle Computer, Volumes mit „Direkte Speicherplätze“, Software-Defined Networking und mehr zu erstellen und zu verwalten. Weitere Informationen finden Sie unter [Verwalten hyperkonvergenter Infrastruktur mit Windows Admin Center](#).

Hier finden Sie ein Video, das Ihnen eine Übersicht bietet, gefolgt von einem Poster, das weitere Informationen enthält:

The screenshot displays the Windows Admin Center interface. It includes a top navigation bar with links for Home, Help, Log out, and a search bar. Below the navigation is a main content area divided into several sections:

- Device management**: Shows a list of devices including Storage, Network, Compute, and Power.
- Configuration**: Shows a list of configuration items including User Accounts, Groups, Local Policies, and Group Policies.
- Security**: Shows a list of security items including Local Security Policy, Audit Policy, and Event Log.
- Architecture**: Shows a diagram of the system architecture with components like Windows Admin Center, Managed Machines, and External Services.

On the right side, there is a sidebar titled "Designed for you. Designed WITH YOU." which highlights features like integrated management tools, hybrid management, and support for Azure Stack HCI.

[PDF herunterladen](#)

Inhalt auf einen Blick

Grundlegende Informationen

- Was ist Windows Admin Center?
- Häufig gestellte Fragen
- Fallstudien
- Verwandte Verwaltungsprodukte

Bereitstellen

- Vorbereiten der Umgebung
- Installieren von Windows Admin Center
- Hohe Verfügbarkeit aktivieren

Planen

- Welche Art von Installation ist für Sie geeignet?
- Zugriffsoptionen für Benutzer

Konfigurieren

- Windows Admin Center – Einstellungen
- Steuerung des Benutzerzugriffs und der Berechtigungen
- Gemeinsam genutzte Verbindungen
- Erweiterungen
- Automatisieren mit PowerShell

<p>Verwendung</p> <ul style="list-style-type: none"> • Starten und Hinzufügen von Verbindungen • Verwalten von Servern • Bereitstellen einer hyperkonvergenten Infrastruktur • Verwalten der hyperkonvergenten Infrastruktur • Verwalten von Failoverclustern • Verwalten von virtuellen Computern • Protokollierung 	<p>Herstellen einer Verbindung mit Azure</p> <ul style="list-style-type: none"> • Azure-Hybriddienste • Verbinden von Windows Admin Center mit Azure • Bereitstellen von Windows Admin Center in Azure • Verwalten von Azure-VMs mit Windows Admin Center
<p>Support</p> <ul style="list-style-type: none"> • Releaseverlauf • Supportrichtlinie • Allgemeine Schritte zur Problembehandlung • Bekannte Probleme 	<p>Erweitern</p> <ul style="list-style-type: none"> • Übersicht der Erweiterungen • Grundlegendes zu Erweiterungen • Entwickeln einer Erweiterung • Handbücher • Veröffentlichen von Erweiterungen

Videobasiertes Lernen

Hier finden Sie einige Videos von Microsoft Ignite 2019-Sitzungen:

- [Windows Admin Center: Unlock Azure Hybrid value](#) (Windows Admin Center: Nutzen des Azure Hybrid-Mehrwerts)
- [Windows Admin Center: What's new and what's next](#) (Windows Admin Center: Was ist neu und wie geht's weiter?)
- [Automatically monitor, secure and update your on-premises servers from Azure with Windows Admin Center](#) (Automatisches Überwachen, Sichern und Aktualisieren Ihrer lokalen Server von Azure über Windows Admin Center)
- [Get more done with Windows Admin Center third-party extensions](#) (Mehr Erledigen mit Windows Admin Center-Erweiterungen von Drittanbietern)
- [Be a Windows Admin Center expert: Best practices for deployment, configuration, and security](#) (Werden Sie ein Windows Admin Center-Experte: Bewährte Methoden für Bereitstellung, Konfiguration und Sicherheit)
- [Windows Admin Center: Better together with System Center and Microsoft Azure](#) (Windows Admin Center: Bessere Zusammenarbeit mit System Center und Microsoft Azure)
- [How to use Microsoft Azure hybrid services together with Windows Admin Center and Windows Server](#) (Verwenden von Microsoft Azure-Hybriddiensten zusammen mit Windows Admin Center und Windows Server)
- [Live Q&A: Manage your hybrid server environment with Windows Admin Center](#) (Live-F&A: Verwalten Ihrer hybriden Serverumgebung mit Windows Admin Center)
- [Learning Path: Hybrid management technologies](#) (Lernpfad: Hybridverwaltungstechnologien)
- [Hands on Lab: Windows Admin Center and Hybrid](#) (Praktische Übungseinheit: Windows Admin Center und Hybridlösungen)

Im folgenden finden Sie einige Videos von Windows Server Summit 2019-Sitzungen:

- [Go hybrid with Windows Admin Center](#) (Umstellen auf eine hybride Umgebung mit Windows Admin Center)
- [What's new with Windows Admin Center v1904](#) (Neuerungen in Windows Admin Center v1904)

Und hier finden Sie einige zusätzliche Ressourcen:

- [Windows Admin Center server management reimaged](#) (Die Serververwaltung von Windows Admin Center wurde neu gestaltet)

- [Manage Servers and Virtual Machines Anywhere with Windows Admin Center](#) (Verwalten von Servern und virtuellen Computern an jedem Ort mit Windows Admin Center)
- [How to get started with Windows Admin Center](#) (Erste Schritte mit Windows Admin Center)

Erfahren Sie, wie Kunden von Windows Admin Center profitieren

„[Windows Admin Center] hat unseren Aufwand bei der Verwaltung des Management Systems um mehr als 75 % verringert.“
Rand Morimoto, President, Convergent Computing

„Dank [Windows Admin Center] können wir unsere Kunden problemlos remote über das HTML5-Portal verwalten, und aufgrund der vollständigen Integration von Azure Active Directory sind wir in der Lage, die Sicherheit mit mehrstufiger Authentifizierung zu erhöhen.“

Silvio Di Benedetto, Gründer und Chefberater, Inside Technologies

„Wir konnten [Server Core] SKUs auf effektivere Weise bereitstellen, die Ressourceneffizienz, Sicherheit und Automatisierung verbessern, trotzdem ein hohes Maß an Produktivität erzielen und Fehler reduzieren, die auftreten können, wenn ausschließlich Skripts eingesetzt werden.“

Guglielmo Mengora, Gründer und CEO, VaiSuWeb

„Mit [Windows Admin Center] steht vor allem im SMB-Markt Kunden jetzt ein einfacher zu verwendendes Tool zum Verwalten ihrer internen Infrastruktur zur Verfügung. Dadurch wird der Verwaltungsaufwand minimiert und viel Zeit gespart. Und das Beste: Es fallen keine zusätzlichen Lizenzgebühren für [Windows Admin Center] an!“

Helmut Otto, Hauptgeschäftsführer, SecureGUARD

[Erfahren Sie mehr über Unternehmen, die Windows Admin Center in ihrer Produktionsumgebung verwenden.](#)

Verwandte Produkte

Windows Admin Center dient zum Verwalten von einzelnen Servern oder Clustern. Es ergänzt vorhandene Überwachungs- und Verwaltungslösungen von Microsoft, wie z.B. Remoteserver-Verwaltungstools (RSAT), System Center, Intune oder Azure Stack, ersetzt diese jedoch nicht.

[Hier erfahren Sie, wie Windows Admin Center andere Microsoft-Management-Lösungen ergänzt.](#)

Bleiben Sie auf dem Laufenden

 [Folgen Sie uns auf Twitter](#)

 [Lesen Sie unsere Blogs](#)

Übersicht über Windows Server Hybrid Cloud Print

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

Gilt für:

- Windows Server 2016

Was ist Hybrid Cloud Print?

Hybrid Cloud Print ist ein neues Feature für Windows Server 2016, das über **Features bei Bedarf** verfügbar ist. Dadurch können IT-Experten Druckanforderungen für Personen unterstützen, die ihre eigenen Geräte verwenden, oder Geräte verwenden, die mit Ihrem Azure Active Directory verknüpft sind. Dies umfasst auch mobile Geräte wie Windows Phone, Laptops oder Tablets, auf denen Windows 10 oder Windows Mobile ausgeführt wird. Es bietet Druckunterstützung von allen Personen, die Zugriff auf das Internet haben.

Für IT-Administratoren bietet **Hybrid Cloud Print** sicheren Benutzer Zugriff auf lokale Drucker mithilfe der Multi-Factor Authentication von Azure, um den Benutzer Zugriff zu überprüfen. Die Funktion für einmaliges Anmelden (Single Sign-on, SSO) vereinfacht die Benutzer Funktionalität. **Hybrid Cloud Print** basiert auf der **Windows-Druck Server** Rolle und bietet IT-Experten eine ähnliche Darstellung wie die Verwaltung von Druckern und Benutzer Zugriffssicherheit.

Hybrid Cloud Print ermöglicht es Personen in Ihrer Organisation, von den Geräten, die Sie zum Abschluss ihrer Arbeit verwenden, zu drucken, auch wenn Sie nicht von Ihrem Desk oder Workplace entfernt sind.

Hybrid Cloud Print wird in Windows 10 Creators Update und Windows 10 S unterstützt.

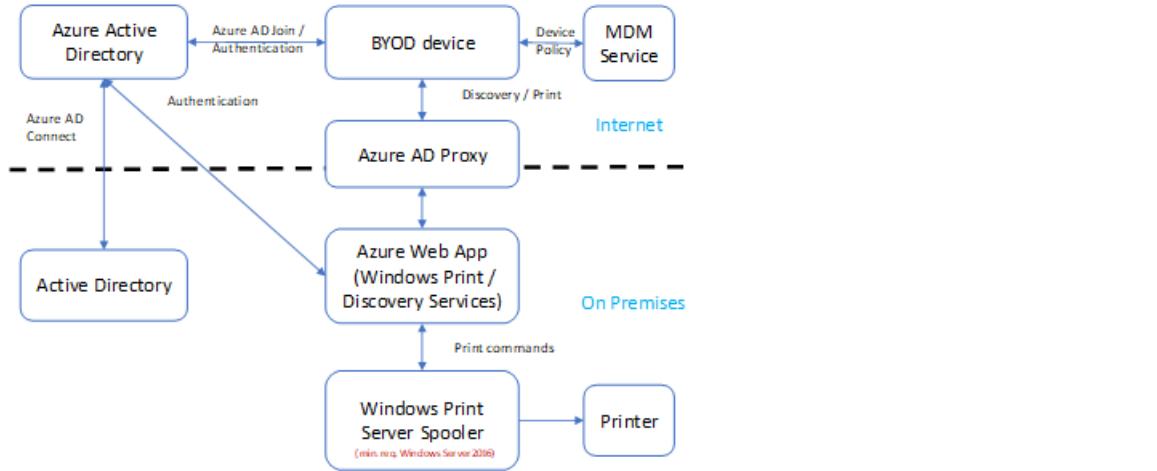
Funktions Zusammenfassung

Hybrid Cloud Print besteht aus zwei Hauptserver seitigen Komponenten: **Ermittlungs Dienst** und **Windows-Druck Dienst**.

- Ermittlungsdienst-Endpunkt, der unter einem IIS -Dienst ausgeführt wird, der einen mopria Alliance-Industriestandard für die Drucker Ermittlung in der Cloud
- Der **Windows-Druck** Dienst Endpunkt, der auf einem IIS-Dienst ausgeführt wird, der das branchenübliche Internet Druck Protokoll (IPP) unterstützt.

Bereitstellung

Hybrid Cloud Print unterstützt verschiedene Bereitstellungs Optionen, je nachdem, wo Ihre Organisation eine Benutzerauthentifizierung erfordert. Eine Bereitstellung könnte wie folgt aussehen:



Hybrid Cloud Print-Lösungs Diagramm

Das Diagramm zeigt Folgendes:

- **Hybrid Cloud Print** using Azure Active Directory als Benutzer Identitäts Anbieter.
- **Windows-Druck Dienst** - und Ermittlungsdienst Endpunkte werden bei Azure Active Directory registriert, damit das Client Gerät das für diese Dienste zu verwendende erforderliche Benutzer Authentifizierungs Token abrufen kann.
- Ein MDM-Dienst, wie z. b. **Microsoft InTune**, stellt dem Client Gerät Richtlinien bereit, die für die Verbindung Azure Active Directory mit dem **Windows-Druck Dienst** und -Ermittlungsdienst

Diese Tabelle enthält weitere Informationen zu den Elementen im Diagramm.

ELEMENT	BESCHREIBUNG
Azure Active Directory	Bietet und steuert die Benutzeridentität und Autorisierungs Funktionalität
Active Directory	Bietet und steuert die Benutzeridentität und Autorisierungs Funktionalität
Azure AD Connect	Synchronisiert Benutzer Anmelde Informationen zwischen Azure AD und lokalem AD.
MDM-Dienst (InTune)	Bietet Funktionen zur Bereitstellung von Geräte Richtlinien, um sicherzustellen, dass das Client Gerät (BYOD-Gerät) den Unternehmensrichtlinien entspricht.
Azure AD Proxy	Bietet eine langlebige Verbindung, die von hinter Ihrer Firewall zu Azure hergestellt wird, damit bestimmter konfigurierter Anwendungs Datenverkehr aus dem Internet in das Unternehmensnetzwerk übertragen werden kann.
Azure-Web-App	Der Kern der Hybrid Cloud-Drucklösung. Stellt die erforderlichen Webendpunkte zum Ermitteln von Drucken und zum Senden von Druck Inhalten für Geräte bereit, die nicht der Domäne beigetreten sind.
BYOD-Gerät/Windows-Druck Server Spooler/Drucker	Diese sind unverändert. Keine Änderung der Funktionalität in der Bereitstellung.

Es gibt zwei Möglichkeiten zum Installieren von Hybrid Cloud Print:

- ** Features bei Bedarf. Weitere Informationen zum Hinzufügen und Entfernen von Rollen-und Featuredateien finden Sie unter [Konfigurieren von Features bei Bedarf in Windows Server](#) .
- ** Einstellungen für Windows Server 2016, die Administratoren zu **Einstellungen -> apps -> Verwalten optionaler Features -> Hinzufügen eines** Features und suchen nach dem Paket "Features bei Bedarf"
- PowerShell-Befehle: führen Sie in einem PowerShell-Administrator Fenster die folgenden Befehle aus:

```
Install-Module -Name PublishCloudPrinter  
Import-Module PublishCloudPrinter  
~~~
```

Bereitstellen von Windows Server Hybrid Cloud Print

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

Gilt für: Windows Server 2016

In diesem Thema für IT-Administratoren wird die End-to-End-Bereitstellung der Microsoft Hybrid Cloud Print (HCP)-Lösung beschrieben. Diese Lösung wird auf vorhandenen Windows-Servern ausgeführt, die als Druck Server ausgeführt werden, und ermöglicht Azure Active Directory (Azure AD) verbundenen und MDM-verwalteten Geräten das Auffinden und Drucken in von der Organisation verwalteten Druckern.

Voraussetzungen

Es gibt eine Reihe von Abonnements, Diensten und Computern, die Sie vor dem Starten dieser Installation erwerben müssen. Sie lauten wie folgt:

- Azure AD Premium-Abonnement.

Weitere Informationen finden [Sie unter Starten eines Azure-Abonnements](#) für ein Testabonnement für Azure.

- MDM-Dienst, z. B. InTune.

Weitere Informationen finden Sie unter [Microsoft InTune](#) für ein Testabonnement für InTune.

- Computer mit Windows Server 2016 oder höher, auf dem Active Directory ausgeführt wird.

[Unterschritt Weise Anleitung: Einrichten von Active Directory in Windows Server 2016](#) finden Sie Hilfe zum Einrichten Active Directory.

- Ein dedizierter, in eine Domäne eingebundener Windows Server 2016-Computer, der als Druck Server ausgeführt wird.
- Ein dedizierter, in eine Domäne eingebundener Windows Server 2016-Computer, der als Connector-Server ausgeführt wird.

Weitere Informationen finden Sie Untergrund Legendes [Azure AD anwendungsproxyconnectors](#).

- Ein Windows 10 Fall Creator-Update oder ein späterer Computer zum Veröffentlichen von Druckern.
- Öffentlicher Domänen Name.

Sie können den für Sie von Azure erstellten Domänen Namen (*DomainName.onmicrosoft.com*) verwenden oder einen eigenen Domänen Namen erwerben. Siehe [Hinzufügen des benutzerdefinierten Domänen Namens mithilfe des Azure Active Directory Portals](#)

Bereitstellungsschritte

Die folgenden Schritte gelten für eine typische Hybrid Cloud-Druck Bereitstellung.

Schritt 1: Installieren von Azure AD Connect

1. Azure AD Connect synchronisiert Azure AD mit lokalem AD. Laden Sie auf dem Windows Server-Computer mit Active Directory die Azure AD Connect Software mit Express-Einstellungen herunter, und installieren Sie Sie. Weitere Informationen finden [Sie unter Getting Started with Azure AD Connect using Express Settings](#).

Schritt 2: Installieren des Anwendungs Proxys

1. Mithilfe des Anwendungs Proxys können Benutzer in Ihrer Organisation über die Cloud auf lokale Anwendungen zugreifen. Installieren Sie den Anwendungs Proxy auf dem Connector-Server.
 - Installationsanweisungen finden Sie unter [Tutorial: Hinzufügen einer lokalen Anwendung für den Remote Zugriff über den Anwendungs Proxy in Azure Active Directory](#).
 - Eine dedizierte Connectorgruppe wird empfohlen, wenn die Organisation über eine komplexe Netzwerktopologie verfügt. Weitere Informationen finden [Sie unter Veröffentlichen von Anwendungen in getrennten Netzwerken und Orten mithilfe von Stecker](#)

Schritt 3: registrieren und Konfigurieren von Anwendungen

Um die authentifizierte Kommunikation mit den HCP-Diensten zu ermöglichen, müssen drei Anwendungen erstellt werden: 2 Webanwendungen, die die beiden HCP-Dienste darstellen, und 1 native Anwendung für die Kommunikation mit diesen Diensten.

1. Melden Sie sich an Azure-Portal, um Web-Apps zu registrieren

- Wechseln Sie unter Azure Active Directory zu **App-Registrierungen > neue Registrierung**.

The screenshot shows the Azure portal interface. On the left, there's a sidebar with various service icons and a 'Create a resource' button. Under 'FAVORITES', 'Azure Active Directory' is selected and highlighted with a red box. In the main content area, the title is 'Cloud Print Demo - App registrations' under 'Cloud Print Demo - App registrations'. Below the title, there's a search bar and a 'New registration' button, which is also highlighted with a red box. To the right of the search bar are links for 'Endpoints', 'Troubleshooting', and 'Got feedback?'. A message box says 'Welcome to the new and improved App registrations (now Generally Available). See what's changed'. Below that, a warning message says 'Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#). Still want to use App registrations (Legacy)? [Go back and tell us why](#)'. At the bottom of the main area, there are tabs for 'All applications' (selected) and 'Owned applications', followed by a search bar and a table header with columns for 'DISPLAY NAME', 'APPLICATION (CLIENT ID)', and 'CREATED ON'.

- Geben Sie einen APP-Namen für den mopria-Ermittlungsdienst ein. Klicken Sie zum Fertigstellen auf **registrieren**.

Home > Cloud Print Demo - App registrations > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

MopriaDiscoveryService ✓

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Cloud Print Demo only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies [\[\]](#)

Register

- Wiederholen Sie den Vorgang für den Enterprise Cloud Print Service
- Wiederholen Sie diesen Schritt für Native App
- Die drei Anwendungen sollten unter **App-Registrierungen** angezeigt werden.

Home > Cloud Print Demo - App registrations

Cloud Print Demo - App registrations X

New registration Endpoints Troubleshooting Got feedback?

Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
Still want to use App registrations (Legacy)? [Go back and tell us why](#)

All applications Owned applications

Start typing a name or Application ID to filter these results

DISPLAY NAME	APPLICATION ...	CREATED ON	CERTIFICATES & SECRETS
MO MopriaDiscoveryService	a018176c-d3a...	9/30/2019	-
EN EnterpriseCloudPrint	7cc2ca13-a599...	9/30/2019	-
NA NativeAppForHCP	be6af4dc-d3e4...	9/30/2019	-

2. Machen Sie die API für die 2 Webanwendungen verfügbar.

- Klicken Sie auf dem Blatt "App-Registrierungen" auf die app "mopria Discovery Service", wählen Sie eine API verfügbar machen aus, und klicken Sie dann neben Anwendungs-ID-URI auf festlegen .

Home > Cloud Print Demo - App registrations > MopriaDiscoveryService - Expose an API

MopriaDiscoveryService - Expose an API

Search (Ctrl+ /) Application ID URI Set

Overview Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions

Expose an API

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Add a scope

SCOPE	WHO CAN ...	ADMIN CONSENT D...	USER CONSENT DIS...	STA...
No scopes have been defined				

- Klicken Sie auf **Speichern**, ohne den Standardwert für Anwendungs-ID-URI zu ändern. Dieser Wert muss jetzt nur noch festgelegt werden und wird später geändert.

MopriaDiscoveryService - Expose an API

Search (Ctrl+ /) Set the App ID URI

Application ID URI api://7cc2ca13-a599-4005-95ac-2c5c4cb02e55

Save Discard

Overview Quickstart

Manage

- Branding

- Klicken Sie auf **Bereich hinzufügen**.

Home > Cloud Print Demo - App registrations > MopriaDiscoveryService - Expose an API

MopriaDiscoveryService - Expose an API

Search (Ctrl+ /) Application ID URI api://7cc2ca13-a599-4005-95ac-2c5c4cb02e55 Edit

Overview Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions

Expose an API

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Add a scope

SCOPE	WHO CAN ...	ADMIN CONSENT D...	USER CONSENT DIS...	STA...
No scopes have been defined				

- Geben Sie einen Bereichs Namen an, gestatten Sie Administratoren und Benutzern die Zustimmung, geben Sie die Zustimmungs Beschreibung ein, und klicken Sie dann auf **Bereich hinzufügen**.

MopriaDiscoveryService - Exp

Add a scope

* Scope name ✓
 api://7cc2ca13-a599-4005-95ac-2c5c4cb02e55/PrinterDiscovery

Who can consent? Admins and users Admins only
 Admin consent display name ✓
 Admin consent description ✓

User consent display name
 User consent description
 State Enabled Disabled

Add scope Cancel

- Wiederholen Sie den Vorgang für den Enterprise Cloud Print Service Verwenden Sie einen anderen Bereichs Namen und eine Beschreibung der Zustimmung.

EnterpriseCloudPrint - Expose

Add a scope

* Scope name ✓
 api://a018176c-d3a6-404a-a573-f61365ca00d0/Print

Who can consent? Admins and users Admins only
 Admin consent display name ✓
 Admin consent description ✓

User consent display name
 User consent description
 State Enabled Disabled

Add scope Cancel

3. API-Berechtigungen hinzufügen

- Wechseln Sie zurück zum Blatt App-Registrierungen. Klicken Sie auf die native APP und wählen Sie API-

Berechtigungen aus. Klicken Sie auf **Berechtigung hinzufügen**.

Home > Cloud Print Demo - App registrations > NativeAppForHCP - API permissions

NativeAppForHCP - API permissions

API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

API / PERMISSIONS	TYPE	DESCRIPTION	ADMIN CONSENT	STATUS
User.Read	Delegated	Sign in and read...	-	-

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

- Wechseln Sie zu den von **meiner Organisation verwendeten APIs**, und verwenden Sie das Suchfeld, um den zuvor hinzugefügten Mopria Discovery-Dienst zu finden. Klicken Sie im Suchergebnis auf den Dienst.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

NAME	APPLICATION (CLIENT) ID
MopriaDiscoveryService	7cc2ca13-a599-4005-95ac-2c5c4cb02e55

- Wählen Sie **Delegierte Berechtigungen** aus. Aktivieren Sie das Kontrollkästchen neben dem API-Bereich. Klicken Sie auf **Berechtigungen hinzufügen**.

Request API permissions

All APIs

MopriaDiscoveryService
api://7cc2ca13-a599-4005-95ac-2c5c4cb02e55

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
---	--

Select permissions

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> PrinterDiscovery PrinterDiscovery ⓘ	-

Add permissions Discard

- Wiederholen Sie den Vorgang, um dem Enterprise Cloud-Druckdienst Berechtigungen

Request API permissions

[◀ All APIs](#)

EnterpriseCloudPrint
api://a018176c-d3a6-404a-a573-f61365ca00d0

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> Print Print	-

[expand all](#)

[Add permissions](#) [Discard](#)

- Nachdem Sie auf das Blatt "API-Berechtigungen" zurückgekehrt sind, warten Sie 10 Sekunden, bevor Sie auf die Zustimmung des Haupt Administrators klicken.

Home > Cloud Print Demo - App registrations > NativeAppForHCP - API permissions

NativeAppForHCP - API permissions

Search (Ctrl+ /)

Overview Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions**
- Expose an API
- Owners
- Roles and administrators (Previous)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Permissions have changed, please wait 10 seconds before granting admin consent. Users and/or admins will have to consent even if they have already done so previously.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CO...	STATUS
▼ EnterpriseCloudPrint (1)	Delegated	Print	-	
▼ Microsoft Graph (1)	Delegated	User.Read	Sign in and read user...	-
▼ MopriaDiscoveryService (1)	Delegated	PrinterDiscovery	PrinterDiscovery	-

These are the permissions that this application requests statically. You may also request user-consentable permissions dynamically through code. See [best practices for requesting permissions](#)

Grant consent

These permissions have been granted for undefined but aren't in the configured permissions list. If your application requires these permissions, you should consider adding them to the configured permissions list.

[Grant admin consent for Cloud Print Demo](#)

- Wenn Sie aufgefordert werden, klicken Sie auf Ja .

Do you want to grant consent for the requested permissions for all accounts in Cloud Print Demo? This will update any existing admin consent records this application already has to match what is listed below.

Yes No

- Vergewissern Sie sich, dass die Spalte Status der API-Berechtigung mit grünen Häkchen angezeigt wird.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CO...	STATUS
Print	Delegated	Print	-	Granted for Cloud Print Demo
User.Read	Delegated	Sign in and read user ...	-	Granted for Cloud Print Demo
PrinterDiscovery	Delegated	PrinterDiscovery	-	Granted for Cloud Print Demo

4. Konfigurieren des Anwendungs Proxys für die Webanwendungen

- Wechseln Sie zu **Azure Active Directory > Unternehmensanwendungen > alle Anwendungen**. Suchen Sie nach dem Dienst "mopria Discovery", und klicken Sie darauf.

NAME	HOMEPAGE URL	OBJECT ID
MopriaDiscoveryService		a4c414aa-9e

- Klicken Sie auf **Anwendungs Proxy**. Geben Sie im Format

`https://<fully qualified domain name of the Print Server>/mcs/` die interne URL ein. Klicken Sie zum Fertigstellen auf "Speichern".

- Wiederholen Sie den Vorgang für den Enterprise Cloud Print Service Beachten Sie, dass die interne URL

`https://<fully qualified domain name of the Print Server>/ecp/` ist.

EnterpriseCloudPrint - Application proxy

Save Discard

Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. [Learn more about Application Proxy](#)

Test Application

Click here to verify application configuration.

Basic Settings

* Internal Url: <https://hcptest-vm01.hcptest.local/ecp/>

External Url: https:// enterprisecloudprint

Pre Authentication: Passthrough

Connector Group: Default

Manage

- Overview
- Getting started
- Deployment Plan
- Diagnose and solve problems
- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy**

- Wechseln Sie zu **Azure Active Directory > App-Registrierungen**. Klicken Sie auf den mopria Discovery-Dienst. Beachten Sie, dass unter **Übersicht** der Anwendungs-ID-URI von der Standardeinstellung in die externe URL unter **Anwendungs Proxy** geändert wurde. Der URI wird bei der Druck Server Einrichtung, in der Client-MDM-Richtlinie und bei der Veröffentlichung des Druckers verwendet.

Create a resource

Home Dashboard All services FAVORITES Storage accounts Virtual networks Azure Active Directory Monitor Advisor Security Center

App registrations MopriaDiscoveryService

Search (Ctrl+ /)

Delete Endpoints

Overview Quickstart Manage Branding Authentication Certificates & secrets API permissions

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →

Display name MopriaDiscoveryService Application (client) ID b3a2779d-2050-4eef-9a8f-4d69a7b612f5 Directory (tenant) ID 6923dc21-4f0f-42e5-800e-ef1e8ba0b218 Object ID 65fc8c1c-9c42-4cd5-ae4d-56e775282242

Supported account types My organization only Redirect URIs 1 web, 0 public client Application ID URI https://mopriadiscoveryservice msappproxy.net/... Managed application in local directory MopriaDiscoveryService

5. Zuweisen von Benutzern zu Anwendungen

- Wechseln Sie zu **Azure Active Directory > Unternehmensanwendungen > alle Anwendungen**. Suchen Sie nach dem mopria Discovery-Dienst, und klicken Sie darauf.
- Klicken Sie entweder auf **Benutzer und Gruppen**, und weisen Sie **Benutzer zu**, oder klicken Sie auf **Eigenschaften**, und ändern Sie die **Benutzer Zuweisung erforderlich?**
- Wiederholen Sie den Vorgang für den Enterprise Cloud Print Service

6. Umleitungs-URI in der nativen App konfigurieren

- Wechseln Sie zu **Azure Active Directory > App-Registrierungen**. Klicken Sie auf die native app. Wechseln Sie zu **Übersicht**, und kopieren Sie die **Anwendungs-ID (Client)**.

Create a resource

Home Dashboard All services FAVORITES Storage accounts Virtual networks Azure Active Directory Monitor Advisor Security Center Cost Management + Bill...

App registrations NativeAppForHCP

Search (Ctrl+ /)

Delete Endpoints

Overview Quickstart Manage Branding Authentication Certificates & secrets API permissions Expose an API

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →

Display name NativeAppForHCP Application (client) ID dbe4feeb-cb69-40fc-91aa-73272f6d8fe1

Directory (tenant) ID 6923dc21-4f0f-42e5-800e-ef1e8ba0b218 Object ID 240d6c24-da5d-4912-a27e-2fbfb8a0b9b

Call APIs

- Wechseln Sie zu **Authentifizierung**. Ändern Sie das Dropdown Feld **Typ** in **Public...**, und geben Sie zwei Umleitungs-URIs in folgendem Format ein, in dem **<NativeClientAppID>** aus dem vorherigen Schritt:

`ms-appx-web://Microsoft.AAD.BrokerPlugin/<NativeClientAppID>`

`ms-appx-web://Microsoft.AAD.BrokerPlugin/S-1-15-2-3784861210-599250757-1266852909-3189164077-45880155-1246692841-283550366`

- Klicken Sie zum Fertigstellen auf **Speichern**.

Schritt 4: Einrichten des Druck Servers

- Stellen Sie sicher, dass alle verfügbaren Windows Update auf dem Druck Server installiert sind. Hinweis: Server 2019 muss für die Erstellung 17763,165 oder höher gepatcht werden.

- Installieren Sie die folgenden Server Rollen:
 - Druck Server Rolle
 - Internet Informationsdienste (IIS)
- Ausführliche Informationen zum Installieren von Server Rollen finden [Sie unter Installieren von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features](#).

- Installieren Sie die PowerShell-Module für Hybrid Cloud Print.

- Führen Sie die folgenden Befehle an einer PowerShell-Eingabeaufforderung mit erhöhten Rechten aus:

```
find-module -Name PublishCloudPrinter , um zu bestätigen, dass der Computer die PowerShell-Katalog (psgallery) erreichen kann.
```

```
install-module -Name PublishCloudPrinter
```

Hinweis: möglicherweise wird ein Messaging angezeigt, das besagt, dass "psgallery" ein nicht vertrauenswürdiges Repository ist. Geben Sie "y" ein, um die Installation fortzusetzen.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd\
PS C:\> find-module -Name "PublishCloudPrinter"

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Version      Name          Repository      Description
-----      ----          -----          -----
1.0.0.0      PublishCloudPrinter      PSGallery      Allows Administration of Cloud Printers

PS C:\> install-module -Name "PublishCloudPrinter"

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\>

```

3. Installieren Sie die Hybrid Cloud-Drucklösung.

- Wechseln Sie in der gleichen PowerShell-Eingabeaufforderung mit erhöhten Rechten zum folgenden Verzeichnis (Anführungszeichen erforderlich):

```
C:\Program Files\WindowsPowerShell\Modules\PublishCloudPrinter\1.0.0.0
```

- Ausführen

```
.\CloudPrintDeploy.ps1 -AzureTenant <Azure Active Directory domain name> -AzureTenantGuid <Azure Active Directory ID>
```

- Informationen zum Azure Active Directory Domänen Namen finden Sie im folgenden Screenshot.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with navigation links: 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (which includes 'Virtual networks', 'Azure Active Directory' (highlighted with a red box), 'Monitor', and 'Advisor'), and 'Azure Active Directory' (highlighted with a red box). The main content area is titled 'Cloud Print Demo - Overview' under 'Azure Active Directory'. It features a search bar, a 'Switch directory' button, and a 'Delete directory' button. Below the search bar, there are two tabs: 'Overview' (highlighted with a red box) and 'Getting started'. On the right, there's a summary card for 'Cloud Print Demo' which says 'Azure AD for Office 365' and lists 'Sign-ins'. The URL 'ecp578.onmicrosoft.com' is visible in the browser address bar.

- Die Azure Active Directory-ID finden Sie im nachfolgenden Screenshot.

- Die Ausgabe des cloudprintbereitstellungs-Skripts sieht wie folgt aus:

```

Administrator: Windows PowerShell
PS C:\Program Files\WindowsPowerShell\Modules\PublishCloudPrinter\1.0.0.0> .\CloudPrintDeploy.ps1 -AzureTenant "Cloud Print Demo" -AzureTenantGuid 8f40ea58-23ce-497e-a4dd-eca0a747e0ad
Enable IIS Web Server Role with Asp.net? [Y] Yes [N] No (default is "N"): Y
** Installing IIS
** Stopping WWW service
** Deploying Enterprise Cloud Print binaries
** Deploying Mopria Discovery Service binaries
** Adding WebServices
** Enabling Windows Authentication for Azure App Proxy PreAuth
Open SSL firewall port (port 443)? [Y] Yes [N] No (default is "N"): Y
** Opening SSL firewall port
** Updating registry
** Restarting IIS
** Creating EcpPrintTest virtual printer
** Done. Refer to installation instructions for further needed setup
PS C:\Program Files\WindowsPowerShell\Modules\PublishCloudPrinter\1.0.0.0>

```

- Überprüfen Sie die Protokolldatei, um festzustellen, ob ein Fehler vorliegt:

C:\Program Files\WindowsPowerShell\Modules\PublishCloudPrinter\1.0.0.0\CloudPrintDeploy.log

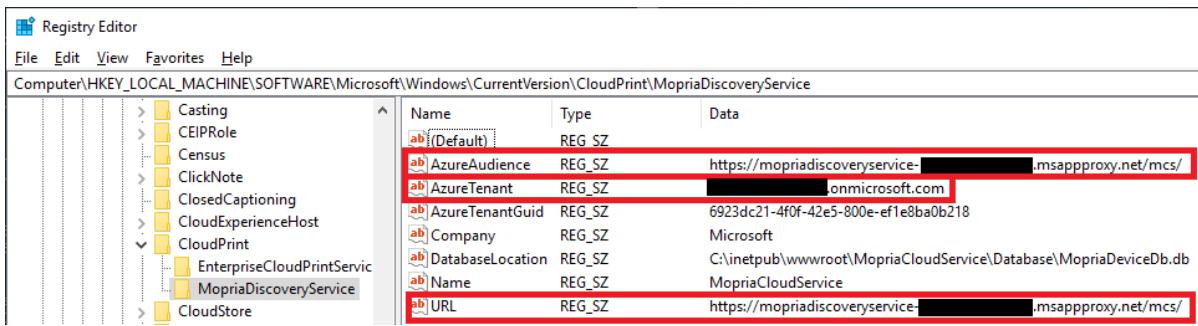
- Führen Sie regedit an einer Eingabeaufforderung mit erhöhten Rechten aus. Wechseln Sie zu Computer \ HKEY_LOCAL_MACHINE \software\microsoft\windows\currentversion\cloudprint\enterprisecloudprintservice.

- Stellen Sie sicher, dass azureaudience auf den Anwendungs-ID-URI der Unternehmens Cloud-Druck-App festgelegt ist
- Stellen Sie sicher, dass für azuretenant der Azure AD Domänen Name festgelegt ist.

Name	Type	Data
(Default)	REG_SZ	
AzureAudience	REG_SZ	https://enterprisecloudprint-[REDACTED].msappproxy.net/ecp/
AzureTenant	REG_SZ	[REDACTED].onmicrosoft.com

- Wechseln Sie zu "Computer \ HKEY_LOCAL_MACHINE \software\microsoft\windows\currentversion\cloudprint\mopriadiscoveryservice".

- Stellen Sie sicher, dass azureaudience der Anwendungs-ID-URI der mopria Discovery Service-APP ist.
- Stellen Sie sicher, dass azuretenant der Azure AD Domänen Name ist.
- Stellen Sie sicher, dass URL der Anwendungs-ID-URI der mopria Discovery Service-APP ist.



6. Führen Sie **iisreset** an einer PowerShell-Eingabeaufforderung mit erhöhten Rechten aus. Dadurch wird sichergestellt, dass alle im vorherigen Schritt vorgenommenen Registrierungs Änderungen wirksam werden.

7. Konfigurieren Sie die IIS-Endpunkte zur Unterstützung von SSL.

- Das SSL-Zertifikat kann ein selbst signiertes Zertifikat oder ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat sein.
- Wenn Sie ein selbst signiertes Zertifikat verwenden, **Stellen Sie sicher, dass das Zertifikat auf die Client Computer importiert wurde.**
- Wenn Sie Ihre Domäne bei einem Drittanbieter registrieren, müssen Sie die IIS-Endpunkte mit SSL-Zertifikat konfigurieren. Ausführliche Informationen finden Sie in diesem [Handbuch](#).

8. Installieren Sie das SQLite-Paket.

- Öffnen Sie eine PowerShell-Eingabeaufforderung mit erhöhten Rechten.
- Führen Sie den folgenden Befehl aus, um die nuget-Pakete System. Data. sqlite herunterzuladen.

```
Register-PackageSource -Name nuget.org -ProviderName NuGet -Location https://www.nuget.org/api/v2/ -Trusted -Force
```

- Führen Sie den folgenden Befehl aus, um die Pakete zu installieren.

```
Install-Package system.data.sqlite [-requiredversion x.x.x.x] -providername nuget
```

Hinweis: Es wird empfohlen, die neueste Version herunterzuladen und zu installieren, indem Sie die Option-Requirements dversion verlassen.

```
PS C:\> Register-PackageSource -Name nuget.org -ProviderName NuGet -Location https://www.nuget.org/api/v2/ -Trusted -Force
Name          ProviderName  IsTrusted  Location
----          -----        -----      -----
nuget.org      NuGet        True       https://www.nuget.org/api/v2/

PS C:\> Install-Package system.data.sqlite -providername nuget
Name          Version  Source   Summary
----          -----   -----   -----
System.Data.SQLite.Core  1.0.111.0  nuget.org  The official SQLite database engine for both x86 and...
System.Data.SQLite.Linq  1.0.111.0  nuget.org  Support for LINQ using System.Data.SQLite.
EntityFramework      6.2.0    nuget.org  Entity Framework is Microsoft's recommended data access...
System.Data.SQLite.EF6  1.0.111.0  nuget.org  Support for Entity Framework 6 using System.Data.SQLite.
System.Data.SQLite     1.0.111.0  nuget.org  The official SQLite database engine for both x86 and...
```

9. Kopieren Sie die SQLite-DLLs in den Ordner "mopriacloudservice webapp bin" (c:\inetpub\wwwroot\mopriacloudservice\bin).

- Erstellen Sie eine PS1-Datei, die das unten stehende PowerShell-Skript enthält.
- Ändern Sie die \$Version Variable in die SQLite-Version, die Sie im vorherigen Schritt installiert haben.
- Führen Sie die PS1-Datei an einer PowerShell-Eingabeaufforderung mit erhöhten Rechten aus.

```

$source = \Program Files\PackageManagement\NuGet\Packages
$core = System.Data.SQLite.Core
$linq = System.Data.SQLite.Linq
$ef6 = System.Data.SQLite.EF6
$version = x.x.x.x
$target = C:\inetpub\wwwroot\MopriaCloudService\bin

xcopy /y $source\$core.$version\lib\net46\System.Data.SQLite.dll $target\
xcopy /y $source\$core.$version\build\net46\x86\SQLite.Interop.dll $target\x86\
xcopy /y $source\$core.$version\build\net46\x64\SQLite.Interop.dll $target\x64\
xcopy /y $source\$linq.$version\lib\net46\System.Data.SQLite.Linq.dll $target\
xcopy /y $source\$ef6.$version\lib\net46\System.Data.SQLite.EF6.dll $target\

```

10. Aktualisieren Sie die Datei "c:\inetpub\wwwroot\mopriacloudservice\web.config", um die SQLite-Version x.x.x.x in den folgenden `<runtime>/<assemblyBinding>` Abschnitten einzubeziehen. Dies ist die gleiche Version, die im vorherigen Schritt verwendet wurde.

```

...
<dependentAssembly>
  assemblyIdentity name=System.Data.SQLite culture=neutral publicKeyToken=db937bc2d44ff139 /
  <bindingRedirect oldVersion=0.0.0.0-x.x.x.x newVersion=x.x.x.x />
</dependentAssembly>
<dependentAssembly>
  assemblyIdentity name=System.Data.SQLite.Core culture=neutral publicKeyToken=db937bc2d44ff139 />
  <bindingRedirect oldVersion=0.0.0.0-x.x.x.x newVersion=x.x.x.x />
</dependentAssembly>
<dependentAssembly>
  assemblyIdentity name=System.Data.SQLite.EF6 culture=neutral publicKeyToken=db937bc2d44ff139 />
  <bindingRedirect oldVersion=0.0.0.0-x.x.x.x newVersion=x.x.x.x />
</dependentAssembly>
<dependentAssembly>
  assemblyIdentity name=System.Data.SQLite.Linq culture=neutral publicKeyToken=db937bc2d44ff139 />
  <bindingRedirect oldVersion=0.0.0.0-x.x.x.x newVersion=x.x.x.x />
</dependentAssembly>
...

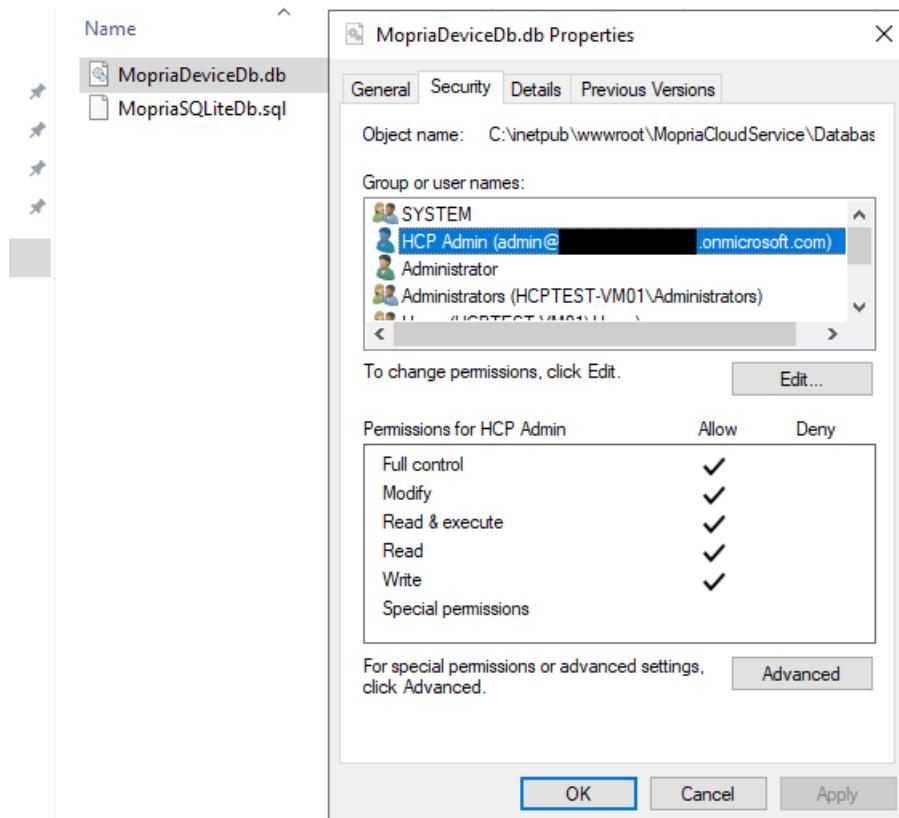
```

11. Erstellen Sie die SQLite-Datenbank.

- Herunterladen und Installieren der Binärdateien der SQLite-Tools aus <https://www.sqlite.org/>.
- Wechseln Sie zu `c:\inetpub\wwwroot\MopriaCloudService\Database` Verzeichnis.
- Führen Sie den folgenden Befehl aus, um die Datenbank in diesem Verzeichnis zu erstellen:

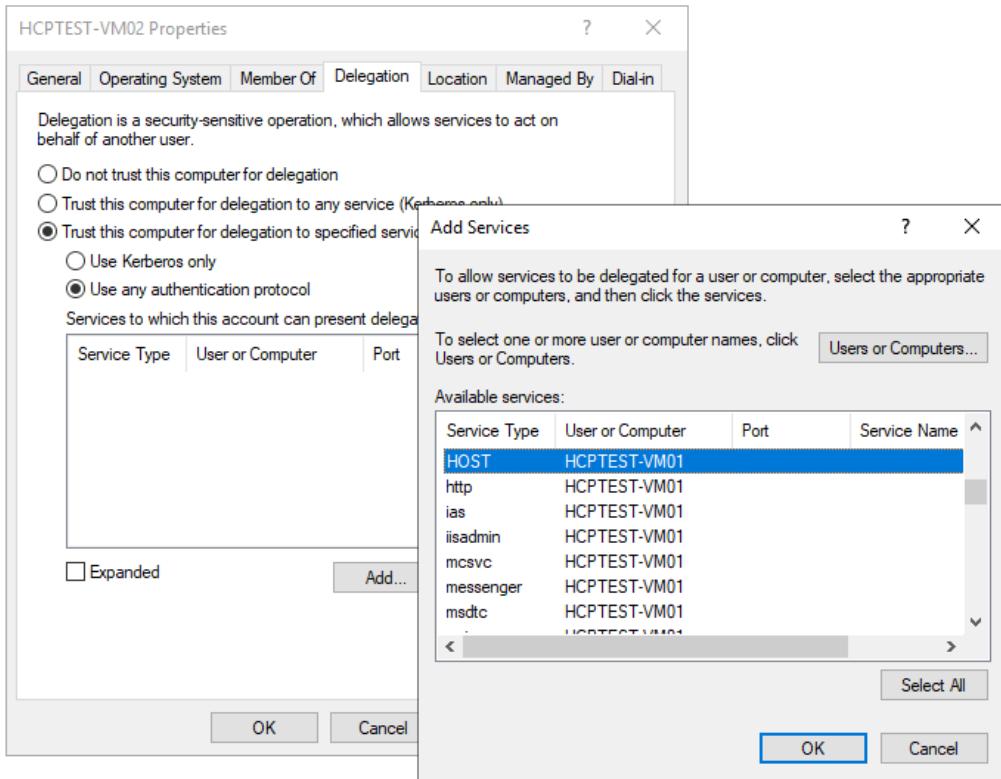
```
sqlite3.exe MopriaDeviceDb.db .read MopriaSQLiteDb.sql
```

- Öffnen Sie im Datei-Explorer die Eigenschaften der Datei "mopriadevicedb.DB", um Benutzer oder Gruppen hinzuzufügen, die auf der Registerkarte "Sicherheit" in der Datenbank "mopria" veröffentlichen dürfen. Die Benutzer oder Gruppen müssen lokal Active Directory vorhanden und mit Azure AD synchronisiert werden.
- Wenn die Lösung in einer nicht Routing fähigen Domäne (z. B. *mydomain.local*) bereitgestellt wird, muss die Azure AD Domäne (z. B. Domain *Name.onmicrosoft.com* oder eine, die von einem Drittanbieter erworben wurde) als UPN-Suffix zu lokalen Active Directory hinzugefügt werden. Dies ist derselbe Benutzer, der Drucker veröffentlichen soll (z. B. *admin@Domain Name.onmicrosoft.com*), kann in der Sicherheitseinstellung der Datenbankdatei hinzugefügt werden. Weitere Informationen finden Sie unter [Vorbereiten einer nicht Routing fähigen Domäne für die Verzeichnis Synchronisierung](#).



Schritt 5 [optionale]: Konfigurieren der Vorauthentifizierung mit Azure AD

1. Überprüfen Sie die [Eingeschränkte Kerberos-Delegierung für Single Sign-on zu ihren apps mit dem Anwendungs Proxy](#).
2. Konfigurieren Sie die lokale Active Directory.
 - Öffnen Sie auf dem Active Directory Computer Server-Manager, und navigieren Sie zu Tools > Active Directory Benutzer und Computer.
 - Navigieren Sie zum Knoten Computer, und wählen Sie den Connector-Server aus.
 - Klicken Sie mit der rechten Maustaste, und wählen Sie -> Registerkarte Delegierung
 - Wählen Sie Computer nur bei Delegierungen angegebener Dienste vertrauen aus.
 - Wählen Sie beliebiges Authentifizierungsprotokoll verwenden aus.
 - Unter Dienste, für die dieses Konto Delegierte Anmelde Informationen vorweisen kann.
 - Fügen Sie den Dienst Prinzipal Namen (SPN) des Druck Server Computers hinzu.
 - Wählen Sie Host als Diensttyp aus.



3. Vergewissern Sie sich, dass die Windows-Authentifizierung in IIS aktiviert ist.

- Öffnen Sie auf dem Druck Server Server-Manager > Tools > Internet Informationsdienste-Manager (IIS).
- Wechseln Sie zum Standort.
- Doppelklicken Sie auf **Authentifizierung**.
- Klicken Sie auf **Windows-Authentifizierung** und dann unter **Aktionen** auf **aktivieren**.

The screenshot shows the IIS Manager interface. In the left navigation pane, 'Default Web Site' is selected. On the right, the 'Authentication' section is displayed. The 'Windows Authentication' row is highlighted with a red box. The 'Actions' pane on the right shows options like 'Disable', 'Advanced Settings...', and 'Providers...'. A tooltip in the 'Alerts' pane suggests configuring Extended Protection.

4. Einmaliges Anmelden konfigurieren.

- Wechseln Sie auf Azure-Portal zu **Azure Active Directory** > **Unternehmensanwendungen** > **alle Anwendungen**.
- Wählen Sie die app "mopriadiscoveryservice" aus.
- Wechseln Sie zu **Anwendungs Proxy**. Ändern Sie die Methode für die Vorauthentifizierung in **Azure Active Directory**.
- Wechseln Sie zu **einmaliges Anmelden**. Wählen Sie integrierte Windows-Authentifizierung als Single Sign-on-Methode aus.
- Legen Sie **interner Anwendungs-SPN** auf den SPN des Druck Server Computers fest.
- Legen Sie die **Delegierte Anmelde Identität** auf den Benutzer Prinzipal Namen fest.
- Wiederholen Sie diesen Schritt für die entperiabdruck-app.

Schritt 6: Konfigurieren der erforderlichen MDM-Richtlinien

1. Melden Sie sich bei Ihrem MDM-Anbieter an.
2. Suchen Sie nach der Unternehmens Cloud-druckrichtlinien Gruppe, und konfigurieren Sie die Richtlinien gemäß den folgenden Richtlinien:
 - Cloudprintoauthauthority = <https://login.microsoftonline.com/<Azure AD Directory ID>>. Die Verzeichnis-ID finden Sie unter Azure Active Directory > Eigenschaften.
 - Cloudprintoauthclientid = Anwendungs (Client) ID-Wert der systemeigenen app. Sie finden diesen unter Azure Active Directory > app-Registrierungen, > Sie die systemeigene app > Übersicht auswählen.
 - Cloudprinterdiscoveryendpoint = externe URL der mopria Discovery Service-APP. Sie finden diesen unter Azure Active Directory > Unternehmensanwendungen > Wählen Sie die app "mopria Discovery Service" > Anwendungs Proxy aus. **Sie muss genau gleich sein, aber ohne das nachfolgende/**.
 - Mopriadiscoveryresourceid = der Anwendungs-ID-URI der mopria Discovery Service-APP. Sie finden dies unter Azure Active Directory > app-Registrierungen > die > Übersicht über den Dienst "mopria Discovery Service APP" auswählen. **Der Wert muss mit dem nachfolgenden/identisch sein.**
 - Cloudprintresourceid = der Anwendungs-ID-URI der Unternehmens-Cloud-Druck-app. Sie finden diesen unter Azure Active Directory > app-Registrierungen > Wählen Sie die > Übersicht der unternehmenscloud-Druck-App aus. **Der Wert muss mit dem nachfolgenden/identisch sein.**
 - Discoverymaxprinterlimit = <eine positive Ganzzahl>.

Hinweis: Wenn Sie Microsoft Intune-Dienst verwenden, finden Sie diese Einstellungen unter der Kategorie clouddrucker.

INTUNE-ANZEIGE NAME	POLICY (RICHTLINIE)
URL für Drucker Ermittlung	Cloudprinterdiscoveryendpoint
URL der Drucker Zugriffs Autorität	Cloudprintoauthauthority
Azure Native Client-App-GUID	Cloudprin"authclientid"
Ressourcen-URI des Druck Diensts	Cloudprintresourceid
Maximal abzufragende Drucker (nur Mobilgeräte)	Discoverymaxprinterlimit
Ressourcen-URI für Drucker Ermittlungsdienst	Mopriadiscoveryresourceid

Hinweis: Wenn die clouddruckrichtliniengruppe nicht verfügbar ist, der MDM-Anbieter jedoch Oma-URI-Einstellungen unterstützt, können Sie dieselben Richtlinien festlegen. Weitere Informationen finden Sie in [diesem Artikel](#).

```
- <span data-ttu-id="f87ed-335">Werte für OMA-URI</span><span class="sxs-lookup"><span data-stu-id="f87ed-335">Values for OMA-URI</span></span>
- <span data-ttu-id="f87ed-336">Cloudprintoauthauthority
= ./Vendor/MSFT/Policy/config/EnterpriseCloudPrint/CloudPrintOAuthAuthority</span><span class="sxs-lookup"><span data-stu-id="f87ed-336">CloudPrintOAuthAuthority =
./Vendor/MSFT/Policy/Config/EnterpriseCloudPrint/CloudPrintOAuthAuthority</span></span>
- <span data-ttu-id="f87ed-337">Wert = https://login.microsoftonline.com/<Azure AD Directory ID></span>
<span class="sxs-lookup"><span data-stu-id="f87ed-337">Value = https://login.microsoftonline.com/<Azure AD Directory ID></span></span>
- <span data-ttu-id="f87ed-338">Cloudprindienst authclientid
= ./Vendor/MSFT/Policy/config/EnterpriseCloudPrint/CloudPrintOAuthClientId</span><span class="sxs-lookup"><span data-stu-id="f87ed-338">CloudPrintOAuthClientId =
./Vendor/MSFT/Policy/Config/EnterpriseCloudPrint/CloudPrintOAuthClientId</span></span>
- <span data-ttu-id="f87ed-339">Wert = < Azure AD Anwendungs-ID der nativen app ></span><span class="sxs-lookup"><span data-stu-id="f87ed-339">Value = <Azure AD Native App's Application ID></span></span>
- <span data-ttu-id="f87ed-340">Cloudprinterdiscoverendpoint
= ./Vendor/MSFT/Policy/config/EnterpriseCloudPrint/CloudPrinterDiscoveryEndPoint</span><span class="sxs-lookup"><span data-stu-id="f87ed-340">CloudPrinterDiscoveryEndPoint =
./Vendor/MSFT/Policy/Config/EnterpriseCloudPrint/CloudPrinterDiscoveryEndPoint</span></span>
- <span data-ttu-id="f87ed-341">Value = externe URL der "mopria Discovery Service"-app (muss genau identisch sein, aber ohne das nachfolgende/)</span><span class="sxs-lookup"><span data-stu-id="f87ed-341">Value = External URL of the Mopria Discovery Service app (must be exactly the same but without the trailing /)</span>
</span>
- <span data-ttu-id="f87ed-342">Mopriadiscoveryresourceid
= ./Vendor/MSFT/Policy/config/EnterpriseCloudPrint/MopriaDiscoveryResourceId</span><span class="sxs-lookup">
<span data-stu-id="f87ed-342">MopriaDiscoveryResourceId =
./Vendor/MSFT/Policy/Config/EnterpriseCloudPrint/MopriaDiscoveryResourceId</span></span>
- <span data-ttu-id="f87ed-343">Value = der Anwendungs-ID-URI der mopria Discovery Service-APP</span>
<span class="sxs-lookup"><span data-stu-id="f87ed-343">Value = The Application ID URI of the Mopria Discovery Service app</span></span>
- <span data-ttu-id="f87ed-344">Cloudprintresourceid
= ./Vendor/MSFT/Policy/config/EnterpriseCloudPrint/CloudPrintResourceId</span><span class="sxs-lookup"><span data-stu-id="f87ed-344">CloudPrintResourceId =
./Vendor/MSFT/Policy/Config/EnterpriseCloudPrint/CloudPrintResourceId</span></span>
- <span data-ttu-id="f87ed-345">Wert = Anwendungs-ID-URI der Unternehmens-Cloud-Druck-App</span><span class="sxs-lookup"><span data-stu-id="f87ed-345">Value = The Application ID URI of the Enterprise Cloud Print app</span></span>
- <span data-ttu-id="f87ed-346">Discoverymaxprinteralimit
= ./Vendor/MSFT/Policy/config/EnterpriseCloudPrint/DiscoveryMaxPrinterLimit</span><span class="sxs-lookup"><span data-stu-id="f87ed-346">DiscoveryMaxPrinterLimit =
./Vendor/MSFT/Policy/Config/EnterpriseCloudPrint/DiscoveryMaxPrinterLimit</span></span>
- <span data-ttu-id="f87ed-347">Value = eine positive ganze Zahl</span><span class="sxs-lookup"><span data-stu-id="f87ed-347">Value = A positive integer</span></span>
```

Schritt 7: Veröffentlichen des freigegebenen Druckers

1. Installieren Sie den gewünschten Drucker auf dem Drucker Server.
2. Geben Sie den Drucker über die Benutzeroberfläche der Druckereigenschaften frei.
3. Wählen Sie den gewünschten Benutzer Satz aus, dem der Zugriff gewährt werden soll.
4. Speichern Sie die Änderungen, und schließen Sie das Fenster Druckereigenschaften.
5. Vorbereiten eines Windows 10 Fall Creator-Updates oder eines späteren Computers. Verknüpfen Sie den Computer mit Azure AD, und melden Sie sich als Benutzer an, der mit der lokalen Active Directory synchronisiert ist und über die entsprechende Berechtigung für die Datei "mopriadevicedb. DB" verfügt.
6. Öffnen Sie auf dem Windows 10-Computer eine Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten.
 - Führen Sie die folgenden Befehle aus.

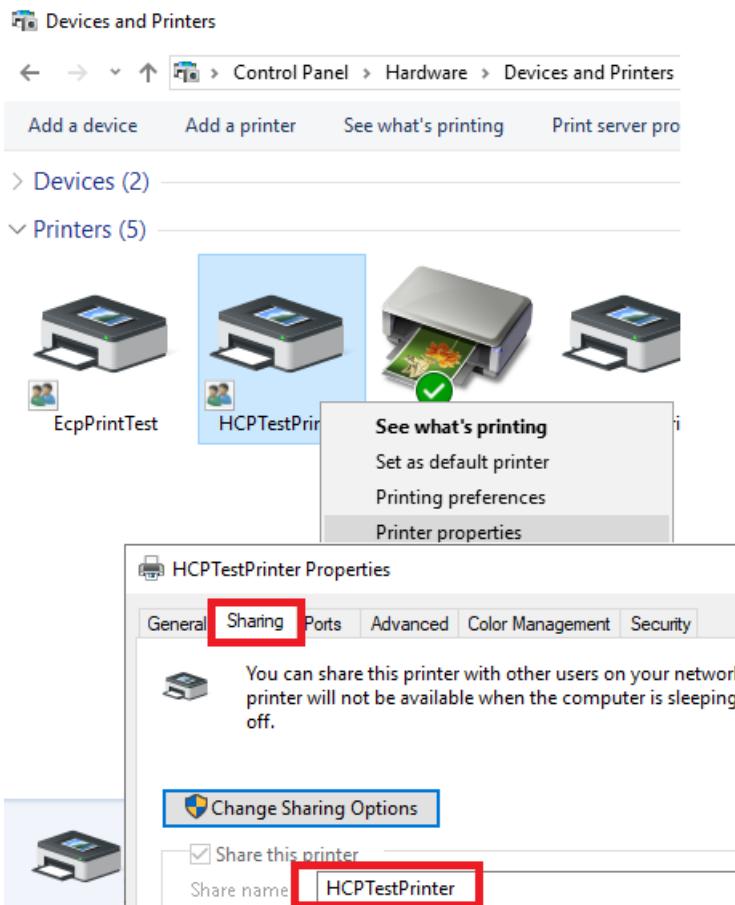
- `find-module -Name PublishCloudPrinter`, um zu bestätigen, dass der Computer die PowerShell-Katalog (psgallery) erreichen kann.

○ `install-module -Name PublishCloudPrinter`

Hinweis: möglicherweise wird ein Messaging angezeigt, das besagt, dass "psgallery" ein nicht vertrauenswürdiges Repository ist. Geben Sie "y" ein, um die Installation fortzusetzen.

○ `Publish-CloudPrinter`

- Printer = der Name des freigegebenen Druckers. Dieser Name muss genau mit dem Freigabe Namen übereinstimmen, der auf der Registerkarte **Freigabe** der Druckereigenschaften angezeigt wird, die auf dem Druck Server geöffnet ist.



- Hersteller = Druckerhersteller.

- Model = Drucker Modell.

- Orgloation = eine JSON-Zeichenfolge, die den Drucker Speicherort angibt, z. b.

```
{ attrs: [{category:country, vs:USA, depth:0}, {category:organization, vs:Microsoft, depth:1}, {category:site, vs:Redmond, WA, depth:2}, {category:building, vs:Building 1, depth:3}, {category:floor_number, vs:1, depth:4}, {category:room_name, vs:1111, depth:5}]} 
```

- SDDL = SDDL-Zeichenfolge, die die Berechtigungen für den Drucker darstellt.

- Melden Sie sich beim Druck Server als Administrator an, und führen Sie dann den folgenden PowerShell-Befehl für den Drucker aus, den Sie veröffentlichen möchten:

`(Get-Printer PrinterName -full).PermissionSDDL`

- Fügen Sie dem Ergebnis aus dem obigen Befehl o:BA als Präfix hinzu. z. B. Wenn die Zeichenfolge, die vom vorherigen Befehl zurückgegeben wurde, g:DUD ist: (A; oici; FA;; WD), dann SDDL = o:Bag: DUD: (A; oici; FA;; WD).

- DiscoveryEndpoint = melden Sie sich bei Azure-Portal an, und erhalten Sie dann die Zeichenfolge aus Unternehmensanwendungen > der mopria Discovery Service-APP > Anwendungs Proxy > externe URL. Lassen Sie das nachfolgende/aus.
- Printserverendpoint = melden Sie sich bei Azure-Portal an, und erhalten Sie dann die Zeichenfolge aus Unternehmensanwendungen > der Unternehmens Cloud-Druck-app > Anwendungs Proxy > externe URL. Lassen Sie das nachfolgende/aus.
- Azureclientid = Anwendungs-ID der registrierten systemeigenen Anwendung.
- Azuretenantguid = Verzeichnis-ID Ihres Azure AD Mandanten.
- Discoveryresourceid = Anwendungs-ID-URI der mopria Discovery Service-Anwendung.
- Sie können auch alle erforderlichen Parameterwerte in der Befehlszeile eingeben. Die Syntax lautet:

```
Publish-CloudPrinter -Printer <string> -Manufacturer <string> -Model <string> -OrgLocation
<string> -Sddl <string> -DiscoveryEndpoint <string> -PrintServerEndpoint <string> -AzureClientId
<string> -AzureTenantGuid <string> -DiscoveryResourceId <string>
```

Beispiel Befehl:

```
Publish-CloudPrinter -Printer HcpTestPrinter -Manufacturer Manufacturer1 -Model Model1 -
OrgLocation '{attrs: [{category:country, vs:USA, depth:0}, {category:organization, vs:MyCompany,
depth:1}, {category:site, vs:MyCity, State, depth:2}, {category:building, vs:Building 1, depth:3},
{category:floor_name, vs:1, depth:4}, {category:room_name, vs:1111, depth:5}]}' -Sddl O:BAG:DUD:
(A;OICI;FA;;;WD) -DiscoveryEndpoint https://mopriadiscoveryservice-contoso.msappproxy.net/mcs -
PrintServerEndpoint https://enterprisecloudprint-contoso.msappproxy.net/ecp -AzureClientId
dbe4feeb-cb69-40fc-91aa-73272f6d8fe1 -AzureTenantGuid 8de6a14a-5a23-4c1c-9ae4-1481ce356034 -
DiscoveryResourceId https://mopriadiscoveryservice-contoso.msappproxy.net/mcs/
```

- Verwenden Sie den folgenden Befehl, um zu überprüfen, ob der Drucker veröffentlicht wurde.

```
Publish-CloudPrinter -Query -DiscoveryEndpoint <string> -AzureClientId <string> -AzureTenantGuid
<string> -DiscoveryResourceId <string>
```

Beispiel Befehl:

```
Publish-CloudPrinter -Query -DiscoveryEndpoint https://mopriadiscoveryservice-
contoso.msappproxy.net/mcs -AzureClientId dbe4feeb-cb69-40fc-91aa-73272f6d8fe1 -AzureTenantGuid
8de6a14a-5a23-4c1c-9ae4-1481ce356034 -DiscoveryResourceId https://mopriadiscoveryservice-
contoso.msappproxy.net/mcs/
```

Überprüfen der Bereitstellung

Auf einem Azure AD eingebundener Gerät, auf dem die MDM-Richtlinien konfiguriert sind:

- Öffnen Sie einen Webbrower, und wechseln Sie zu <https://mopriadiscoveryservice-Tenant-Name.msappproxy.net/MCS/Services>.
- Der JSON-Text, der den Funktions Satz dieses Endpunkts beschreibt, sollte angezeigt werden.
- Wechseln Sie zu **Einstellungen > Geräte > Drucker & Scanner**.
 - Klicken Sie auf **Drucker oder Scanner hinzufügen**.
 - Sie sollten eine Suche nach clouddruckern sehen (oder nach Druckern in meinem Unternehmen auf einem neueren Windows 10-Computer suchen).
 - Klicken Sie auf den Link.
 - Klicken Sie auf den Link Such Speicherort auswählen.
 - Die Hierarchie der Geräte Orte sollte angezeigt werden.
 - Wählen Sie einen Speicherort aus, und klicken Sie auf **OK** und dann auf die Schaltfläche **Suchen**, um die Drucker
 - Wählen Sie Drucker aus, und klicken Sie auf die Schaltfläche
 - Nachdem die Drucker Installation erfolgreich war, können Sie Sie aus Ihrer bevorzugten APP an den Drucker drucken.

Hinweis: Wenn Sie den ecpprinttest-Drucker verwenden, finden Sie die Ausgabedatei auf dem Druck Server Computer unter C:\ecptestoutput\ecptestprint. XPS-Speicherort.

Problembehandlung

Im folgenden sind häufige Probleme bei der HCP-Bereitstellung

ERROR	EMPFOHLENE SCHRITTE
Cloudprintbereitstellungs-PowerShell-Skript fehlgeschlagen	<ul style="list-style-type: none">• Stellen Sie sicher, dass Windows Server das neueste Update aufweist.• Wenn Windows Server Update Services (WSUS) verwendet wird, finden Sie unter Gewusst wie: Bedarfs gesteuerte Features und Sprachpakete bei Verwendung von WSUS/SCCM Weitere Informationen.
Fehler bei der SQLite-Installation mit der folgenden Meldung: Abhängigkeits Schleife für Paket "System. Data. sqlite" erkannt	<p>Install-package System. Data. sqlite. Core-ProviderName nuget-skipdependen</p> <p>Install-package System. Data. sqlite. EF6-ProviderName nuget-skipdependen</p> <p>Install-package System. Data. sqlite. Linq-ProviderName nuget-skipdependen</p> <p>Nachdem die Pakete erfolgreich heruntergeladen wurden, stellen Sie sicher, dass Sie die gleiche Version aufweisen. Wenn dies nicht der Wert ist, fügen Sie den Requirements diversion-Parameter den obigen Befehlen hinzu, und legen Sie diese auf die gleiche Version fest.</p>
Fehler beim Veröffentlichungs Drucker.	<ul style="list-style-type: none">• Stellen Sie für Passthrough-Vorauthentifizierung sicher, dass der Benutzer, der den Drucker veröffentlicht, die richtige Berechtigung für die Veröffentlichungs Datenbank erhält.• Stellen Sie für Azure AD Vorauthentifizierung sicher, dass die Windows-Authentifizierung in IIS aktiviert ist. Siehe Schritt 5,3. Versuchen Sie außerdem, die Passthrough-Vorauthentifizierung zu verwenden. Wenn die Passthrough-Vorauthentifizierung funktioniert, liegt das Problem wahrscheinlich im Zusammenhang mit dem Anwendungs Proxy. Weitere Informationen finden Sie unter Beheben von Problemen mit Anwendungs Proxy und Fehlermeldungen. Beachten Sie, dass der Wechsel zu Passthrough die Single Sign-on Einstellung zurücksetzt. Wiederholen Sie Schritt 5, um die Vorauthentifizierung erneut Azure AD.
Druckaufträge werden in den Drucker Zustand versetzt.	<ul style="list-style-type: none">• Stellen Sie sicher, dass TLS 1,2 auf dem Connector-Server aktiviert ist. Weitere Informationen finden Sie im verknüpften Artikel in Schritt 2,1.• Stellen Sie sicher, dass HTTP2 auf dem Connector-Server deaktiviert ist. Weitere Informationen finden Sie im verknüpften Artikel in Schritt 2,1.

Im folgenden finden Sie Speicherorte von Protokollen zur Problembehandlung.

KOMPONENTE	PROTOKOLL SPEICHERORT
Windows 10-Client	<ul style="list-style-type: none"> • Verwenden Sie Ereignisanzeige, um das Protokoll von Azure AD Vorgängen anzuzeigen. Klicken Sie auf Start, und geben Sie Ereignisanzeige ein. Navigieren Sie zu Anwendungs-und Dienst Protokolle > Microsoft > Windows > Aad-> Vorgang. • Verwenden Sie den Feedback-Hub, um Protokolle zu erfassen. Siehe Senden von Feedback an Microsoft mit der Feedback-Hub-App
Connector-Server	Verwenden Sie Ereignisanzeige, um das Protokoll des Anwendungs Proxys anzuzeigen. Klicken Sie auf Start , und geben Sie Ereignisanzeige ein. Navigieren Sie zu Anwendungs- und Dienst Protokolle > Microsoft > aadapplicationproxy > Connector > admin.
Druckerserver	Die Protokolle für die "mopria Discovery Service"-App und die unternehmenscloud-Druck-App finden Sie unter "c:\inetpub\logs\logfiles\w3svc1.".

Was ist die Server Core-Installationsoption in Windows Server?

22.01.2020 • 6 minutes to read • [Edit Online](#)

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

Bei der Server Core-Option handelt es sich um eine minimale Installationsoption, die verfügbar ist, wenn Sie die Standard- oder Datacenter Edition von Windows Server bereitstellen. Server Core umfasst die meisten, aber nicht alle Server Rollen. Server Core hat einen geringeren Speicherbedarf und somit eine kleinere Angriffsfläche aufgrund einer geringeren Codebasis.

Server (Core) vs-Server mit Desktop Darstellung

Wenn Sie Windows Server installieren, installieren Sie nur die von Ihnen ausgewählten Server Rollen. Dies trägt dazu bei, den Gesamtbedarf für Windows Server zu verringern. Bei der Installationsoption Server mit Desktop Darstellung werden jedoch weiterhin viele Dienste und andere Komponenten installiert, die für ein bestimmtes Verwendungs Szenario häufig nicht benötigt werden.

Dabei kommt Server Core ins Spiel: bei der Server Core-Installation werden alle Dienste und anderen Features eliminiert, die für die Unterstützung bestimmter häufig verwendeter Server Rollen nicht von entscheidender Bedeutung sind. Ein Hyper-v-Server benötigt z. B. keine grafische Benutzeroberfläche (GUI), da Sie praktisch alle Aspekte von Hyper-v entweder über die Befehlszeile mithilfe von Windows PowerShell oder Remote mit dem Hyper-v-Manager verwalten können.

Die Server Core-Differenz-Kern-Funktionen ohne die einfaches

Wenn Sie die Installation von Server Core auf einem System abgeschlossen haben und sich zum ersten Mal anmelden, sind Sie etwas überraschend. Der Hauptunterschied zwischen dem Server und der Desktop Darstellung-Installationsoption und Server Core besteht darin, dass Server Core nicht die folgenden GUI-shellpakete umfasst:

- Microsoft-Windows-Server-Shell-Package
- Microsoft-Windows-Server-GUI-Mgmt-Package
- Microsoft-Windows-Server-GUI-RSAT-Package
- Microsoft-Windows-Cortana-PAL-Desktop-Package

Anders ausgedrückt: Es gibt **keinen Desktop** in Server Core. Wenn Sie die für die Unterstützung herkömmlicher Geschäftsanwendungen und rollenbasierten Workloads erforderlichen Funktionen beibehalten, verfügt Server Core nicht über eine herkömmliche Desktop Schnittstelle. Stattdessen ist Server Core für die Remote Verwaltung über die Befehlszeile, PowerShell oder ein GUI-Tool (wie z. B. RSAT oder [Windows Admin Center](#)) konzipiert.

Neben der Benutzeroberfläche unterscheidet sich auch Server Core vom Server mit Desktop Darstellung wie folgt:

- Server Core verfügt über keine Barrierefreiheits Tools
- Keine OOBE (Out-of-Box-Umgebung) für die Einrichtung von Server Core
- Keine Audiounterstützung

In der folgenden Tabelle sind die Anwendungen aufgeführt, die *lokal*/auf Server Core vs Server mit Desktop Darstellung verfügbar sind. **Wichtig:** In den meisten Fällen können Anwendungen, die unten als "nicht verfügbar" aufgeführt sind, Remote von einem Windows-Client Computer aus ausgeführt und zum Verwalten der Server Core-Installation verwendet werden.

NOTE

Diese Liste ist für kurz Verweise gedacht. Sie ist nicht als umfassende Liste vorgesehen.

APPLICATION	SERVER CORE	SERVER MIT DESKTOPDARSTELLUNG
Eingabeaufforderung	verfügbar	verfügbar
Windows PowerShell/Microsoft .net	verfügbar	verfügbar
Perfmon. exe	nicht verfügbar	verfügbar
WinDbg (GUI)	unterstützt	unterstützt
Resmon. exe	nicht verfügbar	verfügbar
Regedit	verfügbar	verfügbar
"F. exe"	verfügbar	verfügbar
Disksnapshot. exe	nicht verfügbar	verfügbar
Diskpart.exe	verfügbar	verfügbar
Diskmgmt. msc	nicht verfügbar	verfügbar
Devmgmt. msc	nicht verfügbar	verfügbar
Server-Manager	nicht verfügbar	verfügbar
"MMC. exe"	nicht verfügbar	verfügbar
Eventvwr	nicht verfügbar	verfügbar
Wevtutil (Ereignis Abfragen)	verfügbar	verfügbar
Services. msc	nicht verfügbar	verfügbar
Systemsteuerung	nicht verfügbar	verfügbar
Windows Update (GUI)	nicht verfügbar	verfügbar
Windows-Explorer	nicht verfügbar	verfügbar
Taskleiste	nicht verfügbar	verfügbar
Task leisten Benachrichtigungen	nicht verfügbar	verfügbar
Von "taskmgr"	verfügbar	verfügbar
Internet Explorer oder Microsoft Edge	nicht verfügbar	verfügbar

APPLICATION	SERVER CORE	SERVER MIT DESKTOPDARSTELLUNG
Integriertes Hilfesystem	nicht verfügbar	verfügbar
Windows 10 Shell	nicht verfügbar	verfügbar
Windows Media Player	nicht verfügbar	verfügbar
PowerShell	verfügbar	verfügbar
PowerShell ISE	nicht verfügbar	verfügbar
PowerShell-IME	verfügbar	verfügbar
Mstsc. exe	nicht verfügbar	verfügbar
Remotedesktopdienste	verfügbar	verfügbar
Hyper-V-Manager	nicht verfügbar	verfügbar

Weitere Informationen zu den Funktionen von Server Core finden Sie unter [Rollen, Rollen Dienste und Features, die in Windows Server-Server Core enthalten sind](#). Informationen dazu, was nicht in Server Core enthalten *ist*, finden Sie unter [Rollen, Rollen Dienste und Features, die nicht in Server Core enthalten sind](#).

Einstieg in die Verwendung von Server Core

Verwenden Sie die folgenden Informationen, um die Server Core-Installationsoption von Windows Server zu installieren, zu konfigurieren und zu verwalten.

Server Core-Installation:

- [Rollen, Rollen Dienste und Features, die in Server Core enthalten sind](#)
- [Rollen, Rollen Dienste und Features, die nicht in Server Core enthalten sind](#)
- [Installieren der Server Core-Installationsoption](#)
- [Konfigurieren von Server Core mit dem SCONFIG-Tool](#)

Verwenden von Server Core:

- [Grundlegende Server Core-Verwaltungsaufgaben mithilfe von Windows PowerShell oder der Befehlszeile](#)
- [Verwalten von Server Core](#)
- [Patchen von Server Core](#)
- [Konfigurieren von Speicherabbilddateien](#)

Rollen, Rollen Dienste und Features, die in Windows Server-Server Core enthalten sind

02.12.2019 • 11 minutes to read • [Edit Online](#)

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

Im Allgemeinen sprechen wir über **das, was in Server Core *nicht* der Grund** ist: Wir testen nun einen anderen Ansatz und informieren Sie darüber, **was enthalten** ist und ob **standardmäßig etwas installiert** ist. Die folgenden Rollen, Rollen Dienste und Features sind *in* der Server Core-Installationsoption von Windows Server enthalten. Anhand dieser Informationen können Sie herausfinden, ob die Server Core-Option für Ihre Umgebung funktioniert. Da es sich hierbei um eine umfangreiche Liste handelt, sollten Sie die Suche nach der für Sie interessanten Rolle oder dem gewünschten Feature in Erwägung gezogen haben. Wenn diese Suche nicht das gesuchte zurückgibt, ist es nicht in Server Core enthalten.

Wenn Sie z. B. nach "Remotedesktop-Sitzungshost" suchen, wird es auf dieser Seite nicht gefunden. Dies liegt daran, dass der RD-Sitzungshost nicht im Server Core-Image enthalten ist.

Denken Sie daran, dass Sie **immer sehen** können, was *nicht* enthalten ist. Dies ist nur eine andere Möglichkeit, Dinge zu betrachten.

In Server Core enthaltene Rollen

Die Server Core-Installationsoption umfasst die folgenden Server Rollen.

ROLE-EIGENSCHAFT	NAME	STANDARDMÄSSIG INSTALLIERT?
Active Directory-Zertifikatdienste	AD-Zertifikat	N
Active Directory Domain Services	AD-Domain-Services	N
Active Directory-Verbunddienste (AD FS)	AD FS-Verbund	N
Active Directory Lightweight Directory Services	ADLDS	N
Active Directory-Rechteverwaltungsdienste	ADRMS	N
Integritätsnachweis für Geräte	Devicehealthattestationservice	N
DHCP-Server	DHCP	N
DNS-Server	DNS	N
Datei- und Speicherdiensste	Fileandstorage-Dienste	„Y“ zugeordnet ist
Host-Überwachungsdienst	Hostguardianservicerole	N

ROLE-EIGENSCHAFT	NAME	STANDARDMÄSSIG INSTALLIERT?
Hyper-V	Hyper-V	N
Druck- und Dokumentdienste	Druckdienste	N
Remotezugriff	RemoteAccess	N
Remotedesktopdienste	Remote Desktop Services	N
Volumenaktivierungsdienste	VolumeActivation	N
Webserver (IIS)	Web-Server	N
Windows Server Essentials-Umgebung	Serveressentialsrole	N
Windows Server Update Services	Update Services	N

In Server Core enthaltene Rollen Dienste

Die Server Core-Installationsoption umfasst die folgenden Rollen Dienste.

ROLE-EIGENSCHAFT	ROLLENDIENST	NAME	STANDARDMÄSSIG INSTALLIERT?
Active Directory-Zertifikatdienste	Zertifizierungsstelle	ADCS Zertifizierungsstelle	N
	Zertifikatregistrierungsrichtlinien-Webdienst	ADCs-ENROLL-Web-Pol	N
	Zertifikatregistrierungs-Webdienst	ADCs-ENROLL-Web-SVC	N
	Zertifizierungsstellen-Webregistrierung	ADCs-Web-Einschreibung	N
	Registrierungsdienst für Netzwerkgeräte	ADCs-Geräteregistrierung	N
	Online-Responder	ADCs-Online-CERT	N
Active Directory Rights Management	Active Directory-Rechteverwaltungsserver	ADRMS-Server	N
	Unterstützung für Identitätsverbund	ADRMS-Identity	N
Datei- und Speicherdiensste	Datei- und iSCSI-Dienste	Dateidienste	N
	Dateiserver	EA-Dateiserver	N
	BranchCache für Netzwerkdateien	FS-BranchCache	N

ROLE-EIGENSCHAFT	ROLLENDIENST	NAME	STANDARDMÄSSIG INSTALLIERT?
	Datendeduplizierung	FS-Datendeduplizierung	N
	DFS-Namespace	FS-DFS-Namespace	N
	DFS-Replikation	FS-DFS-Replikation	N
	Ressourcen-Manager für Dateiserver	FS-Resource-Manager	N
	Dateiserver-VSS-Agent-Dienst	EA-VSS-Agent	N
	iSCSI-Zielserver	iscsitarget-Server	N
	iSCSI-Zielspeicher Anbieter (VDS- und VSS-Hardware Anbieter)	iscsitarget-VSS-VDS	N
	Server für NFS	FS-NFS-Dienst	N
	Arbeitsordner	FS-syncshareservice	N
	Speicherdiene	Speicherdiene	„Y“ zugeordnet ist
Druck- und Dokumentdienste	Druckerserver	Druck Server	N
	LPD-Dienst	Print-LPD-Service	N
Remotezugriff	DirectAccess und VPN (RAS)	DirectAccess-VPN	N
	Routing	Routing	N
	Webanwendungsproxy	Webanwendungsproxy	N
Remotedesktopdienste	Remotedesktop-Verbindungsbroker	RDS-Connection-Broker	N
	Remotedesktoplizenzierung	RDS-Lizenzierung	N
	Remotedesktop-Virtualisierungshost	RDS-Virtualisierung	N
Webserver (IIS)	Webserver	Web-WebServer	N
	Allgemeine HTTP-Features	Web-Common-Http	N
	Standarddokument	Web-Default-Doc	N
	Verzeichnissuche	Web-Dir-Browsing	N

ROLE-EIGENSCHAFT	ROLLENDIENST	NAME	STANDARDMÄSSIG INSTALLIERT?
	HTTP-Fehler	Web-Http-Fehler	N
	Statischer Inhalt	Statische Webinhalte	N
	HTTP-Umleitung	Web-Http-Umleitung	N
	WebDAV-Veröffentlichung	DAV-Webpublishing	N
	Integrität und Diagnose	Web-Integrität	N
	HTTP-Protokollierung	Web-Http-Protokollierung	N
	Benutzerdefinierte Protokollierung	Web-Custom-Protokollierung	N
	Protokollierungs Tools	Web-Log-Libraries	N
	ODBC-Protokollierung	Web-ODBC-Protokollierung	N
	Anforderungs Monitor	Web-Request-Monitor	N
	Ablaufverfolgung	Web-http-Ablauf Verfolgung	N
	Leistung	Leistung des Webservers	N
	Komprimierung statischer Inhalte	Web-Stat-Compression	N
	Komprimierung dynamischer Inhalte	Web-Dyn-Komprimierung	N
	Sicherheit	Web-Sicherheit	N
	Request Filtering	Web-Filterung	N
	Standardauthentifizierung	Web-Basic-Auth	N
	Zentralisierte SSL-Zertifikat Unterstützung	Web-CertProvider	N
	Authentifizierung mit Client Zertifikat Zuordnung	Web-Client-Authentifizierung	N
	Digestauthentifizierung	Web-Digest-Authentifizierung	N
	Authentifizierung von IIS-Client Zertifikat Zuordnung	Web-Cert-Auth	N
	IP-und Domänen Einschränkungen	Web-IP-Sicherheit	N

ROLE-EIGENSCHAFT	ROLLENDIENST	NAME	STANDARDMÄSSIG INSTALLIERT?
	URL-Autorisierung	Web-Url-Auth	N
	Windows-Authentifizierung	Web-Windows-Authentifizierung	N
	Anwendungsentwicklung	Web-App-Entwickler	N
	.NET-Erweiterbarkeit 3,5	Web-net-ext	N
	.NET-Erweiterbarkeit 4,6	Web-net-Ext45	N
	Anwendungsinitialisierung	Web-AppInit	N
	ASP	Web-ASP	N
	ASP.NET 3,5	Web-ASP-NET	N
	ASP.NET 4.6	Web-ASP-.Net45	N
	CGI	Web-CGI	N
	ISAPI-Erweiterungen	Web-ISAPI-Erweiterung	N
	ISAPI Filters	Web-ISAPI-Filter	N
	Serverseitige Includes (SSI)	Web enthält	N
	WebSocket-Protokoll	Web-WebSockets	N
	FTP-Server	Web-FTP-Server	N
	FTP-Dienst	Web-FTP-Dienst	N
	FTP-Erweiterbarkeit	Web-FTP-ext	N
	Verwaltungstools	Web-Mgmt-Tools	N
	Kompatibilität mit der IIS 6-Verwaltung	Web-Mgmt-Anwendungskompatibilität	N
	IIS 6-Metabasiskompatibilität	Web-Metabasis	N
	IIS 6-Skript Tools	Web-Igcy-Scripting	N
	IIS 6-WMI-Kompatibilität	Web-WMI	N
	IIS-Verwaltungsskripts und -tools	Web-Scripting-Tools	N

ROLE-EIGENSCHAFT	ROLLENDIENST	NAME	STANDARDMÄSSIG INSTALLIERT?
	Verwaltungsdienst	Web-Mgmt-Dienst	N
Windows Server Update Services	WID-Konnektivität	Updateservices-widdb	N
	WSUS-Dienste	Updateservices-Dienste	N
	SQL Server Konnektivität	Updateservices-DB	N

In Server Core enthaltene Features

Die Server Core-Installationsoption umfasst die folgenden Features.

FEATURE	NAME	STANDARDMÄSSIG INSTALLIERT?
.NET Framework 3,5-Features	NET-Framework-Features	N
.NET Framework 3,5 (einschließlich .NET 2,0 und 3,0)	NET-Framework-Core	gestrichen
HTTP-Aktivierung	NET-HTTP-Aktivierung	N
Nicht-HTTP-Aktivierung	Nicht-http-aktiv	N
.NET Framework 4,6-Features	NET-Framework-45-Features	„Y“ zugeordnet ist
.NET Framework 4,6	NET-Framework-45-Core	„Y“ zugeordnet ist
ASP.NET 4,6	NET-Framework-45-ASPNET	N
WCF-Dienste	NET-WCF-Services45	„Y“ zugeordnet ist
HTTP-Aktivierung	NET-WCF-HTTP-Activation45	N
Message Queuing Aktivierung (MSMQ)	NET-WCF-MSMQ-Activation45	N
Named Pipe-Aktivierung	NET-WCF-Pipe-Activation45	N
TCP-Aktivierung	NET-WCF-TCP-Activation45	N
TCP-Port Freigabe	NET-WCF-TCP-PortSharing45	„Y“ zugeordnet ist
BITS (Background Intelligent Transfer Service, Intelligenter Hintergrundübertragungsdienst)	BITS	N
Compact Server	BITS-Compact-Server	N
BitLocker-Laufwerkverschlüsselung	BitLocker	N

FEATURE	NAME	STANDARDMÄSSIG INSTALLIERT?
BranchCache	BranchCache	N
Client für NFS	NFS-Client	N
Container	Container	N
Data Center Bridging	Data-Center-Bridging	N
Erweitertes Speichern	EnhancedStorage	N
Failoverclustering	Failover-Clustering	N
Gruppenrichtlinienverwaltung	GPMC	N
E/A: Quality of Service (QoS, Dienstqualität)	Diskio-QoS	N
Hostfähiger IIS-Webkern	Web-WHC	N
IP-Adressverwaltungsserver (IPAM-Server)	IPAM	N
iSNS-Serverdienst	ISNS	N
IIS-Erweiterung für OData Services for Management	Managementodata	N
Media Foundation	Server-Media-Foundation	N
Message Queuing	MSMQ	N
Message Queuing Dienste	MSMQ-Dienste	N
Message Queuing Server	MSMQ-Server	N
Verzeichnisdienstintegration	MSMQ-Verzeichnis	N
HTTP-Unterstützung	MSMQ-HTTP-Unterstützung	N
Message Queuing Trigger	MSMQ-Trigger	N
Routing Dienst	MSMQ-Routing	N
Message Queuing-DCOM-Proxy	MSMQ-DCOM	N
Multipfad-E/A	Multipfad-e/a	N
MultiPoint-Connector	Multipoint-Connector	N
Multipoint-Connector-Dienste	Multipoint-Connector-Dienste	N

FEATURE	NAME	STANDARDMÄSSIG INSTALLIERT?
Multipoint-Manager und Multipoint-Dashboard	Multipoint-Tools	N
Netzwerklastenausgleich	NLB	N
Peer Name Resolution-Protokoll	PNRP	N
Verbessertes Audio-/Videostreaming unter Windows	qWave	N
RDC (Remote Differential Compression)	RDC	N
Remoteserver-Verwaltungstools	RSAT	N
Verwaltungs Tools für Funktionen	RSAT-Feature-Tools	N
BitLocker-Laufwerkverschlüsselung Verwaltungs Dienstprogramme	RSAT-Feature-Tools-BitLocker	N
Datacenterbridging LLDP-Tools	RSAT-datacenterbridging-LLDP-Tools	N
Failoverclusteringtools	RSAT-Clustering	N
Failoverclustermodul für Windows PowerShell	RSAT-Clustering-PowerShell	N
Failovercluster-Automatisierungs Server	RSAT-Clustering-automationserver umgewandelt	N
Failovercluster-Befehlschnittstelle	RSAT-Clustering-CmdInterface	N
IP-Adressverwaltung (IPAM)-Client	IPAM-Client-Feature	N
Abgeschirmte VM-Tools	RSAT-abgeschirmt-VM-Tools	N
Speicher Replikat Modul für Windows PowerShell	RSAT-Speicher Replikat	N
Rollenverwaltungstools	RSAT-Rollen Tools	N
AD DS- und AD LDS-Tools	RSAT-AD-Tools	N
Active Directory-Modul für Windows PowerShell	RSAT-AD-PowerShell	N
AD DS-Tools	REMOTESERVER-VERWALTUNGSTOOLS WIRD HINZUGEFÜGT	N
Active Directory-Verwaltungscenter	RSAT-AD-AdminCenter	N
AD DS-Snap-Ins und -Befehlszeilentools	RSAT-fügt-Tools	N

FEATURE	NAME	STANDARDMÄSSIG INSTALLIERT?
AD LDS Snap-Ins und Befehlszeilen Tools	RSAT-ADLDS	N
Hyper-V-Verwaltungstools	RSAT-Hyper-V-Tools	N
Hyper-V-Modul für Windows PowerShell	Hyper-V-PowerShell	N
Windows Server Update Services Tools	Updateservices-RSAT	N
API-und PowerShell-Cmdlets	UpdateServices-API	N
DHCP-Server Tools	RSAT-DHCP	N
DNS-Server Tools	RSAT-DNS-Server	N
Tools für die Remote Zugriffs Verwaltung	RSAT-remoteaccess	N
RAS-Modul für Windows PowerShell	RSAT-remoteaccess-PowerShell	N
RPC über HTTP-Proxy	RPC-über-HTTP-Proxy	N
Ereignissammlung für Setup und Start	Setup-und-Boot-Event-Collection	N
Einfache TCP/IP-Dienste	Simple-tcpip	N
SMB 1.0-/CIFS- Dateifreigabeunterstützung	FS-SERVER MESSAGE BLOCK	„Y“ zugeordnet ist
SMB-Bandbreiteneinschränkung	EA-SMBBW	N
SNMP-Dienst	SNMP-Dienst	N
SNMP-WMI-Anbieter	SNMP-WMI-Provider	N
Telnet-Client	Telnet-Client	N
VM-Abschirmungstools für Fabric- Verwaltung	Fabricshieldedtools	N
Windows Defender-Features	Windows-Defender-Features	„Y“ zugeordnet ist
Windows Defender	Windows-Defender	„Y“ zugeordnet ist
Interne Windows-Datenbank	Interne Windows-Datenbank	N
Windows PowerShell	Powershellroot	„Y“ zugeordnet ist
Windows PowerShell 5,1	PowerShell	„Y“ zugeordnet ist

FEATURE	NAME	STANDARDMÄSSIG INSTALLIERT?
Windows PowerShell 2,0-Engine	PowerShell-v2	gestrichen
Windows PowerShell-Dienst zum Konfigurieren des gewünschten Zustands	DSC-Dienst	N
Windows PowerShell Web Access	WindowsPowerShellWebAccess	N
Windows-Prozessaktivierungsdienst	WURDE	N
Prozessmodell	WAR-Prozessmodell	N
.NET-Umgebung 3,5	Was-NET-Umgebung	N
Konfigurations-APIs	WAR-Config-APIs	N
Windows Server-Sicherung	Windows Server-Sicherung	N
Windows Server-Migrationstools	Migration	N
Standardbasierte Windows-Speicherverwaltung	Windowsstoragemanagementservice	N
WinRM-IIS-Erweiterung	WinRM-IIS-ext	N
WINS-Server	WINS	N
WOW64-Unterstützung	WOW64-Unterstützung	„Y“ zugeordnet ist

Verwalten eines Server Core-Servers

18.01.2020 • 16 minutes to read • [Edit Online](#)

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

Da Server Core nicht über eine Benutzeroberfläche verfügt, müssen Sie Windows PowerShell-Cmdlets, Befehlszeilen Tools oder Remote Tools verwenden, um grundlegende Verwaltungsaufgaben auszuführen. In den folgenden Abschnitten werden die PowerShell-Cmdlets und-Befehle für grundlegende Aufgaben erläutert. Sie können auch das [Windows Admin Center](#), ein einheitliches Verwaltungs Portal, das sich zurzeit in der öffentlichen Vorschau befindet, zum Verwalten Ihrer-Installation verwenden.

Administrative Aufgaben mithilfe von PowerShell-Cmdlets

Verwenden Sie die folgenden Informationen, um grundlegende administrative Aufgaben mit Windows PowerShell-Cmdlets auszuführen.

Festlegen einer statischen IP-Adresse

Wenn Sie einen Server Core-Server installieren, verfügt er standardmäßig über eine DHCP-Adresse. Wenn Sie eine statische IP-Adresse benötigen, können Sie Sie mithilfe der folgenden Schritte festlegen.

Verwenden Sie **Get-nettipconfiguration**, um die aktuelle Netzwerkkonfiguration anzuzeigen.

Verwenden Sie **Get-nettipaddress**, um die bereits verwendeten IP-Adressen anzuzeigen.

Gehen Sie folgendermaßen vor, um eine statische IP-Adresse festzulegen:

1. Führen Sie **Get-nettipinterfaceaus**.
2. Notieren Sie sich die Zahl in der **ifindex** -Spalte für Ihre IP-Schnittstelle oder die **interfacedescription** -Zeichenfolge. Wenn Sie über mehrere Netzwerkadapter verfügen, notieren Sie sich die Anzahl oder Zeichenfolge, die der Schnittstelle entspricht, für die Sie die statische IP-Adresse festlegen möchten.
3. Führen Sie das folgende Cmdlet aus, um die statische IP-Adresse festzulegen:

```
New-NetIPAddress -InterfaceIndex 12 -IPAddress 192.0.2.2 -PrefixLength 24 -DefaultGateway 192.0.2.1
```

Dabei gilt Folgendes:

- **InterfaceIndex** ist der Wert von **ifindex** aus Schritt 2. (In unserem Beispiel 12)
- **IPAddress** ist die statische IP-Adresse, die Sie festlegen möchten. (In unserem Beispiel 191.0.2.2)
- **Prefixlength** ist die Präfix Länge (eine andere Form der Subnetzmaske) für die IP-Adresse, die Sie festlegen. (In unserem Beispiel 24)
- **DefaultGateway** ist die IP-Adresse des Standard Gateways. (In unserem Beispiel 192.0.2.1)

4. Führen Sie das folgende Cmdlet aus, um die DNS-Client Server Adresse festzulegen:

```
Set-DNSClientServerAddress -InterfaceIndex 12 -ServerAddresses 192.0.2.4
```

Dabei gilt Folgendes:

- **InterfaceIndex** ist der Wert von **ifindex** aus Schritt 2.
- **ServerAddress** ist die IP-Adresse Ihres DNS-Servers.

5. Wenn Sie mehrere DNS-Server hinzufügen möchten, führen Sie das folgende Cmdlet aus:

```
Set-DNSClientServerAddress -InterfaceIndex 12 -ServerAddresses 192.0.2.4,192.0.2.5
```

Dabei sind in diesem Beispiel **sind 192.0.2.4 und 192.0.2.5** beide IP-Adressen von DNS-Servern.

Wenn Sie zur Verwendung von DHCP wechseln müssen, führen Sie **Set-dnsclientserveraddress – interfakeindex 12 – resetserveraddressaus**.

Beitreten zu einer Domäne

Verwenden Sie die folgenden Cmdlets, um einen Computer einer Domäne hinzuzufügen.

1. Führen Sie **Add-Computeraus**. Sie werden aufgefordert, beide Anmelde Informationen für den Beitritt zur Domäne und den Domänen Namen einzugeben.
2. Wenn Sie ein Domänen Benutzerkonto zur lokalen Administrator Gruppe hinzufügen müssen, führen Sie den folgenden Befehl an einer Eingabeaufforderung aus (nicht im PowerShell-Fenster):

```
net localgroup administrators /add <DomainName>\<UserName>
```

3. Starten Sie den Computer neu. Führen Sie hierzu **Restart-Computeraus**.

Umbenennen des Servers

Führen Sie die folgenden Schritte aus, um den Server umzubenennen.

1. Ermitteln Sie mit dem Befehl **hostname** oder **ipconfig** den aktuellen Namen des Servers.
2. Führen Sie **Rename-Computer-Computername <new_name>** aus.
3. Starten Sie den Computer neu.

Aktivieren des Servers

Führen Sie **sImgr. VSB – IPK<ProductKey>** aus. Führen Sie dann **sImgr. VSB – ATOaus**. Wenn die Aktivierung erfolgreich ist, erhalten Sie keine Nachricht.

NOTE

Sie können den Server auch per Telefon aktivieren, indem Sie einen **KMS-Server (Key Management Service)** oder Remote verwenden. Um Remote zu aktivieren, führen Sie das folgende Cmdlet auf einem Remote Computer aus:

```
cscript windows\system32\sImgr.vbs <ServerName> <UserName> <password>:-ato
```

Konfigurieren der Windows-Firewall

Die Windows-Firewall können Sie lokal auf dem Server Core-Computer mithilfe von Windows PowerShell-Cmdlets und -Skripts konfigurieren. Weitere Informationen finden Sie unter **Netsecurity** für die Cmdlets, mit denen Sie die Windows-Firewall konfigurieren können.

Aktivieren von Windows PowerShell-Remoting

Wenn Sie Windows PowerShell-Remoting aktivieren, werden in Windows PowerShell auf einem Computer eingegebene Befehle auf einem anderen Computer ausgeführt. Aktivieren Sie Windows PowerShell-Remoting mit **enable-psremoting**.

Weitere Informationen finden Sie unter Informationen zu **Remote-FAQ**.

Verwaltungsaufgaben über die Befehlszeile

Verwenden Sie die folgenden Referenzinformationen, um Verwaltungsaufgaben über die Befehlszeile auszuführen.

Konfiguration und Installation

AUFGABE	BEFEHL
Festlegen des lokalen Administratorkennworts	net-Benutzer Administrator *
Fügt einen Computer einer Domäne hinzu	netdom Join% Computername% /Domain: <Domäne>/userd:<Domäne\username>/passwordd: * Starten Sie den Computer neu.
Bestätigen, dass die Domäne geändert wurde	set
Entfernen eines Computer aus einer Domäne	netdom Remove <Computername>
Hinzufügen eines Benutzers zur lokalen Gruppe "Administratoren"	net localgroup-Administratoren/Add <Domäne\Benutzername>
Entfernen eines Benutzers aus der lokalen Gruppe "Administratoren"	net localgroup-Administratoren/DELETE <Domäne\Benutzername>
Hinzufügen eines Benutzers zum lokalen Computer	NET User <Domäne \ Benutzername> */Add
Hinzufügen einer Gruppe zum lokalen Computer	net localgroup <Gruppenname>/Add
Ändern des Namens eines Computers, der einer Domäne angehört	netdom-renamecomputer "% Computername%/newname:<neuer Computername>/userd:<Domäne\Benutzername>/passwordd: *
Bestätigen des neuen Computernamens	set
Ändern des Namens eines Computers in einer Arbeitsgruppe	netdom renamecomputer <currentcomputername>/newname:<newcomputername> Starten Sie den Computer neu.
Deaktivieren der Verwaltung von Auslagerungsdateien	WMIC Computersystem WHERE Name = "<Computername>" Set AutomaticManagedPagefile = False
Konfigurieren der Auslagerungsdatei	WMIC pagefileset WHERE Name = "<Pfad/Dateiname>" Set InitialSize =<InitialSize>, MaximumSize = <MaxSize> Dabei ist <i>Pfad/Dateiname</i> der Pfad und Name der Auslagerungs Datei, <i>InitialSize</i> ist die Anfangs Größe der Auslagerungs Datei in Bytes, und <i>MaxSize</i> ist die maximale Größe der Auslagerungs Datei (in Bytes).

AUFGABE	BEEFEHL
Wechseln zu einer statischen IP-Adresse	<p>ipconfig/all</p> <p>Notieren Sie die relevanten Informationen, oder leiten Sie Sie in eine Textdatei (ipconfig/all > ipconfig.txt) um.</p> <p>Netsh Interface IPv4 Show Interfaces</p> <p>Überprüfen Sie, ob eine Schnittstellen Liste vorhanden ist.</p> <p>Netsh Interface IPv4 set address <Name ID from Interface List> source = static address =<bevorzugte IP-Adresse> Gateway =<Gateway-Adresse></p> <p>Führen Sie ipconfig/all aus, um sicherzustellen, dass DHCP aktiviert auf Neinfestgelegt ist.</p>
Legen Sie eine statische DNS-Adresse fest.	<p>Netsh Interface IPv4 Add DNSServer Name =<Name oder ID der Netzwerkschnittstellenkarte> Address = <IP-Adresse des primären DNS-Servers> Index = 1</p> <p>Netsh Interface IPv4 Add DNSServer Name =<Name des sekundären DNS-Servers> Address =<IP-Adresse des sekundären DNS-Servers> Index = 2**</p> <p>Wiederholen Sie den Vorgang, um weitere Server hinzuzufügen.</p> <p>Führen Sie ipconfig/all aus, um zu überprüfen, ob die Adressen korrekt sind.</p>
Wechseln von einer statischen IP-Adresse zu einer von DHCP bereitgestellten IP-Adresse	<p>Netsh Interface IPv4 set address Name =<IP-Adresse des lokalen Systems> Quelle = DHCP</p> <p>Führen Sie ipconfig/all aus, um zu überprüfen, ob DHCP aktiviert auf Jafestgelegt ist.</p>
Eingeben eines Product Keys	slmgr. VSB – IPK-<Product Key>
Lokales Aktivieren des Servers	slmgr. VSB-ATO
Remotes Aktivieren des Servers	<p>cscript slmgr. VSB – IPK <Product Key> <Servername> <Benutzername> <Kennwort></p> <p>cscript slmgr. vb-ATO <Servername> <username> <Password></p> <p>Holen Sie sich die GUID des Computers durch Ausführen von cscript slmgr. VSB-did</p> <p>Führen Sie cscript slmgr. VSB-DLI <GUID aus></p> <p>Vergewissern Sie sich, dass der Lizenzstatus auf lizenziert (aktiviert) festgelegt ist.</p>

Netzwerk und Firewall

AUFGABE	BEEFEHL
Konfigurieren des Servers für die Verwendung eines Proxy Servers	<p>Netsh WinHTTP Set Proxy <Servername>: <Portnummer></p> <p>Hinweis: Server Core-Installationen können nicht über einen Proxy auf das Internet zugreifen, das ein Kennwort erfordert, um Verbindungen zuzulassen.</p>
Konfigurieren Sie den Server so, dass der Proxy für Internet Adressen umgangan wird.	Netsh WinHTTP Set Proxy <Servername>: <Portnummer> Bypass-List = "<local>"
Anzeigen oder Ändern der IPSec-Konfiguration	Netsh IPSec
Anzeigen oder Ändern der NAP-Konfiguration	netsh nap

AUFGABE	BEFEHL
Anzeigen oder Ändern der IP-Adresse für die physische Adressübersetzung	arp
Anzeigen oder Konfigurieren der lokalen Routing Tabelle	route
Anzeigen oder Konfigurieren von DNS-Servereinstellungen	nslookup
Anzeigen von Protokollstatistiken und von aktuellen TCP/IP-Netzwerkverbindungen	netstat
Anzeigen von Protokoll Statistiken und aktuellen TCP/IP-Verbindungen unter Verwendung von NetBIOS über TCP/IP (NBT)	nbtstat
Anzeigen von Hops für Netzwerkverbindungen	pathping
Ablaufverfolgungs-Hops für Netzwerkverbindungen	tracert
Anzeigen der Konfiguration des Multicastrouters	mrinfo
Aktivieren der Remote Verwaltung der Firewall	netsh advfirewall firewall set rule Group = "Windows Defender Firewall Remote Management" New enable = yes

Updates, Fehlerberichterstattung und Feedback

AUFGABE	BEFEHL
Installieren eines Updates	WUS <Update>. msu/quiet
Auflisten von installierten Updates	systeminfo
Entfernen eines Updates	Erweitern Sie/f:* <Update>. msu c:\test Navigieren Sie zu "" c\test\ "", und öffnen Sie <Update>. XML in einem Text-Editor. Ersetzen Sie install with Remove , und speichern Sie die Datei. pkgmgr/n:<Update>. XML
Konfigurieren von automatischen Updates	So überprüfen Sie die aktuelle Einstellung: cscript%systemroot%\system32\scregedit.wsf/au/v ** , um automatische Updates zu aktivieren: ** cscript scregedit. wsf/au 4 So deaktivieren Sie automatische Updates: cscript%systemroot%\system32\scregedit.wsf/au 1
Aktivieren der Fehlerberichterstattung	So überprüfen Sie die aktuelle Einstellung: serverweroptin/Query "aus So senden Sie automatisch ausführliche Berichte: serverweroptin/detailed So senden Sie automatisch Zusammenfassungs Berichte: serverweroptin/Summary So deaktivieren Sie die Fehlerberichterstattung: serverweroptin/Disable

AUFGABE	BEFEHL
Teilnehmen am Programm zur Verbesserung der Benutzerfreundlichkeit	So überprüfen Sie die aktuelle Einstellung: serverceipoptin/Query "aus" So aktivieren Sie CEIP: serverceipoptin/enable So deaktivieren Sie CEIP: serverceipoptin/Disable

Dienste, Prozesse und Leistung

AUFGABE	BEFEHL
Auflisten der laufenden Dienste	SC-Abfrage oder net Start
Starten eines Diensts	SC Start <Dienst Name> oder net Start <Dienst Name>
Beenden eines Diensts	SC beendet <Dienst Name> oder net- <Dienst Name>
Abrufen einer Liste mit ausgeführten Anwendungen und zugehörigen Prozessen	tasklist
Starten des Task-Managers	von "taskmgr
Erstellen und Verwalten von Ereignis Ablauf Verfolgungs Sitzungen und Leistungs Protokollen	So erstellen Sie einen Counter, eine Ablauf Verfolgung, eine Sammlung von Konfigurationsdaten oder eine API: logman erstellen So Fragen Sie die Datensammler Eigenschaften ab: Logman Query So starten oder starten Sie die Datensammlung: logman startet Beendigung So löschen Sie einen Collector: logman delete So aktualisieren Sie die Eigenschaften eines Sammlers: logman update So importieren Sie einen Datensammler Satz aus einer XML-Datei oder exportieren ihn in eine XML-Datei: logman Import Export

Ereignisprotokolle

AUFGABE	BEFEHL
Auflisten von Ereignisprotokollen	wvtutil El
Ereignisse in einem angegebenen Protokoll Abfragen	wvtutil QE/f: Text <Protokoll Name>
Exportieren eines Ereignis Protokolls	wvtutil EPL <Protokoll Name>
Löschen eines Ereignis Protokolls	wvtutil cl <Protokoll Name>

Datenträger- und Dateisystem

AUFGABE	BEFEHL
Verwalten von Datenträgerpartitionen	Führen Sie DiskPart/? aus, um eine komplette Liste der Befehle zu erhalten.

AUFGABE	BEFEHL
Verwalten von Software-RAID	Führen Sie Diskraid/? aus, um eine komplette Liste der Befehle zu erhalten.
Verwalten von Volumebereitstellungspunkten	Eine komplette Liste der Befehle erhalten Sie, wenn Sie " mountvol/? " ausführen.
Defragmentieren eines Volumes	Führen Sie Defragmentierung/? aus, um eine komplette Liste der Befehle zu erhalten.
Konvertieren eines Volumes in das NTFS-Dateisystem	Konvertieren <Volumebuchstaben>/FS: NTFS
Komprimieren einer Datei	Führen Sie Compact/? aus, um eine komplette Liste der Befehle zu erhalten.
Verwalten geöffneter Dateien	Führen Sie openfiles/? aus, um eine komplette Liste der Befehle zu erhalten.
Verwalten von VSS-Ordnern	Führen Sie vssadmin/? aus, um eine komplette Liste der Befehle zu erhalten.
Verwalten des Dateisystems	Führen Sie für eine komplette Liste der Befehle den Befehl "f" aus.
Übernehmen des Besitzes für eine Datei oder einen Ordner	Führen Sie icacls/? aus, um eine komplette Liste der Befehle zu erhalten.

Hardware

AUFGABE	BEFEHL
Hinzufügen eines Treibers für ein neues Hardwaregerät	Kopieren Sie den Treiber in einen Ordner unter %HOMEDRIVE%\<Treiber Ordner>. Führen Sie "PnPUtil-i-a%HOMEDRIVE%\<Treiber Ordner>\<Treiber>.inf" aus.
Entfernen eines Treibers für ein Hardwaregerät	Um eine Liste geladener Treiber zu erhalten, führen Sie SC Query Type = Driver aus. Führen Sie dann SC DELETE <SERVICE_NAME aus>

Verwalten eines Server Core-Servers

02.12.2019 • 11 minutes to read • [Edit Online](#)

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

Sie können einen Server Core-Server wie folgt verwalten:

- Verwenden des [Windows Admin Centers](#)
- Verwenden von [Remoteserver-Verwaltungstools](#), die unter Windows 10 ausgeführt werden
- Lokal und remote mit Windows PowerShell
- Remote Verwendung [Server-Manager](#)
- Remote mit einem [MMC-Snap-in](#)
- Remote mit [Remotedesktopdienste](#)

Sie können auch Hardware hinzufügen und Treiber lokal verwalten, solange Sie dies über die Befehlszeile ausführen.

Beim Arbeiten mit Server Core sind einige wichtige Einschränkungen und Tipps zu beachten:

- Wenn Sie alle Eingabe Aufforderungs Fenster schließen und ein neues Eingabe Aufforderungs Fenster öffnen möchten, können Sie dies über den Task-Manager tun. Drücken Sie **STRG + alt + löschen**, klicken Sie auf **Task-Manager starten**, klicken Sie auf **Weitere Details > Datei > Ausführen**, und geben Sie dann **cmd. exeein**. (Geben Sie " **PowerShell. exe** " ein, um ein PowerShell-Befehlsfenster zu öffnen.) Alternativ können Sie sich abmelden und dann wieder anmelden.
- Befehle oder Tools, die versuchen, Windows Explorer zu öffnen, funktionieren nicht. Beispiel: Ausführung von **starten. an** einer Eingabeaufforderung funktioniert nicht.
- Das HTML-Rendering oder die HTML-Hilfe in Server Core wird nicht unterstützt.
- Server Core unterstützt Windows Installer im stillen Modus, sodass Sie Tools und Hilfsprogramme aus Windows Installer Dateien installieren können. Verwenden Sie bei der Installation von Windows Installer-Paketen auf Server Core die **/qb** -Option, um die grundlegende Benutzeroberfläche anzuzeigen.
- Um die Zeitzone zu ändern, führen Sie **Set-Dateaus**.
- Um internationale Einstellungen zu ändern, führen Sie **Control Intl. cplaus**.
- " **Control. exe** " wird nicht selbst ausgeführt. Sie müssen ihn entweder mit " **timedate. cpl** " oder " **Intl. cpl** " ausführen.
- " **Winver. exe** " ist in Server Core nicht verfügbar. Verwenden Sie zum Abrufen von Versionsinformationen **Systeminfo. exe**.

Verwalten von Server Core mit Windows Admin Center

[Windows Admin Center](#) ist eine browserbasierte Management-App, die die lokale Verwaltung von Windows-Servern ohne Abhängigkeit von Azure oder der Cloud ermöglicht. Windows Admin Center ermöglicht die vollständige Kontrolle über alle Aspekte der Server-Infrastruktur und ist besonders nützlich für die Verwaltung auf privaten Netzwerken, die nicht mit dem Internet verbunden sind. Sie können Windows Admin Center unter Windows 10, auf einem Gatewayserver oder auf einer Installation von Windows Server mit Desktop Darstellung installieren und dann eine Verbindung mit dem Server Core-System herstellen, das Sie verwalten möchten.

Remote Verwaltung von Server Core mit Server-Manager

Server-Manager ist eine Verwaltungskonsole in Windows Server, mit der Sie lokale Windows-basierte Server und Remote Server von ihren Desktops aus bereitstellen und verwalten können, ohne dass Sie physischen Zugriff auf die Server benötigen oder Remotedesktop Protokoll (RDP) aktivieren müssen. Verbindungen mit den einzelnen Servern. Server-Manager unterstützt die Remote Verwaltung von mehreren Servern.

Damit Ihr lokaler Server durch Server-Manager auf einem Remote Server verwaltet werden kann, führen Sie das Windows PowerShell-Cmdlet **configure-SMRemoting.exe – enableaus**.

Verwalten mit Microsoft Management Console

Sie können viele Snap-Ins für Microsoft Management Console (MMC) Remote verwenden, um Ihren Server Core-Server zu verwalten.

So verwenden Sie ein MMC-Snap-in zum Verwalten eines Server Core-Servers, der ein Domänen Mitglied ist:

1. Starten Sie ein MMC-Snap-in, z. b. Computer Verwaltung.
2. Klicken Sie mit der rechten Maustaste auf das Snap-in, und klicken Sie dann auf **Verbindung mit anderem Computer herstellen**.
3. Geben Sie den Computernamen des Server Core-Servers ein, und klicken Sie dann auf OK. Nun können Sie das MMC-Snap-in verwenden, um den Server Core-Server wie jeden anderen PC oder Server zu verwalten.

So verwenden Sie ein MMC-Snap-in zum Verwalten eines Server Core-Servers, der *kein* Domänen Mitglied ist:

1. Richten Sie alternative Anmelde Informationen für die Verbindung mit dem Server Core-Computer ein, indem Sie den folgenden Befehl an einer Eingabeaufforderung auf dem Remote Computer eingeben:

```
cmdkey /add:<ServerName> /user:<UserName> /pass:<password>
```

Wenn Sie zur Eingabe eines Kennworts aufgefordert werden möchten, lassen Sie die Option /Pass aus.

2. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für den angegebenen Benutzernamen ein. Wenn die Firewall auf dem Server-Core-Server nicht bereits so konfiguriert ist, dass MMC-Snap-Ins eine Verbindung herstellen können, führen Sie die folgenden Schritte aus, um die Windows-Firewall so zu konfigurieren, dass das MMC- Fahren Sie anschließend mit Schritt 3 fort.
3. Starten Sie auf einem anderen Computer ein MMC-Snap-in, z. b. Computer Verwaltung.
4. Klicken Sie im linken Bereich mit der rechten Maustaste auf das Snap-in, und klicken Sie dann auf **Verbindung mit anderem Computer herstellen**. (Beispiel: im Beispiel Computer Verwaltung klicken Sie mit der rechten Maustaste auf Computer Verwaltung (lokal) .)
5. Geben Sie auf einem anderen Computer den Computernamen des Server Core-Servers ein, und klicken Sie dann auf OK. Sie können nun mit dem MMC-Snap-In den Server im Server-Core-Server wie jeden anderen Computer mit einem Windows-Betriebssystem verwalten.

So konfigurieren Sie die Windows-Firewall so, dass MMC-Snap-Ins eine Verbindung herstellen dürfen

Damit alle MMC-Snap-Ins eine Verbindung herstellen können, führen Sie den folgenden Befehl aus:

```
Enable-NetFirewallRule -DisplayGroup "Remote Administration"
```

Damit nur bestimmte MMC-Snap-Ins eine Verbindung herstellen können, führen Sie Folgendes aus:

```
Enable-NetFirewallRule -DisplayGroup "<rulergroup>"
```

Dabei ist *rulergroup* abhängig von dem Snap-in, das Sie verbinden möchten, eine der folgenden:

MMC-SNAP-IN	REGELGRUPPE
Ereignisanzeige	Remote-Ereignisprotokollverwaltung
Dienste	Remotedienstverwaltung
Freigegebene Ordner	Datei- und Druckerfreigabe
Aufgabenplanung	Leistungsprotokolle und-Warnungen, Datei-und Druckerfreigabe
Datenträgerverwaltung	Remotevolumeverwaltung
Windows-Firewall und erweiterte Sicherheit	Windows-Firewallremoteverwaltung

NOTE

Für einige MMC-Snap-Ins gibt es keine entsprechende Regelgruppe, die Ihnen das Herstellen einer Verbindung über die Firewall ermöglicht. Doch das Aktivieren der Regelgruppen für "Ereignisanzeige", "Dienste" oder "Freigegebene Ordner" können die meisten anderen Snap-Ins eine Verbindung herstellen.

Darüber hinaus benötigen bestimmte Snap-Ins eine weitere Konfiguration, ehe Sie durch die Windows-Firewall eine Verbindung herstellen können:

- Datenträgerverwaltung. Sie müssen auf dem Server-Core-Computer zunächst den Dienst für virtuelle Datenträger (Virtual Disk Service, VDS) starten. Außerdem müssen Sie Regeln zur Datenträgerverwaltung auf dem Computer, auf dem das MMC-Snap-In ausgeführt wird, entsprechend konfigurieren.
- IP-Sicherheitsmonitor. Sie müssen zunächst die Remoteverwaltung dieses Snap-Ins aktivieren. Geben Sie dazu an einer Eingabeaufforderung `cscript \windows\system32\scregedit.wsf/im-Befehl 1` ein.
- Zuverlässigkeit- und Leistungsüberwachung. Dieses Snap-In erfordert keine weitere Konfiguration, doch wenn Sie mit ihm einen Server-Core-Computer überwachen, können nur Leistungsdaten überwacht werden. Zuverlässigkeitsdaten sind nicht verfügbar.

Verwalten mit Remotedesktopdienste

Sie können [Remotedesktop](#) verwenden, um einen Server Core-Server von Remote Computern aus zu verwalten.

Bevor Sie auf Server Core zugreifen können, müssen Sie den folgenden Befehl ausführen:

```
cscript C:\Windows\System32\Scregedit.wsf /ar 0
```

Dadurch wird der Remotedesktop für den Verwaltungsmodus zum Akzeptieren von Verbindungen aktiviert.

Hinzufügen von Hardware und lokales Verwalten von Treibern

Befolgen Sie zum Hinzufügen von Hardware zu einem Server Core-Server die Anweisungen des Hardwareherstellers zur Installation neuer Hardware.

Wenn die Hardware nicht Plug & Play ist, müssen Sie den Treiber manuell installieren. Kopieren Sie hierzu die

Treiberdateien an einen temporären Speicherort auf dem Server, und führen Sie dann den folgenden Befehl aus:

```
pnputil -i -a <driverinf>
```

Dabei ist "*driverinf*" der Dateiname der INF-Datei für den Treiber.

Starten Sie den Computer bei entsprechender Aufforderung neu.

Führen Sie den folgenden Befehl aus, um zu sehen, welche Treiber installiert sind:

```
sc query type= driver
```

NOTE

Sie müssen hinter dem Gleichheitszeichen ein Leerzeichen einfügen, damit der Befehl erfolgreich ausgeführt werden kann.

Um einen Gerätetreiber zu deaktivieren, führen Sie Folgendes aus:

```
sc delete <service_name>
```

Dabei ist *SERVICE_NAME* der Name des Dienstanbieter, den Sie beim Durchlaufen der **SC-Abfragetyp = Treibererhalten** haben.

Konfigurieren von Speicher Abbild Dateien für die Server Core-Installation

02.12.2019 • 11 minutes to read • [Edit Online](#)

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

Führen Sie die folgenden Schritte aus, um ein Speicher Abbild für die Server Core-Installation zu konfigurieren.

Schritt 1: Deaktivieren der automatischen Dateiverwaltung von System Seiten

Der erste Schritt besteht darin, die Systemfehler-und Wiederherstellungsoptionen manuell zu konfigurieren. Dies ist erforderlich, um die restlichen Schritte abzuschließen.

Führen Sie den folgenden Befehl aus:

```
wmic computersystem set AutomaticManagedPagefile=False
```

Schritt 2: Konfigurieren des Zielpfads für ein Speicher Abbild

Sie müssen nicht über die Auslagerungs Datei auf der Partition verfügen, auf der das Betriebssystem installiert ist. Wenn Sie die Auslagerungs Datei auf einer anderen Partition platzieren möchten, müssen Sie einen neuen Registrierungs Eintrag mit dem Namen **dedicateddumpfile** erstellen. Sie können die Größe der Auslagerungs Datei mit dem Registrierungs Eintrag **DumpFileSize** definieren. Führen Sie die folgenden Schritte aus, um die Registrierungseinträge **dedicateddumpfile** und **DumpFileSize** zu erstellen:

1. Führen Sie an der Eingabeaufforderung den Befehl **Regedit** aus, um den Registrierungs-Editor zu öffnen.
2. Suchen Sie den folgenden Registrierungs Unterschlüssel, und klicken Sie darauf: HKEY_LOCAL_MACHINE \system\currentcontrolset\control\crashcontrol.
3. Klicken Sie > **neue > Zeichen folgen Wert bearbeiten**.
4. Benennen Sie den neuen Wert **dediereddumpfile**, und drücken Sie dann die EINGABETASTE.
5. Klicken Sie mit der rechten Maustaste auf **dedialisieddumpfile**, und klicken Sie dann auf **ändern**.
6. Geben Sie unter **Wert Datentyp <Laufwerk>:\<Dedi. sys>** ein, und klicken Sie dann auf **OK**.

NOTE

Ersetzen Sie <Laufwerk> durch ein Laufwerk, das über ausreichend Speicherplatz für die Auslagerungs Datei verfügt, und ersetzen Sie <dediereddumpfile. dmp> durch den vollständigen Pfad zu der dedizierten Datei.

7. Klicken Sie auf > **neuen > DWORD-Wert bearbeiten**.
8. Geben Sie **DumpFileSize** ein, und drücken Sie dann die EINGABETASTE.
9. Klicken Sie mit der rechten Maustaste auf **DumpFileSize**, und klicken Sie dann auf **ändern**.
10. Klicken Sie unter **DWORD-Wert bearbeiten** unter Basis auf **Dezimal**.

11. Geben Sie unter **Wertdatenden** entsprechenden Wert ein, und klicken Sie dann auf OK.

NOTE

Die Größe der Dumpdatei liegt in Megabyte (MB).

12. Beenden Sie den Registrierungs-Editor.

Nachdem Sie den Partitions Speicherort des Speicher Abbilds bestimmt haben, konfigurieren Sie den Zielpfad für die Auslagerungs Datei. Führen Sie den folgenden Befehl aus, um den aktuellen Zielpfad für die Auslagerungs Datei anzuzeigen:

```
wmic RECOVEROS get DebugFilePath
```

Das Standardziel für "Debug FilePath " ist%SystemRoot%\Memory.dmp. Um den aktuellen Zielpfad zu ändern, führen Sie den folgenden Befehl aus:

```
wmic RECOVEROS set DebugFilePath = <FilePath>
```

Legen Sie <filePath-> auf den Zielpfad fest. Der folgende Befehl legt z. b. den Zielpfad des Speicher Abbilds auf "c:\WINDOWS\MEMORY" fest. DMP

```
wmic RECOVEROS set DebugFilePath = C:\WINDOWS\MEMORY.DMP
```

Schritt 3: Legen Sie den Typ des Speicher Abbilds fest.

Bestimmen Sie den Typ des Speicher Abbilds, das für den Server konfiguriert werden soll. Führen Sie den folgenden Befehl aus, um den aktuellen speicherdumpotyp anzuzeigen:

```
wmic RECOVEROS get DebugInfoType
```

Führen Sie den folgenden Befehl aus, um den aktuellen Speicherdump-Typ zu ändern:

```
wmic RECOVEROS set DebugInfoType = <Value>
```

<Wert> kann wie unten definiert 0, 1, 2 oder 3 sein.

- 0: Deaktivieren Sie das Entfernen eines Speicher Abbilds.
- 1: vollständiges Speicher Abbild. Zeichnet den gesamten Inhalt des System Arbeitsspeichers auf, wenn der Computer unerwartet angehalten wird. Ein vollständiges Speicher Abbild kann Daten aus Prozessen enthalten, die bei der Erfassung des Speicher Abbilds ausgeführt wurden.
- 2: Kernel Speicher Abbild (Standard). Zeichnet nur den Kernelspeicher auf. Dies beschleunigt den Prozess der Aufzeichnung von Informationen in einer Protokolldatei, wenn der Computer unerwartet angehalten wird.
- 3: kleines Speicher Abbild. Zeichnet die kleinsten nützlichen Informationen auf, anhand derer ermittelt werden kann, warum der Computer unerwartet angehalten wurde.

Schritt 4: Konfigurieren des Servers für den automatischen Neustart nach dem Erstellen eines Speicher Abbilds

Standardmäßig wird der Server automatisch neu gestartet, nachdem ein Speicher Abbild generiert wurde. Führen

Sie den folgenden Befehl aus, um die aktuelle Konfiguration anzuzeigen:

```
wmic RECOVEROS get AutoReboot
```

Wenn der Wert für **AutoReboot** den Wert true hat, wird der Server nach dem Erstellen eines Speicher Abbilds automatisch neu gestartet. Es ist keine Konfiguration erforderlich, und Sie können mit dem nächsten Schritt fortfahren.

Wenn der Wert für **AutoReboot** den Wert false hat, wird der Server nicht automatisch neu gestartet. Führen Sie den folgenden Befehl aus, um den Wert zu ändern:

```
wmic RECOVEROS set AutoReboot = true
```

Schritt 5: Konfigurieren des Servers zum Überschreiben der vorhandenen Speicher Abbild Datei

Standardmäßig überschreibt der Server die vorhandene Speicher Abbild Datei, wenn ein neuer erstellt wird. Führen Sie den folgenden Befehl aus, um zu ermitteln, ob vorhandene Speicher Abbild Dateien bereits überschrieben werden können:

```
wmic RECOVEROS get OverwriteExistingLogFile
```

Wenn der Wert 1 ist, wird die vorhandene Speicher Abbild Datei vom Server überschrieben. Es ist keine Konfiguration erforderlich, und Sie können mit dem nächsten Schritt fortfahren.

Wenn der Wert 0 ist, wird die vorhandene Speicher Abbild Datei vom Server nicht überschrieben. Führen Sie den folgenden Befehl aus, um den Wert zu ändern:

```
wmic RECOVEROS set OverwriteExistingLogFile = 1
```

Schritt 6: Festlegen einer administrativen Warnung

Stellen Sie fest, ob eine administrative Warnung geeignet ist, und legen Sie **sendadminalert** entsprechend fest. Um den aktuellen Wert für sendadminalert anzuzeigen, führen Sie den folgenden Befehl aus:

```
wmic RECOVEROS get SendAdminAlert
```

Die möglichen Werte für sendadminalert sind true oder false. Führen Sie den folgenden Befehl aus, um den vorhandenen sendadminalert-Wert in true zu ändern:

```
wmic RECOVEROS set SendAdminAlert = true
```

Schritt 7: Festlegen der Größe der Auslagerungs Datei des Speicher Abbilds

Führen Sie einen der folgenden Befehle aus, um die aktuellen Seiten Datei Einstellungen zu überprüfen:

```
wmic.exe pagefile
```

oder

```
wmic.exe pagefile list /format:list
```

Führen Sie z. b. den folgenden Befehl aus, um die anfängliche und die maximale Größe der Auslagerungs Datei zu konfigurieren:

```
wmic pagefileset where name="c:\\pagefile.sys" set InitialSize=1000,MaximumSize=5000
```

Schritt 8: Konfigurieren des Servers für die Generierung eines manuellen Speicher Abbilds

Sie können ein Speicher Abbild mithilfe einer PS/2-Tastatur manuell generieren. Diese Funktion ist standardmäßig deaktiviert und nicht für USB (Universal Serial Bus)-Tastaturen verfügbar.

Führen Sie den folgenden Befehl aus, um manuelle Speicher Abbilder mithilfe einer PS/2-Tastatur zu aktivieren:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters /v CrashOnCtrlScroll /t REG_DWORD /d 1 /f
```

Führen Sie den folgenden Befehl aus, um zu ermitteln, ob die Funktion ordnungsgemäß aktiviert wurde:

```
Reg query HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ i8042prt \ Parameters / v CrashOnCtrlScroll
```

Sie müssen den Server neu starten, damit die Änderungen wirksam werden. Sie können den Server neu starten, indem Sie den folgenden Befehl ausführen:

```
Shutdown / r / t 0
```

Sie können manuelle Speicher Abbilder mit einer PS/2-Tastatur generieren, die mit dem Server verbunden ist, indem Sie die Rechte STRG-Taste gedrückt halten, während Sie die scrollsperrtaste zweimal drücken. Dadurch wird die Fehlerüberprüfung des Computers mit dem Fehlercode 0xe2 erstellt. Nachdem Sie den Server neu gestartet haben, wird eine neue Dumpdatei im Zielpfad angezeigt, den Sie in Schritt 2 erstellt haben.

Schritt 9: überprüfen, ob die Speicher Abbild Dateien ordnungsgemäß erstellt werden

Sie können die Utility Dumpchk. exe verwenden, um zu überprüfen, ob die Speicher Abbild Dateien ordnungsgemäß erstellt werden. Das Hilfsprogramm "Dumpchk. exe" wird nicht mit der Server Core-Installationsoption installiert, sodass Sie es von einem Server mit Desktop Darstellung oder Windows 10 ausführen müssen. Außerdem müssen die Debugtools für Windows-Produkte installiert sein.

Mit dem Hilfsprogramm "Dumpchk. exe" können Sie die Speicher Abbild Datei von der Server Core-Installation von Windows Server 2008 auf den anderen Computer übertragen, indem Sie das Mittel ihrer Wahl verwenden.

WARNING

Auslagerungs Dateien können sehr groß sein, daher sollten Sie die Übertragungsmethode und die von der Methode benötigten Ressourcen sorgfältig berücksichtigen.

Weitere Verweise

Allgemeine Informationen zur Verwendung von Speicher Abbild Dateien finden Sie unter Übersicht über die [Optionen für die Speicher Abbild Datei für Windows](#).

Weitere Informationen zu dedizierten Dumpdateien finden Sie unter Gewusst wie: [Verwenden des Registrierungs Werts "dedicateddeumpfile" zum überwinden von Speicherplatz Beschränkungen auf dem Systemlaufwerk beim Erfassen eines Systemspeicher Abbilds](#).

Patchen einer Server Core-Installation

02.12.2019 • 4 minutes to read • [Edit Online](#)

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

Sie können einen Server, auf dem die Server Core-Installation ausgeführt wird, wie folgt Patchen:

- **Automatisches Verwenden von Windows Update oder mit Windows Server Update Services (WSUS)**. Wenn Sie Windows Update entweder automatisch oder mit Befehlszeilen Tools oder Windows Server Update Services (WSUS) verwenden, können Sie Server verwenden, auf denen eine Server Core-Installation ausgeführt wird.
- **Manuell**. Auch in Organisationen, in denen Windows Update oder WSUS nicht verwendet wird, können Sie Updates manuell anwenden.

Anzeigen der auf dem Server-Core-Server installierten Updates

Bevor Sie ein neues Update zu Server Core hinzufügen, empfiehlt es sich, zu sehen, welche Updates bereits installiert wurden.

Wenn Sie Updates mithilfe von Windows PowerShell anzeigen möchten, führen Sie **Get-Hotfix** aus.

Um Updates durch Ausführen eines Befehls anzuzeigen, führen Sie **Systeminfo.exe** aus. Möglicherweise kommt es zu einer kurzen Verzögerung, während das Tool das System prüft.

Sie können auch die **WMIC-QFE-Liste** über die Befehlszeile ausführen.

Automatisches Patchen von Server Core mit Windows Update

Führen Sie die folgenden Schritte aus, um den Server automatisch mit Windows Update zu patchen:

1. Überprüfen Sie die aktuelle Windows Update Einstellung:

```
%systemroot%\system32\cscript %systemroot%\system32\scregedit.wsf /AU /v
```

2. So aktivieren Sie automatische Updates:

```
Net stop wuauserv  
%systemroot%\system32\cscript %systemroot%\system32\scregedit.wsf /AU 4  
Net start wuauserv
```

3. Führen Sie Folgendes aus, um automatische Updates zu deaktivieren:

```
Net stop wuauserv  
%systemroot%\system32\cscript %systemroot%\system32\scregedit.wsf /AU 1  
Net start wuauserv
```

Wenn der Server Mitglied einer Domäne ist, können Sie Windows Update auch mithilfe einer Gruppenrichtlinie konfigurieren. Weitere Informationen finden Sie unter <https://go.microsoft.com/fwlink/?LinkId=192470>. Wenn Sie diese Methode verwenden, ist jedoch nur Option 4 ("Automatisches herunterladen und Planen der Installation") für Server Core-Installationen relevant, weil keine grafische Oberfläche verfügbar ist. Um besser steuern zu können,

welche Updates zu welchem Zeitpunkt installiert werden, können Sie ein Skript verwenden. Das Skript stellt ein Befehlszeilenäquivalent der meisten Optionen der grafischen Windows Update-Benutzeroberfläche dar. Weitere Informationen zum Skript finden Sie unter <https://go.microsoft.com/fwlink/?LinkId=192471>.

Führen Sie den folgenden Befehl aus, um zu erzwingen, dass Windows Update alle verfügbaren Updates sofort erkennt und installiert:

```
Wuauctl /detectnow
```

Je nach den installierten Updates kann es sein, dass Sie den Computer neu starten müssen, auch wenn vom System keine entsprechende Meldung angezeigt wird. Um zu ermitteln, ob der Installationsvorgang abgeschlossen ist, verwenden Sie den Task-Manager, um zu überprüfen, ob die Prozesse **wuauctl** oder **vertrauenswürdiger Installer** nicht aktiv ausgeführt werden. Sie können auch die Methoden in [Anzeigen der auf dem Server-Core-Server installierten Updates](#) verwenden, um die Liste der installierten Updates zu überprüfen.

Patchen des Servers mit WSUS

Wenn der Server Core-Server Mitglied einer Domäne ist, können Sie diesen mithilfe einer Gruppenrichtlinie für die Verwendung eines WSUS-Servers konfigurieren. Weitere Informationen finden Sie unter [Gruppenrichtlinie Referenzinformationen](#). Weitere Informationen finden Sie auch unter [Konfigurieren von Gruppenrichtlinie Einstellungen für automatische Updates](#)

Manuelles Patchen des Servers

Laden Sie das Update herunter, und stellen Sie es für die Server Core-Installation zur Verfügung. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus:

```
Wusa <update>.msu /quiet
```

Je nach den installierten Updates kann es sein, dass Sie den Computer neu starten müssen, auch wenn vom System keine entsprechende Meldung angezeigt wird.

Um ein Update manuell zu deinstallieren, führen Sie den folgenden Befehl aus:

```
Wusa /uninstall <update>.msu /quiet
```

Server-Manager

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Server-Manager ist eine Verwaltungskonsole in Windows Server, mit der IT-Experten lokale Windows-basierte Server und Remote Server von ihren Desktops aus bereitstellen und verwalten können, ohne dass Sie physischen Zugriff auf die Server benötigen oder RDP-Verbindungen (Remotedesktop Protocol) zu jedem Server aktivieren müssen. Obwohl Server-Manager in Windows Server 2008 R2 und Windows Server 2008 verfügbar ist, wurde Server-Manager in Windows Server 2012 aktualisiert, um die Remote Verwaltung mehrerer Server zu unterstützen und die Anzahl der Server zu erhöhen, die ein Administrator verwalten kann.

In unseren Tests können Server-Manager in Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 verwendet werden, um bis zu 100 Server zu verwalten, abhängig von den Workloads, die auf den Servern ausgeführt werden. Die Anzahl der Server, die Sie mit einer einzelnen Server-Manager-Konsole verwalten können, kann von der Datenmenge abhängig sein, die Sie von den verwalteten Servern anfordern, sowie von den Hardware- und Netzwerkressourcen, die für den Computer mit dem Server-Manager zur Verfügung stehen. Wenn die anzuzeigende Datenmenge die Ressourcenkapazität des Computers erreicht, kann es zu langen Reaktionszeiten des Server-Managers und Verzögerungen bei der Durchführung von Aktualisierungen kommen. Um die Anzahl der Server zu erhöhen, die Sie mit dem Server-Manager verwalten können, sollten Sie die Ereignisdaten, die der Server-Manager von den verwalteten Servern empfängt, über das Dialogfeld **Ereignisdaten konfigurieren** beschränken. Sie können das Dialogfeld über das Menü **Aufgaben** in der Kachel **Ereignisse** öffnen. Wenn Sie in Ihrer Organisation eine organisationsübergreifende Anzahl von Servern verwalten müssen, wird empfohlen, die Produkte in der [Microsoft System Center-Suite](#) auszuwerten.

Dieses Thema und seine Unterthemen enthalten Informationen zur Verwendung von Funktionen in der Server-Manager-Konsole. Dieses Thema enthält folgende Abschnitte:

- [Überprüfen der anfänglichen Überlegungen und Systemanforderungen](#)
- [Aufgaben, die Sie in Server-Manager ausführen können](#)
- [Start Server-Manager](#)
- [Neustarten von Remote Servern](#)
- [Exportieren von Server-Manager Einstellungen auf andere Computer](#)

Vorüberlegungen und Systemanforderungen

In den folgenden Abschnitten finden Sie einige Überlegungen, die Sie überprüfen müssen, sowie Hardware- und Softwareanforderungen für Server-Manager.

Hardwareanforderungen

Server-Manager wird standardmäßig mit allen Editionen von Windows Server 2016 installiert. Für Server-Manager sind keine zusätzlichen Hardwareanforderungen vorhanden.

Software- und Konfigurationsanforderungen

Server-Manager wird standardmäßig mit allen Editionen von Windows Server 2016 installiert. Sie können Server-Manager in Windows Server 2016 verwenden, um die [Server Core-Installationsoptionen](#) von Windows Server 2016, Windows Server 2012 und Windows Server 2008 R2, die auf Remote Computern ausgeführt

werden, zu verwalten. Server-Manager wird unter der Server Core-Installationsoption von Windows Server 2016 ausgeführt.

Server-Manager in der grafischen Benutzeroberfläche mit minimalem Server ausgeführt werden. Das heißt, wenn das Feature für die servergrafikshell nicht installiert ist. Das Feature "grafische Shell für Server" wird auf Windows Server 2016 standardmäßig nicht installiert. Wenn Sie die servergrafikshell nicht ausführen, wird die Server-Manager Konsole ausgeführt, aber einige Anwendungen oder Tools, die über die-Konsole verfügbar sind, sind nicht verfügbar. Internet Browser können nicht ohne servergrafikshell ausgeführt werden, sodass Webseiten und Anwendungen wie die HTML-Hilfe (z. b. die MMC-F1-Hilfe) nicht geöffnet werden können. Sie können keine Dialogfelder zum Konfigurieren von automatischen Windows-Updates und Feedback öffnen, wenn die servergrafikshell nicht installiert ist. Befehle, die diese Dialogfelder in der Server-Manager Konsole öffnen, werden umgeleitet, um " SCONFIG. cmd" auszuführen.

Zum Verwalten von Servern, auf denen Windows Server-Versionen älter als Windows Server 2016 ausgeführt werden, installieren Sie die folgende Software und Updates, um die älteren Versionen von Windows Server mithilfe von Server-Manager in Windows Server 2016 verwaltbar zu machen.

BETRIEBSSYSTEM	ERFORDERLICHE SOFTWARE
Windows Server 2012 R2 oder Windows Server 2012	<ul style="list-style-type: none">- .NET Framework 4,6- Windows Management Framework 5,0. Das Windows Management Framework 5,0-Downloadpaket aktualisiert Windows-Verwaltungsinstrumentation (WMI)-Anbieter unter Windows Server 2012 R2 und Windows Server 2012. Mit den aktualisierten WMI-Anbietern können Server-Manager Informationen zu den auf den verwalteten Servern installierten Rollen und Features sammeln. Bis zum Anwenden des Updates haben Server, auf denen Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, den verwaltbarkeitsstatus nicht zugänglich.-Das mit dem Knowledge Base-Artikel 2682011 verknüpfte Leistungs Update ist auf Servern mit Windows Server 2012 R2 oder Windows Server 2012 nicht mehr erforderlich.
Windows Server 2008 R2	<ul style="list-style-type: none">- .NET Framework 4,5- Windows Management Framework 4,0. Das Windows Management Framework 4,0-Downloadpaket aktualisiert Windows-Verwaltungsinstrumentation (WMI)-Anbieter unter Windows Server 2008 R2. Mit den aktualisierten WMI-Anbietern können Server-Manager Informationen zu den auf den verwalteten Servern installierten Rollen und Features sammeln. Bis zum Anwenden des Updates haben Server, auf denen Windows Server 2008 R2 ausgeführt wird, den verwaltbarkeitsstatus nicht zugänglich.-Das mit dem Knowledge Base-Artikel 2682011 verknüpfte Leistungs Update ermöglicht Server-Manager die Erfassung von Leistungsdaten von Windows Server 2008 R2.

BETRIEBSSYSTEM	ERFORDERLICHE SOFTWARE
WindowsServer 2008	<ul style="list-style-type: none"> - .NET Framework 4 - Windows Management Framework 3.0 Windows Management Framework 3.0 Download Package Updates <p>Windows-Verwaltungsinstrumentation (WMI)-Anbieter unter Windows Server 2008. Mit den aktualisierten WMI-Anbietern können Server-Manager Informationen zu den auf den verwalteten Servern installierten Rollen und Features sammeln. Bis zum Anwenden des Updates haben Server, auf denen Windows Server 2008 ausgeführt wird, den verwalbarkeitsstatus nicht verfügbar: Überprüfen Sie, ob frühere Versionen Windows Management Framework 3.0 ausführen.</p> <p>-Das mit dem Knowledge Base-Artikel 2682011 verknüpfte Leistungs Update ermöglicht Server-Manager die Erfassung von Leistungsdaten von Windows Server 2008.</p>

Verwalten von Remotecomputern über einen Clientcomputer

Die Server-Manager Konsole ist in [Remoteserver-Verwaltungstools](#) für Windows 10 enthalten. Beachten Sie Folgendes: Wenn Remoteserver-Verwaltungstools auf einem Client Computer installiert ist, können Sie den lokalen Computer nicht mithilfe von Server-Manager verwalten. Server-Manager können nicht zum Verwalten von Computern oder Geräten verwendet werden, auf denen ein Windows-Client Betriebssystem ausgeführt wird. Sie können Server-Manager nur zum Verwalten von Windows-basierten Servern verwenden.

SERVER-MANAGER QUELL-BETRIEBSSYSTEM	ZIEL AUF WINDOWS SERVER 2016	ZIEL WINDOWS SERVER 2012 R2	ZIEL AUF WINDOWS SERVER 2012	ZIEL WINDOWS SERVER 2008 R2 ODER WINDOWS SERVER 2008	FÜR WINDOWS SERVER 2003
Windows 10 oder Windows Server 2016	Vollständige Unterstützung	Vollständige Unterstützung	Vollständige Unterstützung	Sobald die Software- und Konfigurationsoptionen erfüllt sind, können die meisten Verwaltungsaufgaben, jedoch keine Installation oder Deinstallation von Rollen oder Features durchgeführt werden	Nicht unterstützt
Windows 8.1 oder Windows Server 2012 R2	Nicht unterstützt	Vollständige Unterstützung	Vollständige Unterstützung	Sobald die Software- und Konfigurationsoptionen erfüllt sind, können die meisten Verwaltungsaufgaben, jedoch keine Installation oder Deinstallation von Rollen oder Features durchgeführt werden	Eingeschränkte Unterstützung, nur Online- und Offlinestatus

SERVER-MANAGER QUELL BETRIEBSSYSTEM	ZIEL AUF WINDOWS SERVER 2016	ZIEL WINDOWS SERVER 2012 R2	ZIEL AUF WINDOWS SERVER 2012	ZIEL WINDOWS SERVER 2008 R2 ODER WINDOWS SERVER 2008	FÜR WINDOWS SERVER 2003
Windows 8 oder Windows Server 2012	Nicht unterstützt	Nicht unterstützt	Vollständige Unterstützung	Sobald die Software- und Konfigurationsoptionen erfüllt sind, können die meisten Verwaltungsaufgaben abgenommen werden, jedoch keine Installation oder Deinstallation von Rollen oder Features durchgeführt werden	Eingeschränkte Unterstützung, nur Online- und Offlinestatus

So starten Sie den Server-Manager auf einem Clientcomputer

1. Befolgen Sie die Anweisungen in [Remoteserver-Verwaltungstools](#), um Remoteserver-Verwaltungstools für Windows 10 zu installieren.
2. Klicken Sie auf dem **Start** Bildschirm auf **Server-Manager**. Die **Server-Manager**-Kachel ist verfügbar, nachdem Sie die Remoteserver-Verwaltungstools installiert haben.
3. Wenn nach der Installation von Remoteserver-Verwaltungstools weder die noch die **Server-Manager**-Kacheln auf dem **Start** Bildschirm angezeigt werden und nach Server-Manager auf dem **Start** Bildschirm suchen, überprüfen Sie, ob die Einstellung **Verwaltungs Tools anzeigen** aktiviert ist. Um diese Einstellung anzuzeigen, zeigen Sie mit dem Mauszeiger auf die obere rechte Ecke der **Start** Seite, und klicken Sie dann auf **Einstellungen**. Ist die Einstellung **Verwaltungstools anzeigen** deaktiviert, aktivieren Sie die Einstellung, um Tools anzuzeigen, die Sie als Teil der Remoteserver-Verwaltungstools installiert haben.

Weitere Informationen zum Ausführen von Remoteserver-Verwaltungstools für Windows 10 zur Verwaltung von Remote Servern finden Sie im TechNet wiki unter [Remoteserver-Verwaltungstools](#).

Konfigurieren der Remoteverwaltung auf zu verwaltenden Servern

IMPORTANT

Standardmäßig ist Server-Manager und Windows PowerShell-Remote Verwaltung in Windows Server 2016 aktiviert.

Zum Ausführen von Verwaltungsaufgaben auf Remote Servern mithilfe von Server-Manager müssen Remote Server, die Sie verwalten möchten, so konfiguriert werden, dass Sie die Remote Verwaltung mithilfe von Server-Manager und Windows PowerShell zulassen. Wenn die Remote Verwaltung unter Windows Server 2012 R2 oder Windows Server 2012 deaktiviert wurde und Sie sie erneut aktivieren möchten, führen Sie die folgenden Schritte aus.

So konfigurieren Sie Server-Manager-Remote Verwaltung unter Windows Server 2012 R2 oder Windows Server 2012 mithilfe der Windows-Benutzeroberfläche

1. NOTE

Die Einstellungen, die im Dialogfeld **Remote Verwaltung konfigurieren** gesteuert werden, wirken sich nicht auf Teile von Server-Manager aus, die DCOM für die Remote Kommunikation verwenden.

Führen Sie eine der folgenden Aktionen aus, um Server-Manager zu öffnen, wenn es nicht bereits geöffnet

ist.

- Klicken Sie in der Windows-Taskleiste auf die Schaltfläche Server-Manager.
 - Klicken Sie auf dem Start Bildschirm auf **Server-Manager**.
2. Klicken Sie im Bereich **Eigenschaften** der Seite **lokale Server** auf den hyperverknüpften Wert für die Eigenschaft **Remote Verwaltung**.
3. Führen Sie einen der folgenden Schritte aus, und klicken Sie anschließend auf **OK**:
- Deaktivieren Sie das Kontrollkästchen **Remote Verwaltung dieses Servers von anderen Computern aktivieren**, um zu verhindern, dass dieser Computer mithilfe Server-Manager (oder mithilfe von Windows PowerShell bei der Installation) Remote verwaltet wird.
 - Um die Remote Verwaltung dieses Computers mithilfe von Server-Manager oder Windows PowerShell zuzulassen, wählen Sie **Remote Verwaltung dieses Servers von anderen Computern aktivieren aus**.

So aktivieren Sie Server-Manager-Remote Verwaltung unter Windows Server 2012 R2 oder Windows Server 2012 mithilfe von Windows PowerShell

1. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie Windows PowerShell als Administrator über den Start Bildschirm ausführen möchten, klicken Sie mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf **als Administrator ausführen**.
- Wenn Sie Windows PowerShell als Administrator über den Desktop ausführen möchten, klicken Sie in der Taskleiste mit der rechten Maustaste auf die Verknüpfung **Windows PowerShell**, und klicken Sie dann auf **als Administrator ausführen**.

2. Geben Sie Folgendes ein, und drücken Sie dann die EINGABETASTE, um alle erforderlichen Firewallregelausnahmen zu aktivieren.

Configure-SMRemoting.exe-enable

NOTE

Dieser Befehl kann auch in einer Eingabeaufforderung verwendet werden, die mit erhöhten Benutzerrechten ("Als Administrator ausführen") geöffnet wurde.

Wenn das Aktivieren der Remote Verwaltung fehlschlägt, finden Sie unter [about_remote_Troubleshooting](#) auf Microsoft TechNet Tipps und bewährte Methoden zur Problembehandlung.

So aktivieren Sie die Remoteverwaltung durch den Server-Manager und Windows PowerShell für ältere Betriebssysteme

- Führen Sie einen der folgenden Schritte aus:
 - Informationen zum Aktivieren der Remote Verwaltung auf Servern, auf denen Windows Server 2008 R2 ausgeführt wird, finden Sie unter [Remote Verwaltung mit Server-Manager](#) in der Hilfe zu Windows Server 2008 R2.
 - Informationen zum Aktivieren der Remote Verwaltung auf Servern, auf denen Windows Server 2008 ausgeführt wird, finden Sie unter [aktivieren und Verwenden von Remote Befehlen in Windows PowerShell](#).

Im Server-Manager ausführbare Aufgaben

Server-Manager wird die Serververwaltung effizienter, da Administratoren mithilfe eines einzigen Tools Aufgaben in der folgenden Tabelle ausführen können. In Windows Server 2012 R2 und Windows Server 2012 können

sowohl Standardbenutzer eines Servers als auch Mitglieder der Gruppe "Administratoren" Verwaltungsaufgaben in Server-Manager ausführen. Standardbenutzer werden jedoch standardmäßig daran gehindert, einige Aufgaben auszuführen, wie in der folgenden Tabelle gezeigt.

Administratoren können im Server-Manager Cmdlet-Modul, [enable-servermanagerstandarduserremoting](#) und [Deaktivieren-servermanagerstandarduserremoting](#), zwei Windows PowerShell-Cmdlets verwenden, um den Standardbenutzer Zugriff auf einige zusätzliche Daten weiter zu steuern. Das **enable-servermanagerstandarduserremoting**- Cmdlet kann einen oder mehrere Standardbenutzer ohne Administrator Rechte für den Zugriff auf Ereignis-, Dienst-, Leistungs- und Rollen- und featureinventur Daten bereitstellen.

IMPORTANT

Server-Manager kann nicht verwendet werden, um eine neuere Version des Betriebssystems Windows Server zu verwalten. Server-Manager, die unter Windows Server 2012 oder Windows 8 ausgeführt werden, können nicht zum Verwalten von Servern verwendet werden, auf denen Windows Server 2012 R2 ausgeführt wird.

AUFGABENBESCHREIBUNG	ADMINISTRATOREN (EINSCHLIESSLICH DES DES INTEGRIERTEN ADMINISTRATORKONTOS)	STANDARDSERVERBENUTZER
Hinzufügen von Remote Servern zu einem Pool von Servern, die Server-Manager zur Verwaltung von verwendet werden können.	Ja	Nein
Erstellen und bearbeiten Sie benutzerdefinierte Server Gruppen, z. b. Server, die sich an einem bestimmten geografischen Standort befinden oder einen bestimmten Zweck erfüllen.	Ja	Ja
Installieren oder Deinstallieren von Rollen, Rollen Diensten und Features auf dem lokalen Server oder auf Remote Servern, auf denen Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Definitionen von Rollen, Rollen Diensten und Features finden Sie unter Rollen, Rollen Dienste und Features .	Ja	Nein
Anzeigen und Ändern der auf Servern (lokal oder remote) installierten Serverrollen und Features. Hinweis: In Server-Manager werden Rollen- und Featuredaten in der Basis Sprache des Systems, auch als "System Default GUI Language" bezeichnet, oder der während der Installation des Betriebssystems ausgewählten Sprache angezeigt.	Ja	Standardbenutzer können Rollen und Features anzeigen und verwalten und Aufgaben wie das Anzeigen von Rolleneignissen durchführen, jedoch keine Rollendienste hinzufügen oder entfernen.

AUFGABENBESCHREIBUNG	ADMINISTRATOREN (EINSCHLIESSLICH DES DES INTEGRIERTEN ADMINISTRATORKONTOS)	STANDARDSERVERBENUTZER
Starten Sie Verwaltungs Tools wie Windows PowerShell oder MMC-Snap-Ins. Sie können eine Windows PowerShell-Sitzung für einen Remote Server starten, indem Sie in der Kachel Server mit der rechten Maustaste auf den Server klicken und dann auf Windows PowerShellklicken . Sie können MMC-Snap-Ins über das Menü Extras der Server-Manager -Konssole starten und die MMC nach dem Öffnen des Snap-Ins auf einen Remote Computer verweisen.	Ja	Ja
Verwalten von Remoteservern mit unterschiedlichen Anmeldeinformationen, indem Sie auf der Kachel Server mit der rechten Maustaste auf einen Server klicken und dann auf Verwalten als klicken . Sie können Verwalten als für allgemeine Verwaltungsaufgaben für Server, Dateien und Speicherdiene verwenden.	Ja	Nein
Ausführen von Verwaltungsaufgaben im Zusammenhang mit dem operativen Lebenszyklus von Servern (z. b. starten oder Beenden von Diensten) und starten Sie weitere Tools, mit denen Sie die Netzwerkeinstellungen, Benutzer und Gruppen eines Servers und Remotedesktop Verbindungen konfigurieren können.	Ja	Standardbenutzer können keine Dienste starten oder beenden. Sie können den Namen, die Arbeitsgruppe oder die Domänen Mitgliedschaft des lokalen Servers und Remotedesktop Einstellungen ändern, werden jedoch von der Benutzerkontensteuerung aufgefordert, Administrator Anmelde Informationen bereitzustellen, bevor Sie diese Aufgaben ausführen können. Sie können keine Remoteverwaltungseinstellungen ändern.
Ausführen von Verwaltungsaufgaben in Verbindung mit dem operativen Lebenszyklus der auf dem Server installierten Rollen. Dazu gehört das Überprüfen der Rollen auf die Übereinstimmung mit bewährten Methoden.	Ja	Standard Benutzer können keine Best Practices Analyzer Scans ausführen.
Bestimmen des Serverstatus, Ermitteln kritischer Ereignisse sowie Analysieren und Behandeln von Konfigurationsproblemen oder -fehlern.	Ja	Ja

AUFGABENBESCHREIBUNG	ADMINISTRATOREN (EINSCHLIESSLICH DES DES INTEGRIERTEN ADMINISTRATORKONTOS)	STANDARDSERVERBENUTZER
Passen Sie die Ereignisse, Leistungsdaten, Dienste und Best Practices Analyzer Ergebnisse an, über die Sie im Server-Manager-Dashboard benachrichtigt werden möchten.	Ja	Ja
Neustarten von Servern.	Ja	Nein
Aktualisieren Sie die Daten, die in der Server-Manager Konsole zu verwalteten Servern angezeigt werden.	Ja	Nein

NOTE

Server-Manager können nicht zum Hinzufügen von Rollen und Features zu Servern verwendet werden, auf denen Windows Server 2008 R2 oder Windows Server 2008 ausgeführt wird.

Start Server-Manager

Server-Manager wird standardmäßig auf Servern, auf denen Windows Server 2016 ausgeführt wird, automatisch gestartet, wenn sich ein Mitglied der Gruppe "Administratoren" bei einem Server anmeldet. Wenn Sie Server-Manager schließen, starten Sie ihn mit einer der folgenden Methoden neu. Dieser Abschnitt enthält auch Schritte zum Ändern des Standard Verhaltens und verhindern, dass Server-Manager automatisch gestartet werden.

So starten Sie Server-Manager über den Startbildschirm

- Klicken Sie auf dem Windows- Start Bildschirm auf die Kachel **Server-Manager** .

So starten Sie den Server-Manager über den Windows-Desktop

- Klicken Sie auf der Windows-Taskleiste auf **Server-Manager**.

So verhindern Sie den automatischen Start des Server-Managers

1. Klicken Sie in der Server-Manager-Konsole im Menü **Verwalten** auf **Server-Manager Eigenschaften**.
2. Aktivieren Sie im Dialogfeld **Server-Manager-Eigenschaften** das Kontrollkästchen für **Server-Manager beim Anmelden nicht automatisch starten**. Klicken Sie auf **OK**.
3. Alternativ können Sie verhindern, dass Server-Manager automatisch gestartet wird, indem Sie die Einstellung Gruppenrichtlinie aktivieren, **Server-Manager bei der Anmeldung nicht automatisch starten**. Der Pfad zu dieser Richtlinien Einstellung ist in der Konsole des lokalen Gruppenrichtlinie-Editors Computerkonfiguration\Administrative vorlagen\system\servermanager.

Neustarten von Remoteservern

Sie können einen Remote Server über die Kachel **Server** einer Rollen-oder Gruppenseite in Server-Manager neu starten.

IMPORTANT

Beim eines Remoteservers wird der Server auch dann zum Neustarten gezwungen, wenn noch Benutzer am Remoteserver angemeldet und Programme mit ungespeicherten Daten geöffnet sind. Dieses Verhalten unterscheidet sich um Herunterfahren oder Neustarten des lokalen Computers, auf dem Sie aufgefordert würden, ungespeicherte Programmdaten zu speichern und zu bestätigen, dass angemeldete Benutzer zur Abmeldung gezwungen werden sollen. Stellen Sie sicher, dass Sie Benutzer zur Abmeldung von Remoteservern zwingen und ungespeicherte Daten in Programmen, die auf Remoteservern ausgeführt werden, verwerfen können.

Wenn eine automatische Aktualisierung in Server-Manager erfolgt, während ein verwalteter Server heruntergefahren und neu gestartet wird, können Aktualisierungs- und verwaltbarkeitsstatusfehler für den verwalteten Server auftreten, da Server-Manager keine Verbindung mit dem Remote Server herstellen kann, bis der Neustart abgeschlossen ist.

So starten Sie Remoteserver im Server-Manager

1. Öffnen Sie eine Rollen- oder Server Gruppen-Startseite in Server-Manager.
2. Wählen Sie einen oder mehrere Remote Server aus, die Sie Server-Manager hinzugefügt haben. Halten Sie beim Klicken die STRG-Taste gedrückt, um mehrere Warnungen gleichzeitig auszuwählen. Weitere Informationen zum Hinzufügen von Servern zum Server-Manager-Server Pool finden Sie unter [Hinzufügen von Servern zu Server-Manager](#).
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Server, und klicken Sie anschließend auf **Server neu starten**.

Exportieren von Server-Manager-Einstellungen auf andere Computer

In Server-Manager werden die Liste der verwalteten Server, Änderungen an Server-Manager Konsolen Einstellungen und von Ihnen erstellte benutzerdefinierte Gruppen in den folgenden beiden Dateien gespeichert. Sie können diese Einstellungen auf anderen Computern, auf denen dieselbe Version von Server-Manager ausgeführt wird (oder Windows 10 mit installierter Remoteserver-Verwaltungstools), wieder verwenden. Remoteserver-Verwaltungstools müssen auf Windows-Client basierten Computern ausgeführt werden, um Server-Manager Einstellungen auf diese Computer zu exportieren.

- %AppData% \ microsoft\windows\servermanager\serverlist.XML
- %AppData% \ local \ Microsoft_Corporation \servermanager. exe_StrongName_GUID\6.2.0.0\user.config

NOTE

- Alternative Anmeldeinformationen (bzw. "Verwalten als") für Server im Serverpool werden nicht im Roamingprofil gespeichert. Server-Manager-Benutzer müssen diese auf dem jeweiligen Computer hinzufügen, den sie verwalten wollen.
- Das Netzwerkfreigaben-Roamingprofil wird erst erstellt, wenn sich ein Benutzer erstmalig am Netzwerk anmeldet und dann wieder abmeldet. Die Datei **Serverlist.xml** wird zu diesem Zeitpunkt erstellt.

Sie können Server-Manager Einstellungen exportieren, Server-Manager Einstellungen portierbar machen oder Sie auf anderen Computern mithilfe einer der beiden folgenden Methoden verwenden.

- Zum Exportieren von Einstellungen auf einen anderen in die Domäne eingebundenen Computer konfigurieren Sie den Server-Manager Benutzer so, dass er ein Roamingprofil in Active Directory-Benutzer und-Computer Sie müssen Domänen Administrator sein, um Benutzereigenschaften in Active Directory-Benutzer und-Computer zu ändern.
- Wenn Sie Einstellungen auf einen anderen Computer in einer Arbeitsgruppe exportieren möchten, kopieren Sie die vorangehenden beiden Dateien an den gleichen Speicherort auf dem Computer, von dem

aus Sie mithilfe Server-Manager verwalten möchten.

So exportieren Sie Server-Manager-Einstellungen auf andere Computer in einer Domäne

1. Öffnen Sie unter "Active Directory-Benutzer und-Computer" das Dialogfeld "Eigenschaften" für einen Server-Manager Benutzer.
2. Fügen Sie auf der Registerkarte **Profil** einen Pfad zu einer Netzwerkfreigabe hinzu, um das Benutzerprofil zu speichern.
3. Führen Sie einen der folgenden Schritte aus:
 - Bei US-amerikanischen Builds (en-US) werden Änderungen an der Datei "**serverlist.XML**" automatisch im Profil gespeichert. Fahren Sie mit dem nächsten Schritt fort.
 - Kopieren Sie bei anderen Builds die beiden folgenden Dateien von dem Computer, auf dem Server-Manager ausgeführt wird, auf die Netzwerkfreigabe, die zum Roamingprofil des Benutzers gehört.
 - *%AppData% \ microsoft\windows\servermanager\serverlist.XML*
 - *%LocalAppData% \ Microsoft_Corporation \servermanager.exe_StrongName_GUID\6.2.0.0\user.config*
4. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld **Eigenschaften** zu schließen.

So exportieren Sie Server-Manager-Einstellungen auf andere Computer in Arbeitsgruppen

- Überschreiben Sie auf einem Computer, über den Sie Remote Server verwalten möchten, die beiden folgenden Dateien mit den gleichen Dateien von einem anderen Computer, auf dem Server-Manager ausgeführt wird und der über die gewünschten Einstellungen verfügt.
 - *%AppData% \ microsoft\windows\servermanager\serverlist.XML*
 - *%LocalAppData% \ Microsoft_Corporation \servermanager.exe_StrongName_GUID\6.2.0.0\user.config*

Verwalten des lokalen Servers und der Server-Manager-Konsole

09.04.2020 • 29 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In Windows Server können Sie mit Server-Manager sowohl den lokalen Server (wenn Sie Server-Manager auf Windows Server ausführen, nicht auf einem Windows-basierten Client Betriebssystem) als auch Remote Server verwalten, auf denen Windows Server 2008 und neuere Versionen des Windows Server-Betriebssystems ausgeführt werden.

Auf der Seite **lokaler Server** in Server-Manager werden Server Eigenschaften, Ereignisse, Dienst- und Leistungsdaten und Best Practices Analyzer Ergebnisse (BPA) für den lokalen Server angezeigt. Die Kacheln "Ereignis", "Dienst", "BPA" und "Leistung" funktionieren wie auf den Rollen- und Servergruppenseiten. Weitere Informationen zum Konfigurieren der Daten, die auf diesen Kacheln angezeigt werden, finden Sie unter [View and Configure Performance, Event, and Service Data](#) und [Run Best Practices Analyzer Scans and Manage Scan Results](#).

Menübefehle und Einstellungen in den Überschriften leisten der Server-Manager-Konsole werden global auf alle Server im Server Pool angewendet, und Sie können mit Server-Manager den gesamten Server Pool verwalten.

Dieses Thema enthält folgende Abschnitte:

- [Herunterfahren des lokalen Servers](#)
- [Konfigurieren von Server-Manager Eigenschaften](#)
- [Verwalten der Server-Manager Konsole](#)
- [Anpassen von Tools, die im Menü "Extras" angezeigt werden](#)
- [Verwalten von Rollen auf Rollen-Startseiten](#)

Herunterfahren des lokalen Servers

Im Menü **Aufgaben** auf der Kachel **Eigenschaften** des lokalen Servers können Sie eine Windows PowerShell-Sitzung auf dem lokalen Server starten, das MMC-Snap-in "**Computer Verwaltung**" öffnen oder MMC-Snap-Ins für Rollen oder Features öffnen, die auf dem lokalen Server installiert sind. Zudem kann der lokale Server mithilfe des Befehls **Lokalen Server herunterfahren** im Menü **Aufgaben** heruntergefahren werden. Der Befehl **Lokalen Server herunterfahren** ist für den lokalen Server auch auf der Kachel **Server** auf der Seite **Alle Server** oder auf einer Rollen- oder Gruppenseite verfügbar, auf der der lokale Server dargestellt wird.

Beim Herunterfahren des lokalen Servers mit dieser Methode wird im Gegensatz zum Herunterfahren von Windows Server 2016 über den **Start** Bildschirm das Dialogfeld **Windows herunterfahren** geöffnet, in dem Sie die Gründe für das Herunterfahren im Bereich **Ereignis Protokollierung** Herunterfahren angeben können.

NOTE

Nur Mitglieder der Gruppe "Administratoren" können einen Server herunterfahren oder neu starten. Standardbenutzer können einen Server weder herunterfahren noch neu starten. Wenn Sie auf den Befehl **Lokalen Server herunterfahren** klicken, werden Standardbenutzer von Serversitzungen abgemeldet. Dies entspricht der Erfahrung eines Standardbenutzers, der den Befehl **Alt+F4** zum Herunterfahren über den Server-Desktop ausführt.

Konfigurieren von Server-Manager Eigenschaften

Auf der Kachel **Eigenschaften** auf der Seite **Lokaler Server** können Sie die folgenden Einstellungen anzeigen oder ändern. Um den Wert einer Einstellung zu ändern, klicken Sie auf den Hypertext-Wert der Einstellung.

NOTE

Die auf der Kachel **Eigenschaften** des lokalen Servers angezeigten Eigenschaften können normalerweise nur auf dem lokalen Server geändert werden. Die Eigenschaften des lokalen Servers können nicht von einem Remote Computer mithilfe von Server-Manager geändert werden, da auf der Kachel **Eigenschaften** nur Informationen zum lokalen Computer, nicht für Remote Computer, angezeigt werden können.

Da viele Eigenschaften, die auf der Kachel **Eigenschaften** angezeigt werden, über Tools gesteuert werden, die nicht Teil Server-Manager sind (z. B. die Systemsteuerung), werden Änderungen an den **Eigenschaften** Einstellungen nicht immer sofort in der Kachel **Eigenschaften** angezeigt. Die Daten auf der Kachel **Eigenschaften** werden standardmäßig alle zwei Minuten aktualisiert. Um die Daten der Kachel **Eigenschaften** sofort zu aktualisieren, klicken Sie in der Server-Manager Adressleiste auf **Aktualisieren**.

EINSTELLUNG	BESCHREIBUNG
Computername	Zeigt den anzeigen amen des Computers an, und öffnet das Dialogfeld System Eigenschaften , in dem Sie den Namen des Servers, die Domänen Mitgliedschaft und andere System Einstellungen wie z. B. Benutzerprofile ändern können.
Domäne (oder Arbeitsgruppe, wenn der Server keiner Domäne angehört)	Zeigt die Domäne oder Arbeitsgruppe an, der der Server angehört. Öffnet das Dialogfeld System Eigenschaften , in dem Sie den Namen des Servers, die Domänen Mitgliedschaft und andere System Einstellungen wie z. B. Benutzerprofile ändern können.
Windows-Firewall	Zeigt den Status der Windows-Firewall für den lokalen Server an. Öffnet Systemsteuerung\System und Sicherheit\Windows-Firewall . Weitere Informationen zum Konfigurieren der Windows-Firewall finden Sie unter Windows-Firewall mit erweiterter Sicherheit und IPsec .
Remoteverwaltung	Zeigt Server-Manager und den Windows PowerShell-Remote Verwaltungsstatus an. Öffnet das Dialogfeld Remote Verwaltung konfigurieren . Weitere Informationen zur Remote Verwaltung finden Sie unter Konfigurieren der Remote Verwaltung in Server-Manager .
Remotedesktop	Zeigt an, ob Benutzer mithilfe von Remotedesktsitzungen eine Remoteverbindung mit dem Server herstellen können. Öffnet die Registerkarte Remote im Dialogfeld System Eigenschaften .

EINSTELLUNG	BESCHREIBUNG
NIC-Teamvorgang	Zeigt an, ob der lokale Server am NIC-Teamvorgang teilnimmt. Öffnet das Dialogfeld NIC-Teamvorgang . Wenn Sie möchten, können Sie hier den lokalen Server einem NIC-Team hinzufügen. Weitere Informationen zum NIC-Teamvorgang finden Sie im Whitepaper zum NIC-Teamvorgang .
Ethernet	Zeigt den Netzwerkstatus des Servers an. Öffnet Systemsteuerung\Netzwerk und Internet\Netzwerkverbindungen .
Betriebssystemversion	In diesem schreibgeschützten Feld wird die Versionsnummer des Windows-Betriebssystems angezeigt, das auf dem lokalen Server ausgeführt wird.
Hardwareinformationen	In diesem schreibgeschützten Feld werden Hersteller, Modellname und -nummer der Serverhardware angezeigt.
Zuletzt installierte Updates	Zeigt den Tag und die Uhrzeit der letzten Installation von Windows-Updates an. Öffnet Systemsteuerung\System und Sicherheit\Windows Update .
Windows Update	Zeigt die Windows Update-Einstellungen für den lokalen Server an. Öffnet Systemsteuerung\System und Sicherheit\Windows Update .
Zuletzt auf Updates geprüft	Zeigt den Tag und die Uhrzeit der letzten Überprüfung des Servers auf verfügbare Windows-Updates an. Öffnet Systemsteuerung\System und Sicherheit\Windows Update .
Windows-Fehlerberichterstattung	Zeigt den Anmeldestatus der Windows-Fehlerberichterstattung an. Öffnet das Dialogfeld Windows-Fehlerberichterstattungs-Konfiguration . Weitere Informationen zur Windows-Fehlerberichterstattung, zu den Vorteilen, Datenschutzbestimmungen und Anmeldeeinstellungen finden Sie unter Windows-Fehlerberichterstattung .
Programm zur Verbesserung der Benutzerfreundlichkeit	Zeigt den Anmeldestatus des Programms zur Verbesserung der Benutzerfreundlichkeit von Windows an. Öffnet das Dialogfeld Konfiguration des Programms zur Verbesserung der Benutzerfreundlichkeit . Weitere Informationen zum Programm zur Verbesserung der Benutzerfreundlichkeit von Windows, zu den Vorteilen und Anmeldeeinstellungen finden Sie unter Programm zur Verbesserung der Benutzerfreundlichkeit von Windows .

EINSTELLUNG	BESCHREIBUNG
Verstärkte Sicherheitskonfiguration für Internet Explorer (IE)	Zeigt, ob die Verstärkte Sicherheitskonfiguration für IE (auch als IE Hardening oder IE ESC bezeichnet) aktiviert oder deaktiviert ist. Öffnet das Dialogfeld Verstärkte Sicherheitskonfiguration für Internet Explorer . Die verstärkte Sicherheitskonfiguration für IE ist eine Sicherheitsmaßnahme für Server, mit der verhindert wird, dass Webseiten in Internet Explorer geöffnet werden. Weitere Informationen zur verstärkten Sicherheitskonfiguration für Internet Explorer, zu den Vorteilen und Einstellungen finden Sie unter Verstärkte Sicherheitskonfiguration für Internet Explorer .
Zeitzone	Zeigt die Zeitzone des lokalen Servers an. Öffnet das Dialogfeld Datum und Uhrzeit .
Product ID	Zeigt den Status der Windows-Aktivierung und die Produkt-ID (sofern Windows aktiviert wurde) des Betriebssystems Windows Server 2016 an. Hierbei handelt es sich nicht um den Windows-Product Key. Öffnet das Dialogfeld Windows-Aktivierung .
Prozessoren	In diesem schreibgeschützten Feld werden Hersteller, Modellname und Geschwindigkeitsinformationen zu den Prozessoren des lokalen Servers angezeigt.
Installierter Arbeitsspeicher (RAM)	In diesem schreibgeschützten Feld wird die Größe des verfügbaren Arbeitsspeichers in Gigabyte angezeigt.
Speicherplatz insgesamt	In diesem schreibgeschützten Feld wird die Größe des verfügbaren Festplattenspeichers in Gigabyte angezeigt.

Verwalten der Server-Manager Konsole

Globale Einstellungen, die für die gesamte Server-Manager-Konsole gelten, sowie für alle Remote Server, die dem Server-Manager-Server Pool hinzugefügt wurden, befinden sich in den Überschriften leisten oben im Server-Manager Konsolenfenster.

Server zu Server-Manager hinzufügen

Mit dem Befehl, mit dem das Dialogfeld **Server hinzufügen** geöffnet wird und Sie dem Server-Manager Server-Pool physische oder virtuelle Remote Server hinzufügen können, befindet sich im Menü **Verwalten** der Server-Manager Konsole. Ausführliche Informationen zum Hinzufügen von Servern finden Sie unter [Hinzufügen von Servern zu Server-Manager](#).

Aktualisieren von Daten, die in Server-Manager angezeigt werden

Sie können das Aktualisierungs Intervall für Daten konfigurieren, die in Server-Manager im Dialogfeld **Server-Manager Eigenschaften** angezeigt werden, das Sie über das Menü **Verwalten** öffnen.

So konfigurieren Sie das Aktualisierungsintervall in Server-Manager

1. Klicken Sie in der Server-Manager Konsole im Menü **Verwalten** auf **Server-Manager Eigenschaften**.
2. Geben Sie im Dialogfeld **Eigenschaften von Server-Manager** einen Zeitraum (in Minuten) für die verstrichene Zeit in Minuten zwischen den Aktualisierungen der in Server-Manager angezeigten Daten an. Der Standardwert ist 10 Minuten. Klicken Sie anschließend auf OK.

Aktualisierungsbeschränkungen

Die Aktualisierung gilt global für Daten von allen Servern, die Sie dem Server-Manager-Server Pool hinzugefügt

haben. Es können keine Daten für einzelne Server, Rollen und Gruppen aktualisiert oder für einzelne Server, Rollen und Gruppen unterschiedliche Aktualisierungintervalle konfiguriert werden.

Wenn Server, die sich in einem Cluster befinden, Server-Manager hinzugefügt werden, und zwar unabhängig davon, ob es sich um physische oder virtuelle Computer handelt, kann bei der ersten Datenaktualisierung ein Fehler auftreten, oder es werden nur Daten für den Host Server für Cluster Objekte angezeigt. Bei nachfolgenden Aktualisierungen werden die genauen Daten für physische oder virtuelle Server in einem Servercluster angezeigt.

Daten, die auf den Startseiten der Rolle in Server-Manager für Remotedesktopdienste, die IP-Adressverwaltung und die Datei-und Speicherdiene angezeigt werden, werden nicht automatisch aktualisiert. Aktualisieren Sie die auf diesen Seiten angezeigten Daten manuell, indem Sie F5 drücken oder in der Server-Manager-Konsolen Überschrift auf **Aktualisieren** klicken, während Sie sich auf diesen Seiten befinden.

Rollen oder Features hinzufügen oder entfernen

Die Befehle, mit denen der Assistent zum Hinzufügen von Rollen und Features und der Assistent zum Entfernen von Rollen und Features geöffnet werden, und das Hinzufügen oder Entfernen von Rollen, Rollen Diensten und Features zu Servern in Ihrem Server Pool finden Sie im Menü **Verwalten** der Server-Manager-Konsole und im Menü **Aufgaben** der Kachel **Rollen und Features** auf Rollen-oder Gruppen Seiten. Ausführlichere Informationen zum Hinzufügen oder Entfernen von Rollen oder Features finden Sie unter [Installieren oder Deinstallieren von Rollen, Rollendiensten oder Features](#).

In Server-Manager werden Rollen-und Featuredaten in der Basis Sprache des Systems, auch als "System Default GUI Language" bezeichnet, oder der während der Installation des Betriebssystems ausgewählten Sprache angezeigt.

Erstellen von Server Gruppen

Der Befehl, mit dem das Dialogfeld **Server Gruppe erstellen** geöffnet wird, in dem Sie benutzerdefinierte Server Gruppen erstellen können, befindet sich im Menü **Verwalten** der Server-Manager Konsole. Ausführliche Informationen zum Erstellen von Server Gruppen finden Sie unter [Erstellen und Verwalten von Server Gruppen](#).

Verhindern, dass Server-Manager beim Anmelden automatisch geöffnet wird

Mit dem Kontrollkästchen **Server-Manager nicht automatisch bei der Anmeldung starten** im Dialogfeld **Server-Manager Eigenschaften** wird gesteuert, ob Server-Manager bei der Anmeldung für Mitglieder der Gruppe "Administratoren" auf einem lokalen Server automatisch geöffnet wird. Diese Einstellung wirkt sich nicht auf das Server-Manager Verhalten aus, wenn es unter Windows 10 als Teil Remoteserver-Verwaltungstools ausgeführt wird. Weitere Informationen zum Konfigurieren dieser Einstellung finden Sie unter [Server-Manager](#).

Vergrößern oder Verkleinern

Wenn Sie die Ansicht der Server-Manager Konsole vergrößern oder verkleinern möchten, können Sie entweder die Zoom -Befehle im Menü **Ansicht** verwenden oder Strg + Plus (+) drücken, um zu vergrößern und STRG + minus (-) zu verkleinern.

Anpassen von Tools, die im Menü "Extras" angezeigt werden

Das Menü **Extras** in Server-Manager enthält weiche Links zu Verknüpfungen im Ordner **Verwaltung** unter **Systemsteuerung/System und Sicherheit**. Der Ordner **Verwaltung** enthält eine Liste mit Verknüpfungen oder LNK-Dateien zu verfügbaren Verwaltungs Tools wie MMC-Snap-Ins. Server-Manager füllt das Menü **Extras** mit Links zu diesen Verknüpfungen auf und kopiert die Ordner Struktur des Ordners **Verwaltung** in das Menü Extras. Die Tools im Ordner "Verwaltung" werden standardmäßig in einer flachen Liste angeordnet und nach Typ und nach Name sortiert. Im Menü **Server-Manager Extras** werden Elemente nur nach Name, nicht nach Typ sortiert.

Wenn Sie das Menü **Tools** anpassen möchten, kopieren Sie die gewünschten Tool- oder Skriptverknüpfungen in den Ordner **Verwaltung**. Sie können Ihre Verknüpfungen auch in Ordnern organisieren, die im Menü **Tools** hierarchische Menüs bilden. Wenn Sie den Zugriff auf die benutzerdefinierten Tools im Menü **Extras** einschränken möchten, können Sie außerdem Benutzer Zugriffsrechte für Ihre benutzerdefinierten Tool Ordner in "Verwaltung"

oder direkt auf dem ursprünglichen Tool bzw. in den Skriptdateien festlegen.

Es wird empfohlen, System- und Verwaltungstools sowie Rollen und Features zugeordnete Verwaltungstools, die auf dem lokalen Server installiert sind, nicht neu zu organisieren. Wenn Verwaltungstools von Rollen und Features verschoben werden, können sie bei Bedarf möglicherweise nicht deinstalliert werden. Nach der Deinstallation einer Rolle oder eines Features bleibt möglicherweise ein defekter Link zu einem Tool, dessen Verknüpfung verschoben wurde, im Menü **Tools** zurück. Beim erneuten Installieren der Rolle wird im Menü **Tools** ein doppelter Link zum selben Tool erstellt, aber einer der Links ist defekt.

Rollen- und Featuretools, die als Teil der Remoteserver-Verwaltungstools auf einem clientbasierten Windows-Computer installiert werden, können jedoch in benutzerdefinierten Ordnern organisiert werden. Das Deinstallieren der übergeordneten Rolle oder des übergeordneten Features hat keine Auswirkungen auf die Tool Verknüpfungen, die auf einem Remote Computer unter Windows 10 verfügbar sind.

Im folgenden Verfahren wird beschrieben, wie ein Beispiel Ordner mit dem Namen *mytools* erstellt und Verknüpfungen für zwei Windows PowerShell-Skripts in den Ordner verschoben werden, auf den dann über das Menü Server-Manager Tools zugegriffen werden kann.

So passen Sie das Menü "Extras" durch Hinzufügen von Verknüpfungen in "Verwaltung" an

1. Erstellen Sie einen neuen Ordner mit dem Namen *mytools* an einem geeigneten Speicherort.

NOTE

Aufgrund von restriktiven Zugriffsrechten für den Ordner **Verwaltung** dürfen Sie keinen Ordner direkt im Ordner **Verwaltung** erstellen. Sie müssen einen neuen Ordner an einem anderen Speicherort (z. B. auf dem Desktop) erstellen und ihn anschließend in den Ordner **Verwaltung** kopieren.

2. Verschieben oder kopieren Sie *mytools* in **Systemsteuerung/System und Sicherheit/Verwaltungs Tools**. Sie müssen Mitglied der Gruppe "Administratoren" auf dem Computer sein, um Änderungen am Ordner **Verwaltung** vornehmen zu können.
3. Wenn Sie die Benutzer Zugriffsrechte für Ihre benutzerdefinierten Tool Verknüpfungen nicht einschränken müssen, fahren Sie mit Schritt 6 fort. Andernfalls klicken Sie mit der rechten Maustaste auf die Tooldatei (oder den Ordner *MeineTools*), und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie im Dialogfeld **Eigenschaften** der Datei auf der Registerkarte **Sicherheit** auf **Bearbeiten**.
5. Deaktivieren Sie für Benutzer, für die Sie den Zugriff auf das Tool einschränken möchten, die Kontrollkästchen für **Lese & Berechtigungen ausführen, Lesen und Schreiben**. Diese Berechtigungen werden von der Toolverknüpfung im Ordner **Verwaltung** übernommen.

Wenn Sie die Zugriffsrechte eines Benutzers bearbeiten, während der Benutzer Server-Manager verwendet (oder wenn Server-Manager geöffnet ist), werden Ihre Änderungen im Menü **Extras** erst angezeigt, wenn der Benutzer Server-Manager neu startet.

NOTE

Wenn Sie den Zugriff auf einen vollständigen Ordner beschränken, den Sie in "Verwaltung" kopiert haben, können Benutzer mit eingeschränkten Berechtigungen weder den Ordner noch dessen Inhalt im Menü **Server-ManagerTools** anzeigen.

Bearbeiten Sie die Berechtigungen für den Ordner im Ordner **Verwaltung**. Da ausgeblendete Dateien und Ordner in "Verwaltung" immer im Menü "Server-ManagerTools" angezeigt werden, verwenden Sie die Einstellung **ausgeblendet** im Dialogfeld **Eigenschaften** einer Datei oder eines Ordners nicht, um den Benutzer Zugriff auf Ihre benutzerdefinierten Tool Verknüpfungen einzuschränken.

Mit der Berechtigung **Verweigern** wird die Berechtigung **Zulassen** immer überschrieben.

6. Klicken Sie mit der rechten Maustaste auf das ursprüngliche Tool, das Skript oder die ausführbare Datei, für das Sie im Menü Extras Einträge hinzufügen möchten, und klicken Sie dann auf **Verknüpfung erstellen**.
7. Verschieben Sie die Verknüpfung in den Ordner " *mytools* " unter "Verwaltung".
8. Wenn erforderlich, können Sie Server-Manager aktualisieren oder neu starten, um die Verknüpfung des Benutzer definierten Tools im Menü Extras anzuzeigen.

Verwalten von Rollen auf Rollen-Startseiten

Nachdem Sie dem Server-Manager Server Pool Server hinzugefügt haben und Server-Manager Inventur Daten zu Servern in Ihrem Pool sammelt, werden dem Navigationsbereich von Server-Manager Seiten für Rollen hinzugefügt, die auf verwalteten Servern erkannt werden. Auf der Kachel **Server** auf Rollenseiten werden verwaltete Server aufgelistet, von denen die Rolle ausgeführt wird. Standardmäßig werden auf den Kacheln **Ereignisse, Best Practices Analyzer, Dienste und Leistung** Daten für alle Server angezeigt, von denen die Rolle ausgeführt wird. Durch Auswahl bestimmter Server auf der Kachel **Server** wird der Bereich von Ereignissen, Diensten, Leistungsindikatoren und BPA-Ergebnissen auf die ausgewählten Server eingeschränkt. Verwaltungs Tools sind in der Regel im Menü "Server-Manager-Konsolen Tools" verfügbar, nachdem eine Rolle oder ein Feature auf einem verwalteten Server installiert oder erkannt wurde. Sie können auf der Kachel **Server** für eine Rolle oder Gruppe mit der rechten Maustaste auf Servereinträge klicken und dann das gewünschte Verwaltungstool starten.

In Windows Server 2016 verfügen die folgenden Rollen und Features über Verwaltungs Tools, die in Server-Manager-Konsole als Seiten integriert sind.

- **Datei- und Speicherdienste.** Die Seiten für Datei- und Speicherdienste enthalten benutzerdefinierte Kacheln und Befehle zum Verwalten von Volumes, Freigaben, virtuellen iSCSI-Datenträgern und Speicherpools. Wenn Sie die Startseite der Rolle "Datei- und Speicherdienste" in Server-Manager öffnen, wird ein zurücknahmebereich geöffnet, in dem benutzerdefinierte Verwaltungs Seiten für Datei- und Speicherdienste angezeigt werden. Weitere Informationen zum Bereitstellen und Verwalten von Datei- und Speicherdiensten finden Sie unter [Datei- und Speicherdienste](#).
- **Remotedesktopdienste.** Die Seiten für Remotedesktopdienste enthalten benutzerdefinierte Kacheln und Befehle zum Verwalten von Sitzungen, Lizzen, Gateways und virtuellen Desktops. Weitere Informationen zum Bereitstellen und Verwalten von Remotedesktopdienste finden Sie unter [Remotedesktopdienste \(rdS\)](#).
- **IP-Adressverwaltung (IP Address Management, IPAM)** Die Rollenseite für die IP-Adressverwaltung enthält die benutzerdefinierte Kachel **Willkommen** mit Links zu allgemeinen IPAM-Konfigurations- und IPAM-Verwaltungsaufgaben, inklusive eines Assistenten zum Bereitstellen eines IPAM-Servers. Die IPAM-Homepage enthält zudem Kacheln zum Anzeigen des verwalteten Netzwerks, einer Übersicht über die Konfiguration sowie geplanter Aufgaben.

Es gibt einige Einschränkungen für die IPAM-Verwaltung in Server-Manager. Im Gegensatz zu anderen Rollen- und Gruppenseiten befinden sich auf der IPAM-Seite keine Kacheln für **Server, Ereignisse, Leistung, Best Practices Analyzer und Dienste**. Für IPAM ist kein Best Practices Analyzer Modell verfügbar. Best Practices Analyzer Scans in IPAM werden nicht unterstützt. Wenn Sie auf Server in Ihrem Serverpool zugreifen möchten, auf denen IPAM ausgeführt wird, erstellen Sie eine benutzerdefinierte Gruppe mit diesen Servern, und greifen Sie über die Kachel **Server** auf der benutzerdefinierten Gruppenseite auf die Serverliste zu. Sie können auf IPAM-Server auch über die Kachel **Server** auf der Gruppenseite **Alle Server** zugreifen.

In Miniaturansichten im Dashboard wird im Vergleich zu Miniaturansichten für andere Rollen und Gruppen nur eine begrenzte Anzahl Zeilen für IPAM angezeigt. Wenn Sie auf die Zeile mit IPAM-Miniaturansichten klicken, können Sie Ereignisse, Leistungsdaten und Verwaltbarkeitsstatuswarnungen für Server anzeigen, auf denen IPAM ausgeführt wird. IPAM-bezogene Dienste können über Seiten für Servergruppen verwaltet werden, die IPAM-Server enthalten, wie die Seite für die Gruppe **Alle Server**.

Weitere Informationen zum Bereitstellen und Verwalten von IPAM finden Sie unter [IP Address Management \(IPAM\)](#).

Weitere Informationen

[Server-Manager Hinzufügen von Servern zu Server-Manager](#) [Erstellen und Verwalten von Server Gruppen anzeigen und Konfigurieren von Leistungs-, Ereignis-und Dienst Daten](#) [Datei- und Speicherdiene](#) [Remotedesktopdienste \(rdS\)](#) [IP-Adressverwaltung \(IPAM\)](#)

Konfigurieren der Remote Verwaltung in Server-Manager

09.04.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In Windows Server können Sie Server-Manager verwenden, um Verwaltungsaufgaben auf Remote Servern auszuführen. die Remote Verwaltung ist auf Servern, auf denen Windows Server 2016 ausgeführt wird, standardmäßig aktiviert. Wenn Sie einen Server mithilfe von Server-Manager Remote verwalten möchten, fügen Sie den Server zum Server-Manager Server Pool hinzu.

Sie können Server-Manager zum Verwalten von Remote Servern verwenden, auf denen ältere Versionen von Windows Server ausgeführt werden, aber die folgenden Updates sind erforderlich, um diese älteren Betriebssysteme vollständig verwalten zu können.

Zum Verwalten von Servern, auf denen Windows Server-Versionen älter als Windows Server 2016 ausgeführt werden, installieren Sie die folgende Software und Updates, um die älteren Versionen von Windows Server mithilfe von Server-Manager in Windows Server 2016 verwaltbar zu machen.

BETRIEBSSYSTEM	ERFORDERLICHE SOFTWARE	VERWALTBARKEIT
Windows Server 2012 R2 oder Windows Server 2012	<ul style="list-style-type: none">- .NET Framework 4.6- Windows Management Framework 5.0. Das Windows Management Framework 5.0 Download Package Updates Windows-Verwaltungsinstrumentation (WMI)-Anbieter unter Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2. Mit den aktualisierten WMI-Anbietern können Server-Manager Informationen zu den auf den verwalteten Servern installierten Rollen und Features sammeln. Bis zum Anwenden des Updates haben Server, auf denen Windows Server 2012 R2, Windows Server 2012 oder Windows Server 2008 R2 ausgeführt wird, den verwaltbarkeitsstatus nicht zugänglich. -Das mit dem Knowledge Base-Artikel 2682011 verknüpfte Leistungs Update ist auf Servern mit Windows Server 2012 R2 oder Windows Server 2012 nicht mehr erforderlich.	

BETRIEBSSYSTEM	ERFORDERLICHE SOFTWARE	VERWALTBARKEIT
Windows Server 2008 R2	<ul style="list-style-type: none"> - .NET Framework 4,5 - Windows Management Framework 4,0. Das Windows Management Framework 4,0-Downloadpaket aktualisiert Windows-Verwaltungsinstrumentation (WMI)-Anbieter unter Windows Server 2008 R2. Mit den aktualisierten WMI-Anbietern können Server-Manager Informationen zu den auf den verwalteten Servern installierten Rollen und Features sammeln. Bis zum Anwenden des Updates haben Server, auf denen Windows Server 2008 R2 ausgeführt wird, den verwaltbarkeitsstatus nicht zugänglich. -Das mit dem Knowledge Base-Artikel 2682011 verknüpfte Leistungs Update ermöglicht Server-Manager die Erfassung von Leistungsdaten von Windows Server 2008 R2. 	
WindowsServer 2008	<ul style="list-style-type: none"> - .NET Framework 4 - Windows Management Framework 3,0 Windows Management Framework 3,0 Download Package Updates Windows-Verwaltungsinstrumentation (WMI)-Anbieter unter Windows Server 2008. Mit den aktualisierten WMI-Anbietern können Server-Manager Informationen zu den auf den verwalteten Servern installierten Rollen und Features sammeln. Bis zum Anwenden des Updates haben Server, auf denen Windows Server 2008 ausgeführt wird, den verwaltbarkeitsstatus nicht verfügbar: Überprüfen Sie, ob frühere Versionen Windows Management Framework 3,0 ausführen. -Das mit dem Knowledge Base-Artikel 2682011 verknüpfte Leistungs Update ermöglicht Server-Manager die Erfassung von Leistungsdaten von Windows Server 2008. 	

Ausführliche Informationen zum Hinzufügen von Servern in zu verwaltenden Arbeitsgruppen oder zum Verwalten von Remote Servern über einen Arbeitsgruppen Computer, auf dem Server-Manager ausgeführt wird, finden [Sie unter Hinzufügen von Servern zu Server-Manager](#).

Aktivieren oder Deaktivieren der Remoteverwaltung

In Windows Server 2016 ist die Remote Verwaltung standardmäßig aktiviert. Bevor Sie mit Server-Manager eine Remote Verbindung mit einem Computer herstellen können, auf dem Windows Server 2016 ausgeführt wird, muss Server-Manager Remote Verwaltung auf dem Zielcomputer aktiviert sein, wenn er deaktiviert wurde. In den Prozeduren dieses Abschnitts werden die Vorgehensweise zum Deaktivieren der Remoteverwaltung sowie die Vorgehensweise zum Reaktivieren der deaktivierten Remoteverwaltung beschrieben. In der Server-Manager

Konsole wird der Remote Verwaltungsstatus für den lokalen Server im Bereich **Eigenschaften** der Seite **lokaler Server** angezeigt.

Von den lokalen Administratorkonten verfügt unter Umständen nur das integrierte Administratorkonto über Rechte für die Remoteverwaltung eines Servers. Dies gilt auch bei aktivierter Remoteverwaltung. Die Registrierungs Einstellung **LocalAccountTokenFilterPolicy** der Remote-Benutzerkontensteuerung (User Account Control, UAC) muss so konfiguriert werden, dass lokale Konten der Gruppe "Administratoren" außer dem integrierten Administrator Konto für die Remote Verwaltung des Servers zugelassen werden.

In Windows Server 2016 stützt Server-Manager die Windows-Remote Verwaltung (WinRM) und das verteilte Component Object Model (DCOM) für die Remote Kommunikation. Die Einstellungen, die im Dialogfeld **Remote Verwaltung konfigurieren** gesteuert werden, wirken sich nur auf Teile von Server-Manager und Windows PowerShell aus, von denen WinRM für die Remote Kommunikation verwendet wird. Sie wirken sich nicht auf Teile von Server-Manager aus, die DCOM für die Remote Kommunikation verwenden. Beispielsweise verwendet Server-Manager WinRM für die Kommunikation mit Remote Servern, auf denen Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, verwendet aber DCOM für die Kommunikation mit Servern, auf denen Windows Server 2008 und Windows Server 2008 R2 ausgeführt wird, auf denen jedoch nicht [Windows Management Framework 4.0](#) oder [Windows Management Framework 3.0](#) installiert ist. Die Microsoft Management Console (MMC) und andere Legacy Verwaltungs Tools verwenden DCOM. Weitere Informationen zum Ändern dieser Einstellungen finden Sie unter so [Konfigurieren Sie MMC oder andere Tools Remote Verwaltung über DCOM](#) in diesem Thema.

NOTE

Die Prozeduren in diesem Abschnitt können nur auf Computern unter Windows Server ausgeführt werden. Mithilfe der folgenden Verfahren können Sie die Remote Verwaltung auf einem Computer unter Windows 10 nicht aktivieren oder deaktivieren, da das Client Betriebssystem nicht mithilfe von Server-Manager verwaltet werden kann.

- Wählen Sie zum Aktivieren der WinRM-Remoteverwaltung eines der folgenden Verfahren:
 - [So aktivieren Sie Server-Manager-Remote Verwaltung mithilfe der Windows-Benutzeroberfläche](#)
 - [So aktivieren Sie Server-Manager-Remote Verwaltung mithilfe von Windows PowerShell](#)
 - [So aktivieren Sie Server-Manager-Remote Verwaltung über die Befehlszeile](#)
 - [So aktivieren Sie die Remote Verwaltung von Server-Manager und Windows PowerShell unter früheren Versionen von Windows Server](#)
- Wählen Sie eines der folgenden Verfahren aus, um WinRM und Server-Manager Remote Verwaltung zu deaktivieren.
 - [So deaktivieren Sie die Remote Verwaltung mithilfe von Gruppenrichtlinie](#)
 - [So deaktivieren Sie die Remote Verwaltung mithilfe einer Antwortdatei während der unbeaufsichtigten Installation](#)
- Informationen zum Konfigurieren der DCOM-Remoteverwaltung finden Sie unter [So konfigurieren Sie die Remoteverwaltung mit der MMC oder einem anderen Tool über DCOM](#).

So aktivieren Sie die Remoteverwaltung des Server-Managers auf der Windows-Benutzeroberfläche

1. **NOTE**

Die Einstellungen, die im Dialogfeld **Remote Verwaltung konfigurieren** gesteuert werden, wirken sich nicht auf Teile von Server-Manager aus, die DCOM für die Remote Kommunikation verwenden.

Öffnen Sie auf dem Computer, den Sie remote verwalten möchten, Server-Manager, falls dieser nicht bereits geöffnet ist. Klicken Sie auf der Windows-Taskleiste auf **Server-Manager**. Klicken Sie auf dem **Start** Bildschirm auf die Kachel **Server-Manager**.

2. Klicken Sie im Bereich **Eigenschaften** der Seite **lokale Server** auf den hyperverknüpften Wert für die Eigenschaft **Remote Verwaltung**.

3. Führen Sie einen der folgenden Schritte aus, und klicken Sie anschließend auf **OK**:

- Deaktivieren Sie das Kontrollkästchen **Remote Verwaltung dieses Servers von anderen Computern aktivieren**, um zu verhindern, dass dieser Computer mithilfe Server-Manager (oder mithilfe von Windows PowerShell bei der Installation) Remote verwaltet wird.
- Um die Remote Verwaltung dieses Computers mithilfe von Server-Manager oder Windows PowerShell zuzulassen, wählen Sie **Remote Verwaltung dieses Servers von anderen Computern aktivieren aus**.

So aktivieren Sie die Remoteverwaltung des Server-Managers mithilfe von Windows PowerShell

1. Führen Sie auf dem Computer, den Sie per Remote Zugriff verwalten möchten, eine der folgenden Aktionen aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.

- Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
- Klicken Sie auf dem Windows- **Start** Bildschirm mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.

2. Geben Sie Folgendes ein, und drücken **Sie** dann die **EINGABETASTE**, um alle erforderlichen Firewallregelausnahmen zu aktivieren.

Configure-SMRemoting.exe-enable

So aktivieren Sie die Remoteverwaltung des Server-Managers über die Befehlszeile

1. Öffnen Sie auf dem Computer, den Sie per Remotezugriff verwalten möchten, eine Eingabeaufforderungssitzung mit erhöhten Benutzerrechten. Geben Sie hierzu im **Start** Bildschirm **cmd** ein, klicken Sie mit der rechten Maustaste auf die Kachel **Eingabeaufforderung**, wenn diese in den **apps - Ergebnissen** angezeigt wird, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.

2. Führen Sie die folgende ausführbare Datei aus:

%windir%\system32\konfiguriert-SMRemoting.exe

3. Führen Sie eine der folgenden Aktionen aus:

- Um die Remote Verwaltung zu deaktivieren, geben Sie **configure-SMRemoting.exe-deaktiviere** ein, und drücken Sie dann die **EingabeTaste**.
- Um die Remote Verwaltung zu aktivieren, geben Sie **configure-SMRemoting.exe-enable** ein, und drücken Sie dann die **EingabeTaste**.
- Wenn Sie die aktuelle Remote Verwaltungs Einstellung anzeigen möchten, geben Sie **configure-SMRemoting.exe-get** ein, und drücken Sie dann die **EINGABETASTE**.

So aktivieren Sie die Remoteverwaltung von Server-Manager und Windows PowerShell für ältere Versionen von Windows Server

• Führen Sie eine der folgenden Aktionen aus:

- Informationen zum Aktivieren der Remote Verwaltung auf Servern, auf denen Windows Server 2012 ausgeführt wird, finden Sie unter so [Aktivieren Sie Server-Manager-Remote Verwaltung mithilfe der](#)

[Windows-Benutzeroberfläche](#) in diesem Thema.

- Informationen zum Aktivieren der Remote Verwaltung auf Servern, auf denen Windows Server 2008 R2 ausgeführt wird, finden Sie unter [Remote Verwaltung mit Server-Manager](#) in der Hilfe zu Windows Server 2008 R2.
- Informationen zum Aktivieren der Remote Verwaltung auf Servern, auf denen Windows Server 2008 ausgeführt wird, finden Sie unter [aktivieren und Verwenden von Remote Befehlen in Windows PowerShell](#).

So konfigurieren Sie die Remote Verwaltung von MMC oder einem anderen Tool über DCOM

1. Führen Sie eine der folgenden Aktionen aus, um die Windows-Firewall mit dem Snap-In für erweiterte Sicherheit zu öffnen:
 - Klicken Sie im Bereich **Eigenschaften** der Seite **lokaler Server** in Server-Manager auf den Hypertext-Wert für die Eigenschaft **Windows-Firewall**, und klicken Sie dann auf **Erweiterte Einstellungen**.
 - Geben Sie auf dem **Start** Bildschirm **WF. mscein**, und klicken Sie dann auf die Snap-in-Kachel, wenn Sie in den **apps**-Ergebnissen angezeigt wird.
2. Wählen Sie im Bereich mit der Struktur die Option **Eingehende Regeln** aus.
3. Vergewissern Sie sich, dass Ausnahmen für die folgenden Firewallregeln aktiviert sind und nicht durch Gruppenrichtlinie Einstellungen deaktiviert wurden. Ist eine der Optionen nicht aktiviert, fahren Sie mit dem nächsten Schritt fort.
 - COM+-Netzwerkzugriff (DCOM-In)
 - Remote-Ereignisprotokoll Verwaltung (NP eingehend)
 - Remote-Ereignisprotokoll Verwaltung (RPC)
 - Remote-Ereignisprotokoll Verwaltung (RPC-EPMAP)
4. Klicken Sie mit der rechten Maustaste auf die nicht aktivierte Regeln, und klicken Sie anschließend im Kontextmenü auf **Regel aktivieren**.
5. Schließen Sie das Snap-In **Windows-Firewall mit erweiterter Sicherheit**.

So deaktivieren Sie die Remoteverwaltung mithilfe von Gruppenrichtlinien

1. Führen Sie eine der folgenden Aktionen aus, um den Editor für lokale Gruppenrichtlinie zu öffnen
 - Geben Sie auf einem Server unter Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 auf dem **Start** Bildschirm **gpeer dit. mscein**, und klicken Sie dann auf die Kachel **gpeer dit**, wenn diese angezeigt wird.
 - Geben Sie auf einem Server unter Windows Server 2008 R2 oder Windows Server 2008 im Dialogfeld **Ausführen** den Befehl **gpeer dit. mscein**, und drücken Sie dann die **EingabeTaste**.
2. Öffnen Sie **Computerkonfiguration\Administrative Vorlagen\Windows-komponenten\windows-Remoteverwaltung (WinRM) \winrm-Dienst**.
3. Doppelklicken Sie im Inhaltsbereich auf **Remoteserververwaltung über WinRM zulassen**.
4. Wählen Sie im Dialogfeld für die Richtlinieneinstellung **Remoteserververwaltung über WinRM zulassen** die Option **Deaktiviert** aus, um die Remoteverwaltung zu deaktivieren. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld für die Richtlinieneinstellung zu schließen.

So deaktivieren Sie die Remoteverwaltung mithilfe einer Antwortdatei während einer unbeaufsichtigten Installation

1. Erstellen Sie mithilfe von Windows System Image Manager (Windows SIM) eine Antwortdatei für die unbeaufsichtigte Installation für Windows Server 2016-Installationen. Weitere Informationen zum Erstellen einer Antwortdatei und zum Verwenden von Windows SIM finden Sie unter [Was ist der Windows System Image Manager?](#) und [Schrittweise Anleitung: Grundlegende Windows-Bereitstellung für IT-Spezialisten.](#)
2. Suchen Sie in der Antwortdatei die Einstellung **Microsoft-Windows-Web-Services-for-Management-Core\EnableServerremoteManagement**.
3. Wenn Sie Server-Manager Remote Verwaltung standardmäßig auf allen Servern deaktivieren möchten, auf die die Antwortdatei angewendet werden soll, legen Sie **Microsoft-Windows-Web-Services-for-Management-Core\enableserverremotemanagement** auf **false**fest.

NOTE

Durch diese Einstellung wird die Remoteverwaltung bei der Installation des Betriebssystems deaktiviert. Durch das Konfigurieren dieser Einstellung wird verhindert, dass ein Administrator Server-Manager Remote Verwaltung auf einem Server aktiviert, nachdem das Betriebssystem Setup beendet wurde. Administratoren können Server-Manager Remote Verwaltung erneut aktivieren, indem Sie die Schritte in [zum Konfigurieren Server-Manager der Remote Verwaltung mithilfe der Windows-Benutzeroberfläche](#) oder [zum Aktivieren der Server-Manager-Remote Verwaltung mithilfe von Windows PowerShell](#) in diesem Thema ausführen.

Wenn Sie die Remote Verwaltung standardmäßig im Rahmen einer unbeaufsichtigten Installation deaktivieren und die Remote Verwaltung auf dem Server nach der Installation nicht wieder aktivieren, können Server, auf die diese Antwortdatei angewendet wird, nicht vollständig mithilfe Server-Manager verwaltet werden. Server, auf denen Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird (und die Remote Verwaltung standardmäßig deaktiviert haben), generieren verwaltbarkeitsstatusfehler in der Server-Manager-Konsole, nachdem Sie dem Server-Manager Server Pool hinzugefügt wurden.

WinRM-Listenereinstellungen (Windows Remote Management)

Server-Manager stützt sich auf den Remote Servern, die Sie verwalten möchten, auf den Standardeinstellungen des WinRM-Listener. Wenn der Standard Authentifizierungsmechanismus oder die WinRM-listenerportnummer auf einem Remote Server von den Standardeinstellungen geändert wurde, kann Server-Manager nicht mit dem Remote Server kommunizieren.

In der folgenden Liste werden die WinRM-Standard Listenereinstellungen für die Verwaltung von mit Server-Manager angezeigt.

- Der WinRM-Dienst wird ausgeführt.
- Ein WinRM-Listener wird erstellt, um HTTP-Anforderungen über die Portnummer 5985 zu akzeptieren.
- Die Portnummer 5985 ist in den Einstellungen der Windows-Firewall aktiviert, um Anforderungen über WinRM zuzulassen.
- Die Authentifizierungstypen **Kerberos** und **Negotiate** sind beide aktiviert.

Die Standardportnummer für die WinRM-Kommunikation mit einem Remotecomputer lautet 5985.

Weitere Informationen zum Konfigurieren von WinRM-Listenereinstellungen erhalten Sie, wenn Sie an einer Eingabeaufforderung **WinRM Help config** eingeben und dann die EINGABETASTE drücken.

Weitere Informationen

[Hinzufügen von Servern zu Server-Manager Windows PowerShell: about_remote_Troubleshooting im Windows Server TechCenter](#) Beschreibung der Benutzerkontensteuerung

Hinzufügen von Servern zu Server-Manager

09.04.2020 • 22 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In Windows Server können Sie mehrere Remoteserver mit einer einzigen Server-Manager-Konsole verwalten. Server, die Sie mithilfe von Server-Manager verwalten möchten, können Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 ausführen. Beachten Sie, dass eine neuere Version von Windows Server nicht mit einer älteren Version des Server-Manager verwaltet werden kann.

In diesem Thema wird beschrieben, wie Sie dem Server-Manager-Serverpool Server hinzufügen können.

NOTE

Bei unseren Tests lassen sich mit dem Server-Manager in Windows Server 2012 und späteren Versionen von Windows Server bis zu 100 Server verwalten, die mit einer typischen Arbeitsauslastung konfiguriert sind. Die Anzahl der Server, die Sie mit einer einzelnen Server-Manager-Konsole verwalten können, kann von der Datenmenge abhängig sein, die Sie von den verwalteten Servern anfordern, sowie von den Hardware- und Netzwerkressourcen, die für den Computer mit dem Server-Manager zur Verfügung stehen. Wenn die anzuzeigende Datenmenge die Ressourcenkapazität des Computers erreicht, kann es zu langsamem Reaktionszeiten des Server-Managers und Verzögerungen bei der Durchführung von Aktualisierungen kommen. Um die Anzahl der Server zu erhöhen, die Sie mit dem Server-Manager verwalten können, sollten Sie die Ereignisdaten, die der Server-Manager von den verwalteten Servern empfängt, über das Dialogfeld **Ereignisdaten konfigurieren** beschränken. Sie können das Dialogfeld über das Menü **Aufgaben** in der Kachel **Ereignisse** öffnen. Wenn Sie in Ihrer Organisation eine organisationsübergreifende Anzahl von Servern verwalten müssen, wird empfohlen, die Produkte in der [Microsoft System Center-Suite](#) auszuwerten.

Server-Manager kann von Servern unter Windows Server 2003 nur den Online- oder Offlinestatus empfangen. Obwohl Sie Server-Manager zum Ausführen von Verwaltungsaufgaben auf Servern unter Windows Server 2008 R2 oder Windows Server 2008 verwenden können, können Sie keine Rollen und Features auf Server hinzufügen, auf denen Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003 ausgeführt wird.

Server-Manager kann nicht verwendet werden, um eine neuere Version des Betriebssystems Windows Server zu verwalten. Server-Manager auf Windows Server 2012 R2, Windows Server 2012, Windows 8.1 oder Windows 8 kann nicht verwendet werden, um Server unter Windows Server 2016 zu verwalten.

Dieses Thema enthält folgende Abschnitte:

- [Hinzufügen von zu verwaltenden Servern](#)
- [Angeben von Anmelde Informationen mit dem Befehl "verwalten als"](#)

Angeben von Anmelde Informationen mit dem Befehl "verwalten als"

Wenn Sie dem Server-Manger Remoteserver hinzufügen, sind für den Zugriff auf einige dieser Server sowie für deren Verwaltung unterschiedliche Benutzerkonten-Anmeldeinformationen erforderlich. Um Anmeldeinformationen für einen verwalteten Server anzugeben, die sich von denen unterscheiden, die Sie verwenden, um sich bei dem Computer anzumelden, auf dem Sie den Server-Managern ausführen, verwenden Sie den Befehl **Verwalten als**, nachdem Sie dem Server-Manager einen Server hinzugefügt haben. Hierzu klicken Sie mit der rechten Maustaste auf der Kachel **Server** einer Rollen- oder Gruppen-Homepage auf den Eintrag für einen verwalteten Server. Beim Klicken auf **Verwalten als** wird das Dialogfeld **Windows-**

Sicherheit geöffnet, in dem Sie einen Benutzernamen, der auf dem verwalteten Server über Zugriffsrechte verfügt, in einem der folgenden Formate eingeben können.

- *Benutzername*
- *Benutzername@example.domain.com*
- *Domäne\Benutzername*

Das Dialogfeld **Windows-Sicherheit**, das mit dem Befehl **Verwalten als** geöffnet wird, kann keine Smartcardanmeldeinformationen akzeptieren; die Bereitstellung von Smartcardanmeldeinformationen über den Server-Manager wird nicht unterstützt. Anmeldeinformationen, die Sie mit dem Befehl **Verwalten als** für einen verwalteten Server eingeben, werden zwischengespeichert und beibehalten, solange Sie den Server mit dem gleichen Computer verwalten, auf dem Sie derzeit den Server-Manager ausführen, oder solange Sie sie nicht mit leeren oder anderen Anmeldeinformationen für den gleichen Server überschreiben. Wenn Sie Ihre Server-Manager-Einstellungen auf andere Computer exportieren, oder Ihr Domänenprofil als servergespeichert konfigurieren, um die Nutzung von Server-Manager-Einstellungen auf anderen Computern zu ermöglichen, werden **Verwalten als**-Anmeldeinformationen für Server in Ihrem Serverpool nicht als servergespeichertes Profil gespeichert. Server-Manager-Benutzer müssen diese auf dem jeweiligen Computer hinzufügen, den sie verwalten wollen.

Nachdem Sie anhand der in diesem Thema beschriebenen Verfahren zu verwaltende Server hinzugefügt haben, jedoch vor der Verwendung des Befehls **Verwalten als** zum Angeben alternativer Anmeldeinformationen, die zum Verwalten eines von Ihnen hinzugefügten Servers erforderlich sein könnten, können die folgenden Verwaltbarkeitsstatusfehler für den Server angezeigt werden:

- Fehler bei Kerberos-Zielauflösung
- Fehler bei Kerberos-Authentifizierung
- Online – Zugriff verweigert

NOTE

Zu den Rollen und Features, die den Befehl **Verwalten als** nicht unterstützen, zählen Remotedesktopdienste (Remotedesktopdienste, RDS) und IP-Adressverwaltung-Server (IP Address Management, IPAM). Wenn Sie den RDS oder IPAM-Server nicht mit den gleichen Anmeldeinformationen verwalten können, die Sie auf dem Computer verwenden, auf dem Sie den Server-Manager ausführen, versuchen Sie, das Konto, das Sie in der Regel verwenden, um diese Remoteserver zu verwalten, der Gruppe "Administratoren" auf dem Computer hinzuzufügen, der den Server-Manager ausführt. Melden Sie sich dann bei dem Computer, auf dem der Server-Manager ausgeführt wird, mit dem Konto an, das Sie verwenden, um den Remoteserver zu verwalten, auf dem RDS oder IPAM ausgeführt wird.

Hinzufügen von zu verwaltenden Servern

Sie können Server-Manager zu verwaltende Server hinzufügen, indem Sie eine der drei Methoden verwenden, die im Dialogfeld **Server hinzufügen** verfügbaren sind.

- **Active Directory Domain Services (AD DS)** Fügen Sie zu verwaltende Server hinzu, die von Active Directory in derselben Domäne gefunden werden, in der sich der lokale Computer befindet.
- **Domain Name System (DNS)-Eintrag** Suchen Sie anhand des Computernamens oder der IP-Adresse nach zu verwaltenden Servern.
- **Mehrere Server importieren** Geben Sie mehrere zu importierende Server in einer Datei an, in der die Server anhand des Computernamens oder der IP-Adresse aufgelistet sind.

So fügen Sie Server zum Serverpool hinzu

1. Wenn der Server-Manager bereits geöffnet ist, fahren Sie mit dem nächsten Schritt fort. Ist der Server-Manager noch nicht geöffnet, öffnen Sie ihn mit einer der folgenden Aktionen.

- Starten Sie auf dem Windows-Desktop den Server-Manager, indem Sie in der Windows-Taskleiste auf **Server-Manager** klicken.
- Klicken Sie auf der Windows-Startseite auf die Kachel **Server-Manager**.

2. Klicken Sie im Menü **Verwalten** auf **Server hinzufügen**.

3. Führen Sie einen der folgenden Schritte aus:

- Wählen Sie auf der Registerkarte **Active Directory** die Server aus, die sich in der aktuellen Domäne befinden. Halten Sie die STRG-Taste gedrückt, um mehrere Server auszuwählen. Klicken Sie auf die Schaltfläche mit dem Pfeil nach rechts, um die ausgewählten Server in die Liste **ausgewählt** zu verschieben.
- Geben Sie auf der Registerkarte **DNS** die ersten Zeichen eines Computernamens oder einer IP-Adresse ein, und drücken Sie dann die EINGABETASTE, oder klicken Sie auf **Suchen**. Wählen Sie die hinzuzufügenden Server aus, und klicken Sie dann auf die Schaltfläche mit dem Pfeil nach rechts.
- Suchen Sie auf der Registerkarte **Import** nach einer Textdatei mit den DNS-Namen oder IP-Adressen der Computer, die Sie hinzufügen möchten (die Datei enthält jeweils einen Namen oder eine IP-Adresse pro Zeile).

4. Klicken Sie nach dem Hinzufügen der Server auf **OK**.

Hinzufügen und Verwalten von Servern in Arbeitsgruppen

Es kann möglich sein, dem Server-Manager Server hinzuzufügen, die sich in Arbeitsgruppen befinden. Aber nach dem Hinzufügen werden in der Spalte **Verwaltbarkeit** der Kachel **Server** (auf einer Rollen- oder Gruppenseite, die einen Arbeitsgruppenserver enthält) ggf. Fehler vom Typ **Anmeldeinformationen nicht gültig** angezeigt, wenn versucht wird, eine Verbindung mit einem Remote-Arbeitsgruppenserver herzustellen oder Daten von diesem Server zu sammeln.

Diese oder ähnliche Fehler können unter den folgenden Bedingungen auftreten.

- Der verwaltete Server befindet sich in der gleichen Arbeitsgruppe wie der Computer, auf dem der Server-Manager ausgeführt wird.
- Der verwaltete Server befindet sich in einer anderen Arbeitsgruppe als der Computer, auf dem der Server-Manager ausgeführt wird.
- Einer der Computer befindet sich in einer Arbeitsgruppe, der andere in einer Domäne.
- Der Computer, auf dem der Server-Manager ausgeführt wird, befindet sich in einer Arbeitsgruppe, und verwaltete Remoteserver befinden sich in einem anderen Subnetz.
- Beide Computer befinden sich in Domänen, aber es besteht keine Vertrauensstellung zwischen den beiden Domänen.
- Beide Computer befinden sich in Domänen, aber es besteht nur eine einseitige Vertrauensstellung zwischen den beiden Domänen.
- Der Server, den Sie verwalten möchten, wurde mithilfe seiner IP-Adresse hinzugefügt.

So fügen Sie Remotearbeitsgruppenserver zum Server-Manager hinzu

1. Fügen Sie auf dem Computer, auf dem der Server-Manager ausgeführt wird, den Namen des Arbeitsgruppenservers der Liste **TrustedHosts** hinzu. Dies ist eine Voraussetzung für die NTLM-Authentifizierung. Um einen Computernamen einer vorhandenen Liste vertrauenswürdiger Hosts

hinzuzufügen, fügen Sie dem Befehl den Parameter `Concatenate` hinzu. Verwenden Sie beispielsweise den folgenden Befehl, um den Computer `Server01` zu einer vorhandenen Liste vertrauenswürdiger Hosts hinzuzufügen.

```
Set-Item wsman:\localhost\Client\TrustedHosts Server01 -Concatenate -force
```

2. Stellen Sie fest, ob die Arbeitsgruppe, die Sie verwalten möchten, sich im gleichen Subnetz wie der Arbeitsgruppencomputer befindet, auf dem Sie Server-Manager ausführen.

Wenn sich die beiden Computer im gleichen Subnetz befinden oder wenn das Netzwerkprofil des Arbeitsgruppenservers im **Netzwerk- und Freigabecenter** auf **Privat** gesetzt ist, fahren Sie mit dem nächsten Schritt fort.

Wenn sie sich nicht im gleichen Subnetz befinden oder wenn das Netzwerkprofil des Arbeitsgruppenservers nicht auf **Privat** gesetzt ist, ändern Sie auf dem Arbeitsgruppenserver in der Windows-Firewall die eingehende Einstellung **Windows-Remoteverwaltung (HTTP eingehend)**, um Verbindungen von Remotecomputern explizit zuzulassen. Fügen Sie hierzu die Computernamen auf der Registerkarte **Computer** im Dialogfeld **Eigenschaften** der Einstellung hinzu.

3. **IMPORTANT**

Durch das Ausführen des Cmdlets in diesem Schritt werden Mechanismen der Benutzerkontensteuerung außer Kraft gesetzt, die die Ausführung von Prozessen mit erhöhen Rechten auf Arbeitsgruppencomputern verhindern, sofern die Prozesse nicht über das integrierte Administrator- oder Systemkonto ausgeführt werden. Das Cmdlet ermöglicht es, dass Mitglieder der Administratorengruppe den Arbeitsgruppenserver verwalten, ohne dass sie sich über das integrierte Administratorkonto anmelden müssen. Wenn zusätzlichen Benutzern das Verwalten des Arbeitsgruppenservers ermöglicht wird, kann dies die Sicherheit des Servers herabsetzen. Diese Vorgehensweise ist jedoch sicherer, als die Anmeldeinformationen des integrierten Administratorkontos möglicherweise einer ganzen Gruppe von Personen zur Verfügung zu stellen, die für die Verwaltung des Arbeitsgruppenservers zuständig sind.

Wenn Sie für Prozesse, die mit erhöhen Rechten auf Arbeitsgruppencomputern ausgeführt werden, die Einschränkungen der Benutzerkontensteuerung (UAC) überschreiben möchten, erstellen Sie auf dem Arbeitsgruppenserver einen Registrierungseintrag namens **LocalAccountTokenFilterPolicy**, indem Sie das folgende Cmdlet ausführen.

```
New-ItemProperty -Name LocalAccountTokenFilterPolicy -path  
HKLM:\SOFTWARE\Microsoft\Windows\Currentversion\Policies\System -propertytype DWord -value 1
```

4. Öffnen Sie auf dem Computer, auf dem Server-Manager ausgeführt wird, die Seite **Alle Server**.
5. Wenn sich der Computer, auf dem Server-Manager ausgeführt wird, und der Ziel-Arbeitsgruppenserver in derselben Arbeitsgruppe befinden, fahren Sie mit dem letzten Schritt fort. Befinden sich die beiden Computer nicht in derselben Arbeitsgruppe, klicken Sie mit der rechten Maustaste in der Kachel **Server** auf den Ziel-Arbeitsgruppenserver, und klicken Sie dann auf **Verwalten als**.
6. Melden Sie sich am Arbeitsgruppenserver an, und verwenden Sie hierfür das integrierte Administratorkonto für den Arbeitsgruppenserver.
7. Stellen Sie sicher, dass Server-Manager eine Verbindung mit dem Arbeitsgruppenserver herstellen und Daten von diesem Server sammeln kann, indem Sie die Seite **Alle Server** aktualisieren und dann den Verwaltbarkeitsstatus für den Arbeitsgruppenserver anzeigen.

1. Fügen Sie auf dem Computer, auf dem Server-Manager ausgeführt wird, der Liste **TrustedHosts** des lokalen Computers in einer Windows PowerShell-Sitzung Remoteserver hinzu. Um einen Computernamen einer vorhandenen Liste vertrauenswürdiger Hosts hinzuzufügen, fügen Sie dem Befehl den Parameter **Concatenate** hinzu. Verwenden Sie beispielsweise den folgenden Befehl, um den Computer **Server01** zu einer vorhandenen Liste vertrauenswürdiger Hosts hinzuzufügen.

```
Set-Item wsman:\localhost\Client\TrustedHosts Server01 -Concatenate -force
```

2. Stellen Sie fest, ob die Arbeitsgruppe, die Sie verwalten möchten, sich im gleichen Subnetz wie der Arbeitsgruppencomputer befindet, auf dem Sie Server-Manager ausführen.

Wenn sich die beiden Computer im gleichen Subnetz befinden oder wenn das Netzwerkprofil des Arbeitsgruppencomputers im **Netzwerk- und Freigabecenter** auf **Privat** gesetzt ist, fahren Sie mit dem nächsten Schritt fort.

Wenn sie sich nicht im gleichen Subnetz befinden oder wenn das Netzwerkprofil des Arbeitsgruppencomputers nicht auf **Privat** gesetzt ist, ändern Sie auf dem Arbeitsgruppencomputer, auf dem Server-Manager ausgeführt wird, in der Windows-Firewall die eingehende Einstellung **Windows-Remoteverwaltung (HTTP eingehend)**, um Verbindungen von Remotecomputern explizit zuzulassen. Fügen Sie hierzu die Computernamen auf der Registerkarte **Computer** im Dialogfeld **Eigenschaften** der Einstellung hinzu.

3. Öffnen Sie auf dem Computer, auf dem Server-Manager ausgeführt wird, die Seite **Alle Server**.
4. Stellen Sie sicher, dass Server-Manager eine Verbindung mit dem Remoteserver herstellen und Daten von diesem Server sammeln kann, indem Sie die Seite **Alle Server** aktualisieren und dann den Verwaltbarkeitsstatus für den Remoteserver anzeigen. Wenn auf der Kachel **Server** immer noch ein Verwaltbarkeitsfehler für den Remoteserver angezeigt wird, fahren Sie mit dem nächsten Schritt fort.
5. Melden Sie sich vom Computer ab, auf dem Server-Manager ausgeführt wird, und melden Sie sich dann wieder mit dem integrierten Administratorkonto an. Wiederholen Sie den vorherigen Schritt, um sicherzustellen, dass Server-Manager über eine Verbindung mit dem Remoteserver hergestellt und Daten vom Remoteserver gesammelt werden können.

Wenn Sie die Verfahren in diesem Abschnitt befolgt haben und weiter Probleme mit dem Verwalten von Arbeitsgruppencomputern oder Verwalten anderer Computer von Arbeitsgruppencomputern aus haben, finden Sie weitere Informationen im Thema [zur Remoteproblembehandlung](#) auf der Microsoft-Website.

Hinzufügen und Verwalten von Servern in Clustern

Sie können den Server-Manager zur Verwaltung von Servern verwenden, die sich in Failoverclustern (auch Servercluster oder MSCS genannt) befinden. Server in Failoverclustern – unabhängig davon, ob die Clusterknoten physisch oder virtuell sind – weisen einige eindeutige Verhaltensweisen und Verwaltungseinschränkungen im Server-Manager auf.

- Physische und virtuelle Server in Clustern werden dem Server-Manager automatisch hinzugefügt, wenn ein Server im Cluster dem Server-Manager hinzugefügt wird. Wenn Sie einen gruppierten Server aus dem Server-Manager entfernen, werden Sie entsprechend gefragt, ob andere Server im Cluster entfernt werden sollen.
- Server-Manager zeigt keine Daten für gruppierte virtuelle Server an, da die Daten dynamisch und identisch mit den Daten für den Server sind, auf dem der virtuelle Clusterknoten gehostet wird. Sie können den Server auswählen, der den virtuellen Server zum Anzeigen der Daten hostet.
- Wenn Sie dem Server-Manager einen Server unter Verwendung des Namens seines virtuellen Clusterobjekts hinzufügen, wird in Server-Manager der Name des virtuellen Objekts anstelle des Namens des physischen Servers angezeigt (erwartet).

- Sie können auf einem gruppierten virtuellen Server keine Rollen und Features installieren.

Weitere Informationen

[Server-Manager Erstellen und Verwalten von Servergruppen](#)

Installieren oder Deinstallieren von Rollen, Rollendiensten oder Features

09.04.2020 • 57 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In Windows Server ermöglichen die Server-Manager-Konsole und Windows PowerShell-Cmdlets für Server-Manager die Installation von Rollen und Features auf lokalen oder Remote Servern oder virtuellen Festplatten (VHDs) im Offline Modus. Sie können mehrere Rollen und Features auf einem einzelnen Remote Server oder einer Offline-VHD in einem einzelnen Assistenten zum Hinzufügen von Rollen und Features oder in einer Windows PowerShell-Sitzung installieren.

IMPORTANT

Server-Manager kann nicht verwendet werden, um eine neuere Version des Betriebssystems Windows Server zu verwalten. Server-Manager, die unter Windows Server 2012 R2 oder Windows 8.1 ausgeführt werden, können nicht zum Installieren von Rollen, Rollen Diensten und Features auf Servern verwendet werden, auf denen Windows Server 2016 ausgeführt wird.

Sie müssen bei einem Server als Administrator angemeldet sein, um Rollen, Rollen Dienste und Features zu installieren oder zu deinstallieren. Wenn Sie am lokalen Computer mit einem Konto angemeldet sind, das nicht über Administratorrechte auf dem Zielserver verfügt, klicken Sie auf der Kachel **Server** mit der rechten Maustaste auf den Zielserver, und klicken Sie dann auf **Verwalten als**, um ein Konto mit Administratorrechten anzugeben. Der Server, auf dem eine Offline-VHD eingebunden werden soll, muss Server-Manager hinzugefügt werden. Zudem müssen Sie über Administratorrechte für diesen Server verfügen.

Weitere Informationen zu Rollen, Rollen Diensten und Features finden Sie unter [Rollen, Rollen Dienste und Features](#).

Dieses Thema enthält folgende Abschnitte:

- [Installieren von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features](#)
- [Installieren von Rollen, Rollendiensten und Features mit Windows PowerShell-Cmdlets](#)
- [Entfernen von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Entfernen von Rollen und Features](#)
- [Entfernen von Rollen, Rollendiensten und Features mit Windows PowerShell-Cmdlets](#)
- [Installieren von Rollen und Features auf mehreren Servern per Ausführung eines Windows PowerShell-Skripts](#)
- [Installieren von .NET Framework 3.5 und anderen Features bei Bedarf](#)

Installieren von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features

In einer einzelnen Sitzung des Assistenten zum Hinzufügen von Rollen und Features können Sie Rollen, Rollen Dienste und Features auf dem lokalen Server, einem Remote Server, der Server-Manager hinzugefügt wurde, oder

einer Offline-VHD installieren. Weitere Informationen zum Hinzufügen eines Servers zu Server-Manager zur Verwaltung von finden Sie unter [Hinzufügen von Servern zu Server-Manager](#).

NOTE

Wenn Sie Server-Manager unter Windows Server 2016 oder Windows 10 ausführen, können Sie den Assistenten zum Hinzufügen von Rollen und Features verwenden, um Rollen und Features nur auf Servern und Offline-VHDs zu installieren, auf denen Windows Server 2016 ausgeführt wird.

So installieren Sie Rollen und Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features

1. Wenn der Server-Manager bereits geöffnet ist, fahren Sie mit dem nächsten Schritt fort. Ist der Server-Manager noch nicht geöffnet, öffnen Sie ihn mit einer der folgenden Aktionen.
 - Starten Sie auf dem Windows-Desktop den Server-Manager, indem Sie in der Windows-Taskleiste auf **Server-Manager** klicken.
 - Klicken Sie auf dem Windows- Start Bildschirm auf die Kachel **Server-Manager** .
2. Klicken Sie im Menü **Verwalten** auf **Rollen und Features hinzufügen**.
3. Überprüfen Sie auf der Seite **Vorbemerkungen**, ob der Zielserver und die Netzwerkumgebung für die Installation der Rolle und des Features vorbereitet sind. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Installationstyp auswählen** die Option **Rollenbasierte oder featurebasierte Installation** aus, um alle Teile von Rollen oder Features auf einem Server zu installieren. Wählen Sie alternativ **Installation von Remotedesktopdiensten** aus, um entweder eine Desktopinfrastruktur mit virtuellen Computern oder eine sitzungsbasierte Desktopinfrastruktur für die Remotedesktopdienste zu installieren. Bei Verwendung der Option **Szenariobasierte Installation von Remotedesktopdiensten** werden logische Teile der Remotedesktopdienste-Rolle von Administratoren je nach Bedarf auf verschiedene Server verteilt. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Zielserver auswählen** einen Server aus dem Serverpool aus, oder wählen Sie eine Offline-VHD aus. Um eine Offline-VHD als Zielserver auszuwählen, müssen Sie zuerst den Server auswählen, auf dem die VHD eingebunden werden soll. Wählen Sie anschließend die VHD-Datei aus. Weitere Informationen zum Hinzufügen von Servern zum-Server Pool finden Sie unter [Hinzufügen von Servern zu Server-Manager](#). Klicken Sie nach dem Auswählen des Zielservers auf **Weiter**.

NOTE

Zum Installieren von Rollen und Features auf Offline-VHDs müssen Ziel-VHDs die folgenden Anforderungen erfüllen.

- Auf VHDs muss die Version von Windows Server ausgeführt werden, die mit der Version von Server-Manager übereinstimmt, die Sie ausführen. Weitere Informationen finden Sie im Hinweis zu Beginn der [Installation von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features](#).
- VHDs dürfen nicht mehr als ein Systemvolume oder eine Partition aufweisen.
- Der freigegebene Netzwerkordner, in dem die VHD-Datei gespeichert ist, muss dem Computerkonto (bzw. lokalen System) des Servers, den Sie zum Einbinden der VHD ausgewählt haben, die folgenden Zugriffsrechte gewähren. Die Zugriffsberechtigungen des Benutzerkontos reichen nicht aus. Die Freigabe kann der Gruppe **Jeder** die Berechtigungen **Lesen** und **Schreiben** gewähren, um den Zugriff auf die VHD zu ermöglichen, dies wird aber aus Sicherheitsgründen nicht empfohlen.
 - Zugriffsrecht **Lesen/Schreiben** im Dialogfeld **Dateifreigabe**
 - **Voll** Zugriff auf die Registerkarte " **Sicherheit** ", Dialogfeld " **Datei- oder Ordner Eigenschaften** ".

6. Wählen Sie Rollen und ggf. Rollendienste für die Rolle aus, und klicken Sie dann auf **Weiter**, um Features

auszuwählen.

Wenn Sie fortfahren, werden Sie vom Assistenten zum Hinzufügen von Rollen und Features automatisch informiert, wenn Konflikte auf dem Zielserver gefunden wurden, die die Installation oder den normalen Betrieb von ausgewählten Rollen oder Features verhindern können. Sie werden außerdem aufgefordert, Rollen, Rollendienste oder Features hinzuzufügen, die für die ausgewählten Rollen oder Features erforderlich sind.

Wenn die Rolle von einem anderen Server oder einem Windows Client-basierten Computer mit Remoteserver-Verwaltungstools aus verwaltet werden soll, brauchen Sie die Verwaltungstools und Snap-Ins für Rollen auf dem Zielserver nicht zu installieren. Standardmäßig werden im Assistenten zum Hinzufügen von Rollen und Features Verwaltungs Tools für die Installation ausgewählt.

7. Überprüfen Sie auf der Seite **Installationsauswahl** bestätigen Ihre Rollen-, Feature- und Serverauswahl. Wenn Sie bereit sind, die Installation zu starten, klicken Sie auf **Installieren**.

Sie können Ihre Auswahl auch in eine XML-basierte Konfigurationsdatei exportieren, die Sie für unbeaufsichtigte Installationen mit Windows PowerShell verwenden können. Um die in dieser Sitzung zum Hinzufügen von Rollen und Features angegebene Konfiguration zu exportieren, klicken Sie auf **Konfigurationseinstellungen exportieren**, und speichern Sie die XML-Datei dann an einem geeigneten Speicherort.

Mit dem Befehl **Alternativen Quellpfad angeben** auf der Seite **Installationsauswahl** bestätigen können Sie einen alternativen Quellpfad für die Dateien angeben, die zum Installieren von Rollen und Features auf dem ausgewählten Server erforderlich sind. In Windows Server 2012 und neueren Versionen von Windows Server können Sie mithilfe von **Features bei Bedarf** die Menge des vom Betriebssystem genutzten Speicherplatzes verringern, indem Sie Rollen- und Featuredateien von Servern entfernen, die ausschließlich Remote verwaltet werden. Wenn Sie Rollen- und Featuredateien mit dem Cmdlet `Uninstall-WindowsFeature -remove` von einem Server entfernt haben, können Sie später Rollen und Features auf dem Server installieren, indem Sie einen alternativen Quellpfad oder eine Freigabe angeben, an dem bzw. auf der die erforderlichen Rollen- und Featuredateien gespeichert sind. Der Quellpfad oder die Dateifreigabe muss entweder der Gruppe **jeder** (nicht empfohlen aus Sicherheitsgründen) oder dem Computer Konto (*Domänen\Servername\$*) des Zielservers **Lese** Berechtigungen erteilen. das Gewähren des Benutzerkonto Zugriffs ist nicht ausreichend. Weitere Informationen zu Features bei Bedarf finden Sie unter [Windows Server-Installationsoptionen](#).

Sie können eine WIM-Datei als Alternative Funktions Datei Quelle angeben, wenn Sie Rollen, Rollen Dienste und Features auf einem laufenden physischen Server installieren. Der Quellpfad für eine WIM-Datei sollte das folgende Format haben, wobei **WIM** als Präfix und der Index, unter dem sich die Featuredateien befinden, als Suffix angegeben wird: **WIM:e:\sources\install.wim:4**. Sie können eine WIM-Datei jedoch nicht direkt als Quelle zum Installieren von Rollen, Rollen Diensten und Features auf einer Offline-VHD verwenden. Sie müssen entweder die Offline-VHD einbinden und auf den zugehörigen einstellungspfad für Quelldateien verweisen, oder Sie müssen auf einen Ordner verweisen, der eine Kopie des Inhalts der WIM-Datei enthält.

8. Nachdem Sie auf **Installieren**klicken, werden auf der Seite **Installations Status** der Installationsfortschritt, Ergebnisse und Meldungen wie Warnungen, Fehler oder nach der Installation erforderliche Konfigurationsschritte angezeigt, die für die installierten Rollen oder Features erforderlich sind. In Windows Server 2012 und neueren Versionen von Windows Server können Sie den Assistenten zum Hinzufügen von Rollen und Features schließen, während die Installation noch läuft, und Installations Ergebnisse oder andere Meldungen im **Benachrichtigungen** Bereich oben in der Server-Manager-Konsole anzeigen. Klicken Sie auf das Symbol **Benachrichtigungen** , um weitere Details zu Installationen oder anderen Aufgaben anzuzeigen, die Sie in Server-Manager ausführen.

Installieren von Rollen, Rollendiensten und Features mit Windows

PowerShell-Cmdlets

Die Server-Manager Bereitstellungs-Cmdlets für Windows PowerShell funktionieren ähnlich wie der GUI-basierte Assistent zum Hinzufügen von Rollen und Features und der Assistent zum Entfernen von Rollen und Features mit einem wichtigen Unterschied. Im Gegensatz zum Assistenten zum Hinzufügen von Rollen und Features sind in Windows PowerShell die Verwaltungs Tools und Snap-Ins für eine Rolle nicht standardmäßig enthalten. Um Verwaltungstools in eine Rolleninstallation einzuschließen, fügen Sie dem Cmdlet den `IncludeManagementTools`-Parameter hinzu. Wenn Sie Rollen und Features auf einem Server installieren, auf dem die Server Core-Installationsoption von Windows Server 2012 oder höher ausgeführt wird, können Sie einer Installation die Verwaltungs Tools einer Rolle hinzufügen. GUI-basierte Verwaltungs Tools und Snap-Ins können jedoch nicht auf Servern installiert werden, auf denen die Server Core-Installationsoption von Windows Server ausgeführt wird. Nur die Befehlszeilen- und Windows PowerShell-Verwaltungs Tools können auf der Server Core-Installationsoption installiert werden.

So installieren Sie Rollen und Features mit dem Cmdlet `Install-WindowsFeature`:

1. Führen Sie einen der folgenden Schritte aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.

NOTE

Wenn Sie Rollen und Features auf einem Remote Server installieren, müssen Sie Windows PowerShell nicht mit erhöhten Benutzerrechten ausführen.

- Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
 - Klicken Sie im Windows- **Start** Bildschirm mit der rechten Maustaste auf die Kachel für Windows PowerShell, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.
2. Geben Sie **Get-WindowsFeature** ein, und drücken Sie anschließend die **EINGABETASTE**, um eine Liste der auf dem lokalen Server verfügbaren und installierten Rollen und Features anzuzeigen. Wenn der lokale Computer kein Server ist oder Sie Informationen zu einem Remote Server benötigen, führen Sie **Get-Windows Feature-Computername < computer_name >** aus, bei dem *computer_name* den Namen eines Remote Computers darstellt, auf dem Windows Server 2016 ausgeführt wird. Die Ergebnisse des Cmdlets enthalten die Befehlsnamen der Rollen und Features, die Sie Ihrem Cmdlet in Schritt 4 hinzufügen.

NOTE

In Windows PowerShell 3,0 und neueren Versionen von Windows PowerShell müssen Sie das Server-Manager Cmdlet-Modul nicht in die Windows PowerShell-Sitzung importieren, bevor Sie die Cmdlets ausführen, die Teil des Moduls sind. Module werden automatisch importiert, wenn Sie ein zum Modul gehörendes Cmdlet zum ersten Mal ausführen. Außerdem wird bei beiden Windows PowerShell-Cmdlets und den Funktionsnamen, die mit den Cmdlets verwendet werden, die Groß-/Kleinschreibung beachtet.

3. geben Sie **Get-Help install-Windows Feature** ein, und drücken Sie dann die **Eingabe** Taste, um die Syntax und akzeptierte Parameter für das `Install-WindowsFeature`-Cmdlet anzuzeigen.
4. Geben Sie Folgendes ein, und drücken Sie dann die **EINGABETASTE**, wobei *feature_name* den Befehlsnamen einer Rolle oder eines Features darstellt, die Sie installieren möchten (abgerufen in Schritt 2), und *computer_name* einen Remote Computer darstellt, auf dem Sie Rollen und Features installieren möchten. Trennen Sie mehrere Werte für *FeatureName* durch Kommata. Der `Restart`-Parameter startet den Zielserver automatisch neu, wenn die Installation der Rolle bzw. des Features dies erfordert.

```
Install-WindowsFeature -Name <feature_name> -computerName <computer_name> -Restart
```

Fügen Sie zum Installieren von Rollen oder Features auf einer Offline-VHD die Parameter `computerName` und `VHD` hinzu. Wird der `computerName`-Parameter nicht hinzugefügt, geht das Cmdlet davon aus, dass der lokale Computer zum Zugreifen auf die VHD eingebunden wird. Der Parameter `computerName` enthält den Namen des Servers, auf dem die VHD eingebunden werden soll, und der Parameter `VHD` enthält den Pfad zur VHD-Datei auf dem angegebenen Server.

NOTE

Wenn Sie das Cmdlet auf einem Computer ausführen, auf dem ein Windows-Client Betriebssystem ausgeführt wird, müssen Sie den `computerName`-Parameter hinzufügen.

Zum Installieren von Rollen und Features auf Offline-VHDs müssen Ziel-VHDs die folgenden Anforderungen erfüllen.

- Auf VHDs muss die Version von Windows Server ausgeführt werden, die mit der Version von Server-Manager übereinstimmt, die Sie ausführen. Weitere Informationen finden Sie im Hinweis zu Beginn der [Installation von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features](#).
- VHDs dürfen nicht mehr als ein Systemvolume oder eine Partition aufweisen.
- Der freigegebene Netzwerkordner, in dem die VHD-Datei gespeichert ist, muss dem Computerkonto (bzw. lokalen System) des Servers, den Sie zum Einbinden der VHD ausgewählt haben, die folgenden Zugriffsrechte gewähren. Die Zugriffsberechtigungen des Benutzerkontos reichen nicht aus. Die Freigabe kann der Gruppe **Jeder** die Berechtigungen **Lesen** und **Schreiben** gewähren, um den Zugriff auf die VHD zu ermöglichen, dies wird aber aus Sicherheitsgründen nicht empfohlen.
 - Zugriffsrecht **Lesen/Schreiben** im Dialogfeld **Dateifreigabe**
 - **Voll** Zugriff auf die Registerkarte "Sicherheit", Dialogfeld "Datei-oder Ordner Eigenschaften".

```
Install-WindowsFeature -Name <feature_name> -VHD <path> -computerName <computer_name> -Restart
```

Beispiel: Mit dem folgenden Cmdlet werden die Active Directory-Domänen Dienste-Rolle und das Gruppenrichtlinie Verwaltungs Feature auf einem Remote Server, ContosoDC1, installiert. Die Verwaltungstools und Snap-Ins werden mit dem Parameter `IncludeManagementTools` hinzugefügt, und der Zielsystem wird automatisch neu gestartet, falls dies für die Installation erforderlich ist.

```
Install-WindowsFeature -Name AD-Domain-Services,GPMC -computerName ContosoDC1 -IncludeManagementTools -Restart
```

5. Wenn die Installation abgeschlossen ist, überprüfen Sie die Installation, indem Sie in Server-Manager die Seite **alle Server** öffnen, einen Server auswählen, auf dem Sie Rollen und Features installiert haben, und die Kachel **Rollen und Features** auf der Seite für den ausgewählten Server anzeigen. Sie können auch das `Get-WindowsFeature`-Cmdlet für den ausgewählten Server (`Get-Windows Feature-Computername <computer_name>`) ausführen, um eine Liste der Rollen und Features anzuzeigen, die auf dem Server installiert sind.

Entfernen von Rollen, Rollen Diensten und Features mithilfe des Assistenten zum Entfernen von Rollen und Features

Sie müssen bei einem Server als Administrator angemeldet sein, um Rollen, Rollen Dienste und Features zu deinstallieren. Wenn Sie am lokalen Computer mit einem Konto angemeldet sind, das nicht über Administratorrechte auf dem Deinstallationszielserver verfügt, klicken Sie auf der Kachel **Server** mit der rechten

Maustaste auf den Zielserver, und klicken Sie dann auf **Verwalten als**, um ein Konto mit Administratorrechten anzugeben. Der Server, auf dem eine Offline-VHD eingebunden werden soll, muss Server-Manager hinzugefügt werden. Zudem müssen Sie über Administratorrechte für diesen Server verfügen.

So entfernen Sie Rollen und Features mithilfe des Assistenten zum Entfernen von Rollen und Features

1. Wenn der Server-Manager bereits geöffnet ist, fahren Sie mit dem nächsten Schritt fort. Ist der Server-Manager noch nicht geöffnet, öffnen Sie ihn mit einer der folgenden Aktionen.
 - Starten Sie auf dem Windows-Desktop den Server-Manager, indem Sie in der Windows-Taskleiste auf **Server-Manager** klicken.
 - Klicken Sie auf der Windows-Startseite auf die Kachel **Server-Manager**.
2. Klicken Sie im Menü **Verwalten** auf **Rollen und Funktionen entfernen**.
3. Vergewissern Sie sich auf der Seite **Vorbemerkungen**, dass die Umgebung zum Entfernen von Rollen oder Features von einem Server vorbereitet ist. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Ziel Server auswählen** einen Server aus dem Server Pool aus, oder wählen Sie eine Offline-VHD aus. Um eine Offline-VHD auszuwählen, müssen Sie zuerst den Server auswählen, auf dem die VHD eingebunden werden soll. Wählen Sie anschließend die VHD-Datei aus.

NOTE

Der freigegebene Netzwerkordner, in dem die VHD-Datei gespeichert ist, muss dem Computerkonto (bzw. lokalen System) des Servers, den Sie zum Einbinden der VHD ausgewählt haben, die folgenden Zugriffsrechte gewähren. Die Zugriffsberechtigungen des Benutzerkontos reichen nicht aus. Die Freigabe kann der Gruppe **Jeder** die Berechtigungen **Lesen** und **Schreiben** gewähren, um den Zugriff auf die VHD zu ermöglichen, dies wird aber aus Sicherheitsgründen nicht empfohlen.

- Zugriffsrecht **Lesen/Schreiben** im Dialogfeld **Dateifreigabe**
- Zugriffsrecht **Vollzugriff** auf der Registerkarte **Sicherheit** im Datei- oder Ordnerdialogfeld **Eigenschaften**

Weitere Informationen zum Hinzufügen von Servern zum-Server Pool finden Sie unter [Hinzufügen von Servern zu Server-Manager](#). Klicken Sie nach dem Auswählen des Zielservers auf **Weiter**.

NOTE

Mit dem Assistenten zum Entfernen von Rollen und Features können Sie Rollen und Features von Servern entfernen, auf denen dieselbe Version von Windows Server ausgeführt wird, die die von Ihnen verwendete Version von Server-Manager unterstützt. Es ist nicht möglich, Rollen, Rollen Dienste oder Features von Servern zu entfernen, auf denen Windows Server 2016 ausgeführt wird, wenn Sie Server-Manager unter Windows Server 2012 R2, Windows Server 2012 oder Windows 8 ausführen. Sie können den Assistenten zum Entfernen von Rollen und Features nicht zum Entfernen von Rollen und Features von Servern verwenden, auf denen Windows Server 2008 oder Windows Server 2008 R2 ausgeführt wird.

5. Wählen Sie Rollen und ggf. Rollendienste für die Rolle aus, und klicken Sie dann auf **Weiter**, um Features auszuwählen.

Wenn Sie fortfahren, werden Sie vom Assistenten zum Entfernen von Rollen und Features automatisch aufgefordert, Rollen, Rollen Dienste oder Features zu entfernen, die nicht ohne die zu entfernenden Rollen oder Features ausgeführt werden können.

Außerdem können Sie die Verwaltungs Tools und Snap-Ins für Rollen auf dem Zielserver entfernen. Standardmäßig sind die Verwaltungs Tools im Assistenten zum Entfernen von Rollen und Features zum Entfernen ausgewählt. Sie können die Verwaltungstools und Snap-Ins behalten, wenn Sie vorhaben, den ausgewählten Server zur Verwaltung der Rolle auf anderen Remoteservern zu verwenden.

6. Überprüfen Sie auf der Seite **Entfernungsauswahl** bestätigen Ihre Rollen-, Feature- und Serverauswahl.

Wenn Sie bereit sind, die Rollen oder Features zu entfernen, klicken Sie auf **Entfernen**.

7. Nachdem Sie auf **Entfernen**klicken, werden auf der Seite **Entfernungs** Status der Entfernungs Status, Ergebnisse und Meldungen, wie z. b. Warnungen, Fehler oder nach der Entfernung erforderliche Konfigurationsschritte, wie z. b. der Neustart des Zielservers, angezeigt. In Windows Server 2012 und neueren Versionen von Windows Server können Sie den Assistanten zum Entfernen von Rollen und Features schließen, während der Deinstallations Vorgang noch ausgeführt wird, und die Entfernungs Ergebnisse oder andere Meldungen im **Benachrichtigungs** Bereich oben in der Server-Manager-Konsole anzeigen. Klicken Sie auf das **Benachrichtigungs** Kennzeichen, um weitere Details zu Entfernungen oder anderen Aufgaben anzuzeigen, die Sie in Server-Manager ausführen.

Entfernen von Rollen, Rollendiensten und Features mit Windows PowerShell-Cmdlets

Die Server-Manager Bereitstellungs-Cmdlets für Windows PowerShell funktionieren ähnlich wie der GUI-basierte Assistent zum Entfernen von Rollen und Features mit einem wichtigen Unterschied. Im Gegensatz zum Assistanten zum Entfernen von Rollen und Features werden in Windows PowerShell die Verwaltungs Tools und Snap-Ins für eine Rolle nicht standardmäßig entfernt. Um Verwaltungstools im Rahmen einer Rollenentfernung zu entfernen, fügen Sie dem Cmdlet den `IncludeManagementTools` -Parameter hinzu. Wenn Sie Rollen und Features von einem Server deinstallieren, auf dem die Server Core-Installationsoption von Windows Server 2012 oder einer neueren Version von Windows Server ausgeführt wird, entfernt dieser Parameter die Befehlszeilen- und Windows PowerShell-Verwaltungs Tools für die angegebenen Rollen und Features.

So entfernen Sie Rollen und Features mit dem Cmdlet `UnInstall-WindowsFeature`:

1. Führen Sie einen der folgenden Schritte aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.

NOTE

Wenn Sie Rollen und Features von einem Remote Server deinstallieren, müssen Sie Windows PowerShell nicht mit erhöhten Benutzerrechten ausführen.

- Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
 - Klicken Sie im Windows- **Start** Bildschirm mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.
2. Geben Sie **Get-WindowsFeature** ein, und drücken Sie anschließend die **EINGABETASTE**, um eine Liste der auf dem lokalen Server verfügbaren und installierten Rollen und Features anzuzeigen. Wenn der lokale Computer kein Server ist oder Sie Informationen zu einem Remote Server benötigen, führen Sie **Get-Windows Feature-Computername < computer_name >** aus, bei dem *computer_name* den Namen eines Remote Computers darstellt, auf dem Windows Server 2016 ausgeführt wird. Die Ergebnisse des Cmdlets enthalten die Befehlsnamen der Rollen und Features, die Sie Ihrem Cmdlet in Schritt 4 hinzufügen.

NOTE

In Windows PowerShell 3,0 und neueren Versionen von Windows PowerShell müssen Sie das Server-Manager Cmdlet-Modul nicht in die Windows PowerShell-Sitzung importieren, bevor Sie die Cmdlets ausführen, die Teil des Moduls sind. Module werden automatisch importiert, wenn Sie ein zum Modul gehörendes Cmdlet zum ersten Mal ausführen. Außerdem wird bei beiden Windows PowerShell-Cmdlets und den Funktionsnamen, die mit den Cmdlets verwendet werden, die Groß-/Kleinschreibung beachtet.

3. geben Sie **Get-Help Uninstall-Windows Feature** ein, und drücken Sie dann die **Eingabe** Taste, um die Syntax und akzeptierte Parameter für das **Uninstall-WindowsFeature** -Cmdlet anzuzeigen.

4. Geben Sie Folgendes ein, und drücken Sie dann die **EINGABETASTE**. Dabei steht *FeatureName* für den Befehlsnamen einer Rolle oder eines Features, die bzw. das entfernt werden soll (abgerufen in Schritt 2), und *computer_name* für einen Remotecomputer, von dem Rollen und Features entfernt werden sollen. Trennen Sie mehrere Werte für *FeatureName* durch Kommata. Der **Restart** -Parameter startet Zielserver automatisch neu, wenn die Entfernung der Rolle bzw. des Features dies erfordert.

```
Uninstall-WindowsFeature -Name <feature_name> -computerName <computer_name> -Restart
```

Fügen Sie zum Deinstallieren von Rollen oder Features auf einer Offline-VHD die Parameter **computerName** und **VHD** hinzu. Wird der **computerName** -Parameter nicht hinzugefügt, geht das Cmdlet davon aus, dass der lokale Computer zum Zugreifen auf die VHD eingebunden wird. Der Parameter **computerName** enthält den Namen des Servers, auf dem die VHD eingebunden werden soll, und der Parameter **VHD** enthält den Pfad zur VHD-Datei auf dem angegebenen Server.

NOTE

Wenn Sie das Cmdlet auf einem Computer ausführen, auf dem ein Windows-Client Betriebssystem ausgeführt wird, müssen Sie den **computerName** -Parameter hinzufügen.

Der freigegebene Netzwerkordner, in dem die VHD-Datei gespeichert ist, muss dem Computerkonto (bzw. lokalen System) des Servers, den Sie zum Einbinden der VHD ausgewählt haben, die folgenden Zugriffsrechte gewähren. Die Zugriffsberechtigungen des Benutzerkontos reichen nicht aus. Die Freigabe kann der Gruppe **Jeder** die Berechtigungen **Lesen** und **Schreiben** gewähren, um den Zugriff auf die VHD zu ermöglichen, dies wird aber aus Sicherheitsgründen nicht empfohlen.

- Zugriffsrecht **Lesen/Schreiben** im Dialogfeld **Dateifreigabe**
- **Voll** Zugriff auf die Registerkarte "Sicherheit", Dialogfeld "Datei- oder Ordner Eigenschaften".

```
Uninstall-WindowsFeature -Name <feature_name> -VHD <path> -computerName <computer_name> -Restart
```

Beispiel: Mit dem folgenden Cmdlet werden die Active Directory-Domänen Dienste-Rolle und die Gruppenrichtlinie Verwaltungsfunktion von einem Remote Server (ContosoDC1) entfernt. Die Verwaltungstools und Snap-Ins werden ebenfalls entfernt, und der Zielserver wird automatisch neu gestartet, falls dies für das Entfernen erforderlich ist.

```
Uninstall-WindowsFeature -Name AD-Domain-Services,GPMC -computerName ContosoDC1 -IncludeManagementTools  
-Restart
```

5. Wenn die Deinstallation abgeschlossen ist, überprüfen Sie, ob die Rollen und Features entfernt wurden, indem Sie in Server-Manager die Seite **alle Server** öffnen, den Server auswählen, von dem Sie Rollen und Features entfernt haben, und die Kachel **Rollen und Features** auf der Seite für den ausgewählten Server anzeigen. Sie können auch das **Get-WindowsFeature** -Cmdlet für den ausgewählten Server (**Get-WindowsFeature-Computername <computer_name>**) ausführen, um eine Liste der Rollen und Features anzuzeigen, die auf dem Server installiert sind.

Installieren von Rollen und Features auf mehreren Servern per Ausführung eines Windows PowerShell-Skripts

Obwohl Sie den Assistenten zum Hinzufügen von Rollen und Features nicht zum Installieren von Rollen, Rollen

Diensten und Features auf mehr als einem Zielserver in einer einzelnen Assistenten Sitzung verwenden können, können Sie mithilfe eines Windows PowerShell-Skripts Rollen, Rollen Dienste und Features auf mehreren Ziel Servern installieren, die Sie mit Server-Manager verwalten. Das Skript, das Sie zum Ausführen der Batch Bereitstellung verwenden, wenn dieser Vorgang aufgerufen wird, verweist auf eine XML-Konfigurationsdatei, die Sie mithilfe des Assistenten zum Hinzufügen von Rollen und Features auf einfache Weise erstellen können, und auf **Konfigurationseinstellungen exportieren**, nachdem Sie den Assistenten im Assistenten zum Hinzufügen von Rollen und Features auf die Seite "Installations Auswahl bestätigen" geklickt haben.

IMPORTANT

Auf allen in Ihrem Skript angegebenen Ziel Servern muss die Version von Windows Server ausgeführt werden, die mit der Version von übereinstimmt, die Server-Manager auf dem lokalen Computer ausgeführt wird. Wenn Sie z. b. Server-Manager unter Windows 10 ausführen, können Sie Rollen, Rollen Dienste und Features auf Servern installieren, auf denen Windows Server 2016 ausgeführt wird. Wenn der Installation GUI-basierte Verwaltungs Tools hinzugefügt werden, werden Zielserver, auf denen die Server Core-Installationsoption von Windows Server ausgeführt wird, beim Installationsvorgang automatisch in die vollständige Installationsoption (Server mit einer vollständigen GUI, auch als "Running Server Graphical Shell" bezeichnet) konvertiert.

Das in diesem Abschnitt angegebene Skript ist ein Beispiel dafür, wie die Batch Bereitstellung mithilfe des-Cmdlets `Install-WindowsFeature` und eines Windows PowerShell-Skripts ausgeführt werden kann. Es gibt noch weitere mögliche Skripts und Methoden zur Durchführung der Batchbereitstellung auf mehreren Servern. Sie können das [Script Center-Repository](#) nutzen, um nach anderen Skripts zum Bereitstellen von Rollen und Features zu suchen oder diese bereitzustellen.

So installieren Sie Rollen und Features auf mehreren Servern

1. Wenn Sie dies nicht bereits getan haben, erstellen Sie eine XML-Konfigurationsdatei, die die Rollen, Rollen Dienste und Features enthält, die auf mehreren Servern installiert werden sollen. Sie können diese Konfigurationsdatei erstellen, indem Sie den Assistenten zum Hinzufügen von Rollen und Features ausführen, Rollen, Rollen Dienste und Features auswählen und auf **Konfigurationseinstellungen exportieren** klicken, nachdem Sie den Assistenten auf der Seite **Installations Auswahl bestätigen** fortfahren. Speichern Sie die Konfigurationsdatei an einem geeigneten Speicherort. Sie müssen nicht auf **Installieren** klicken bzw. den Assistenten nicht bis zum Ende ausführen, wenn Sie lediglich eine Konfigurationsdatei erstellen möchten.
2. Führen Sie einen der folgenden Schritte aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.
 - Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
 - Klicken Sie im Windows- **Start** Bildschirm mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.
3. Kopieren Sie das folgende Skript, und fügen Sie es in Ihre Windows PowerShell-Sitzung ein.

```

function Invoke-WindowsFeatureBatchDeployment {
    param (
        [parameter(mandatory)]
        [string[]] $computerNames,
        [parameter(mandatory)]
        [string] $ConfigurationFilepath
    )

    # Deploy the features on multiple computers simultaneously.
    $jobs = @()
    foreach($computerName in $computerNames) {
        $jobs += start-Job -Command {
            Install-WindowsFeature -ConfigurationFilepath $using:ConfigurationFilepath -computerName
$using:computerName -Restart
        }
    }

    Receive-Job -Job $jobs -Wait | select-Object Success, RestartNeeded, exitCode, FeatureResult
}

```

Die Zielserver werden automatisch neu gestartet, falls dies für die von Ihnen gewählten Rollen und Features erforderlich ist.

4. Führen Sie die Funktion wie folgt aus.

- Erstellen Sie eine Variable, in der die Namen der Zielcomputer getrennt durch Kommas gespeichert werden. Im folgenden Beispiel sind in der Variablen `$ServerNames` die Namen der Zielserver *Contoso_01* und *Contoso_02* gespeichert. Drücken Sie die **EINGABETASTE**.

```

# Sample Invocation
$ServerNames = 'Contoso_01','Contoso_02'
Invoke-WindowsFeatureBatchDeployment -computerNames $ServerNames -ConfigurationFilepath
C:\Users\sampleuser\Desktop\DeploymentConfigTemplate.xml

```

- Geben Sie zum Ausführen der Funktion Folgendes ein, und drücken Sie die **EINGABETASTE**. Hierbei ist `$ServerNames` ein Beispiel für die Variable, die Sie im vorherigen Schritt erstellt haben, und *C:\Users\Sampleuser\Desktop\DeploymentConfigTemplate.xml* ist ein Beispiel für einen Pfad zur Konfigurationsdatei, den Sie in Schritt 1 erstellt haben.

**Aufrufen-`windowsfeaturebatchdeployment`-Computer Names `$ServerNames-`
`configurationfilepath` `c:\users\sampleuser\desktop\deploymentconfigtemplate.XML`**

5. Wenn die Installation abgeschlossen ist, überprüfen Sie die Installation, indem Sie in Server-Manager die Seite **alle Server** öffnen, einen Server auswählen, auf dem Sie Rollen und Features installiert haben, und die Kachel **Rollen und Features** auf der Seite für den ausgewählten Server anzeigen. Sie können auch das `Get-WindowsFeature` Cmdlet für einen bestimmten Server (`Get-WindowsFeature -computerName <computer_name>`) ausführen, um eine Liste der Rollen und Features anzuzeigen, die auf dem Server installiert sind.

Installieren von .NET Framework 3.5 und anderen Features bei Bedarf

ab Windows Server 2012 und Windows 8 sind die Featuredateien für .NET Framework 3.5 (einschließlich .NET Framework 2.0 und .NET Framework 3.0) nicht standardmäßig auf dem lokalen Computer verfügbar. Die Dateien wurden entfernt. Dateien für Features, die bei der Konfiguration von %"Features bei Bedarf%" entfernt wurden, und Featuredateien für .NET Framework 3.5 stehen über Windows Update zur Verfügung. Wenn Featuredateien auf dem Zielserver, auf dem Windows Server 2012 oder höhere Versionen ausgeführt werden, nicht verfügbar sind, wird beim Installationsvorgang standardmäßig nach den fehlenden Dateien gesucht, indem eine Verbindung mit Windows Update hergestellt wird. Sie können das Standardverhalten

überschreiben, indem Sie eine Gruppenrichtlinie Einstellung konfigurieren oder während der Installation einen alternativen Quellpfad angeben. Dies ist unabhängig davon, ob Sie die Installation mit dem Assistenten zum Hinzufügen von Rollen und Features oder einer Befehlszeile durchlaufen.

Sie installieren .NET Framework 3.5 mit einer der folgenden Aktionen:

- Fügen Sie anhand von [So installieren Sie .NET Framework 3.5 durch Ausführen des Install-WindowsFeature-Cmdlets](#) den `Source`-Parameter hinzu, und geben Sie eine Quelle an, aus der .NET Framework 3.5-Featuredateien abgerufen werden sollen. Wenn Sie den `Source`-Parameter nicht hinzufügen, wird vom Installationsprozess zunächst ermittelt, ob von den Gruppenrichtlinieneinstellungen ein Pfad zu Featuredateien angegeben wurde. Wird kein solcher Pfad gefunden, wird mithilfe von Windows Update nach fehlenden Featuredateien gesucht.
- Verwenden [Sie zum Installieren von .NET Framework 3.5 mithilfe des Assistenten zum Hinzufügen von Rollen und Features](#) auf der Seite **Installationsoptionen bestätigen** des Assistenten zum Hinzufügen von Rollen und Features.
- Rufen Sie anhand von [So installieren Sie .NET Framework 3.5 mithilfe von DISM](#) standardmäßig Dateien aus Windows Update oder durch Angabe eines Quellpfads zum Installationsmedium ab.

[Konfigurieren alternativer Quellen für Featuredateien in der Gruppenrichtlinie](#) für .NET Framework 3.5 oder andere Features, falls auf dem lokalen Computer keine Featuredateien gefunden werden.

IMPORTANT

Bei der Installation von Featuredateien aus einer Remotequelle muss der Quellpfad oder die Dateifreigabe entweder der Gruppe **Jeder** (nicht empfohlen aus Sicherheitsgründen) oder dem Computerkonto (lokales System) des Zielservers Berechtigungen zum **Lesen** gewähren. Das Gewähren des Benutzerkontozugriffs ist nicht ausreichend.

Server in Arbeitsgruppen können nicht auf externe Dateifreigaben zugreifen, auch wenn das Computerkonto des Arbeitsgruppenservers für die externe Freigabe über die Berechtigung **Lesen** verfügt. Alternative Quellspeicherorte, die für Arbeitsgruppenserver funktionieren, sind u. a. Installationsmedien, Windows Update sowie VHD- oder WIM-Dateien, die auf dem lokalen Arbeitsgruppenserver gespeichert sind.

Sie können eine WIM-Datei als Alternative Funktions Datei Quelle angeben, wenn Sie Rollen, Rollen Dienste und Features auf einem laufenden physischen Server installieren. Der Quellpfad für eine WIM-Datei sollte das folgende Format haben, wobei **WIM** als Präfix und der Index, unter dem sich die Featuredateien befinden, als Suffix angegeben wird:
WIM:e:\sources\install.wim:4. Sie können eine WIM-Datei jedoch nicht direkt als Quelle zum Installieren von Rollen, Rollen Diensten und Features auf einer Offline-VHD verwenden. Sie müssen entweder die Offline-VHD einbinden und auf den zugehörigen einstellungspfad für Quelldateien verweisen, oder Sie müssen auf einen Ordner verweisen, der eine Kopie des Inhalts der WIM-Datei enthält.

So installieren Sie .NET Framework 3.5 durch Ausführen des Install-WindowsFeature-Cmdlets

1. Führen Sie einen der folgenden Schritte aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.

NOTE

Wenn Sie Rollen und Features von einem Remote Server installieren, müssen Sie Windows PowerShell nicht mit erhöhten Benutzerrechten ausführen.

- Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
- Klicken Sie im Windows- **Start** Bildschirm mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.

- Geben Sie auf einem Server, auf dem die Server Core-Installationsoption von Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, PowerShell in die Eingabeaufforderung ein, und drücken Sie dann die **Eingabe**Taste.
2. Geben Sie den folgenden Befehl ein, und drücken Sie dann die **Eingabe**Taste. Im folgenden Beispiel befinden sich die Quelldateien in einem Seite-an-Seite-Speicher (als SxS bezeichnet) auf dem Installationsmedium in Laufwerk D.

```
Install-WindowsFeature NET-Framework-Core -Source D:\Sources\Sxs
```

Falls der Befehl Windows Update als Quelle für fehlende Featuredateien verwenden soll oder bereits eine Standardquelle mithilfe der Gruppenrichtlinie konfiguriert wurde, muss der Parameter **Source** nur hinzugefügt werden, wenn Sie eine andere Quelle angeben möchten.

So installieren Sie .NET Framework 3,5 mithilfe des Assistenten zum Hinzufügen von Rollen und Features

1. Klicken Sie in Server-Manager im Menü **Verwalten** auf **Rollen und Features hinzufügen**.
2. Wählen Sie einen Zielserver aus, auf dem Windows Server 2016 ausgeführt wird.
3. Wählen Sie im Assistenten zum Hinzufügen von Rollen und Features auf der Seite **Features auswählen** die Option **.NET Framework 3,5aus**.
4. Ist dies durch die Gruppenrichtlinieneinstellungen für den lokalen Computer zugelassen, wird beim Installationsprozess versucht, die fehlenden Featuredateien mithilfe von Windows Update abzurufen. Klicken Sie auf **Installieren**. Sie müssen nicht mit dem nächsten Schritt fortfahren.

Wenn Gruppenrichtlinie Einstellungen dies nicht zulassen oder Sie eine andere Quelle für die .NET Framework 3,5-Featuredateien verwenden möchten, klicken Sie auf der Seite **Installations Auswahl bestätigen** des Assistenten auf **Alternativen Quellpfad angeben**.

5. Geben Sie einen Pfad zu einem Seite-an-Seite-Speicher (als SxS bezeichnet) auf einem Installationsmedium oder zu einer WIM-Datei an. Im folgenden Beispiel befindet sich das Installationsmedium in Laufwerk D.

D:\sources\sxs\

Fügen Sie zum Angeben einer WIM-Datei das Präfix **WIM:** und den Index des in der WIM-Datei zu verwendenden Images als Suffix hinzu. Dies wird im folgenden Beispiel dargestellt:

Wim:\\ server_name\share\install.Wim: 3

6. Klicken Sie auf **OK** und dann auf **Installieren**.

So installieren Sie .NET Framework 3.5 mithilfe von DISM

1. Führen Sie einen der folgenden Schritte aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.

NOTE

Wenn Sie Rollen und Features von einem Remote Server installieren, müssen Sie Windows PowerShell nicht mit erhöhten Benutzerrechten ausführen.

- Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
- Klicken Sie im Windows- **Start** Bildschirm mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.

- Geben Sie auf einem Server, auf dem die Server Core-Installationsoption ausgeführt wird, **PowerShell** in die Eingabeaufforderung ein, und drücken Sie dann die **Eingabetaste**.
2. Führen Sie einen der folgenden DISM-Befehle aus.
- Wenn der Computer Zugriff auf Windows Update hat oder in Gruppenrichtlinie bereits ein Standard Speicherort für Quelldateien konfiguriert wurde, führen Sie den folgenden Befehl aus.

```
DISM /online /Enable-Feature /Featurename:NetFx3 /All
```

- Wenn der Computer Zugriff auf die Installationsmedien hat, führen Sie einen Befehl aus, der dem folgenden ähnelt. Im folgenden Beispiel befindet sich das Installationsmedium in Laufwerk D. Der **LimitAccess**-Parameter verhindert, dass der Befehl versucht, Windows Update oder einen Server mit WSUS zu kontaktieren.

```
DISM /online /Enable-Feature /Featurename:NetFx3 /All /LimitAccess /Source:d:\sources\sxs
```

NOTE

Beim DISM-Befehl muss die Groß-/Kleinschreibung beachtet werden.

Konfigurieren alternativer Quellen für Featuredateien in der Gruppenrichtlinie

Die in diesem Abschnitt beschriebene Gruppenrichtlinieneinstellung gibt autorisierte Quellspeicherorte für .NET Framework 3.5-Dateien und andere Featuredateien an, die im Rahmen der Konfiguration von %quot;Features bei Bedarf%quot; entfernt wurden. Die Richtlinien Einstellung **Einstellungen für die Installation optionaler Komponenten und die Reparatur von Komponenten angeben** befindet sich im Ordner **Computerkonfiguration\Administrative Vorlagen\System** im Gruppenrichtlinien-Verwaltungskonsole-oder lokalen Gruppenrichtlinie-Editor.

NOTE

Sie müssen Mitglied der Administratorgruppe sein, um Gruppenrichtlinieneinstellungen auf dem lokalen Computer ändern zu können. Falls die Gruppenrichtlinieneinstellungen für den zu verwaltenden Computer auf der Domänenebene gesteuert werden, müssen Sie Mitglied der Gruppe %quot;Domänenadministratoren%quot; sein, um Gruppenrichtlinieneinstellungen ändern zu können.

So konfigurieren Sie einen alternativen Standardquellpfad in der Gruppenrichtlinie

1. Öffnen Sie im Editor für lokale Gruppenrichtlinie oder Gruppenrichtlinien-Verwaltungskonsole die folgende Richtlinien Einstellung.

Computerkonfiguration\Administrative vorlagen\system\einstellungen für die Installation optionaler Komponenten und die Reparatur von Komponenten angeben

2. Das Aktivieren der Richtlinien Einstellung wurde von sselect **aktiviert**, wenn Sie nicht bereits aktiviert ist.
3. Geben Sie im Textfeld **Alternativer Dateiquellpfad** im Bereich **Optionen** einen vollqualifizierten Pfad zu einem freigegebenen Ordner oder einer WIM-Datei an. Fügen Sie zum Angeben einer WIM-Datei als alternativer Quelldateispeicherort dem Pfad das Präfix **WIM:** und den Index des in der WIM-Datei zu verwendenden Images als Suffix hinzu. Die folgenden Beispiele enthalten Werte, die Sie angeben können.
 - Pfad zu einem freigegebenen Ordner: \\ *server_name*\Freigabe\ *FOLDER_NAME*
 - Pfad zu einer WIM-Datei, in der 3 den Index des Images darstellt, in dem sich die Featuredateien befinden: **Wim:\\ server_name\share\install.Wim: 3**

4. Wenn Sie nicht möchten, dass Computer, die von dieser Richtlinien Einstellung gesteuert werden, in Windows Update nach fehlenden Featuredateien suchen, wählen Sie **nie versuchen, Nutzlast von Windows Update herunterzuladen**.
5. Falls die von dieser Richtlinieneinstellung gesteuerten Richtlinieneinstellung in der Regel Updates über WSUS erhalten, Sie jedoch fehlende Featuredateien lieber über Windows Update und nicht über WSUS suchen möchten, aktivieren Sie **Stellen Sie direkt eine Verbindung mit Windows Update her, um Inhalte für das Reparieren herunterzuladen, anstatt WSUS (Windows Server Update Services) zu verwenden**.
6. Klicken Sie auf OK, wenn Sie diese Richtlinieneinstellung geändert haben. Schließend Sie dann den Gruppenrichtlinien-Editor.

Weitere Informationen

[Windows Server-Installationsoptionen](#)

[Bereitstellungsüberlegungen für Microsoft .NET Framework 3.5](#)

[Aktivieren oder Deaktivieren von Windows-Features](#)

Konfigurieren von "Features bei Bedarf" unter Windows Server

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

In diesem Thema wird beschrieben, wie Featuredateien in einer Features-bei-Bedarf-Konfiguration mithilfe des Cmdlets "Uninstall-WindowsFeature" entfernt werden.

Features bei Bedarf ist ein Feature, das in Windows 8 und Windows Server 2012 eingeführt wurde, mit dem Sie Rollen- und Featuredateien (manchmal auch als Funktions *Nutzlastbezeichnet*) aus dem Betriebssystem entfernen können, um Speicherplatz zu sparen, und Rollen und Features von Remote Standorten oder Installationsmedien anstelle von lokalen Computern installieren. Sie können Featuredateien von ausgeführten physischen und virtuellen Computern entfernen. Sie können Featuredateien Windows-Imagedateien (WIM) oder offline geschalteten virtuellen Festplatten (VHDs) hinzufügen oder von diesen entfernen, um eine reproduzierbare Kopie von „Features bei Bedarf“-Konfigurationen zu erstellen.

Wenn in einer Features-bei-Bedarf-Konfiguration Featuredateien auf einem Computer nicht verfügbar sind und eine Installation diese Featuredateien erfordert, kann Windows Server 2012 R2 oder Windows Server 2012 angewiesen werden, die Dateien aus einem parallelen featurespeicher (einem freigegebenen Ordner mit Featuredateien, der dem Computer im Netzwerk zur Verfügung steht) zu erhalten, von Windows Update oder vom Installationsmedium. Wenn Featuredateien nicht auf dem Zielserver verfügbar sind, sucht die Funktion "Features bei Bedarf" nach fehlenden Featuredateien, indem die folgenden Schritte in der angegebenen Reihenfolge erfolgen.

1. Durchsuchen eines Speicher Orts, der von Benutzern des Assistenten zum Hinzufügen von Rollen und Features oder von "-Installations Befehlen" angegeben wurde
2. Auswerten der Konfiguration der Gruppenrichtlinie Einstellung, **Computerkonfiguration\Administrative vorlagen\system\einstellungen für die Installation optionaler Komponenten und die Reparatur von Komponenten angeben**
3. Durchsuchen von Windows Update

Sie können das standardmäßige Features-bei-Bedarf-Verhalten über eine der folgenden Aktionen überschreiben.

- Angeben eines anderen Quellpfads als Teil des Cmdlets `Install-WindowsFeature` durch Hinzufügen des `Source` -Parameters
- Angeben eines alternativen Quell Pfads auf der Seite **Installationsoptionen bestätigen** während der Installation von Features mithilfe des Assistenten zum Hinzufügen von Rollen und Features
- Konfigurieren der Gruppenrichtlinieneinstellung **Einstellungen für die Installation optionaler Komponenten und die Reparatur von Komponenten angeben**

Dieses Thema enthält folgende Abschnitte:

- [Erstellen einer Featuredatei oder eines parallelen Stores](#)
- [Methoden zum Entfernen von Featuredateien](#)
- [Entfernen von Featuredateien mithilfe von "Uninstall-Windows Feature"](#)

Erstellen einer Featuredatei oder eines parallelen Stores

In diesem Abschnitt wird das Einrichten eines freigegebenen Remote Ordners für Featuredateien beschrieben, in dem die Dateien gespeichert werden, die zum Installieren von Rollen, Rollen Diensten und Features auf Servern, auf denen Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, erforderlich sind. Nachdem Sie einen featurespeicher eingerichtet haben, können Sie Rollen, Rollen Dienste und Features auf Servern mit diesen Betriebssystemen installieren und den featurespeicher als Speicherort der Installations Quelldateien angeben.

So erstellen Sie einen Speicher für Featuredateien

1. Erstellen Sie auf einem Server im Netzwerk einen freigegebenen Ordner. Beispielsweise `\network\share\sxs`.
2. Vergewissern Sie sich, dass Sie über die ordnungsgemäßen Berechtigungen für den Featurespeicher verfügen. Der Quellpfad oder die Dateifreigabe muss entweder der Gruppe **jeder** (nicht empfohlen aus Sicherheitsgründen) oder den Computer Konten (`Domänen\Servername$`) der Server, auf denen Sie Features mithilfe dieses featurestores installieren möchten, **Lese** Berechtigungen erteilen. das Gewähren des Benutzerkonto Zugriffs ist nicht ausreichend.

Sie können auf Einstellungen zu Dateifreigaben und Berechtigungen über eine der folgenden Aktionen auf dem Windows-Desktop zugreifen.

- Klicken Sie mit der rechten Maustaste auf den freigegebenen Ordner, klicken Sie auf **Eigenschaften**, und ändern Sie anschließend auf der Registerkarte **Sicherheit** die zulässigen Benutzer und ihre Zugriffsrechte.
- Klicken Sie mit der rechten Maustaste auf den freigegebenen Ordner, zeigen Sie auf **Freigeben für**, und klicken Sie anschließend auf **Bestimmte Personen**.

NOTE

Server in Arbeitsgruppen können nicht auf externe Dateifreigaben zugreifen, auch wenn das Computerkonto des Arbeitsgruppenservers für die externe Freigabe über die Berechtigung **Lesen** verfügt. Alternative Quellspeicherorte, die für Arbeitsgruppenserver funktionieren, sind u. a. Installationsmedien, Windows Update sowie VHD- oder WIM-Dateien, die auf dem lokalen Arbeitsgruppenserver gespeichert sind.

3. Kopieren Sie den Ordner `Sources\Sxs` vom Installationsmedium von Windows Server in den freigegebenen Ordner, den Sie in Schritt 1 erstellt haben.

Methoden zum Entfernen von Featuredateien

Es gibt zwei Möglichkeiten zum Entfernen von Featuredateien aus Windows Server in einer „Features bei Bedarf“-Konfiguration.

- Der `remove`-Parameter des `Uninstall-WindowsFeature`-Cmdlets ermöglicht das Löschen von Featuredateien von einem Server oder einer offline geschalteten virtuellen Festplatte (VHD), auf dem Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Gültige Werte für den `remove`-Parameter sind die Namen von Rollen, Rollen Diensten und Features.
- DISM-Befehle (Deployment Image Servicing and Management, Abbildverwaltung für die Bereitstellung) ermöglichen das Erstellen benutzerdefinierter WIM-Dateien zum Einsparen von Festplattenspeicher, indem Featuredateien weggelassen werden, die entweder nicht benötigt werden oder aus anderen Remotequellen abgerufen werden können. Weitere Informationen zum Vorbereiten benutzerdefinierter Images mit DISM finden Sie unter [How to Enable or Disable Windows Features](#).

Entfernen von Featuredateien mithilfe von "Uninstall-Windows Feature"

Mit dem Cmdlet "Uninstall-Windows Feature" können Sie sowohl Rollen, Rollen Dienste und Features von Servern

als auch offline-VHDs, auf denen Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, deinstallieren und Featuredateien löschen. Wenn gewünscht, können Sie dieselben Rollen, Rollen Dienste und Features im gleichen Befehl deinstallieren und löschen.

IMPORTANT

Wenn Sie Featuredateien für eine Rolle, einen Rollen Dienst oder eine Funktion löschen, werden Rollen, Rollen Dienste und Features, die von den Dateien abhängen, die Sie entfernen, ebenfalls gelöscht. Wenn Sie Featuredateien für einen Rollendienst oder Unterfeature löschen und keine anderen Rollendienste oder Unterfeatures für die übergeordnete Rolle bzw. das übergeordnete Feature installiert sind, werden Dateien für die gesamte übergeordnete Rolle bzw. das gesamte übergeordnete Feature gelöscht. Fügen Sie zum Anzeigen aller Features, die durch den Befehl `Uninstall-WindowsFeature -remove` gelöscht würden, den `-whatif` -Parameter dem Befehl hinzu, um diesen auszuführen und Ergebnisse anzuzeigen, ohne Featuredateien tatsächlich zu löschen.

So entfernen Sie Rollen- und Featuredateien mithilfe von "Uninstall-WindowsFeature"

1. Führen Sie einen der folgenden Schritte aus, um eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten zu öffnen.

NOTE

Wenn Sie Rollen und Features von einem Remote Server deinstallieren, müssen Sie Windows PowerShell nicht mit erhöhten Benutzerrechten ausführen.

- Klicken Sie auf dem Windows-Desktop auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **Als Administrator ausführen**.
- Klicken Sie im Windows- **Start** Bildschirm mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.
- Geben Sie auf einem Server, auf dem die Server Core-Installationsoption ausgeführt wird, **PowerShell** in die Eingabeaufforderung ein, und drücken Sie dann die **EingabeTaste**.

2. Geben Sie Folgendes ein, und drücken Sie dann die **EINGABETASTE**.

```
Uninstall-WindowsFeature -Name <feature_name> -computerName <computer_name> -remove
```

Beispiel: "Remotedesktoplizenzierung" ist der letzte verbleibende Rollendienst der installierten Remotedesktopdienste. Der Befehl deinstalliert "Remotedesktoplizenzierung" und anschließend die Featuredateien der gesamten Rolle "Remotedesktopdienste" vom angegebenen Server *contoso_1*.

```
Uninstall-WindowsFeature -Name rdS-Licensing -computerName contoso_1 -remove
```

Beispiel: Im folgenden Beispiel entfernt der Befehl Active Directory-Domänen Dienste und Gruppenrichtlinie Verwaltung von einer Offline-VHD. Zunächst werden die Rolle und das Feature deinstalliert. Anschließend werden die Featuredateien vollständig von der Offline-VHD *Contoso.vhd* entfernt.

NOTE

Sie müssen den `computerName`-Parameter hinzufügen, wenn Sie das Cmdlet auf einem Computer mit Windows 8.1 oder Windows 8 ausführen.

Wenn Sie den Namen einer VHD-Datei auf einer Netzwerkfreigabe eingeben, muss diese Freigabe dem Computer Konto des Servers, den Sie zum Einbinden der VHD ausgewählt haben, **Lese**- und **Schreib** Berechtigungen erteilen. Die Zugriffsberechtigungen des Benutzerkontos reichen nicht aus. Die Freigabe kann der Gruppe **Jeder** die Berechtigungen **Lesen** und **Schreiben** gewähren, um den Zugriff auf die VHD zu ermöglichen, dies wird aber aus Sicherheitsgründen nicht empfohlen.

```
Uninstall-WindowsFeature -Name AD-Domain-Services,GPMC -VHD C:\WS2012VHDs\Contoso.vhd -computerName  
ContosoDC1
```

Weitere Informationen

[Installieren oder Deinstallieren von Rollen, Rollen Diensten oder Features](#) [Windows Server-Installationsoptionen](#)
[Gewusst wie: Aktivieren oder Deaktivieren von Windows-Features](#) [Bereitstellung](#) [Abbildung](#) [Verwaltung \(Mage\)](#)
[Übersicht](#)

Anzeigen und Konfigurieren von Leistungs-, Ereignis- und Dienstdaten

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In diesem Thema wird beschrieben, wie Sie die Ereignisprotokoll Einträge, Leistungsindikatoren und Dienst Warnungen anzeigen und konfigurieren, die für lokale und Remote Server in Server-Manager angezeigt werden.

Ereignis-, Dienst-und Leistungs Protokolldaten werden an zwei Stellen in der Server-Manager-Konsole in Windows Server angezeigt.

- Auf dem Dashboard können Sie auf die Zeilen **Ereignisse**, **Leistung** und **Dienste** klicken, um die Ereignis-, Leistungs- und Dienst Protokolldaten zu konfigurieren, die Sie für Rollen, den gesamten Server-Manager Server Pool, vom Benutzer erstellte Server Gruppen und den lokalen Server anzeigen möchten. Durch Klicken auf die Textzeilen werden die Dialogfelder **Detailansicht** geöffnet, in denen Sie die Daten angeben können, über die Sie im Dashboard benachrichtigt werden möchten. Nachdem Sie die Ereignis-, Dienst- und Leistungs Protokolldaten konfiguriert haben, die in den Miniaturansichten des Dashboards hervorgehoben werden sollen, werden Protokolleinträge, die den angegebenen Kriterien entsprechen, unten in den Dialogfeldern **Detailansicht** aufgelistet.
- Die Kacheln **Ereignisse**, **Dienste** und **Leistung** sind Teil der Rollen- und Gruppen-Homepages. Mit den Befehlen im Menü **Aufgaben** dieser Kacheln können Sie die Daten angeben, die Sie von verwalteten Servern sammeln möchten. Die Kacheln enthalten Filter und Abfragen, mit denen die in der Kachel angezeigten Protokolleinträge weiter eingeschränkt werden können, sofern dies gewünscht wird.

Dieses Thema enthält folgende Abschnitte:

- [Was sind Miniaturansichten?](#)
- [Anzeigen und Konfigurieren von Ereignissen](#)
- [Anzeigen und Konfigurieren von Leistungsindikatoren](#)
- [Dienste verwalten und Dienst Warnungen konfigurieren](#)
- [Anzeigen und Kopieren von Ereignis- oder Leistungs Einträgen](#)

Was sind Miniaturansichten?

Miniaturansichten werden auf dem Server-Manager-Dashboard für jede Rolle angezeigt (die Miniaturansicht einer Rolle spiegelt die gesammelten Daten zu allen Servern im Server-Manager Pool wider, auf denen die Rolle ausgeführt wird), für jede Server Gruppe, für die Gruppe **alle** Server (alle Server im Server-Manager Pool) und für den lokalen Server. Nachdem Server-Manager Daten von verwalteten Servern abgerufen hat, werden für Rollen, die auf Servern im Server Pool ausgeführt werden, automatisch Miniaturansichten erstellt.

Wenn die Server-Manager-Konsole im Rahmen Remoteserver-Verwaltungstools auf einem Client Computer ausgeführt wird, gibt es keine Miniaturansicht für den **lokalen Server**.

Die Miniaturansicht zeigt eine kurze Übersicht über den Status und die Verwaltbarkeit von Rollen, Servern und Servergruppen. Die Farbe der Zeile für die Miniaturansicht-Überschrift ändert sich (und hervorgehobene Zahlen

werden am linken Rand angezeigt), wenn Ereignisse, Leistungsindikatoren, Best Practices Analyzer Ergebnisse, Dienste oder allgemeine verwaltbarkeitsprobleme Kriterien erfüllen, die Sie in den durch Klicken auf Miniatur Ansichts Zeilen geöffneten Dialogfeldern der **Detailansicht** konfigurieren. In der folgenden Tabelle werden die in den Miniaturansichten angezeigten Daten erläutert.

MINIATURANSICHTSZEILE	BESCHREIBUNG
Verwaltbarkeit	<p>Die Verwaltbarkeit eines Servers umfasst mehrere Measures: ob der Server Online oder offline ist, ob auf ihn zugegriffen werden kann und welche Daten Server-Manager werden, ob der Benutzer, der am lokalen Computer angemeldet ist, über ausreichende Benutzerrechte für den Zugriff auf den Remote Server verfügt und ob auf dem Remote Server die gesamte für die Remote Verwaltung erforderliche Software verfügbar ist. oder, ob der Server so konfiguriert wurde, dass er mit Server-Manager abgefragt und verwaltet werden kann. Die einzigen verwaltbarkeitsdaten, die Server-Manager von einem Server, auf dem Windows Server 2003 ausgeführt wird, erfassen können, ist, ob der Server Online oder offline ist. Ausführliche Informationen zu Verwaltbarkeitsstatusfehlern und deren Behebung finden Sie im Server Manager Troubleshooting Guide.</p>
Ereignisse	<p>Sie können die Zeile Ereignisse einer Miniaturansicht so konfigurieren, dass Benachrichtigungen angezeigt werden, wenn Ereignisse mit den von Ihnen angegebenen Schweregraden, Quellen, Zeiträumen, Servern oder Ereignis-IDs protokolliert werden. Zeigen Sie Details zu Ereignissen an, und ändern Sie die Warnungen, die Sie anzeigen möchten, indem Sie auf die Zeile Ereignisse klicken und das Dialogfeld Detailansicht Ereignisse für die Rolle oder Server Gruppe öffnen.</p>
Dienste	<p>Sie können die Zeile Dienste so konfigurieren, dass Warnungen angezeigt werden, wenn Dienste in einer Rolle oder Server Gruppe gefunden werden, die Start Typen, Dienststatus, Dienstnamen und Servern entsprechen, die Sie im Dialogfeld Dienst Detailansicht angeben.</p> <p>Nachdem ein Server dem Server-Manager-Server Pool hinzugefügt wurde, können Dienst Warnungen zum Dienst für die Shellhardwareerkennung angezeigt werden, wenn keine Benutzer am verwalteten Server angemeldet sind. Dies geschieht, weil der Dienst für die Shellhardwareerkennung nur ausgeführt wird, wenn Benutzer am verwalteten Server angemeldet oder mit einer Remotedesktopsitzung auf dem verwalteten Server verbunden sind. Damit in diesem Fall keine Shellhardwareerkennung-Dienstwarnungen angezeigt werden, klicken Sie in den Miniaturansichten für Servergruppen, einschließlich der Gruppe Alle Server, auf Dienste. Deaktivieren Sie im Dialogfeld Dienst Detailansicht in der Dropdown Liste Dienste das Kontrollkästchen für Shellhardwareerkennung, und klicken Sie dann auf OK.</p>

MINIATURANSICHTSZEILE	BESCHREIBUNG
Leistung	<p>Sie können die Zeile Leistung so konfigurieren, dass Warnungen für eine Rolle oder Server Gruppe angezeigt werden, wenn Leistungs Warnungen auftreten, die Ressourcentypen, Servern oder Zeiträumen entsprechen, die Sie im Dialogfeld Leistungs Detailansicht angeben.</p> <p>Leistungsindikatoren sind standardmäßig deaktiviert. Verwaltete Server, auf denen Betriebssysteme ausgeführt werden, die neuer als Windows Server 2003 sind und für die keine Leistungsindikatoren gestartet wurden, zeigen normalerweise verwaltbarkeitsstatusfehler von Online-Leistungsindikatoren, die auf der Kachel Server der Rollen-oder Gruppen Seiten nicht gestartet sind, an. Um die Leistungsindikatoren für verwaltete Server zu aktivieren, klicken Sie auf der Seite alle Server mit der rechten Maustaste auf Einträge auf der Kachel Leistung, die den Indikator Status Wert auszeigt, und klicken Sie dann auf Leistungsindikatoren starten. Sie können Leistungsindikatoren auch starten, indem Sie in der Kachel Server der Rollen-oder Gruppen Seiten mit der rechten Maustaste auf Einträge für Server klicken und dann auf Leistungsindikatoren startenklicken.</p>
BPA-Ergebnisse	<p>Sie können die Zeile BPA-Ergebnisse so konfigurieren, dass Warnungen für eine Rolle oder Server Gruppe angezeigt werden, wenn BPA-Scanergebnisse gefunden werden, die Schweregraden, Servern oder BPA-Kategorien entsprechen, die Sie im Dialogfeld mit der BPA-Ergebnis Detailansicht angeben.</p>

Anzeigen und Konfigurieren von Ereignissen

In diesem Abschnitt erfahren Sie, wie Sie konfigurieren können, welche Ereignisprotokoll Daten von den Servern im Server-Manager Server Pool gesammelt werden und welche Ereignisse Sie in den Miniaturansichten hervorheben möchten.

NOTE

Die Ereignisse, über die Sie in den Miniaturansichten benachrichtigt werden, sind eine Teilmenge der Gesamt Ereignisse, die Sie anweisen, Server-Manager von verwalteten Servern zu erfassen. Obwohl das Ändern von Ereignis Kriterien im Dialogfeld **Ereignisdaten konfigurieren** in den Kacheln **Ereignisse** die Anzahl der Warnungen ändern kann, die auf dem Server-Manager-Dashboard angezeigt werden, wirkt sich das Ändern der Kriterien für Ereignis Warnungen in den Miniaturansichten nicht auf die Ereignisprotokoll Daten aus, die von den verwalteten Servern gesammelt werden.

So konfigurieren Sie Ereignisse, die von verwalteten Servern gesammelt werden

1. Öffnen Sie in der Server-Manager Konsole eine beliebige Seite außer dem Dashboard. Sie können die Ereignisse, die Sie von den verwalteten Servern sammeln möchten, in der Kachel **Ereignisse** auf der Seite der entsprechenden Rolle, Servergruppe oder des lokalen Servers konfigurieren.
2. Klicken Sie in der Kachel **Ereignisse** im Menü **Aufgaben** auf **Ereignisdaten konfigurieren**.
3. Wählen Sie die Ereignis Schwergrade aus, die von den Servern in der ausgewählten Gruppe gesammelt werden sollen. Standardmäßig sind die Schwergrade **Kritisch**, **Fehler** und **Warnung** ausgewählt.
4. Geben Sie einen Zeitraum an, in dem die Ereignisse auftreten. Das Standardalter für Ereignisse beträgt 24 Stunden.

5. Wählen Sie die Ereignisprotokoll Dateien aus, aus denen die Ereignisse gesammelt werden sollen. Die Standardwerte sind **Anwendung**, **Setup** und **System**.
6. Klicken Sie zum Speichern der Änderungen auf **OK**, um das Dialogfeld **Ereignisdaten konfigurieren** zu schließen. Ereignisdaten werden automatisch aktualisiert, wenn Ihre Änderungen gespeichert werden.

So konfigurieren Sie die Ereignisse, die in Miniaturansichten hervorgehoben werden

1. Wenn Server-Manager bereits geöffnet ist, fahren Sie mit dem nächsten Schritt fort. Ist der Server-Manager noch nicht geöffnet, öffnen Sie ihn mit einer der folgenden Aktionen.
 - Starten Sie auf dem Windows-Desktop den Server-Manager, indem Sie in der Windows-Taskleiste auf **Server-Manager** klicken.
 - Klicken Sie auf der Windows-Startseite auf die Kachel **Server-Manager**.
2. Klicken Sie auf der Dashboardseite in der Kachel **Rollen und Servergruppen** in einer Miniaturansicht auf die Zeile **Ereignisse**.
3. Fügen Sie im Dialogfeld **Ereignis Detailansicht** den Ereignissen, die Sie anzeigen möchten, einen Schweregrad hinzu. Standardmäßig werden in der Miniaturansicht nur Warnungen zu kritischen Ereignissen hervorgehoben. Beachten Sie, dass die Anzahl der im Dialogfeld **Detailansicht** angezeigten Ereignisse zunimmt, wenn Sie einen Schweregrad hinzufügen, über den Sie benachrichtigt werden möchten.
4. Wählen Sie im Feld **Ereignisquellen** die Ereignisquellen aus, über die Sie benachrichtigt werden möchten. Der Standardwert ist **All**.
5. Wenn diese Miniaturansicht für eine Rolle gilt, die auf mehreren Servern oder einer Gruppe von mehreren Servern installiert ist, können Sie die Server, für die Sie Ereignis Warnungen erhalten möchten, in der Dropdown Liste **Server** auswählen.
6. Geben Sie im Feld **Zeitraum** einen Zeitraum von bis zu 1440 Minuten, 24 Stunden oder 1 Tag an.
7. Geben Sie im Feld **Ereignis-IDs** die Ereignis-IDs bestimmter Ereignisse an, über die Sie benachrichtigt werden möchten. Sie können einen Bereich von Ereignis-IDs getrennt durch einen Bindestrich (-) eingeben und Ereignis-IDs aus dem Bereich ausschließen, indem Sie den Bindestrich vor der Ereignis-ID oder dem Bereich von Ereignis-IDs eingeben, die Sie ausschließen möchten. Beispielsweise bedeutet der Wert **1,3,5-99,-76**, dass Warnungen für die Ereignis-IDs 1,3,5-99 und 76 und für alle Ereignisse-IDs zwischen 1 und 3 ausgelöst werden, mit Ausnahme von Ereignis-ID 5.
8. Wenn Sie die Kriterien dafür ändern, welche Warnungen angezeigt werden, ändert sich möglicherweise die Anzahl der Ereigniswarnungen, die im Ergebnisbereich unten im Dialogfeld angezeigt werden. Wählen Sie Einträge in der Liste aus, und klicken Sie auf **Warnungen ausblenden**, um zu verhindern, dass die Anzahl der in der Quell Miniaturansicht angezeigten Warnungen beeinträchtigt wird. Halten Sie bei der Auswahl der Warnungen die **STRG**-Taste gedrückt, um mehrere Warnungen gleichzeitig auszuwählen. Sie können Warnungen ausblenden, die Ihren Warnkriterien entsprechen, die Sie jedoch nicht anzeigen lassen möchten.
9. Klicken Sie auf **Alle anzeigen**, um ausgeblendete Warnungen wieder in der Liste sichtbar zu machen.
10. Klicken Sie auf **OK**, um die Änderungen zu speichern, das Dialogfeld **Detailansicht** zu schließen und die Änderungen an den Ereignis Warnungen in der Quell Miniaturansicht anzuzeigen.

Anzeigen und Konfigurieren von Leistungs Protokolldaten

In diesem Abschnitt erfahren Sie, wie Sie konfigurieren können, welche Leistungs Protokolldaten von den Servern im Server-Manager Server Pool gesammelt werden und welche Leistungs Warnungs Warnungen Sie in den Miniaturansichten hervorheben möchten.

Leistungsindikatoren sind standardmäßig deaktiviert. Verwaltete Server, auf denen Betriebssysteme ausgeführt werden, die neuer als Windows Server 2003 sind und für die keine Leistungsindikatoren gestartet wurden, zeigen normalerweise verwaltbarkeitsstatusfehler von **Online-Leistungsindikatoren**, die auf der Kachel **Server** der Rollen-oder Gruppen Seiten nicht gestartet sind, an. Um die Leistungsindikatoren für verwaltete Server zu aktivieren, klicken Sie auf der Seite **alle Server** mit der rechten Maustaste auf Einträge auf der Kachel **Leistung**, die den Indikator **Status Wert** ausanzeigt, und klicken Sie dann auf **Leistungsindikatoren starten**. Sie können Leistungsindikatoren auch starten, indem Sie in der Kachel **Server** der Rollen-oder Gruppen Seiten mit der rechten Maustaste auf Einträge für Server klicken und dann auf **Leistungsindikatoren starten**klicken.

NOTE

Die Leistungs Warnungen, die Sie in den Miniaturansichten anzeigen, sind eine Teilmenge der gesamten Leistungsdaten, die Sie anweisen, Server-Manager von verwalteten Servern zu erfassen. Obwohl das Ändern der Kriterien für die Leistungs Warnung im Dialogfeld **Leistungs Warnungen konfigurieren** in den Kacheln **Leistung** die Anzahl der Warnungen ändern kann, die auf dem Server-Manager-Dashboard angezeigt werden, hat das Ändern der Kriterien für die Leistungs Warnung in den Miniaturansichten keine Auswirkung auf die Leistungs Protokolldaten, die von verwalteten Servern gesammelt werden.

Aus diesem Grund kann das maximale Alter von Leistungsdaten, die Sie in den Miniaturansichten anzeigen können, nicht größer als der maximale Zeitraum der Diagrammanzeige sein, der im Dialogfeld **Leistungswarnungen konfigurieren** konfiguriert ist. Wenn der Wert des **Diagramms für die Diagramm Anzeige** in **Leistungs Warnungen konfigurieren** z. b. **1 Tag**ist, kann der Maximalwert für das Feld **Zeitraum** im Dialogfeld mit der **Leistungs Detailansicht**, das Sie über das Server-Manager Dashboard geöffnet haben, **1 Tag, 24 Stunden**oder **1.440 Minuten**sein.

So konfigurieren Sie die Leistungsprotokolldaten, die von den verwalteten Servern gesammelt werden

1. Öffnen Sie in der Server-Manager Konsole eine beliebige Seite außer dem Dashboard. Sie können die Leistungsdaten, die Sie von den verwalteten Servern sammeln möchten, in der Kachel **Leistung** auf der Seite der entsprechenden Rolle, Servergruppe oder des lokalen Servers konfigurieren.
2. Um Leistungsprotokolldaten von verwalteten Servern sammeln zu können, müssen die Leistungsindikatoren aktiviert sein. Wenn die Leistungsindikatoren ausgeschaltet sind, klicken Sie mit der rechten Maustaste auf einen Eintrag in der Kachel **Leistung**, und klicken Sie dann auf **Leistungsindikatoren starten**. Das Sammeln von Leistungsindikatordaten kann einige Zeit in Anspruch nehmen, je nach der Anzahl der Server, von denen die Daten gesammelt werden, und der zur Verfügung stehenden Netzwerkbandbreite. Zeigen Sie den Status in der Spalte **Zählerstatus** an.
3. Klicken Sie im Menü **Aufgaben** der Kachel **Leistung** auf **Leistungswarnungen konfigurieren**.
4. Geben Sie für die Server in der ausgewählten Gruppe oder, auf denen die ausgewählte Rolle ausgeführt wird, an, in welchem Prozentsatz der CPU-Auslastung von Server-Manager Warnungen gesammelt werden sollen. Der Standardwert liegt bei 85 %.
5. Geben Sie den verbleibenden verfügbaren Arbeitsspeicher in Megabyte an, den die Server haben sollen, bevor Leistungsindikatorwarnungen gesammelt werden. Der Standardwert ist 2 MB.
6. Geben Sie für die Ressourcen **CPU-Auslastung** und **Verfügbarer Arbeitsspeicher** in der Kachel **Leistung** einen Zeitraum, der in den Diagrammen wiedergespiegelt werden soll. Der Standardzeitraum ist ein Tag. Klicken Sie auf **Speichern**.

Beachten Sie, dass sich die Anzahl der Leistungswarnungen in der Kachel **Leistung** und die im Diagramm dargestellte Zuordnung der Warnungen im Zeitverlauf ändern können, nachdem Sie auf **Speichern** geklickt haben.

NOTE

bei virtuellen Maschinen, für die **dynamischer Arbeitsspeicher** aktiviert ist, kann das Erhöhen des Schwellenwerts für die Leistungs Warnungen zu falsch positiven Warnungen führen.

7. Klicken Sie im Menü **Aufgaben** auf **Aktualisieren**, um die Liste der Leistungswarnungen zu aktualisieren, die von den Servern gesammelt werden.

So konfigurieren Sie sie Leistungswarnungen, die in den Miniaturansichten hervorgehoben werden

1. Klicken Sie auf der Dashboardseite in der Kachel **Rollen und Servergruppen** in einer Miniaturansicht auf die Zeile **Leistung**.

2. Aktivieren bzw. deaktivieren Sie im Dialogfeld **Leistungs Detailansicht** im Feld **Ressourcentyp** die Kontrollkästchen für Ressourcen Leistungs Schwellenwerte, über die Sie benachrichtigt werden möchten. Beachten Sie, dass sich die Anzahl der im Dialogfeld **Detailansicht** angezeigten Leistungs Warnungen erhöhen kann, wenn Sie einen Schwellenwert für die Ressourcen Leistung hinzufügen, über den Sie benachrichtigt werden möchten.

3. Wenn diese Miniaturansicht für eine Rolle gilt, die auf mehreren Servern oder einer Gruppe von mehreren Servern installiert ist, können Sie die Server, für die Sie Leistungs Warnungen erhalten möchten, in der Dropdown Liste **Server** auswählen.

4. Geben Sie im **Feld Zeitraum** einen Zeitraum von bis zu 1440 Minuten, 24 Stunden oder 1 Tag an.

5. Wenn Sie die Kriterien dafür ändern, welche Warnungen angezeigt werden, ändert sich möglicherweise die Anzahl der Warnungen, die im Ergebnisbereich unten im Dialogfeld angezeigt werden. Klicken Sie auf **Warnungen ausblenden**, um alle Warnungen auszublenden, die sich nicht auf den aktuellen Zeitpunkt beziehen. Sie wirken sich dann nicht auf die Anzahl der Warnungen aus, die in der Quellminiaturansicht angezeigt wird.

6. Klicken Sie auf **Alle anzeigen**, um ausgeblendete Warnungen wieder in der Liste sichtbar zu machen.

7. Klicken Sie auf **OK**, um die Änderungen zu speichern. Schließen Sie das Dialogfeld **Detailansicht**, und zeigen Sie die Änderungen der Leistungs Warnung in der Quell Miniaturansicht an.

So zeigen Sie die Eigenschaften der Leistungswarnungen an

1. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf der Dashboardseite in der Kachel **Rollen und Servergruppen** in einer Miniaturansicht auf die Zeile **Leistung**.
- Öffnen Sie die Homepage einer Rolle oder Gruppe, und suchen Sie nach der Kachel **Leistung** für die Rolle oder Gruppe.

2. Doppelklicken Sie auf eine Leistungswarnung in der Liste, um die dazugehörigen Eigenschaften anzuzeigen. Alternativ können Sie mit der rechten Maustaste auf eine Leistungswarnung klicken und dann **Eigenschaften anzeigen** auswählen.

3. Wählen Sie im Dialogfeld **Leistungsalarmeigenschaften** Protokolleinträge aus, um Informationen über die Prozesse anzuzeigen, die mit dem Eintrag im Bereich **Prozesse** verknüpft sind.

4. Wenn Sie die Leistungsalarmeigenschaften geprüft haben, schließen Sie das Dialogfeld.

Analyse von Leistungsdaten und Problembehebung

Weitere Informationen zum Analysieren von Leistungsdaten in Server-Manager und zur Behebung von Leistungsproblemen auf verwalteten Servern finden Sie in den folgenden Ressourcen.

- [Analysieren von Leistungsdaten](#)

- [Lösen von Leistungsproblemen](#)

Weitere Informationen zu erweiterten Tools für die Leistungsüberwachung und-Analyse, die für Windows Server 2012 und spätere Versionen von Windows Server verfügbar sind, einschließlich Server Performance Advisor 3.0, finden Sie unter Performance on MSDN ([Leistung](#) auf MSDN).

Dienste verwalten und Dienst Warnungen konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie Dienste starten, anhalten, neu starten, anhalten oder fortsetzen, die auf den Rollen-und Server Gruppen Seiten in Server-Manager auf der Kachel **Dienste** angezeigt werden. Sie können auch die Dienste konfigurieren, über die Sie in den Miniaturansichten auf dem Server-Manager-Dashboard benachrichtigt werden.

NOTE

Der Starttyp für Dienste, Dienst Abhängigkeiten, Wiederherstellungsoptionen oder andere Dienst Eigenschaften kann auf der Kachel **Dienste** in Server-Manager nicht geändert werden. Wenn Sie andere Diensteigenschaften als den Dienststatus ändern möchten, öffnen Sie das Snap-In **Dienste**. Eine Verknüpfung zum Öffnen des Snap-Ins " **Dienste** " ist im Menü " **Tools** " in Server-Manager verfügbar.

So können Sie Dienste starten, beenden, neu starten, anhalten und fortsetzen

1. Öffnen Sie in der Server-Manager Konsole eine beliebige Seite außer dem Dashboard (d. h. eine beliebige Rollen-oder Gruppen Startseite).
2. Klicken Sie in der Kachel **Dienste** für die Rolle oder Gruppe mit der rechten Maustaste auf einen Dienst.
3. Klicken Sie im Kontextmenü auf die gewünschte Aktion, mit der dieser Dienst ausgeführt werden soll.
Wurde der Dienst beendet, ist die einzige Aktion, die Sie ausführen können, den Dienst zu starten. Wird der Dienst angehalten, ist dementsprechend die einzige Aktion, die Sie ausführen können, den Dienst fortzusetzen.
4. Beachten Sie, dass sich der Wert der Spalte **Status** für den in der Kachel **Dienste** ausgewählten Dienst ändert, wenn Sie einen Dienst starten, stoppen, neu starten, anhalten oder fortsetzen.

So konfigurieren Sie die Dienstbenachrichtigungen, die in Miniaturansichten hervorgehoben werden

1. Klicken Sie auf der Dashboardseite in der Kachel **Rollen und Servergruppen** in einer Miniaturansicht auf die Zeile **Dienste**.
2. Wählen Sie im Dialogfeld **Dienst Detailansicht** die Start Typen für Dienste aus, über die Sie benachrichtigt werden möchten. Standardmäßig sind **automatisch (verzögerter Start)** und **automatisch** ausgewählt.
3. Wählen Sie die Dienststatus aus, über die Sie benachrichtigt werden möchten. Standardmäßig ist **Alle** ausgewählt.
4. Wählen Sie Dienste aus, über die Sie benachrichtigt werden möchten. Standardmäßig ist **Alle** ausgewählt.
5. Wählen Sie die Server aus, die der Rolle oder Gruppe zugeordnet sind, für die Sie Warnungen zu Diensten erhalten möchten. Standardmäßig ist **Alle** ausgewählt.
6. Wenn Sie die Kriterien dafür ändern, welche Warnungen angezeigt werden, ändert sich möglicherweise die Anzahl der Warnungen, die im Ergebnisbereich unten im Dialogfeld angezeigt werden. Klicken Sie auf **Warnungen ausblenden**, um alle Warnungen auszublenden, die sich nicht auf den aktuellen Zeitpunkt beziehen. Sie wirken sich dann nicht auf die Anzahl der Warnungen aus, die in der Quellminiaturansicht angezeigt wird.
7. Klicken Sie auf **Alle anzeigen**, um ausgeblendete Warnungen wieder in der Liste sichtbar zu machen.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern, das Dialogfeld **Detailansicht** zu schließen und die

Änderungen an den Dienst Warnungen in der Quell Miniaturansicht anzuzeigen.

Anzeigen und Kopieren von Ereignis-, Dienst-oder Leistungs Einträgen

Sie können in den Dialogfeldern **Detailansicht** und in den Kacheln **Ereignisse** und **Leistung** für eine Rolle oder eine Gruppe Eigenschaften für Ereignis-, Dienst-oder Leistungs Einträge kopieren. Klicken Sie mit der rechten Maustaste auf einen Ereignis-oder leistungseintrag, und klicken Sie auf **Kopieren**.

Über die Kachel **Ereignisse** können Sie auch in der unteren Hälfte der Kachel Ereigniseigenschaften in der Vorschau anzeigen, indem Sie in der Liste einen Eintrag auswählen. Zum Kopieren der in der Vorschau angezeigten Eigenschaften klicken Sie mit der rechten Maustaste auf den Vorschaubereich, und klicken Sie dann auf **Kopieren**.

Weitere Informationen

[Server-Manager](#)

[Filtern, Sortieren und Abfragen von Daten in Server-Manager-Kacheln](#)

Anzeigen von Aufgabendetails und Benachrichtigungen

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Wenn Sie in Server-Manager unter Windows Server 2012 R2 oder Windows Server 2012 Verwaltungsaufgaben durchführen, z. B. Rollen und Features hinzufügen, Dienste starten, Daten aktualisieren, die in der Server-Manager-Konsole angezeigt werden, oder eine benutzerdefinierte Gruppe von Servern erstellen, wird im **Benachrichtigungen** Bereich des Server-Manager-Konsolen Headers eine Benachrichtigung angezeigt. Benachrichtigungen und das Dialogfeld **Aufgaben Details**, das Sie über das Menü **Benachrichtigungen** öffnen können, indem Sie auf das Flag-Symbol klicken, den Status von Benutzer Aufgaben oder-Anforderungen anzeigen, anzeigen, wenn eine Aufgabe fehlgeschlagen ist, und bei der Problembehandlung helfen, indem Sie auf detaillierte Fehlermeldungen zu Aufgaben Fehlern verweisen.

Infobereich

Der **Benachrichtigungen** Bereich in der Menüleiste Server-Manager, der durch ein flagsymbol gekennzeichnet ist, zeigt die Ergebnisse der Aufgaben an, die Sie in Server-Manager starten. Benachrichtigungen informieren Sie darüber, ob Aufgaben, die Sie in Server-Manager gestartet haben, erfolgreich waren oder fehlgeschlagen sind. Wenn Benachrichtigungen zur Ansicht verfügbar sind, wird die Anzahl verfügbarer Benachrichtigungen neben dem Flaggensymbol angezeigt. Falls eine Aufgabe fehlgeschlagen ist, nur teilweise abgeschlossen werden konnte (wenn sie beispielsweise nicht auf allen gewünschten Remoteservern durchgeführt werden konnte) oder mit Warnungen abgeschlossen wurde, wird die Benachrichtigungsflagge rot. Für folgende Aufgaben werden Benachrichtigungen angezeigt.

- Manuelles Aktualisieren der in Server-Manager angezeigten Daten (Benachrichtigungen werden nur für automatische Aktualisierungen angezeigt, wenn die Aktualisierungen fehlschlagen)
- Starten oder Beenden von Diensten
- Installieren oder Deinstallieren von Rollen, Rollen Diensten und Features
- Starten eines Best Practices Analyzer-Scans (BPA)
- Hinzufügen von zu verwaltenden Remote Servern (Benachrichtigungen werden angezeigt, um die für Remote Server angezeigten Daten zu kontaktieren oder zu aktualisieren)

Zu den Elementen im Menü **Benachrichtigungen** gehören eine Statusleiste, eine kurze Beschreibung der Aufgabe, der Name des Zielservers für die Aufgabe (oder eines der Zielserver, falls mehrere Zielserver ausgewählt wurden), ggf. ein Link zu einem dazugehörigen Steuerelement oder Dialogfeld und das Menü **Aufgaben**. Das Menü **Aufgaben** zeigt Befehle für die aktive Benachrichtigung an (die Benachrichtigung, über die der Mauszeiger bewegt wird). Wenn Sie beispielsweise einen Dienst beenden, können Sie im Menü **Aufgaben** der Benachrichtigung auf **Neu starten** klicken, um den Dienst neu zu starten.

Benachrichtigungen sind besonders nützlich für das Installieren oder Deinstallieren von Rollen, Rollen Diensten und Features. Wenn Sie z. B. eine Featureinstallation auf einem Remote Server starten, können Sie den Assistenten zum Hinzufügen von Rollen und Features schließen, während die Installation noch läuft, die aktive Aufgabe bleibt jedoch in der **Benachrichtigungen** Liste. Das **Benachrichtigungen** Element zeigt eine Statusanzeige für die Installation an, und Sie können den Assistenten zum Hinzufügen von Rollen und Features bei Bedarf erneut öffnen, indem Sie auf **Assistent zum Hinzufügen von Rollen und Features**klicken. Die Elemente in der Liste informieren Sie darüber,

ob eine Installation fehlgeschlagen ist oder zusätzliche Konfigurationsschritte erforderlich sind, um die Bereitstellung des Features abzuschließen.

Benachrichtigungen spielen auch einen wichtigen Teil bei der Behebung von Problemen mit Aufgaben oder Prozessen in Server-Manager. Weitere Informationen zur Problembehandlung bei fehlgeschlagenen Tasks oder Prozessen mithilfe von Meldungen im **Benachrichtigungs** Bereich und im Dialogfeld **Aufgaben Details** finden Sie im [Handbuch zur Problembehandlung für Server-Manager](#).

Um eine Benachrichtigung zu löschen, die Sie nicht mehr in der **Benachrichtigungs** Liste anzeigen möchten, zeigen Sie mit dem Mauszeiger auf die Benachrichtigung, und klicken Sie dann auf **Aufgabe entfernen (X)**.

Anzeigen und Problembehandlung von Aufgaben mithilfe von Aufgaben Details

Der **Task Details** -Befehl unten im **Benachrichtigungs** Menü öffnet das Dialogfeld **Aufgaben Details**, das vollständige Beschreibungen von Aufgaben Ereignissen (starten, beenden, Warnungen, Erfolg oder Fehlern) bereitstellt. Wie bei anderen Listen Steuerelementen in Server-Manager, z. b. **Ereignisse**, **Dienste und Best Practices Analyzer Kacheln**, können Sie Abfragen filtern und erstellen, die für die Aufgaben ausgeführt werden, die im Dialogfeld **Aufgaben Details** angezeigt werden. (Weitere Informationen zum Filtern und Erstellen von Abfragen für Listen Steuerelemente finden Sie unter [Filtern, Sortieren und Abfragen von Daten in Server-Manager Kacheln](#).) Im oberen Bereich können Sie Benachrichtigungen überprüfen, wie Sie im Menü **Benachrichtigungen** angezeigt werden, und sehen, wie viele Benachrichtigungen zu derselben Aufgabe generiert wurden. Wenn Sie im oberen Bereich eine Benachrichtigung auswählen, werden im unteren Bereich vollständige Details zu der Benachrichtigung angezeigt.

Der untere Bereich ist vor allem bei der Problembehandlung fehlgeschlagener Aufgaben hilfreich. Wenn Server-Manager keine Verbindung mit einem Server herstellen oder Daten für einen Server mit dem Server Pool erhalten kann, enthalten Einträge in diesem Bereich häufig detaillierte Meldungen, darunter den vollständigen Text der zugrunde liegenden Windows-Remote Verwaltung (WinRM), Netzwerk- oder Sicherheitsprobleme, die verhindern, dass Server-Manager mit einem Ziel Server kommunizieren.

Weitere Informationen

[Filtern, Sortieren und Abfragen von Daten in Server-Manager Kacheln](#) [Server-Manager Handbuch zur Problembehandlung](#)

Ausführen von Best Practices Analyzer-Scans und Verwalten der Scanergebnisse

09.04.2020 • 28 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Bei der Verwaltung von Windows stellen *bewährte Methoden* Richtlinien dar, nach denen ein Server im normalen Betrieb optimal und gemäß den Vorschlägen von Experten konfiguriert werden kann. Beispielsweise ist es bei den meisten Serveranwendungen eine bewährte Methode, nur die Ports geöffnet zu lassen, die für die Kommunikation mit anderen Netzwerkcomputern erforderlich sind, und nicht verwendete Ports zu blockieren. Zwar sind selbst gravierende Verstöße gegen bewährte Methoden nicht unbedingt problematisch, doch weisen Verstöße auf Serverkonfigurationen hin, bei denen eine schlechte Leistung, mangelnde Zuverlässigkeit, unerwartete Konflikte, erhöhte Sicherheitsrisiken und andere potenzielle Probleme auftreten können.

Best Practices Analyzer (BPA) ist ein Server Verwaltungs Tool, das in Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2 verfügbar ist. Mithilfe von BPA können Administratoren Verstöße gegen bewährte Methoden verringern, indem Sie die auf verwalteten Servern mit Windows Server 2012 oder Windows Server 2008 R2 installierten Rollen überprüfen und Verstöße gegen bewährte Methoden für den Administrator melden.

Sie können Best Practices Analyzer (BPA)-Scans entweder über Server-Manager, mithilfe der grafischen Benutzeroberfläche von BPA oder mithilfe von Cmdlets in Windows PowerShell ausführen. ab Windows Server 2012 können Sie eine oder mehrere Rollen gleichzeitig auf mehreren Servern Scannen, unabhängig davon, ob Sie die Best Practices Analyzer-Kachel in der Server-Manager-Konsole oder Windows PowerShell-Cmdlets zum Ausführen von Scans verwenden. Sie können in BPA auch festlegen, dass Scanergebnisse ausgeschlossen oder ignoriert werden, die Sie nicht anzeigen möchten.

Dieses Thema enthält folgende Abschnitte:

- [BPA suchen](#)
- [Funktionsweise von BPA](#)
- [Ausführen von Best Practices Analyzer Scans für Rollen](#)
- [Überprüfungs Ergebnisse verwalten](#)

BPA suchen

Die Best Practices Analyzer-Kachel finden Sie auf den Rollen-und Server Gruppen Seiten Server-Manager in Windows Server 2012 R2 und Windows Server 2012, oder Sie können eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten öffnen, um Best Practices Analyzer-Cmdlets auszuführen.

Funktionsweise von BPA

BPA misst die Konformität einer Rolle mit Best Practices-Regeln in acht verschiedenen Kategorien von Effektivität, Vertrauenswürdigkeit und Zuverlässigkeit. Die Bewertungsergebnisse werden in einem der drei Schweregrade zurückgegeben, die in der folgenden Tabelle beschrieben werden.

SCHWEREGRAD	BESCHREIBUNG
Error	Fehlerergebnisse werden zurückgegeben, wenn eine Rolle den Bedingungen einer Regel für bewährte Methoden nicht entspricht und Funktionalitätsprobleme erwartet werden können.
Information	Informationsergebnisse werden zurückgegeben, wenn eine Rolle den Bedingungen einer Regel für bewährte Methoden entspricht.
Warnung	Warnungsergebnisse werden zurückgegeben, wenn die Ergebnisse der Nichtkompatibilität zu Problemen führen können, falls keine Änderungen vorgenommen werden. Die Anwendung ist zwar möglicherweise im aktuellen Betrieb kompatibel, entspricht den Bedingungen einer Regel jedoch nur, wenn ihre Konfiguration oder Richtlinieneinstellungen geändert werden. Beispielsweise kann beim Scan von Remotedesktopdienste eine Warnung angezeigt werden, wenn ein Lizenzserver für die Rolle nicht verfügbar ist. Denn selbst wenn zum Zeitpunkt des Scans keine Remoteverbindungen aktiv sind, bedeutet das Fehlen des Lizenzservers, dass neue Remoteverbindungen keine gültige Clientzugriffslicenzen erhalten.

Regelkategorien

In der folgenden Tabelle werden die Kategorien der Best Practices-Regeln beschrieben, mit denen Rollen während eines Best Practices Analyzer Scans gemessen werden.

KATEGORIENNAME	BESCHREIBUNG
Sicherheit	Sicherheitsregeln werden angewendet, um das relative Risiko einer Rolle für Bedrohungen wie nicht autorisierte oder böswillige Benutzer oder den Verlust oder Diebstahl vertraulicher oder proprietärer Daten zu messen.
Leistung	Leistungs Regeln werden angewendet, um die Fähigkeit einer Rolle zum Verarbeiten von Anforderungen und zum Ausführen der vorgeschriebenen Aufgaben im Unternehmen innerhalb der erwarteten Zeitspanne in der Arbeitsauslastung der Rolle zu messen.
Konfiguration	Mit Konfigurationsregeln werden die Einstellungen einer Rolle identifiziert, die für eine optimale Leistung ggf. Änderungen erfordern. Konfigurationsregeln können Konflikte bei Einstellungen vermeiden, die Fehlermeldungen verursachen oder verhindern können, dass eine Rolle ihre zugewiesenen Aufgaben im Unternehmen erfüllt.
Policy (Richtlinie)	Richtlinien Regeln werden angewendet, um Gruppenrichtlinie oder Windows-Registrierungs Einstellungen zu identifizieren, die möglicherweise geändert werden müssen, damit eine Rolle optimal und sicher funktioniert.
Vorgang	Mit Vorgangsregeln werden mögliche Fehler einer Rolle beim Ausführen der vorgeschriebenen Aufgaben im Unternehmen identifiziert.

KATEGORIENNAME	BESCHREIBUNG
Vor der Bereitstellung	Regeln vor der Bereitstellung werden vor dem Bereitstellen einer installierten Rolle im Unternehmen angewendet. Damit können Administratoren auswerten, ob die bewährten Methoden erfüllt werden, bevor die Rolle in der Produktion verwendet wird.
Nach der Bereitstellung	Regeln nach der Bereitstellung werden angewendet, nachdem alle erforderlichen Dienste für eine Rolle gestartet wurden und die Rolle im Unternehmen ausgeführt wird.
Erforderliche Komponenten	Voraussetzungsregeln erläutern Konfigurationseinstellungen, Richtlinieneinstellungen und Features, die für eine Rolle erforderlich sind, bevor bestimmte Regeln aus anderen Kategorien von BPA angewendet werden können. Eine Voraussetzung in den Scanergebnissen gibt an, dass BPA aufgrund einer falschen Einstellung, eines fehlenden Programms, einer falsch aktivierten oder deaktivierten Richtlinie, einer Registrierungsschlüsseleinstellung oder sonstigen Konfiguration eine oder mehrere Regeln während des Scans nicht anwenden konnte. Die Kompatibilität oder Nichtkompatibilität mit Regeln wird somit nicht bewertet. Da eine Regel nicht angewendet werden konnte, ist sie nicht Bestandteil der Scanergebnisse.

Ausführen von Best Practices Analyzer Scans für Rollen

Sie können BPA-Scans für Rollen ausführen, indem Sie entweder die BPA-GUI in Server-Manager oder Windows PowerShell-Cmdlets verwenden.

In Windows Server 2012 R2 und Windows Server 2012 werden Sie von einigen Rollen aufgefordert, zusätzliche Parameter anzugeben, z. B. die Namen bestimmter Server oder Freigaben, auf denen Teile der Rolle ausgeführt werden, oder die IDs von Teilmodellen, bevor ein BPA-Scan gestartet wird. Verwenden Sie bei BPA-Scans für Modelle, bei denen Sie zusätzliche Parameter angeben müssen, die BPA-Cmdlets. Die grafische Benutzeroberfläche von BPA kann keine zusätzlichen Parameter wie Teilmodell-IDs annehmen. Beispielsweise stellt die Teilmodell-ID **FSRM** das Dateidienste-BPA-Teilmodell für den Ressourcen-Manager für Dateiserver dar, einen Rollendienst der Datei- und Speicherdiene. Führen Sie einen BPA-Scan mithilfe von Windows PowerShell-Cmdlets aus, und fügen Sie dem Cmdlet den Parameter `SubmodelId` hinzu, um eine Überprüfung nur auf dem Datei Server Ressourcen-Manager Rollen Dienst auszuführen.

Obwohl Sie keine zusätzlichen Parameter an einen Scan übergeben können, den Sie auf der grafischen Benutzeroberfläche von BPA starten, zeigt die BPA-Kachel in Server-Manager Ergebnisse für den letzten BPA-Scan an, unabhängig davon, wie der Scanvorgang gestartet wurde.

- [Überprüfen von Rollen mithilfe der grafischen Benutzeroberfläche von BPA](#)
- [Überprüfen von Rollen mithilfe von Windows PowerShell-Cmdlets](#)

Überprüfen von Rollen mithilfe der grafischen Benutzeroberfläche von BPA

Führen Sie die folgenden Schritte aus, um eine oder mehrere Rollen auf der grafischen Benutzeroberfläche von BPA zu überprüfen.

So überprüfen Sie Rollen mithilfe der grafischen Benutzeroberfläche von BPA

1. Führen Sie eine der folgenden Aktionen aus, um Server-Manager zu öffnen, wenn es nicht bereits geöffnet ist.
 - Klicken Sie in der Windows-Taskleiste auf die Schaltfläche Server-Manager.

- Klicken Sie auf dem **Start** Bildschirm auf die Kachel Server-Manager.
2. Öffnen Sie im Navigationsbereich eine Rollen- oder Gruppenseite.
Beim Ausführen von BPA-Scans über eine Rollen- oder Gruppenseite werden alle Rollen überprüft, die auf Servern in dieser Gruppe installiert sind.
 3. Klicken Sie im Menü **Aufgaben** der Kachel Best Practices Analyzer auf **BPA-Scan starten**.
 4. Je nach Anzahl der Regeln, die für die von Ihnen ausgewählte Rolle oder Gruppe ausgewertet werden, kann es einige Minuten dauern, bis der BPA-Scan abgeschlossen ist.

Überprüfen von Rollen mithilfe von Windows PowerShell-Cmdlets

Verwenden Sie die folgenden Verfahren, um eine oder mehrere Rollen mithilfe von Windows PowerShell-Cmdlets zu scannen.

NOTE

Die Verfahren in diesem Abschnitt stellen nicht alle BPA-Cmdlets und -Parameter vor. Weitere Informationen zu BPA-Vorgängen in Windows PowerShell erhalten Sie, wenn Sie in Ihrer Windows PowerShell -Sitzung **Get-Help bpacmdlet-Fulldatei** eingeben, wobei *bpacmdlet* einer der folgenden Werte sein kann. Sie finden auch Hilfe Themen zu BPA-Cmdlets im [Windows Server TechCenter](#).

- **Get-BPAModel**
- **Aufrufen-BPAModel**
- **Get-bparameesult**
- **Set-bparameesult**

So scannen Sie eine einzelne Rolle mithilfe von Windows PowerShell-Cmdlets

1. Führen Sie eine der folgenden Aktionen aus, um Windows PowerShell mit erhöhten Benutzerrechten auszuführen.
 - Wenn Sie Windows PowerShell als Administrator über den **Start** Bildschirm ausführen möchten, klicken Sie in den **apps** -Ergebnissen mit der rechten Maustaste auf die Kachel **Windows PowerShell**, und klicken Sie dann auf der APP-Leiste auf **als Administrator ausführen**.
 - Wenn Sie Windows PowerShell als Administrator über den Desktop ausführen möchten, klicken Sie in der Taskleiste mit der rechten Maustaste auf die Verknüpfung **Windows PowerShell**, und klicken Sie dann auf **als Administrator ausführen**.
2. ab Windows PowerShell 3,0 werden Cmdlet-Module automatisch in Ihre Windows PowerShell-Sitzung importiert, wenn ein Cmdlet aus dem Modul zum ersten Mal verwendet wird. Das BPA-Cmdlet-Modul muss nicht importiert oder geladen werden.
3. Suchen Sie die Modell-IDs aller Rollen, für die BPA-Scans ausgeführt werden können, indem Sie das Cmdlet **Get-BPAModel** eingeben, wie im folgenden Beispiel gezeigt.

Get-BPAModel

4. Suchen Sie in den Ergebnissen aus Schritt 3 die Modell-IDs der Rollen, für die Sie einen BPA-Scan ausführen möchten.
5. Geben Sie einen der folgenden Befehle ein, um den BPA-Scan für eine bestimmte Rolle zu starten. Trennen Sie die Modell-IDs bei mehreren Rollen durch Kommas.

Invoke-BPAModel -modelID <modelID_from_Step3>

```
Invoke-BPAModel <modelID_from_Step3>
```

Beispiel: `Invoke-BPAModel -modelId Microsoft/Windows/DNSServer,Microsoft/Windows/FileServices`

NOTE

Die Modell-ID enthält den gesamten Pfad, der in der Spalte **Id** angezeigt wird, z. B. **Microsoft/Windows/Hyper-V**.

Sie können auch einen Scan für eine bestimmte Rolle aus den Ergebnissen von Schritt 3 starten, indem Sie die Ergebnisse des `Get-BPAModel` -Cmdlets an das `Invoke-BPAModel` -Cmdlet weitergeben, wie im folgenden Beispiel gezeigt.

```
Get-BPAModel <model_ID> | Invoke-BPAModel
```

Wenn Sie dieses Cmdlet ausführen, ohne eine Modell-ID anzugeben, werden alle vom `Get-BPAModel` -Cmdlet zurückgegebenen Modelle an das `Invoke-BPAModel` -Cmdlet weitergeleitet, und es werden Scans für alle Modelle gestartet, die auf Servern verfügbar sind, die dem Server-Manager-Server Pool hinzugefügt wurden.

So scannen Sie alle Rollen mithilfe von Windows PowerShell-Cmdlets

1. Öffnen Sie eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten, sofern nicht bereits eine geöffnet ist. Anweisungen finden Sie im vorherigen Verfahren.
2. Leiten Sie alle Rollen, die für den BPA-Scan ausgeführt werden können, zum Starten von Scans an das `Invoke-BPAModel` -Cmdlet weiter.

```
Get-BPAModel | Invoke-BPAModel
```

3. Nach Abschluss der Überprüfung gibt Windows PowerShell Ergebnisse ähnlich der folgenden für jede überprüfte Rolle zurück.

```
modelId          : Microsoft/Windows/FileServices
SubmodelId       :
Success          : True
Scantime         : 1/01/2012 12:18:40 PM
ScantimeUtcOffset: -08:00:00
detail           : {server_name1, server_name2}
```

Überprüfungs Ergebnisse verwalten

Nachdem ein BPA-Scan auf der grafischen Benutzeroberfläche abgeschlossen wurde, können Sie Scanergebnisse in der BPA-Kachel anzeigen. Wenn Sie ein Ergebnis in der Kachel auswählen, werden in einem Vorschaubereich in der Kachel Ergebniseigenschaften angezeigt, und es wird angegeben, ob die Rolle mit der zugeordneten bewährten Methode kompatibel ist. Wenn ein Ergebnis nicht kompatibel ist und Sie wissen möchten, wie die in den Ergebnis Eigenschaften beschriebenen Probleme gelöst werden können, öffnen die Links unter Fehler- und Warnungs Ergebnis Eigenschaften detaillierte Lösungs Hilfe Themen im Windows Server TechCenter.

NOTE

BPA-Scanergebnisse werden nicht automatisch gespeichert oder archiviert. Beim Ausführen eines neuen Scans für ein Modell oder Teilmodell werden die Ergebnisse des letzten Scans überschrieben. Informationen zum Speichern der Ergebnisse von BPA-Scans, damit diese archiviert, gedruckt oder an andere gesendet werden können, finden Sie unter [So können Sie BPA-Ergebnisse aus Windows PowerShell-Sitzungen in verschiedenen Formaten anzeigen oder speichern](#) in diesem Abschnitt.

Ausschließen und Einschließen von BPA-Ergebnissen

Wenn keine BPA-Ergebnisse angezeigt werden müssen, z. B. Ergebnisse, die häufig in den BPA-Scans auftreten, aber keine Auflösung erfordern, können Sie die Ergebnisse ausschließen, indem Sie entweder die Benutzeroberfläche von BPA oder BPA-Cmdlets in Windows PowerShell verwenden. Sie können diese Ergebnisse jederzeit wieder einschließen.

NOTE

Wenn Sie Ergebnisse ausschließen, werden sie auch nicht auf verwalteten Servern angezeigt. Andere Administratoren können ausgeschlossene Ergebnisse auf verwalteten Servern nicht anzeigen. Wenn Sie Ergebnisse nur in einer lokalen Server-Manager Konsole ausschließen möchten, erstellen Sie eine benutzerdefinierte Abfrage, anstatt den Befehl **Ergebnis ausschließen** zu verwenden.

Scanergebnisse ausschließen

Die Einstellung **Ausschließen** ist persistent. Die von Ihnen ausgeschlossenen Ergebnisse bleiben bei künftigen Scans desselben Modells auf demselben Computer ausgeschlossen, sofern Sie sie nicht wieder einschließen.

Sie können Scanergebnisse mit dem `Set-BPAResult` -Cmdlet in Verbindung mit dem `-Exclude` -Parameter ausschließen. Wie in der Best Practices Analyzer Kachel in Server-Manager können Sie einzelne Ergebnis Objekte ausschließen. Sie können auch eine Reihe von Ergebnissen ausschließen, deren Felder (z. B. Kategorie, Titel oder Schweregrad) mit den angegebenen Werten übereinstimmen oder diese enthalten. Beispielsweise können Sie aus einer Reihe von Scanergebnissen für ein Modell alle **Leistungsergebnisse** ausschließen.

NOTE

Sie müssen mindestens einen BPA-Scan für ein Modell ausführen, bevor Sie die Verfahren in diesem Abschnitt verwenden können.

So schließen Sie Scanergebnisse mithilfe der grafischen Benutzeroberfläche aus

1. Öffnen Sie eine Rollen-oder Server Gruppenseite in Server-Manager.
2. Klicken Sie in der Kachel Best Practices Analyzer für die Rolle oder Server Gruppe mit der rechten Maustaste auf ein Ergebnis in der Liste, und klicken Sie dann auf **Ergebnis ausschließen**.

Das Ergebnis wird nicht mehr in der Liste der Ergebnisse angezeigt.

3. Führen Sie die integrierte Abfrage **Ausgeschlossene Ergebnisse** aus, um die ausgeschlossenen Ergebnisse auf der grafischen Benutzeroberfläche anzuzeigen. Klicken Sie auf **Gespeicherte Suchabfragen**, und klicken Sie dann auf **Ausgeschlossene Ergebnisse**.

Beachten Sie, dass nach dem Ausführen der Abfrage **Ausgeschlossene Ergebnisse** der Untertitel der Kachel (eine Beschreibung der in der Liste angezeigten Ergebnisse) sich in **Ausgeschlossene Ergebnisse** ändert. Es werden nur ausgeschlossene Ergebnisse in der Liste angezeigt.

So schließen Sie Scanergebnisse mithilfe von Windows PowerShell-Cmdlets aus

1. Öffne Sie eine Windows PowerShell-Sitzung mit erhöhten Benutzerberechtigungen.
2. Führen Sie den folgenden Befehl aus, um bestimmte Ergebnisse aus einem Modellscan auszuschließen.

```
Get-BPAResult -modelId <model ID> | Where { $_.<Field Name> -eq Value} | Set-BPAResult -Exclude $true
```

Mit dem vorangehenden Befehl werden Ergebnis Elemente des BPA-Scans für die Modell-ID abgerufen, die durch die *Modell-/ID*dargestellt wird.

Mit dem zweiten Abschnitt des Befehls werden die Ergebnisse des `Get-BPAResult` -Cmdlets gefiltert, sodass nur die Scanergebnisse abgerufen werden, bei denen der Wert für ein durch *Feldname* dargestelltes Ergebnisfeld mit dem Text in Anführungszeichen übereinstimmt.

Mit dem letzten Abschnitt des Befehls, der auf den zweiten senkrechten Strich folgt, werden die vom

vorherigen Cmdlet-Abschnitt gefilterten Ergebnisse ausgeschlossen.

Beispiel:

```
Get-BPAResult -Microsoft/Windows/FileServices | Where { $_.Severity -eq Information} | Set-BPAResult -Exclude $true
```

Einschließen von Scanergebnissen

Wenn Sie ausgeschlossene Scanergebnisse anzeigen möchten, können Sie diese Ergebnisse einschließen. Die Einstellung **Einschließen** ist persistent. Eingeschlossene Ergebnisse bleiben bei künftigen Scans desselben Modells auf demselben Computer eingeschlossen.

So schließen Sie Scanergebnisse mithilfe der grafischen Benutzeroberfläche ein

1. Öffnen Sie eine Rollen- oder Server Gruppenseite in Server-Manager.
2. Klicken Sie in der Kachel Best Practices Analyzer für die Rolle oder Server Gruppe mit der rechten Maustaste in der Abfrage Liste **ausgeschlossene Ergebnisse** auf ein ausgeschlossenes Ergebnis, und klicken Sie dann auf **Ergebnis einschließen**.

Das Ergebnis wird nicht mehr in der Liste der ausgeschlossenen Ergebnisse angezeigt. Löschen Sie die Abfrage, indem Sie auf **Alle löschen** klicken, um das eingeschlossene Ergebnis in die Liste aller eingeschlossenen Ergebnisse anzuzeigen.

So schließen Sie Scanergebnisse mithilfe von Windows PowerShell-Cmdlets ein

1. Öffne Sie eine Windows PowerShell-Sitzung mit erhöhten Benutzerberechtigungen.
2. Geben Sie zum Einschließen bestimmter Ergebnisse aus einem Modellscan den folgenden Befehl ein, und drücken Sie dann die **EINGABETASTE**.

```
Get-BPAResult -modelId <model Id> | Where { $_.<Field Name> -eq Value } | Set-BPAResult -Exclude $false
```

Der vorherige Befehl ruft BPA-Scanergebnis Elemente für das Modell ab, das durch die *Modell-ID*dargestellt wird.

Mit dem zweiten Teil des Befehls, nach dem ersten senkrechter Strich (|) werden die Ergebnisse des Cmdlets **Get-bparser** gefiltert, sodass nur die Scanergebnisse abgerufen werden, bei denen der Wert des durch *Feldnamen*dargestellten Ergebnis Felds mit dem Text in Anführungszeichen übereinstimmt.

Mit dem letzten Abschnitt des Befehls, der auf den zweiten senkrechten Strich folgt, werden die Filterergebnisse des zweiten Cmdlet-Abschnitts eingeschlossen. Dabei wird der **-Exclude**-Parameter auf **false** festgelegt.

Beispiel:

```
Get-BPAResult -Microsoft/Windows/FileServices | Where { $_.Severity -eq Information} | Set-BPAResult -Exclude $false
```

Anzeigen und Exportieren von BPA-Scanergebnissen in Windows PowerShell

Informationen zum Anzeigen und Verwalten der Scanergebnisse mithilfe von Windows PowerShell-Cmdlets finden Sie in den folgenden Prozeduren. Bevor Sie eines der folgenden Verfahren verwenden können, müssen Sie mindestens einen BPA-Scan auf mindestens einem Modell oder Teilmodell ausführen.

So zeigen Sie die Ergebnisse des letzten Scans einer Rolle mithilfe von Windows PowerShell an

1. Öffne Sie eine Windows PowerShell-Sitzung mit erhöhten Benutzerberechtigungen.
2. Rufen Sie die Ergebnisse des letzten Scans für eine angegebene Modell-ID ab. Geben Sie Folgendes ein, in dem das Modell durch die *Modell-ID*dargestellt wird, und drücken Sie dann die **EingabeTaste**. Sie können Ergebnisse für mehrere Modell-IDs abrufen, indem Sie die Modell-IDs durch Kommas trennen.

```
Get-BPAResult <model ID>
```

Beispiel: Get-BPAResult Microsoft/Windows/DNSServer,Microsoft/Windows/FileServices

Wenn Sie ein Teil Modell eines Modells (z. b. einen Rollen Dienst) gescannt haben, können Sie nur die Ergebnisse für dieses Teil Modell Abfragen, indem Sie die Teil Modell-ID in das Cmdlet einschließen.

Beispiel: `Get-BPAsyncResult Microsoft/Windows/FileServices -SubmodelID FSRM`

So können Sie BPA-Ergebnisse aus Windows PowerShell-Sitzungen in verschiedenen Formaten anzeigen oder speichern

- In Windows PowerShell ähnelt jedes BPA-Ergebnis dem folgenden.

```
ResultNumber      : 14
ResultId         : 1557706192
modelId          : Microsoft/Windows/FileServices
SubmodelId       : FSRM
RuleId           : 16
computerName     : server_name1, server_name2
Context          : FileServices
Source           : server_name1
Severity         : Information
Category         : Configuration
Title            : Access Denied remediation requires remote management be enabled on this server
Problem          :
Impact           :
Resolution       :
compliance       : The File Server Best Practices Analyzer scan has determined that you are in compliance with this best practice.
help             :
Excluded         : False
```

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie BPA-Ergebnisse in einer Tabelle formatieren möchten, führen Sie das folgende Cmdlet aus, und fügen Sie aus dem vorherigen Beispiel die Ergebniseigenschaften hinzu, die Sie anzeigen möchten.

```
Get-BPAsyncResult model ID | format-Table -Property <property1,property2,property3...>
```

Beispiel:

```
Get-BPAsyncResult Microsoft/Windows/FileServices | format-Table -Property modelId,SubmodelId,computerName,Source,Severity,Category,Title,Problem,Impact,Resolution,compliance,help
```

- Wenn Sie BPA-Ergebnisse in einer auf der grafischen Benutzeroberfläche basierenden Rasteransicht mit einem Textzeichenfolgenfilter und Spaltenüberschriften formatieren möchten, auf die zum Sortieren von Ergebnissen geklickt werden kann, führen Sie das folgende Cmdlet aus.

```
Get-BPAsyncResult <model ID> | OGV
```

- Um BPA-Ergebnisse in eine HTML-Datei zu exportieren, die archiviert oder an e-Mail-Empfänger gesendet werden kann, führen Sie das folgende Cmdlet aus, wobei *Pfad* den Pfad und den Dateinamen darstellt, in dem die HTML-Ergebnisse gespeichert werden sollen.

```
Get-BPAsyncResult <model ID> | convertTo-HTML | Set-Content <path>
```

Beispiel:

```
Get-BPAsyncResult Microsoft/Windows/FileServices | convertTo-HTML | Set-Content C:\BPAResults\FileServices.htm
```

- Um BPA-Ergebnisse in eine CSV-Textdatei (Comma-Separated Values) zu exportieren, führen Sie das folgende Cmdlet aus, wobei *Pfad* den Pfad und den Namen der Textdatei darstellt, in der die CSV-Ergebnisse gespeichert werden sollen. CSV-Ergebnisse können in Microsoft Excel oder andere Programme importiert werden, die Daten in Tabellen oder Rastern anzeigen.

```
Get-BPAsyncResult <model ID> | Export-CSV <path>
```

Beispiel: `Get-BPAResult Microsoft/Windows/FileServices | Export-Csv C:\BPAResults\FileServices.txt`

Weitere Informationen

[Best Practices Analyzer Auflösungs Inhalt im Windows Server TechCenter Filtern, Sortieren und Abfragen von Daten in Server-Manager Kacheln Verwalten mehrerer Remote Server mit Server-Manager](#)

Erstellen und Verwalten von Server Gruppen

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In diesem Thema wird beschrieben, wie benutzerdefinierte benutzerdefinierte Server Gruppen in Server-Manager in Windows Server erstellt werden.

Server Gruppen

Server, die Sie dem Server Pool hinzufügen, werden auf der Seite **alle Server** in Server-Manager angezeigt. Sie können benutzerdefinierte Gruppen von Servern erstellen, die Sie hinzugefügt haben. Mit Server Gruppen können Sie eine kleinere Teilmenge des Server Pools als logische Einheit anzeigen und verwalten. Sie können z. B. eine Gruppe namens **Buchhaltungsserver** für alle Server in der Buchhaltungsabteilung Ihrer Organisation oder eine Gruppe namens **Chicago** für alle Server erstellen, die sich geografisch in Chicago befinden. Nachdem Sie eine Server Gruppe erstellt haben, werden auf der Startseite der Gruppe in Server-Manager Informationen zu Ereignissen, Diensten, Leistungsindikatoren, Best Practices Analyzer Ergebnissen sowie zu installierten Rollen und Features für die Gruppe als Ganzes angezeigt.

Server können mehreren Gruppen angehören.

So erstellen Sie eine neue Servergruppe

1. Klicken Sie im Menü **Verwalten** auf **Server Gruppe erstellen**.
2. Geben Sie im Textfeld **Servergruppenname** einen Anzeigenamen für die Servergruppe ein, z. B. **Buchhaltungsserver**.
3. Fügen Sie der **ausgewählten** Liste Server aus dem Server Pool hinzu, oder fügen Sie der Gruppe mithilfe der Registerkarten **Active Directory**, **DNS** oder **importieren** weitere Server hinzu. Weitere Informationen zur Verwendung dieser Registerkarten finden [Sie unter Hinzufügen von Servern zu Server-Manager](#) in diesem Handbuch.
4. Klicken Sie nach dem Hinzufügen der Server auf **OK**. Die neue Gruppe wird im Navigationsbereich Server-Manager unter der Gruppe **alle Server** angezeigt.

So bearbeiten Sie eine vorhandene Servergruppe

1. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie im Navigationsbereich Server-Manager mit der rechten Maustaste auf eine Server Gruppe, und klicken Sie dann auf **Server Gruppe bearbeiten**.
 - Öffnen Sie auf der Startseite der Server Gruppe das Menü **Aufgaben** auf der Kachel **Server**, und klicken Sie dann auf **Server Gruppe bearbeiten**.
2. Ändern Sie den Gruppennamen, oder fügen Sie der Gruppe Server hinzu, oder entfernen Sie Sie.

NOTE

durch das Entfernen von Servern aus einer Server Gruppe werden keine Server aus Server-Manager entfernt. Server, die Sie aus einer Gruppe entfernen, bleiben in der Gruppe **Alle Server** im Serverpool erhalten.

3. Klicken Sie nach dem Ändern der Gruppe auf OK.

So löschen Sie eine vorhandene Servergruppe

1. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Navigationsbereich Server-Manager mit der rechten Maustaste auf eine Server Gruppe, und klicken Sie dann auf **Server Gruppe löschen**.
 - Öffnen Sie auf der Startseite der Server Gruppe das Menü **Aufgaben** auf der Kachel **Server**, und klicken Sie dann auf **Server Gruppe löschen**.
2. Klicken Sie auf **Ja**, wenn Sie aufgefordert werden, das Löschen der Servergruppe zu bestätigen.

NOTE

durch das Löschen einer Server Gruppe werden keine Server aus Server-Manager entfernt. Server, die in einer gelöschten Gruppe enthalten waren, bleiben in der Gruppe **Alle Server** im Serverpool erhalten.

3. Klicken Sie nach dem Ändern der Gruppe auf OK.

Weitere Informationen

[fügen Sie Server-Manager Server hinzu](#) [Server-Manager](#)

Filtern, Sortieren und Abfragen von Daten in Server-Manager-Kacheln

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In Windows Server können Sie mit Kacheln in Server-Manager Daten filtern und sortieren sowie benutzerdefinierte Abfragen erstellen und speichern. Sie können in den Kacheln "Ereignisse", "Leistung", "Best Practices Analyzer", "Dienste", "Rollen" und "Features" in Server-Manager Kacheln zum Sortieren, verwenden von Schlüsselwort Filtern und Ausführen von Abfragen für Listeneinträge ausführen.

Dieses Thema enthält folgende Abschnitte:

- [Filtern von Listeneinträgen in Kacheln](#)
- [Sortieren von Listeneinträgen in Kacheln](#)
- [Erstellen und Ausführen benutzerdefinierter Abfragen für Kachel Daten](#)

Filtern von Listeneinträgen in Kacheln

Mit dem Textfeld **Filtern** können Sie die Liste der Einträge, die in einer Kachel angezeigt werden, schnell auf Einträge reduzieren, die eine bestimmte Zeichenfolge enthalten.

So wenden Sie einen Filter auf die Listeneinträge in Kacheln an

1. Öffnen Sie eine Rollen- oder Server Gruppenseite in Server-Manager.
2. Geben Sie im Textfeld **Filter** auf der Kachel Ereignisse, Leistung, Best Practices Analyzer, Dienste oder Rollen und Features eine Zeichenfolge ein, nach der Sie filtern möchten.

Wenn Sie z. B. nur Ereignisse mit der Ereignis-ID 1014 anzeigen möchten, geben Sie im **Filter** Textfeld **1014** ein. Alle gesammelten Ereignisse, in denen die Zeichenfolge **1014** in mindestens einem Feld enthalten ist, werden als Ergebnisse zurückgegeben.

3. Hinweis: Der Filter ändert die Beschreibung unter dem Titel der Kachel. Anstelle von **Alle** steht nun **Gefilterte Ergebnisse**.
4. Um den Filter zu löschen, löschen Sie die Zeichenfolge im Filterfeld, oder klicken Sie auf **X**.

Sortieren von Listeneinträgen in Kacheln

Sortieren Sie die Listeneinträge in Server-Manager Kacheln durch Klicken auf Spaltenüberschriften. Durch einmaliges Klicken auf eine Spaltenüberschrift werden die Spaltenwerte in aufsteigender alphanumerischer Reihenfolge sortiert (Pfeil zeigt nach oben). Durch erneutes Klicken werden die Spaltenwerte in absteigender alphanumerischer Reihenfolge sortiert (Pfeil zeigt nach unten).

Erstellen und Ausführen benutzerdefinierter Abfragen für Kachel Daten

In den Kacheln Ereignisse, Leistung, Best Practices Analyzer, Dienste oder Rollen und Features in Server-Manager können Sie benutzerdefinierte Abfragen erstellen. Der Bereich der Kachel Symbolleiste, in dem Sie Kriterien zum

Erstellen einer benutzerdefinierten Abfrage auswählen, ist standardmäßig ausgeblendet. Klicken Sie auf **erweitern** (Chevron-Schaltfläche am rechten Rand der Kachel Symbolleiste), um die Abfrage Kriterien anzuzeigen.

So erstellen Sie eine benutzerdefinierte Abfrage für Kacheldaten

1. Öffnen Sie eine Rollen-oder Server Gruppenseite in Server-Manager.
2. Erweitern Sie auf der Kachel Ereignisse, Leistung, Best Practices Analyzer, Dienste oder Rollen und Features den Bereich Abfrage-Building, indem Sie auf **erweitern**klicken.
3. Klicken Sie auf **Kriterien hinzufügen**, um eine Liste mit Attributen (oder Feldern) zu öffnen, die auf die Einträge in der Kachel angewendet werden.
4. Wählen Sie Kriterien zum Hinzufügen aus. Wenn Sie fertig sind, klicken Sie auf **Hinzufügen**. Die ausgewählten Kriterien werden dem Bereich zum Erstellen von Abfragen hinzugefügt.
5. Klicken Sie auf den Hypertextoperator, um einen Operator auszuwählen. Der Standardoperator für numerische Kriterien bzw. datums- und uhrzeitbezogene Kriterien ist **Kleiner oder gleich**.
6. Geben Sie akzeptable Werte für die Kriterien ein. Wenn Sie z. b. **Datum und Uhrzeit**ausgewählt haben, geben Sie ein Datum im Format *m/d/yyyyan*.
7. Wiederholen Sie die Schritte ab Schritt 3, um der Abfrage weitere Kriterien hinzuzufügen.

Sie können Kriterien, die bereits in der Abfrage vorhanden sind, duplizieren. Die Duplikate werden der Abfrage jedoch mit dem Operator **oder** hinzugefügt.

Wenn Sie z. b. die Ereignis-IDs 1003 oder 1014 Abfragen möchten, fügen Sie zuerst die ID-Kriterien zu Ihrer Abfrage hinzu, legen Sie den Wert der ID auf **1003**fest, und fügen Sie dann der Abfrage ein zweites ID-Kriterium hinzu, wobei der Wert der zweiten ID **1014**entspricht. Sie erhalten die Abfrage **und ID gleich 1003 oder ID gleich 1014**.

8. Klicken Sie nach dem Hinzufügen der Kriterien und der Angabe der Operatoren und Werte auf **Speichern**, um die Abfrage zu speichern.
9. Geben Sie einen Anzeigennamen für die Abfrage an. Beispielsweise können Sie die im zuvor beschriebenen Schritt erstellte Abfrage **Lizenzierungsereignisse** nennen.
10. Klicken Sie nach dem Anzeigen der Ergebnisse auf **Alle löschen**, um alle Filter und Abfragen zu löschen und alle Listeneinträge anzuzeigen
11. Um eine gespeicherte Abfrage auszuführen, klicken Sie auf **Gespeicherte Suchabfragen**, und klicken Sie auf den Namen der gespeicherten Abfragen, die Sie ausführen möchten.
12. Um eine gespeicherte Abfrage zu löschen, klicken Sie auf **Gespeicherte Suchabfragen**, und klicken Sie auf **X** neben dem Namen der gespeicherten Abfragen, die Sie löschen möchten.

Weitere Informationen

[Server-Manager](#)

[Anzeigen und Konfigurieren von Leistungs-, Ereignis- und Dienstdaten](#)

Tastenkombinationen für den Server-Manager

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Da Server-Manager ab Windows Server 2012 vollständig neu gestaltet wurde, entsprechen die Tastenkombinationen, die in der Server-Manager-Konsole in Windows Server 2008 R2 oder Windows Server 2008 funktionieren, nicht notwendigerweise denselben Befehlen. In diesem Thema werden die neuen Tastenkombinationen und Zugriffstasten für Server-Manager in Windows Server 2012 und neueren Versionen von Windows Server beschrieben.

Auf Befehle, die keine eigenen Tastenkombination oder Zugriffstaste haben, können Sie zugreifen, indem Sie mithilfe der **TAB-TASTE** durch die entsprechende Steuerelementgruppe navigieren, wenn diese den Fokus hat.

Zugriffsschlüssel

aktive Steuerungs Bereich in Server-Manager

Willkommens Kachel

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Willkommens Kachel-Registerkarte "Schnellstart"	Alt + Q
Kachel für Willkommen - Registerkarte „Neues“	Alt + W
Willkommens Kachel-Weitere Informationen Registerkarte	Alt + L
Kachel für Willkommen - Befehl „Ausblenden“	Alt + D

Rollen-und Gruppen Miniaturansichten

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Kachel „Rollen und Servergruppen“	Alt + R

Konsolen Header-Steuerelemente

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Schaltfläche „Zurück“ in der Adressleiste	ALT+NACH-LINKS-TASTE oder RÜCKTASTE
Vorwärts Schaltfläche in der Adressleiste	Alt + nach-rechts-Taste
Aktualisieren	Aktualisieren

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Benachrichtigungsbereich, Dialogfeld "Aufgaben Details öffnen"	Alt + N
Menü "Verwalten"	Alt + M
Menü "Ansicht"	Alt + V
Menü "Hilfe"	ALT + H
Öffnen Server-Manager Hilfe	1
Vergrößern	Strg + Plus (+)
Verkleinern	STRG + minus (-)
Konsole zu 100 % anzeigen	STRG + 0

Kacheln auf Rollen-, Gruppen-oder lokalen Server Seiten

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Kachel "%quot;Eigenschaften%" auf lokaler Serverseite	Alt + P
Kachel "%quot;Ereignisse%" auf Rollen-, Gruppen- oder lokaler Serverseite	ALT + E
Kachel "%quot;Dienste%" auf Rollen-, Gruppen- oder lokaler Serverseite	Alt + R
Kachel "Rollen-, Gruppen-oder lokaler Server Page Best Practices Analyzer (BPA)"	ALT + B
Kachel "%quot;Leistung%" auf Rollen-, Gruppen- oder lokaler Serverseite	ALT + O
Kachel "%quot;Rollen und Features%" auf Rollen-, Gruppen- oder lokaler Serverseite	Alt + A
Kachel "%quot;Server%" auf der Seite "%quot;Alle Server%"	Alt + A

Navigieren in der Kachel "Eigenschaften" des lokalen Servers

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Computername	Alt + C
Zuletzt installierte Updates	Alt + L
Domäne oder Arbeitsgruppe	Alt + D

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Windows Update	Alt + W
Zuletzt auf Updates geprüft	Alt + S
Remoteverwaltung	Alt + R
Windows-Firewall	Alt + F
Remotedesktop	ALT + K
Windows-Fehlerberichterstattung	Alt + G
NIC-Teamvorgang	Alt + T
Programm zur Verbesserung der Benutzerfreundlichkeit	ALT + X
Verkabelte Ethernetverbindung	ALT + O
Verstärkte Sicherheitskonfiguration für IE	ALT + Y
Zeitzone	ALT + Z

Navigieren in den Kacheln Ereignisse, Dienste, BPA, Leistung und Rollen und Features

STEUERELEMENTGRUPPE	ZUGRIFFSSCHLÜSSELS
Menü %quot;Aufgaben%quot;	Alt + T
Filtersteuerelement	Alt + F
Abfrage Steuerelement	Alt + Q
Speicherabfragen	Alt + S

Remoteserver-Verwaltungstools

18.05.2020 • 21 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Dieses Thema unterstützt die Remoteserver-Verwaltungstools für Windows 10.

IMPORTANT

Ab dem Windows 10-Update vom Oktober 2018 ist RSAT als Sammlung von **Features bei Bedarf** in Windows 10 selbst enthalten. Weitere Anweisungen zur Installation finden Sie unter [Wann welche RSAT-Version verwendet werden sollte](#).

Mit RSAT können IT-Administratoren Windows Server-Rollen und -Funktionen von einem Windows 10-PC aus verwalten.

Die Remoteserver-Verwaltungstools beinhalten Server-Manager, Microsoft Management Console-Snap-Ins (MMC), Konsolen, Windows PowerShell-Cmdlets und -Anbieter sowie Befehlszeilertools für die Verwaltung von Rollen und Features, die auf Windows Server ausgeführt werden.

Zu den Remoteserver-Verwaltungstools zählen Windows PowerShell-Cmdlet-Module, die zum Verwalten von Rollen und Features verwendet werden können, die auf Remoteservern ausgeführt werden. Obwohl die Windows PowerShell-Remoteverwaltung unter Windows Server 2016 standardmäßig aktiviert ist, ist sie unter Windows 10 standardmäßig nicht aktiviert. Führen Sie zur Ausführung von Cmdlets, die Teil der Remoteserver-Verwaltungstools sind, für einen Remoteserver `Enable-PSremoting` in einer Windows PowerShell-Sitzung aus, die mit erhöhten Benutzerrechten (d. h. „Als Administrator ausführen“) nach der Installation der Remoteserver-Verwaltungstools auf Ihrem Windows-Clientcomputer geöffnet wurde.

Remoteserver-Verwaltungstools für Windows 10

Verwenden Sie die Remoteserver-Verwaltungstools für Windows 10, um bestimmte Technologien auf Computern zu verwalten, auf denen Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 und in eingeschränkten Fällen Windows Server 2012 oder Windows Server 2008 R2 ausgeführt wird.

Die Remoteserver-Verwaltungstools für Windows 10 umfassen Unterstützung für die Remoteverwaltung von Computern, auf denen die Server Core-Installationsoption oder die Konfiguration „Minimale Serverschnittstelle“ von Windows Server 2016, Windows Server 2012 R2 ausgeführt wird (in eingeschränkten Fällen auch die Server Core-Installationsoptionen von Windows Server 2012). Die Remoteserver-Verwaltungstools für Windows 10 können nicht unter allen Versionen des Windows Server-Betriebssystems installiert werden.

Tools, die in dieser Version verfügbar sind

Eine Liste der Tools, die in den Remoteserver-Verwaltungstools für Windows 10 verfügbar sind, finden Sie in der Tabelle unter [Remoteserver-Verwaltungstools \(Remote Server Administration Tools, RSAT\) für Windows-Betriebssysteme](#).

Systemanforderungen

Remoteserver-Verwaltungstools für Windows 10 können nur auf Computern mit Windows 10 installiert werden. Remoteserver-Verwaltungstools können nicht auf Computern mit Windows RT 8.1 oder auf anderen SOC-Geräten (System on a Chip) installiert werden.

Remoteserver-Verwaltungstools für Windows 10 können unter x86- und x64-basierten Editionen von

Windows 10 ausgeführt werden.

IMPORTANT

Es ist nicht ratsam, Remoteserver-Verwaltungstools für Windows 10 auf einem Computer zu installieren, auf dem Verwaltungsprogramme für Windows 8.1, Windows 8, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 oder Windows 2000 Server ausgeführt werden. Entfernen Sie alle älteren Versionen von Verwaltungsprogrammen oder Remoteserver-Verwaltungstools – einschließlich ältere Vorabversionen und Versionen der Tools für unterschiedliche Sprachen oder Gebietsschemas – vom Computer, bevor Sie die Remoteserver-Verwaltungstools für Windows 10 installieren.

Um diese Version von Server-Manager für den Zugriff auf und die Verwaltung von Remoteservern mit Windows Server 2012 R2, Windows Server 2012 oder Windows Server 2008 R2 zu verwenden, müssen Sie mehrere Updates installieren, um die älteren Windows Server-Betriebssysteme mit Hilfe von Server-Manager verwaltbar zu machen. Ausführliche Informationen dazu, wie Sie Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2 für die Verwaltung mit dem Server-Manager in den Remoteserver-Verwaltungstools für Windows 10 vorbereiten können, finden Sie unter [Verwalten von mehreren Remoteservern mit dem Server-Manager](#).

Die Windows PowerShell- und Server-Manager-Remoteverwaltung muss auf Remoteservern aktiviert werden, um diese mithilfe von Tools verwalten zu können, die Teil der Remoteserver-Verwaltungstools für Windows 10 sind. Remoteverwaltung ist auf Servern mit Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 standardmäßig aktiviert. Weitere Informationen zum Aktivieren der deaktivierten Remoteverwaltung finden Sie unter [Verwalten von mehreren Remoteservern mit dem Server-Manager](#).

Installieren, Deinstallieren und Aktivieren/Deaktivieren der RSAT-Tools

Verwenden von FoD (Features on Demand, Features bei Bedarf), um bestimmte RSAT-Tools unter dem Windows 10 October 2018 Update oder höher zu installieren

Ab dem Windows 10-Update vom Oktober 2018 ist RSAT als Sammlung von **Features bei Bedarf** in Windows 10 selbst enthalten. Anstatt ein RSAT-Paket herunterzuladen, können Sie jetzt einfach zu **Optionale Features verwalten** unter **Einstellungen** navigieren und auf **Feature hinzufügen** klicken, um die Liste der verfügbaren RSAT-Tools anzuzeigen. Wählen Sie die gewünschten RSAT-Tools aus, und installieren Sie sie. Um den Installationsfortschritt anzuzeigen, klicken Sie auf die Schaltfläche **Zurück**, um den Status auf der Seite **Optionale Features verwalten** anzuzeigen.

Weitere Informationen finden Sie in der [Liste der RSAT-Tools, die über **Features bei Bedarf** verfügbar ist] (<https://docs.microsoft.com/windows-hardware/manufacture/desktop/features-on-demand-non-language-fod#remote-server-administration-tools-rsat>). Zusätzlich zur Installation über die grafische App für **Einstellungen** können Sie auch bestimmte RSAT-Tools über die Befehlszeile oder über Automatisierung mithilfe von [DISM/Add-Capability](#) installieren.

Ein Vorteil von Features bei Bedarf besteht darin, dass die installierten Features über Windows 10-Versionsupgrades hinweg bestehen bleiben.

So deinstallieren Sie bestimmte RSAT-Tools unter dem Windows 10-Update vom Oktober 2018 oder höher (nach der Installation mit FoD)

Öffnen Sie unter Windows 10 die App **Einstellungen**, navigieren Sie zu **Optionale Features verwalten**, wählen Sie die gewünschten RSAT-Tools aus, die Sie entfernen möchten, und deinstallieren Sie sie dann. Beachten Sie, dass Abhängigkeiten in einigen Fällen manuell deinstalliert werden müssen. Insbesondere wenn das RSAT-Tool A vom RSAT-Tool B benötigt wird, tritt bei der Deinstallation von RSAT-Tool A ein Fehler auf, wenn RSAT-Tool B noch installiert ist. Deinstallieren Sie in diesem Fall zuerst das RSAT-Tool B, und deinstallieren Sie dann das RSAT-Tool A. Beachten Sie auch, dass das Deinstallieren eines RSAT-Tools in einigen Fällen möglicherweise zu gelingen scheint, auch wenn das Tool noch installiert ist. In diesem Fall wird das Tool durch das Neustarten des

PCs entfernt.

Weitere Informationen finden Sie in der [Liste der RSAT-Tools und seiner Abhängigkeiten](#). Zusätzlich zur Deinstallation über die grafische App für Einstellungen können Sie auch bestimmte RSAT-Tools über die Befehlszeile oder über Automatisierung mithilfe von [DISM/Remove-Capability](#) deinstallieren.

Wann sollte welche RSAT-Version verwendet werden?

Wenn Sie eine Version von Windows 10 vor dem Update vom Oktober 2018 (1809) verwenden, können Sie **Features bei Bedarf** nicht verwenden. Sie müssen das RSAT-Paket herunterladen und installieren.

- **Installieren Sie RSAT-FoDs direkt aus Windows 10, wie oben beschrieben:** Bei der Installation unter Windows 10, Update vom Oktober 2018 (1809) oder höher für die Verwaltung von Windows Server 2019 oder früheren Versionen.
- **Laden Sie das WS_1803 RSAT-Paket herunter, und installieren Sie es wie unten beschrieben:** Bei der Installation unter Windows 10, Update vom April 2018 (1803) oder früher für die Verwaltung von Windows Server, Version 1803 oder Windows Server, Version 1709.
- **Laden Sie das WS_2016 RSAT-Paket herunter, und installieren Sie es wie unten beschrieben:** Bei der Installation unter Windows 10, Update vom April 2018 (1803) oder früher für die Verwaltung von Windows Server 2016 oder früheren Versionen.

Herunterladen des RSAT-Pakets, um die Remoteserver-Verwaltungstools für Windows 10 zu installieren

1. Laden Sie die Remoteserver-Verwaltungstools für das Windows 10-Paket aus dem [Microsoft Download Center](#) herunter. Sie können das Installationsprogramm entweder über die Download Center-Website ausführen oder das Downloadpaket auf einem lokalen Computer oder einer lokalen Freigabe speichern.

IMPORTANT

Sie können Remoteserver-Verwaltungstools für Windows 10 nur auf Computern installieren, die Windows 10 ausführen. Remoteserver-Verwaltungstools können nicht auf Computern mit Windows RT 8.1 oder auf anderen SOC-Geräten (System on a Chip) installiert werden.

2. Wenn Sie das Downloadpaket auf einem lokalen Computer oder einer Freigabe speichern, doppelklicken Sie auf das Installationsprogramm **WindowsTH-KB2693643-x64.msu** oder **WindowsTH-KB2693643-x86.msu**. Dies richtet sich nach der Architektur des Computers, auf dem Sie die Tools installieren möchten.
3. Wenn Sie im Dialogfeld **Eigenständiges Windows Update-Installationsprogramm** zum Installieren des Updates aufgefordert werden, klicken Sie auf **Ja**.
4. Lesen Sie die Lizenzbedingungen, und akzeptieren Sie sie. Klicken Sie auf **Ich stimme zu**.
5. Es dauert einige Minuten, bis die Installation beendet ist.

So deinstallierst du die Remoteserver-Verwaltungstools für Windows 10 (nach der Installation des RSAT-Pakets)

1. Klicken Sie auf dem Desktop auf **Start, Alle Apps, Windows System** und **Systemsteuerung**.
2. Klicken Sie unter **Programme** auf **Programm deinstallieren**.
3. Klicken Sie auf **Installierte Updates anzeigen**.
4. Klicken Sie mit der rechten Maustaste auf **Update für Microsoft Windows (KB2693643)**, und klicken Sie dann auf **Deinstallieren**.
5. Wenn Sie gefragt werden, ob Sie das Update wirklich deinstallieren möchten, klicken Sie auf **Ja**.
So deaktivieren Sie bestimmte Tools (nach der Installation des RSAT-Pakets)
6. Klicken Sie auf dem Desktop auf **Start, Alle Apps, Windows System** und **Systemsteuerung**.

7. Klicken Sie auf **Programme** und dann unter **Programme und Features** auf **Windows-Features ein- oder ausschalten**.
8. Erweitern Sie im Dialogfeld **Windows-Features** die Option **Remoteserver-Verwaltungstools** und dann entweder den Unterpunkt **Rollenverwaltungstools** oder **Featureverwaltungstools**.
9. Deaktivieren Sie die Kontrollkästchen für alle Tools, die Sie deaktivieren möchten.

NOTE

Wenn Sie Server-Manager deaktivieren, muss der Computer neu gestartet werden, und Tools, auf die über das Menü **Extras** von Server-Manager zugegriffen werden konnte, müssen über den Ordner **Verwaltungstools** geöffnet werden.

10. Klicken Sie auf **OK**, wenn Sie alle Tools deaktiviert haben, die Sie nicht verwenden möchten.

Ausführen der Remoteserver-Verwaltungstools

NOTE

Nach der Installation der Remoteserver-Verwaltungstools für Windows 10 wird der Ordner **Verwaltungstools** im **Startmenü** angezeigt. Sie können von folgenden Orten auf die Tools zugreifen.

- Das Menü **Extras** in der Server-Manager-Konsole.
- **Systemsteuerung\System und Sicherheit\Verwaltungstools**
- Eine Verknüpfung aus dem Ordner **Verwaltungstools**, die auf dem Desktop gespeichert wird (klicken Sie dazu mit der rechten Maustaste auf den Link **Systemsteuerung\System und Sicherheit\Verwaltungstools** und dann auf **Verknüpfung erstellen**).

Die als Teil der Remoteserver-Verwaltungstools für Windows 10 installierten Tools können nicht zum Verwalten des lokalen Clientcomputers verwendet werden. Unabhängig vom ausgeführten Tool müssen Sie einen Remoteserver oder mehrere Remoteserver angeben, für die das Tool ausgeführt werden soll. Da die meisten Tools in Server-Manager integriert sind, fügen Sie Remoteserver, die Sie verwalten möchten, dem Server Manager-Serverpool hinzu. Danach können Sie den Server mit den Tools im Menü **Extras** verwalten. Weitere Informationen zum Hinzufügen von Servern zum Serverpool und zum Erstellen benutzerdefinierter Gruppen von Servern finden Sie unter [Hinzufügen von Servern zu Server-Manager](#) und [Erstellen und Verwalten von Servergruppen](#).

In den Remoteserver-Verwaltungstools für Windows 10 wird auf alle GUI-basierten Serververwaltungstools (z. B. MMC-Snap-Ins und Dialogfelder) über das Menü **Extras** der Server-Manager-Konsole zugegriffen. Obwohl auf dem Computer mit den Remoteserver-Verwaltungstools für Windows 10 ein clientbasiertes Betriebssystem ausgeführt wird, wird Server-Manager (in Remoteserver-Verwaltungstools für Windows 10 integriert) auf dem Clientcomputer standardmäßig automatisch geöffnet. Beachten Sie, dass in der Server-Manager-Konsole, die auf einem Clientcomputer ausgeführt wird, keine Seite **Lokaler Server** vorhanden ist.

So starten Sie den Server-Manager auf einem Clientcomputer

1. Klicken Sie im Menü **Start** auf **Alle Apps** und **Verwaltungstools**.
2. Klicken Sie im Ordner **Verwaltungstools** auf **Server-Manager**.

Obwohl sie im Menü **Extras** der Server-Manager-Konsole nicht aufgeführt sind, werden Windows PowerShell-Cmdlets und Eingabeaufforderung-Verwaltungstools für Rollen und Features ebenfalls als Teil der Remoteserver-Verwaltungstools installiert. Wenn Sie z. B. eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten („Als Administrator ausführen“) öffnen und das Cmdlet `Get-Command -Module RDManagement` ausführen, ist in den Ergebnissen eine Liste von Remotedesktopdienste-Cmdlets enthalten, die nach der Installation der Remoteserver-Verwaltungstools für die Ausführung auf dem lokalen Computer verfügbar sind. Dazu müssen die Cmdlets jedoch

einen Remoteserver als Ziel verwenden, auf dem die Rolle „Remotedesktopdienste“ ganz oder teilweise ausgeführt wird.

So starten Sie Windows PowerShell mit erhöhten Benutzerrechten („Als Administrator ausführen“)

1. Klicken Sie im Menü Start auf Alle Apps, Windows System und Windows PowerShell.
2. Wenn Sie Windows PowerShell als Administrator über den Desktop ausführen möchten, klicken Sie mit der rechten Maustaste auf die Windows PowerShell-Verknüpfung und dann auf Als Administrator ausführen.

NOTE

Sie können eine Windows PowerShell-Sitzung starten, die einen bestimmten Server als Ziel verwendet, indem Sie mit der rechten Maustaste auf einer Rollen- oder Gruppenseite von Server-Manager auf einen verwalteten Server klicken und dann auf Windows PowerShell klicken.

Bekannte Probleme

Problem: RSAT-FoD-Installation schlägt mit Fehlercode 0x800f0954 fehl

Auswirkungen: RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018) in WSUS-/Configuration Manager-Umgebungen

Lösung: Zum Installieren von FoDs auf einem in die Domäne eingebundenen PC, der Updates über WSUS oder Configuration Manager erhält, müssen Sie eine Gruppenrichtlinieneinstellungen ändern, um das Herunterladen von FoDs direkt von Windows Update oder aus einer lokalen Freigabe zu aktivieren. Weitere Informationen und Anweisungen zum Ändern dieser Einstellung finden Sie unter [Vorgehensweise: Verfügbarmachen von Features on Demand und Language Packs bei Verwendung von WSUS/SCCM](#).

Problem: RSAT-FoD-Installation über die App „Einstellungen“ zeigt Status/Fortschritt nicht an

Auswirkungen: RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018)

Lösung: Um den Installationsfortschritt anzuzeigen, klicken Sie auf die Schaltfläche Zurück, um den Status auf der Seite Optionale Features verwalten anzuzeigen.

Problem: RSAT-FoD-Deinstallation über die App „Einstellungen“ schlägt möglicherweise fehl

Auswirkungen: RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018)

Lösung: In einigen Fällen sind Deinstallationsfehler darauf zurückzuführen, dass Abhängigkeiten manuell deinstalliert werden müssen. Insbesondere wenn das RSAT-Tool A vom RSAT-Tool B benötigt wird, tritt bei der Deinstallation von RSAT-Tool A ein Fehler auf, wenn RSAT-Tool B noch installiert ist. Deinstallieren Sie in diesem Fall zuerst das RSAT-Tool B, und deinstallieren Sie dann das RSAT-Tool A. Weitere Informationen finden Sie in der Liste der RSAT-FoDs einschließlich ihrer Abhängigkeiten.

Problem: Die RSAT-FoD-Installation ist anscheinend erfolgreich, aber das Tool ist weiterhin installiert

Auswirkungen: RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018)

Lösung: Das Tool wird durch Neustarten des PCs entfernt.

Problem: RSAT fehlt nach dem Windows 10-Upgrade

Auswirkungen: Beliebige RSAT .MSU-Paketinstallation (vor RSAT-FoDs) wird nicht automatisch neu installiert.

Lösung: Eine RSAT-Installation kann über Betriebssystemupgrades hinweg nicht beibehalten werden, weil RSAT .MSU als Windows Update-Paket übermittelt wird. Installieren Sie RSAT nach dem Upgrade von Windows 10 erneut. Beachten Sie, dass diese Einschränkung einer der Gründe für die Umstellung auf FoDs ab Windows 10, Version 1809 ist. Die installierten RSAT-FoDs bleiben in zukünftigen Windows 10-Versionsupgrades erhalten.

Weitere Informationen

- [Remoteserver-Verwaltungstools für Windows 10](#)
- [Remoteserver-Verwaltungstools \(Remote Server Administration Tools, RSAT\) für Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2](#)

OpenSSH in Windows

24.04.2020 • 2 minutes to read • [Edit Online](#)

OpenSSH ist die Open-Source-Version der SSH-Tools (Secure Shell), die von Administratoren von Linux- und anderen Windows-fremden Produkten für die plattformübergreifende Verwaltung von Remotesystemen verwendet wird. OpenSSH wurde Windows im Herbst 2018 hinzugefügt und ist in Windows 10 und Windows Server 2019 enthalten.

SSH basiert auf einer Client/Server-Architektur, bei der das System, auf dem der Benutzer arbeitet, der Client und das verwaltete Remotesystem der Server ist. OpenSSH umfasst verschiedene Komponenten und Tools, die einen sicheren und einfachen Ansatz für die Remotesystemverwaltung ermöglichen, z. B.:

- „sshd.exe“: Dies ist die SSH-Serverkomponente, die auf dem remote verwalteten System ausgeführt werden muss.
- „ssh.exe“: Dies ist die SSH-Clientkomponente, die auf dem lokalen System des Benutzers ausgeführt wird.
- „ssh-keygen.exe“: Dient zum Generieren, Verwalten und Konvertieren von Authentifizierungsschlüsseln für SSH.
- „ssh-agent.exe“: Dient zum Speichern von privaten Schlüsseln für die Authentifizierung mit öffentlichem Schlüssel.
- „ssh-add.exe“: Fügt der Liste mit den zulässigen Elementen des Servers private Schlüssel hinzu.
- „ssh-keyscan.exe“: Dient als Hilfe beim Erfassen der öffentlichen SSH-Hostschlüssel für eine Reihe von Hosts.
- „sftp.exe“: Der Dienst, der das Secure File Transfer Protocol bereitstellt und per SSH ausgeführt wird.
- „scp.exe“: Ein Hilfsprogramm zum Kopieren von Dateien, das unter SSH ausgeführt wird.

In der Dokumentation in diesem Abschnitt geht es darum, wie OpenSSH unter Windows verwendet wird (einschließlich der Installation), und um Windows-spezifische Konfigurationen und Anwendungsfälle. Hier sind die Themen angegeben:

- Installieren und Deinstallieren von OpenSSH für Windows Server 2019 und Windows 10

Eine zusätzliche ausführliche Dokumentation zu häufig verwendeten OpenSSH-Features ist unter [OpenSSH.com](#) online verfügbar.

Das [Open-Source-Hauptprojekt von OpenSSH](#) wird von Entwicklern unter dem „OpenBSD Project“ verwaltet. Die Microsoft-Verzweigung dieses Projekts findest du auf [GitHub](#). Feedback zu Windows OpenSSH ist willkommen und kann bereitgestellt werden, indem in unserem [OpenSSH-GitHub-Repository](#) Anfragen zu GitHub-Problemen erstellt werden.

Installation von OpenSSH für Windows Server 2019 und Windows 10

24.04.2020 • 5 minutes to read • [Edit Online](#)

Der OpenSSH-Client und der OpenSSH-Server sind unter Windows Server 2019 und Windows 10 1809 separat installierbare Komponenten. Benutzer mit diesen Windows-Versionen sollten die folgenden Anweisungen zum Installieren und Konfigurieren von OpenSSH befolgen.

NOTE

Benutzer, die OpenSSH aus dem PowerShell-GitHub-Repository (<https://github.com/PowerShell/OpenSSH-Portable>) bezogen haben, sollten die Anweisungen dort und nicht diese Anweisungen befolgen.

Installieren von OpenSSH unter Windows Server 2019 oder Windows 10 1809

OpenSSH-Client und -Server sind Installierbare Features von Windows 10 1809.

Zum Installieren von OpenSSH wechseln Sie zu „Einstellungen“ und dann zu „Apps“ > „Apps und Features“ > Optionale Features“.

Durchsuchen Sie diese Liste, um festzustellen, ob „OpenSSH-Client“ bereits installiert ist. Falls nicht, wählen Sie oben auf der Seite „Feature hinzufügen“ aus.

- Um den OpenSSH-Client zu installieren, navigieren Sie zu „OpenSSH-Client“, und klicken Sie dann auf „Installieren“.
- Um den OpenSSH-Server zu installieren, navigieren Sie zu „OpenSSH-Server“, und klicken Sie dann auf „Installieren“.

Kehren Sie nach der Installation zu „Apps“ > „Apps und Features“ > „Optionale Features“ zurück. Die OpenSSH-Komponenten sollten aufgeführt sein.

NOTE

Durch die Installation von OpenSSH-Server wird eine Firewallregel mit dem Namen „OpenSSH-Server-in-TCP“ erstellt und aktiviert. Diese lässt eingehenden SSH-Datenverkehr an Port 22 zu.

Installieren von OpenSSH mit PowerShell

Um OpenSSH mithilfe von PowerShell zu installieren, starten Sie zunächst PowerShell als Administrator. So stellen Sie sicher, dass die OpenSSH-Features für die Installation zur Verfügung stehen

```

Get-WindowsCapability -Online | ? Name -like 'OpenSSH*'

# This should return the following output:

Name : OpenSSH.Client~~~~0.0.1.0
State : NotPresent
Name : OpenSSH.Server~~~~0.0.1.0
State : NotPresent

```

Installieren Sie dann die Server- und/oder Clientfeatures:

```

# Install the OpenSSH Client
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

# Install the OpenSSH Server
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

# Both of these should return the following output:

Path          :
Online        : True
RestartNeeded : False

```

Deinstallieren von OpenSSH

Zum Deinstallieren von OpenSSH in den Windows-Einstellungen wechseln Sie zu „Einstellungen“ und dann zu „Apps“ > „Apps und Features“ > Optionale Features“. Wählen Sie in der Liste der installierten Features die Komponente „OpenSSH-Client“ oder „OpenSSH-Server“ und dann „Deinstallieren“ aus.

Führen Sie zum Deinstallieren von OpenSSH mithilfe von PowerShell einen der folgenden Befehle aus:

```

# Uninstall the OpenSSH Client
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

# Uninstall the OpenSSH Server
Remove-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

```

Nach dem Entfernen von OpenSSH ist möglicherweise ein Neustart von Windows erforderlich, wenn der Dienst zum Zeitpunkt der Deinstallation verwendet wird.

Erstkonfiguration des SSH-Servers

Um den OpenSSH-Server für die erstmalige Verwendung unter Windows zu konfigurieren, starten Sie PowerShell als Administrator. Führen Sie dann die folgenden Befehle aus, um den SSHD-Dienst zu starten:

```

Start-Service sshd
# OPTIONAL but recommended:
Set-Service -Name sshd -StartupType 'Automatic'
# Confirm the Firewall rule is configured. It should be created automatically by setup.
Get-NetFirewallRule -Name *ssh*
# There should be a firewall rule named "OpenSSH-Server-In-TCP", which should be enabled
# If the firewall does not exist, create one
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

```

Erstmalige Verwendung von SSH

Nachdem Sie den OpenSSH-Server unter Windows installiert haben, können Sie ihn schnell mithilfe von PowerShell auf jedem Windows-Gerät testen, auf dem der SSH-Client installiert ist. Geben Sie in PowerShell folgenden Befehl ein:

```
Ssh username@servername
```

Die erste Verbindung mit einem beliebigen Server führt zu einer Meldung ähnlich der folgenden:

```
The authenticity of host 'servername (10.00.00.001)' can't be established.  
ECDSA key fingerprint is SHA256:(<a large string>).  
Are you sure you want to continue connecting (yes/no)?
```

Die Antwort muss entweder „yes“ oder „no“ sein. Wenn Sie mit „Yes“ antworten, wird dieser Server der Liste bekannter SSH-Hosts des lokalen Systems hinzugefügt.

An dieser Stelle werden Sie zur Eingabe des Kennworts aufgefordert. Als Sicherheitsmaßnahme wird Ihr Kennwort nicht angezeigt, während Sie es eingeben.

Nachdem Sie eine Verbindung hergestellt haben, wird eine Befehlsshell-Eingabeaufforderung ähnlich der folgenden angezeigt:

```
domain\username@SERVERNAME C:\Users\username>
```

Die Standardshell, die vom OpenSSH-Server unter Windows verwendet wird, ist die Windows-Befehlsshell.

Konfiguration des OpenSSH-Servers für Windows 10 1809 und Windows Server 2019

24.04.2020 • 6 minutes to read • [Edit Online](#)

In diesem Thema wird die Windows-spezifische Konfiguration für OpenSSH Server (sshd) behandelt.

OpenSSH bietet online unter [OpenSSH.com](#) eine ausführliche Dokumentation der Konfigurationsoptionen, die in dieser Dokumentation nicht dupliziert wird.

Konfigurieren der Standardshell für OpenSSH unter Windows

Die Standardbefehlsshell stellt die Benutzeroberfläche bereit, die einem Benutzer beim Herstellen einer Verbindung mit dem Server über SSH angezeigt wird. Das erste Standardfenster ist die Windows-Befehlsshell (cmd. exe). Windows bietet auch PowerShell und Bash sowie Befehlsshells von Drittanbietern, die auch für Windows verfügbar sind und als Standardshell für einen Server konfiguriert werden können.

Um die Standardbefehlsshell festzulegen, vergewissern Sie sich zunächst, dass sich der OpenSSH-Installationsordner im Systempfad befindet. Der Standardinstallationsordner unter Windows ist `SystemDrive:WindowsDirectory\System32\openssh`. Die folgenden Befehle zeigen die aktuelle Pfadeinstellung und fügen den Standardordner der OpenSSH-Installation hinzu.

BEFEHLSSHELL	ZU VERWENDENDER BEFEHL
Befehl	Pfad
PowerShell	\$env:path

Die Konfiguration der standardmäßigen SSH-Shell erfolgt in der Windows-Registrierung, indem der vollständige Pfad zur ausführbaren Shell-Datei dem Zeichenfolgenwert `DefaultShell` in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\OpenSSH` hinzugefügt wird.

Als Beispiel legt der folgende PowerShell-Befehl die Standardshell auf `PowerShell.exe` fest:

```
New-ItemProperty -Path "HKLM:\SOFTWARE\OpenSSH" -Name DefaultShell -Value "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -PropertyType String -Force
```

Windows-Konfigurationen in sshd_config

Unter Windows liest sshd Konfigurationsdaten standardmäßig aus `%programdata%\ssh\sshd_config`, oder es kann eine andere Konfigurationsdatei angegeben werden, indem `sshd.exe` mit dem Parameter `-f` gestartet wird. Wenn die Datei fehlt, erzeugt sshd beim Start des Diensts eine mit der Standardkonfiguration.

Die unten aufgeführten Elemente bieten eine Windows-spezifische Konfiguration, die durch Einträge in `sshd_config` möglich ist. Es gibt weitere mögliche Konfigurationseinstellungen, die hier nicht aufgeführt sind, da sie in der [Onlinedokumentation zu Win32 OpenSSH](#) ausführlich behandelt werden.

AllowGroups, AllowUsers, DenyGroups, DenyUsers

Das Steuern, welche Benutzer und Gruppen eine Verbindung mit dem Server herstellen können, erfolgt mithilfe der Anweisungen `AllowGroups`, `AllowUsers`, `DenyGroups` und `DenyUsers`. Die Anweisungen zum Zulassen und Verweigern werden in der folgenden Reihenfolge verarbeitet: `DenyUsers`, `AllowUsers`, `DenyGroups`, und schließlich

`AllowGroups`. Alle Kontonamen müssen in Kleinbuchstaben angegeben werden. Weitere Informationen zu Mustern für Platzhalter finden Sie in `ssh_config` unter `PATTERNS`.

Wenn Sie benutzer-/gruppenbasierte Regeln mit einem Domänenbenutzer oder einer Domänengruppe konfigurieren, verwenden Sie das folgende Format: `user?domain*`. Windows lässt mehrere Formate für die Angabe von Domänenprinzipialen zu, aber viele stehen im Konflikt mit Linux-Standardmustern. Aus diesem Grund wird `*` zum Abdecken von FQDNs hinzugefügt. Außerdem verwendet dieser Ansatz `?` anstelle von `@`, um Konflikte mit dem Format `username@host` zu vermeiden.

Arbeitsgruppenbenutzer, Gruppen und mit dem Internet verbundene Konten werden stets in Ihren lokalen Kontonamen aufgelöst (ohne Domäne teil vergleichbar mit UNIX-Standardnamen). Domänenbenutzer und -gruppen werden streng in das Format `NameSamCompatible` aufgelöst: Kurzname_der_Domäne\Benutzername. Alle Benutzer-/gruppenbasierten Konfigurationsregeln müssen sich an dieses Format halten.

Beispiele für Domänenbenutzer und -gruppen

```
DenyUsers contoso\admin@192.168.2.23 : blocks contoso\admin from 192.168.2.23
DenyUsers contoso\* : blocks all users from contoso domain
AllowGroups contoso\sshusers : only allow users from contoso\sshusers group
```

Beispiele für lokale Benutzer und Gruppen

```
AllowUsers localuser@192.168.2.23
AllowGroups sshusers
```

AuthenticationMethods

Für Windows OpenSSH sind die einzigen verfügbaren Authentifizierungsmethoden „password“ und „publickey“.

AuthorizedKeysFile

Der Standardwert ist „`ssh/authorized_keys .ssh/authorized_keys2`“. Wenn der Pfad nicht absolut ist, wird er relativ zum Basisverzeichnis des Benutzers (oder Pfad des Profilbilds) erstellt. Beispiel: `c:\users\user`. Beachte, dass stattdessen „`%programdata%\ssh/administrators_authorized_keys`“ verwendet wird, wenn der Benutzer der Administratorgruppe angehört.

ChrootDirectory (Unterstützung in v7.7.0.0 hinzugefügt)

Dieses Verzeichnis wird nur für sftp-Sitzungen unterstützt. Eine Remotesitzung in cmd.exe würde es nicht beachten. Um einen chroot-Server für ausschließlich sftp einzurichten, legen Sie ForceCommand auf internal-sftp fest. Sie können scp auch mit chroot einrichten, indem Sie eine benutzerdefinierte Shell implementieren, die nur scp und sftp zulässt.

HostKey

Die Standardwerte sind `%programdata%\ssh\ssh_host_ecdsa_key`, `%programdata%\ssh\ssh_host_ed25519_key`, `%programdata%\ssh\ssh_host_dsa_key` und `%programdata%\ssh\ssh_host_rsa_key`. Wenn die Standardwerte nicht vorhanden sind, generiert sshd diese automatisch beim Start eines Diensts.

Übereinstimmung

Beachten Sie die Musterregeln in diesem Abschnitt. Benutzer- und Gruppennamen erfordern Kleinschreibung.

PermitRootLogin

Gilt nicht unter Windows. Um die Administratoranmeldung zu verhindern, verwenden Sie „Administrators“ mit der DenyGroups-Anweisung.

SyslogFacility

Wenn Sie eine dateibasierte Protokollierung benötigen, verwenden Sie LOCAL0. Protokolle werden unter

%programdata%\ssh\logs generiert. Jeder andere Wert, einschließlich des Standardwerts AUTH, leitet die Protokollierung an ETW. Weitere Informationen finden Sie unter „Protokollierungsmöglichkeiten unter Windows“.

Nicht unterstützt

Die folgenden Konfigurationsoptionen sind in der OpenSSH-Version unter Windows Server 2019 und Windows 10 1809 nicht verfügbar:

- AcceptEnv
- AllowStreamLocalForwarding
- AuthorizedKeysCommand
- AuthorizedKeysCommandUser
- AuthorizedPrincipalsCommand
- AuthorizedPrincipalsCommandUser
- Komprimierung
- ExposeAuthInfo
- GSSAPIAuthentication
- GSSAPICleanupCredentials
- GSSAPIStrictAcceptorCheck
- HostbasedAcceptedKeyTypes
- HostbasedAuthentication
- HostbasedUsesNameFromPacketOnly
- IgnoreRhosts
- IgnoreUserKnownHosts
- KbdInteractiveAuthentication
- KerberosAuthentication
- KerberosGetAFSToken
- KerberosOrLocalPasswd
- KerberosTicketCleanup
- PermitTunnel
- PermitUserEnvironment
- PermitUserRC
- PidFile
- PrintLastLog
- RDomain
- StreamLocalBindMask
- StreamLocalBindUnlink
- StrictModes
- X11DisplayOffset
- X11Forwarding
- X11UseLocalhost
- XAuthLocation

OpenSSH-Schlüsselverwaltung

24.04.2020 • 9 minutes to read • [Edit Online](#)

Die meisten Authentifizierungen in Windows-Umgebungen erfolgen mit einem Paar aus Benutzernamen und Kennwort. Dies funktioniert besonders gut bei Systemen, die eine gemeinsame Domäne verwenden. Bei domänenübergreifenden Arbeiten wie beispielsweise zwischen lokalen und in der Cloud gehosteten Systemen gestaltet sich dies schon schwieriger.

Im Vergleich dazu verwenden Linux-Umgebungen für die Authentifizierung häufig Paare aus einem öffentlichen und einem privaten Schlüssel. OpenSSH enthält Tools zur Unterstützung dieser Authentifizierungsmethoden einschließlich der folgenden:

- **ssh-keygen** zum Generieren sicherer Schlüssel
- **ssh-agent** und **ssh-add** zum sicheren Speichern privater Schlüssel
- **scp** und **sftp** zum sicheren Kopieren öffentlicher Schlüssel bei der erstmaligen Verwendung eines Servers

Dieses Dokument bietet eine Übersicht über die Verwendung dieser Tools unter Windows für die Schlüsselauthentifizierung mit SSH. Wenn Sie mit der SSH-Schlüsselverwaltung nicht vertraut sind, empfehlen wir Ihnen dringend, das [NIST-Dokument IR 7966](#) mit dem Titel „Security of Interactive and Automated Access Management Using Secure Shell (SSH)“ (Sicherheit der interaktiven und automatisierten Zugriffsverwaltung mit Secure Shell (SSH)) zu lesen.

Informationen zu Schlüsselpaaren

Schlüsselpaare verweisen auf die Dateien für öffentliche und private Schlüssel, die von bestimmten Authentifizierungsprotokollen verwendet werden.

Bei der SSH-Authentifizierung mit öffentlichem Schlüssel werden asymmetrische Kryptografiealgorithmen verwendet, um zwei Schlüsseldateien (privat und öffentlich) zu generieren. Die Dateien des privaten Schlüssels entsprechen einem Kennwort und sollten unter allen Umständen gut geschützt werden. Wenn jemand Ihren privaten Schlüssel erhält, kann sich diese Person bei jedem beliebigen SSH-Server anmelden, auf den Sie Zugriff haben. Der öffentliche Schlüssel wird auf dem SSH-Server abgelegt und ggf. freigegeben, ohne dass dabei der private Schlüssel kompromittiert wird.

Bei Verwendung der Schlüsselauthentifizierung mit einem SSH-Server vergleichen der SSH-Server und der SSH-Client den öffentlichen Schlüssel für den Benutzernamen, der für den privaten Schlüssel bereitgestellt wird. Wenn der öffentliche Schlüssel nicht anhand des clientseitigen privaten Schlüssels überprüft werden kann, schlägt die Authentifizierung fehl.

Die mehrstufige Authentifizierung kann mit Schlüsselpaaren implementiert werden, indem gefordert wird, dass eine Passphrase angegeben wird, wenn das Schlüsselpaar generiert wird (siehe Schlüsselgenerierung unten). Während der Authentifizierung wird der Benutzer zur Eingabe dieser Passphrase aufgefordert. Diese wird zusammen mit dem privaten Schlüssel auf dem SSH-Client verwendet, um den Benutzer zu authentifizieren.

Generierung des Hostschlüssels

Öffentliche Schlüssel weisen bestimmte ACL-Anforderungen auf, die unter Windows nur den Zugriff auf Administratoren und das System erlauben. Folgende Maßnahmen dienen hierbei der Vereinfachung:

- Das PowerShell-Modul „OpenSSHUtils“ wurde erstellt, um die Schlüssel-ACLs ordnungsgemäß festzulegen. Es muss auf dem Server installiert werden.

- Bei der ersten Verwendung von SSHD wird das Schlüsselpaar für den Host automatisch generiert. Wenn „ssh-agent“ ausgeführt wird, werden die Schlüssel automatisch dem lokalen Speicher hinzugefügt.

Führen Sie über eine PowerShell-Eingabeaufforderung mit erhöhten Rechten die folgenden Befehle aus, um die Authentifizierung mit dem SSH-Server zu vereinfachen:

```
# Install the OpenSSHUtils module to the server. This will be valuable when deploying user keys.  
Install-Module -Force OpenSSHUtils -Scope AllUsers  
  
# Start the ssh-agent service to preserve the server keys  
Start-Service ssh-agent  
  
# Now start the sshd service  
Start-Service sshd
```

Da dem SSHD-Dienst kein Benutzer zugeordnet ist, werden die Hostschlüssel unter „\ProgramData\ssh“ gespeichert.

Generierung des Benutzerschlüssels

Sie müssen für den Client zunächst einige Schlüsselpaare aus öffentlichen und privaten Schlüsseln generieren, um die schlüsselbasierte Authentifizierung verwenden zu können. Verwenden Sie in PowerShell oder cmd „ssh-keygen“, um einige Schlüsseldateien zu generieren.

```
cd ~\.ssh\  
ssh-keygen
```

Anschließend sollte in etwa Folgendes angezeigt werden („Benutzername“ wird dabei durch Ihren Benutzernamen ersetzt):

```
Generating public/private ed25519 key pair.  
Enter file in which to save the key (C:\Users\username\.ssh\id_ed25519):
```

Sie können die EINGABETASTE drücken, um die Standardeinstellung zu übernehmen, oder einen Pfad angeben, in dem die Schlüssel generiert werden sollen. An diesem Punkt werden Sie aufgefordert, eine Passphrase zum Verschlüsseln der Dateien für den privaten Schlüssel zu verwenden. Zusammen mit der Schlüsseldatei kann mit der Passphrase die zweistufige Authentifizierung bereitgestellt werden. In diesem Beispiel wird die Passphrase leer gelassen.

```

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\username\.ssh\id_ed25519.
Your public key has been saved in C:\Users\username\.ssh\id_ed25519.pub.
The key fingerprint is:
SHA256:0Izc1yE7joL2Bzy8!gS0j8eGK7bYaH1FmF3sDuMeSj8 username@server@LOCAL-HOSTNAME

The key's randomart image is:
+--[ED25519 256]--+
|         .         |
|         o         |
|     . + + .       |
|   o= B * = .     |
|   o= B S .       |
|   ..B O o       |
|   + =+% o       |
| *oo.O.E        |
|+.o+=o. .       |
+---[SHA256]---+

```

Nun haben Sie ein ED25519-Schlüsselpaar aus öffentlichen und privaten Schlüsseln (die PUB-Dateien sind öffentliche Schlüssel, und die übrigen sind private Schlüssel):

Mode	LastWriteTime	Length	Name
---	-----	-----	-----
-a----	9/28/2018 11:09 AM	1679	id_ed25519
-a----	9/28/2018 11:09 AM	414	id_ed25519.pub

Beachten Sie, dass die Dateien des privaten Schlüssels dem Kennwort entsprechen und daher auf dieselbe Weise geschützt werden müssen wie Ihr Kennwort. Verwenden Sie hierfür „ssh-agent“, um die privaten Schlüssel innerhalb eines sicheren Windows-Sicherheitskontexts zu speichern, der Ihrem Windows-Anmeldenamen zugeordnet ist. Starten Sie hierzu den „ssh-agent“-Dienst als Administrator, und verwenden Sie „ssh-add“, um den privaten Schlüssel zu speichern.

```

# Make sure you're running as an Administrator
Start-Service ssh-agent

# This should return a status of Running
Get-Service ssh-agent

# Now load your key files into ssh-agent
ssh-add ~\.ssh\id_ed25519

```

Nachdem Sie diese Schritte ausgeführt haben, ruft „ssh-agent“ immer automatisch den privaten Schlüssel ab und übergibt ihn an Ihren SSH-Client, wenn für die Authentifizierung dieses Clients ein privater Schlüssel erforderlich ist.

NOTE

Es wird dringend empfohlen, dass Sie den privaten Schlüssel an einem sicheren Speicherort verwahren und aus dem lokalen System löschen, *nachdem* Sie ihn zu „ssh-agent“ hinzugefügt haben. Der private Schlüssel kann nicht vom Agent abgerufen werden. Wenn Sie keinen Zugriff mehr auf den privaten Schlüssel haben, müssten Sie ein neues Schlüsselpaar erstellen und den öffentlichen Schlüssel auf allen Systemen aktualisieren, mit denen Sie interagieren.

Bereitstellen des öffentlichen Schlüssels

Der öffentliche Schlüssel muss auf dem Server in einer Textdatei namens *authorized_keys* unter „Benutzer\Benutzername\.ssh.“ platziert werden, um den oben erstellten Schlüssel zu verwenden. Das OpenSSH-Tool umfasst mit scp ein sicheres Dienstprogramm für den Dateitransfer.

Auf diese Weise verschieben Sie den Inhalt Ihres öffentlichen Schlüssels (~.ssh\id_ed25519.pub) in eine Textdatei namens „authorized_keys“ in „~.ssh\“ auf Ihrem Server/Host.

In diesem Beispiel wird die Funktion „Repair-AuthorizedKeyPermissions“ im OpenSSHUtils-Modul verwendet, das wie in den obigen Anweisungen beschrieben auf dem Host installiert wurde.

```
# Make sure that the .ssh directory exists in your server's home folder
ssh user1@domain1@contoso.com mkdir C:\users\user1\.ssh\

# Use scp to copy the public key file generated previously to authorized_keys on your server
scp C:\Users\user1\.ssh\id_ed25519.pub user1@domain1@contoso.com:C:\Users\user1\.ssh\authorized_keys

# Appropriately ACL the authorized_keys file on your server
ssh --% user1@domain1@contoso.com powershell -c $ConfirmPreference = 'None'; Repair-AuthorizedKeyPermission
C:\Users\user1\.ssh\authorized_keys
```

Mit diesen Schritten wird die Konfiguration vervollständigt, die für die Verwendung der schlüsselbasierten Authentifizierung mit SSH unter Windows erforderlich ist. Danach kann der Benutzer von jedem Client, der über den privaten Schlüssel verfügt, eine Verbindung mit dem SSHD-Host herstellen.

Windows Server Update Services (WSUS)

24.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Windows Server Update Services (WSUS) ermöglicht IT-Administratoren das Bereitstellen der aktuellen Microsoft-Produktupdates. Du kannst WSUS verwenden, um die Verteilung von Updates, die über Microsoft Update veröffentlicht werden, auf den Computern in deinem Netzwerk vollständig zu verwalten. Dieses Thema enthält einen Überblick über diese Serverrolle sowie weitere Informationen zum Bereitstellen und Warten von WSUS.

Beschreibung der WSUS-Serverrolle

Ein WSUS-Server stellt Features bereit, die du zum Verwalten und Verteilen von Updates über eine Verwaltungskonsole verwenden kannst. Ein WSUS-Server kann auch als Updatequelle für andere WSUS-Server in der Organisation dienen. Der als Updatequelle eingesetzte WSUS-Server wird als Upstreamserver bezeichnet. In einer WSUS-Implementierung muss mindestens ein WSUS-Server im Netzwerk eine Verbindung mit Microsoft Update herstellen können, um verfügbare Updateinformationen herunterzuladen. Als Administrator kannst du – basierend auf der Netzwerksicherheit und -konfiguration – festlegen, wie viele weitere WSUS-Server eine direkte Verbindung mit Microsoft Update herstellen.

Praktische Anwendung

Unter der Updateverwaltung versteht man das Steuern der Bereitstellung und Wartung von Zwischensoftwareversionen in Produktionsumgebungen. Sie hilft Ihnen, die betriebliche Effizienz zu wahren, Sicherheitsrisiken zu bewältigen und die Stabilität der Produktionsumgebung aufrecht zu erhalten. Wenn Ihre Organisation nicht in der Lage ist, eine bekannte Vertrauensebene in den Betriebssystemen und der Anwendungssoftware herzustellen und aufrecht zu erhalten, können verschiedene Sicherheitsrisiken auftreten, die – sofern sie ausgenutzt werden – zu einem Verlust von Umsatzerlösen und geistigem Eigentum führen können. Um diese Gefahr zu minimieren, müssen Sie Ihre Systeme korrekt konfigurieren, die aktuelle Software verwenden und die empfohlenen Softwareupdates installieren.

In den folgenden Szenarien kann Ihr Unternehmen von WSUS profitieren:

- Zentrale Updateverwaltung
- Automatisierung der Updateverwaltung

Neue und geänderte Funktionalität

NOTE

Wenn du ein Upgrade von einer beliebigen Windows Server-Version mit WSUS 3.2-Unterstützung auf Windows Server 2012 R2 ausführen möchtest, musst du zuerst WSUS 3.2 deinstallieren.

In Windows Server 2012 wird das Upgraden von einer beliebigen Version von Windows Server mit WSUS 3.2-Installation während des Installationsvorgangs blockiert, falls WSUS 3.2 erkannt wird. In diesem Fall wirst du aufgefordert, zunächst Windows Server Update Services zu deinstallieren, bevor du das Update für den Server durchführst.

Aufgrund von Änderungen in diesem Release von Windows Server und Windows Server 2012 R2 wird die Installation beim Upgraden einer beliebigen Version von Windows Server und WSUS 3.2 nicht blockiert. Wenn du WSUS 3.2 vor dem Windows Server 2012 R2-Upgrade nicht deinstallierst, können die Aufgaben nach der Installation für WSUS unter Windows Server 2012 R2 nicht erfolgreich ausgeführt werden. In diesem Fall kannst du nur noch die Festplatte formatieren und Windows Server neu installieren.

Windows Server Update Services (WSUS) ist eine integrierte Serverrolle mit den folgenden Verbesserungen:

- Kann mit dem Server-Manager hinzugefügt und entfernt werden.
- Enthält Windows PowerShell-Cmdlets zum Verwalten der wichtigsten administrativen Aufgaben in WSUS.
- Enthält eine SHA256-Hashfunktion für verbesserte Sicherheit.
- Ermöglicht die Trennung von Client und Server: Versionen des Windows Update-Agents (WUA) sind unabhängig von WSUS erhältlich

Verwendung von Windows PowerShell zum Verwalten von WSUS

Damit Systemadministratoren ihre Aufgaben automatisieren können, ist eine entsprechende Unterstützung durch Befehlszeilenautomatisierung erforderlich. Diese Funktion dient in erster Linie dazu, die WSUS-Verwaltung zu vereinfachen, indem Systemadministratoren die Möglichkeit geboten wird, ihre alltäglichen Aufgaben zu automatisieren.

Welchen Nutzen bietet diese Änderung?

Indem die wichtigsten WSUS-Vorgänge über Windows PowerShell verfügbar gemacht werden, können Systemadministratoren ihre Produktivität steigern, den Lernaufwand für neue Tools verringern und Fehler reduzieren, die aufgrund fehlender Konsistenz zwischen ähnlichen Vorgängen entstehen, weil Vorgänge nicht wie erwartet funktionieren.

Worin bestehen die Unterschiede?

In früheren Versionen des Windows Server-Betriebssystems waren keine Windows PowerShell-Cmdlets verfügbar, und die Automatisierung der Updateverwaltung war sehr schwierig. Die Windows PowerShell-Cmdlets für WSUS-Vorgänge bieten dem Systemadministrator mehr Flexibilität.

Inhalt dieser Sammlung

Die folgenden Leitfäden für die Planung, Bereitstellung und Verwaltung von WSUS sind in dieser Sammlung enthalten:

- [Bereitstellen von Windows Server Update Services](#)
- [Verwalten von Updates mit Windows Server Update Services](#)

Bereitstellen von Windows Server Update Services

24.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Windows Server Update Services (WSUS) ermöglicht IT-Administratoren das Bereitstellen der aktuellen Microsoft-Produktupdates. WSUS ist eine Windows Server-Serverrolle, die zum Verwalten und Verteilen von Updates installiert werden kann. Ein WSUS-Server kann als Updatequelle für andere WSUS-Server in der Organisation dienen. Der als Updatequelle eingesetzte WSUS-Server wird als Upstreamserver bezeichnet.

In einer WSUS-Implementierung muss mindestens ein WSUS-Server im Netzwerk eine Verbindung mit Microsoft Update herstellen, um verfügbare Updateinformationen herunterzuladen. Sie können basierend auf der Netzwerksicherheit und -konfiguration festlegen, wie viele weitere Server eine direkte Verbindung mit Microsoft Update herstellen.

In diesem Leitfaden erhalten Sie grundlegende Informationen zur Planung und Bereitstellung von Windows Server Update Services.

- [Planen der WSUS-Bereitstellung](#)
- [Schritt 1: Installieren Sie die WSUS-Serverrolle](#)
- [Schritt 2: Konfigurieren von WSUS](#)
- [Schritt 3: Genehmigen und Bereitstellen von Updates in WSUS](#)
- [Schritt 4: Konfigurieren von Gruppenrichtlinien für automatische Updates](#)

Planen der WSUS-Bereitstellung

28.04.2020 • 55 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Der erste Schritt bei der Bereitstellung von Windows Server Update Services (WSUS) sind einige wichtige Entscheidungen, z. B. die Auswahl des WSUS-Bereitstellungsszenarios und der Netzwerktopologie sowie die Prüfung der Systemanforderungen. In der folgenden Prüfliste sind die Schritte zur Vorbereitung der Bereitstellung zusammengefasst.

AUFGABE	BESCHREIBUNG
1.1. Vorüberlegungen und Systemanforderungen	Prüfen Sie die Liste der Bereitstellungshinweise und Systemanforderungen, um sicherzustellen, dass Sie über alle notwendige Hardware und Software für die Bereitstellung von WSUS verfügen.
1.2. Wählen eines WSUS-Bereitstellungsszenarios	Entscheiden Sie, welches WSUS-Bereitstellungsszenario verwendet werden soll.
1.3. Wählen einer WSUS-Speicherstrategie	Entscheiden Sie, welche WSUS-Speicherstrategie am besten für Ihre Bereitstellung geeignet ist.
1.4. Wählen der WSUS-Updatesprachen	Entscheiden Sie, welche WSUS-Updatesprachen installiert werden sollen.
1.5. Planen von WSUS-Computergruppen	Planen Sie, wie WSUS-Computergruppen in Ihrer Bereitstellung verwendet werden sollen.
1.6. Aspekte beim Planen der WSUS-Leistung: Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)	Erstellen Sie einen WSUS-Entwurf für optimierte Leistung.
1.7. Planen der Einstellungen für automatische Updates	Planen Sie, wie die Einstellungen für automatische Updates für Ihr Szenario konfiguriert werden sollen.

1.1. Vorüberlegungen und Systemanforderungen

Systemanforderungen

Die Anforderungen an Hardware und Datenbanksoftware richten sich nach der Anzahl der Clientcomputer, die in Ihrem Unternehmen aktualisiert werden. Stellen Sie vor dem Aktivieren der WSUS-Serverrolle anhand der folgenden Richtlinien sicher, dass der Server die Systemanforderungen erfüllt und Sie die erforderlichen Berechtigungen zum Durchführen der Installation besitzen:

- Serverhardwareanforderungen zum Aktivieren der WSUS-Rolle sind an die Hardware gebunden. Die Mindesthardwareanforderungen für WSUS sind:
 - **Prozessor:** 1,4 GHz x64-Prozessor (min. 2 GHz empfohlen)
 - **Arbeitsspeicher:** WSUS erfordert 2 GB RAM zusätzlich zum vom Server und allen anderen

Diensten und Programmen benötigten Arbeitsspeicher.

- **Verfügbarer Speicherplatz:** min. 40 GB empfohlen
- **Netzwerkadapter:** min. 100 MBit/s (1 GB empfohlen)

NOTE

Diese Richtlinien gehen davon aus, dass WSUS-Clients bei einem Rullup von 30.000 Clients alle acht Stunden mit dem Server synchronisiert werden. Wenn sie öfter synchronisieren, erhöht sich die Serverlast entsprechend.

- Softwareanforderungen:

- Zum Anzeigen von Berichten benötigt WSUS [Microsoft Report Viewer Redistributable 2008](#). Unter Windows Server 2016 erfordert WSUS [Microsoft Report Viewer Runtime 2012](#).
- Starten Sie den Server vor dem Aktivieren der WSUS-Serverrolle neu, falls Sie Rollen oder Softwareupdates installieren, bei denen der Server nach der Installation neu gestartet werden muss.
- Microsoft .NET Framework 4.0 muss auf dem Server installiert sein, auf dem die WSUS-Serverrolle installiert wird.
- Das Konto %quot;NT-Autorität\Netzwerkdienst%quot; muss über die Berechtigung %quot;Vollzugriff%quot; für die folgenden Ordner verfügen, damit das WSUS-Verwaltungs-Snap-In korrekt angezeigt wird:
 - %windir%\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files

NOTE

Dieser Pfad ist vor der Installation der Webserverrolle, in der Internetinformationsdienste (IIS) enthalten ist, möglicherweise nicht vorhanden.

- %windir%\Temp
- Stellen Sie sicher, dass das Konto, das Sie zum Installieren von WSUS verwenden, ein Mitglied der lokalen Administratorgruppe ist.

Überlegungen zur Installation

Während des Installationsvorgangs installiert WSUS standardmäßig die folgenden Komponenten:

- .NET-API und Windows PowerShell-Cmdlets
- Interne Windows-Datenbank (Windows Internal Database, WID), wird von WSUS verwendet
- Folgende von WSUS verwendete Dienste:
 - Updatedienst
 - Berichterstattungswebdienst
 - Clientwebdienst
 - Webdienst für die einfache Webauthentifizierung
 - Serversynchronisierungsdienst
 - DSS-Authentifizierungswebdienst

Überlegungen zu Features bei Bedarf

Beachten Sie, dass das Konfigurieren von Clientcomputern (einschließlich Server) für die Aktualisierung über WSUS zu folgenden Einschränkungen führt:

1. Serverrollen, deren Nutzlasten mit Features bei Bedarf entfernt wurden, können nicht bei Bedarf von Microsoft Update installiert werden. Sie müssen entweder zum Zeitpunkt des Versuchs, solche Serverrollen zu installieren, eine Installationsquelle bereitstellen oder eine Quelle für „Features bei Bedarf“ in der Gruppenrichtlinie konfigurieren.
2. Windows-Client-Editionen können .NET 3.5 nicht bei Bedarf über das Web installieren. Die gleichen Überlegungen wie Serverrollen gelten für .NET 3.5.

NOTE

Das Konfigurieren einer Installationsquelle für „Features bei Bedarf“ umfasst nicht WSUS. Informationen zum Konfigurieren von Features finden Sie unter [Configure Features on Demand in Windows Server](#).

3. Auf Unternehmensgeräten, auf denen Windows 10, Version 1709 oder Version 1803 ausgeführt wird, können „Features bei Bedarf“ nicht direkt über WSUS installiert werden. Um „Features bei Bedarf“ zu installieren, erstellen Sie [eine Featuredatei \(oder einen Seite-an-Seite-Speicher\)](#), oder beziehen Sie das „Features bei Bedarf“-Paket aus einer der folgenden Quellen:
 - [Volume Licensing Service Center \(VLSC\)](#): VL-Zugriff erforderlich
 - OEM-Portal: OEM-Zugriff erforderlich
 - MSDN-Download: MSDN-Abonnement erforderlich

Einzelne bezogene „Features bei Bedarf“-Pakete können über [DISM-Befehlszeilenoptionen](#) installiert werden.

WSUS-Datenbankanforderungen

WSUS erfordert eine der folgenden Datenbanken:

- Interne Windows-Datenbank (WID)
- Alle unterstützten Microsoft SQL Server-Versionen. Weitere Informationen finden Sie in der [Lebenszyklusrichtlinie für Microsoft](#).

Die folgenden Editionen von SQL Server werden von WSUS unterstützt:

- Standard
- Enterprise
- Express

NOTE

Bei SQL Server Express 2008 R2 beträgt die maximale Datenbankgröße 10 GB. Die Größe dieser Datenbank ist für WSUS meist ausreichend, ihre Verwendung bietet gegenüber WID jedoch keinen spürbaren Vorteil. Die WID-Datenbank weist eine RAM-Mindestanforderung von 2 GB zuzüglich der standardmäßigen Windows Server-Systemanforderungen auf.

Sie können die WSUS-Rolle auf einem anderen Computer als dem Datenbankservercomputer installieren. In diesem Fall gelten folgende zusätzliche Kriterien:

1. Der Datenbankserver kann nicht als Domänencontroller konfiguriert werden.
2. Auf dem WSUS-Server können die Remotedesktopdienste nicht ausgeführt werden.

3. Der Datenbankserver muss derselben Active Directory-Domäne angehören wie der WSUS-Server oder über eine Vertrauensstellung mit der Active Directory-Domäne des WSUS-Servers verfügen.
4. Der WSUS-Server und der Datenbankserver müssen sich in der gleichen Zeitzone befinden oder mit der gleichen UTC-Quelle (Universal Time Coordinated = koordinierte Weltzeit bzw. Greenwich Mean Time) synchronisiert werden.

1.2. Auswählen des WSUS-Bereitstellungsszenarios

In diesem Abschnitt werden die grundlegenden Features aller WSUS-Bereitstellungen beschrieben. Sie finden hier Informationen zu einfachen Bereitstellungen mit nur einem WSUS-Server und komplexeren Szenarien, z. B. einer WSUS-Serverhierarchie oder einem WSUS-Server in einem isolierten Netzwerksegment.

Einfache WSUS-Bereitstellung

Die einfachste WSUS-Bereitstellung besteht aus einem Server innerhalb der Unternehmensfirewall, der Updates für Clientcomputer in einem privaten Intranet verarbeitet. Der WSUS-Server stellt eine Verbindung mit Microsoft Update her, um Updates herunterzuladen. Dieser Vorgang wird als *Synchronisierung* bezeichnet. Während der Synchronisierung überprüft WSUS, ob seit der letzten Synchronisierung Updates verfügbar gemacht wurden. Bei der ersten Synchronisierung von WSUS werden alle Updates zum Download verfügbar gemacht.

NOTE

Die Erstsynchronisierung kann mehr als eine Stunde in Anspruch nehmen. Alle anschließenden Synchronisierungen sollten deutlich schneller vonstatten gehen.

Der WSUS-Server verwendet standardmäßig Port 80 für das HTTP-Protokoll und Port 443 für das HTTPS-Protokoll, um Updates von Microsoft Update herunterzuladen. Falls eine Unternehmensfirewall zwischen dem Netzwerk und dem Internet vorhanden ist, müssen Sie diese Ports auf dem Server öffnen, der direkt mit Microsoft Update kommuniziert. Wenn Sie benutzerdefinierte Ports für diese Kommunikation verwenden möchten, müssen Sie stattdessen diese Ports öffnen. Sie können mehrere WSUS-Server zur Synchronisierung mit einem übergeordneten WSUS-Server konfigurieren. Der WSUS-Server verwendet standardmäßig Port 8530 für das HTTP-Protokoll und Port 8531 für das HTTPS-Protokoll, um Updates an Clientworkstations zu verteilen.

Mehrere WSUS-Server

Administratoren können mehrere Server mit WSUS bereitstellen, die alle Inhalte innerhalb des Intranets der Organisation synchronisieren. Sie können nur einen Server für das Internet verfügbar machen, der der einzige Server ist, der Updates von Microsoft Update herunterlädt. Dieser Server wird als Upstreamserver eingerichtet, d. h. als die Quelle, mit der die Downstreamserver synchronisiert werden. Server können bei Bedarf in einem geografisch verteilten Netzwerk eingerichtet werden, um für alle Clientcomputer die bestmögliche Konnektivität bereitzustellen.

Nicht verbundener WSUS-Server

Wenn der Zugriff auf das Internet aufgrund von Unternehmensrichtlinien oder aus anderen Gründen eingeschränkt ist, können Administratoren einen internen Server für WSUS einrichten. Ein Beispiel hierfür ist ein Server, der mit dem Intranet verbunden, aber vom Internet isoliert ist. Nachdem die Updates auf diesem Server heruntergeladen, getestet und genehmigt wurden, exportiert der Administrator Updatemetadaten und -inhalte auf eine DVD. Anschließend werden die Updatemetadaten und -inhalte von der DVD auf die WSUS-Server im Intranet importiert.

WSUS-Serverhierarchien

Sie können komplexe Hierarchien von WSUS-Servern erstellen. Da es möglich ist, einen WSUS-Server nicht mit Microsoft Update, sondern mit einem anderen WSUS-Server zu synchronisieren, benötigen Sie nur einen mit Microsoft Update verbundenen WSUS-Server. Wenn Sie WSUS-Server miteinander verbinden, haben Sie einen

WSUS-Upstreamserver und einen WSUS-Downstreamserver. Die Bereitstellung einer WSUS-Serverhierarchie bietet die folgenden Vorteile:

- Sie können Updates einmal aus dem Internet herunterladen und anschließend mithilfe von Downstreamservern an Clientcomputer verteilen. Durch diese Methode können Sie Bandbreite auf der Internetverbindung Ihres Unternehmens sparen.
- Sie können Updates auf einen WSUS-Server herunterladen, der den Clientcomputern physisch näher ist, z. B. in Filialen.
- Sie können separate WSUS-Server für Clientcomputer einrichten, auf denen Microsoft-Produkte in unterschiedlichen Sprachen verwendet werden.
- Sie können WSUS für eine große Organisation skalieren, in der mehr Clientcomputer vorhanden sind als ein WSUS-Server effektiv verwalten kann.

NOTE

Es wird empfohlen, die WSUS-Serverhierarchie auf maximal drei Ebenen zu beschränken, da der Zeitaufwand für die Verteilung von Updates an die verbundenen Server durch jede Ebene zunimmt. Obwohl es keine theoretische Grenze für eine Hierarchie gibt, wurden von Microsoft nur Implementierungen mit einer Hierarchie mit einer Tiefe von fünf Ebenen getestet.

Außerdem müssen Downstreamserver die gleiche oder eine frühere Version von WSUS wie die Synchronisationsquelle des Upstreamservers aufweisen.

Sie können WSUS-Server im autonomen Modus (verteilte Verwaltung) oder im Replikatmodus (zentrale Verwaltung) verbinden und ggf. eine Serverhierarchie mit beiden Modi bereitstellen: Die WSUS-Lösung kann sowohl autonome WSUS-Server als auch WSUS-Replikatserver enthalten.

Autonomer Modus

Der autonome Modus (auch als verteilte Verwaltung bezeichnet) ist die Standardinstallationsoption für WSUS. Im autonomen Modus gibt ein WSUS-Upstreamserver während der Synchronisierung Updates für Downstreamserver frei. WSUS-Downstreamserver werden separat verwaltet und müssen weder den Genehmigungsstatus von Updates noch Computergruppeninformationen vom Upstreamserver empfangen. Beim verteilten Verwaltungsmodell werden von jedem WSUS-Serveradministrator Updatesprachen ausgewählt, Computergruppen erstellt, Computer Gruppen zugewiesen sowie Updates getestet und genehmigt. Außerdem stellt der Administrator sicher, dass die richtigen Updates auf den entsprechenden Computergruppen installiert werden. Die folgende Abbildung zeigt, wie autonome WSUS-Server in einer Filialenumgebung bereitgestellt werden können.

Replikatmodus

Beim Replikatmodus (auch als zentrale Verwaltung bezeichnet) wird ein WSUS-Upstreamserver eingesetzt, der Updates, Genehmigungsstatus und Computergruppen für Downstreamserver freigibt. Replikatserver erben Updategenehmigungen und werden nicht getrennt vom WSUS-Upstreamserver verwaltet. Die folgende Abbildung zeigt, wie WSUS-Replikatserver in einer Filialenumgebung bereitgestellt werden können.

NOTE

Wenn Sie mehrere Replikatserver einrichten, die eine Verbindung mit einem einzigen WSUS-Upstreamserver herstellen, sollten Sie die Synchronisierung auf den einzelnen Replikatservern für unterschiedliche Zeitpunkte planen. So können Sie einen plötzlichen Anstieg der Bandbreitennutzung vermeiden.

Filialen

Sie können das Filialenfeature in Windows nutzen, um die WSUS-Bereitstellung zu optimieren. Dieser

Bereitstellungstyp bietet die folgenden Vorteile:

1. Sie können die Nutzung der WAN-Verbindung reduzieren und das Reaktionsverhalten von Anwendungen verbessern. Sie können die Bereitstellung der vom WSUS-Server verarbeiteten Inhalte mithilfe von BranchCache beschleunigen, indem Sie BranchCache auf dem Server und den Clients installieren und sicherstellen, dass der BranchCache-Dienst gestartet wurde. Weitere Schritte sind nicht erforderlich.
2. In Filialen, bei denen die Verbindungen mit der Zentrale eine niedrige Bandbreite haben, die Verbindungen mit dem Internet aber eine hohe Bandbreite, kann das Filialenfeature ebenfalls verwendet werden. In diesem Fall können Sie WSUS-Downstreamserver so konfigurieren, dass sie Informationen zu den zu installierenden Updates vom zentralen WSUS-Server abrufen, die Updates selbst aber von Microsoft Update herunterladen.

Netzwerklastenausgleich

Der Netzwerklastenausgleich (Network Load Balancing, NLB) verbessert die Zuverlässigkeit und Leistung Ihres WSUS-Netzwerks. Sie können mehrere WSUS-Server mit einem gemeinsamen Failovercluster mit SQL Server wie z. B. SQL Server 2008 R2 SP1 einrichten. In dieser Konfiguration müssen Sie eine vollständige SQL Server-Installation verwenden (nicht die von WSUS bereitgestellte interne Windows-Datenbank), und die Datenbankrolle muss auf allen WSUS-Front-End-Servern installiert werden. Sie können auch auf allen WSUS-Servern ein verteiltes Dateisystem (Distributed File System, DFS) zum Speichern der Inhalte verwenden.

WSUS-Setup für Netzwerklastenausgleich: Im Vergleich zum WSUS 3.2-Setup für den Netzwerklastenausgleich sind keine besonderen Setupaufrufe und -parameter mehr erforderlich, um WSUS für den Netzwerklastenausgleich zu konfigurieren. Sie müssen lediglich beim Einrichten der einzelnen WSUS-Server Folgendes beachten.

- WSUS muss unter Verwendung der SQL-Datenbank-Option anstelle von WID eingerichtet werden.
- Wenn Updates lokal gespeichert werden, muss der gleiche Inhaltsordner zwischen den WSUS-Servern freigegeben werden, die die gleiche SQL-Datenbank gemeinsam nutzen.
- WSUS-Setup muss nacheinander durchgeführt werden. Postinstallationsaufgaben können nicht auf mehreren Servern gleichzeitig ausgeführt werden, wenn eine gemeinsame SQL-Datenbank genutzt wird.

WSUS-Bereitstellung mit Roamingclientcomputern

Wenn sich mobile Benutzer an unterschiedlichen Orten beim Netzwerk anmelden, können Sie WSUS so konfigurieren, dass Roamingbenutzer ihre Clientcomputern mit dem geografisch am nächsten gelegenen WSUS-Server aktualisieren können. So können Sie beispielsweise einen WSUS-Server pro Region bereitstellen und für jede Region ein anderes DNS-Subnetz verwenden. Alle Clientcomputer können zum gleichen WSUS-Server geleitet werden, der in jedem Subnetz zum physisch nächsten WSUS-Server aufgelöst wird.

1.3. Auswählen der WSUS-Speicherstrategie

Windows Server Update Services (WSUS) verwendet zwei Arten von Speichersystemen: eine Datenbank zum Speichern der WSUS-Konfiguration und Updatemetadaten und ein optionales lokales Dateisystem zum Speichern von Updatedateien. Bevor Sie WSUS installieren, sollten Sie entscheiden, wie Sie den Speicher implementieren möchten.

Updates bestehen aus zwei Teilen: Metadaten, die das Update beschreiben, und Dateien, die zum Installieren des Updates erforderlich sind. Updatemetadaten sind in der Regel sehr viel kleiner als das eigentliche Update und werden in der WSUS-Datenbank gespeichert. Updatedateien werden auf einem lokalen WSUS-Server oder einem Microsoft Update-Webserver gespeichert.

WSUS-Datenbank

WSUS erfordert eine Datenbank für jeden WSUS-Server. WSUS unterstützt – mit einigen Einschränkungen – die Verwendung einer Datenbank, die sich auf einem anderen Computer als dem WSUS-Server befindet. Eine Liste der

unterstützten Datenbanken und Einschränkungen für Remotedatenbanken finden Sie im Abschnitt „1.1 Vorüberlegungen und Systemanforderungen“ in dieser Anleitung.

In der WSUS-Datenbank werden die folgenden Informationen gespeichert:

- Informationen zur WSUS-Serverkonfiguration
- Metadaten, die die einzelnen Updates beschreiben
- Informationen zu Clientcomputern, Updates und Interaktionen

Wenn Sie mehrere WSUS-Server installieren, ist eine separate Datenbank für jeden WSUS-Server erforderlich, unabhängig davon, ob es sich um einen autonomen Server oder einen Replikatserver handelt. Mit Ausnahme von NLB-Clustern mit SQL Server-Failover ist es nicht möglich, mehrere WSUS-Datenbanken auf einer einzigen SQL Server-Instanz zu speichern.

In einer Einzelserverkonfiguration, bei der sich die Datenbank und der WSUS-Dienst auf demselben Computer befinden, bieten SQL Server, SQL Server Express und die interne Windows-Datenbank die gleichen Leistungsmerkmale. Eine Einzelserverkonfiguration kann mehrere tausend WSUS-Clientcomputer unterstützen.

NOTE

Versuchen Sie nicht, WSUS durch direkten Zugriff auf die Datenbank zu verwalten. Die Datenbank kann beschädigt werden, wenn Sie sie direkt bearbeiten. Die Beschädigung macht sich möglicherweise nicht sofort bemerkbar, kann aber dazu führen, dass Upgrades auf die nächste Version des Produkts nicht möglich sind. Sie können WSUS mithilfe der WSUS-Konsole oder mit WSUS-Anwendungsprogrammierschnittstellen (Application Programming Interface, API) verwalten.

WSUS mit interner Windows-Datenbank

Standardmäßig erstellt und verwendet der Installations-Assistent eine interne Windows-Datenbank mit dem Namen %"SUSDB.mdf%". Diese Datenbank befindet sich im Ordner %"%windir%\wid\data%", wobei %"%windir%%" das lokale Laufwerk ist, auf dem die WSUS-Serversoftware installiert ist.

NOTE

Die interne Windows-Datenbank (WID) wurde unter Windows Server 2008 eingeführt.

WSUS unterstützt für die Datenbank nur die Windows-Authentifizierung. Die SQL Server-Authentifizierung kann nicht mit WSUS verwendet werden. Wenn Sie die interne Windows-Datenbank für die WSUS-Datenbank verwenden, erstellt das WSUS-Setup eine SQL Server-Instanz mit dem Namen %"Server\Microsoft##WID%", wobei %"Server%" der Name des Computers ist. Bei beiden Datenbankoptionen erstellt das WSUS-Setup eine Datenbank namens %"SUSDB%". Der Name dieser Datenbank ist nicht konfigurierbar.

In den folgenden Fällen wird empfohlen, die interne Windows-Datenbank zu verwenden:

- Die Organisation hat noch kein SQL Server-Produkt für eine andere Anwendung erworben und benötigt kein SQL Server-Produkt.
- Die Organisation benötigt keine WSUS-Lösung mit Netzwerklastenausgleich (NLB).
- Sie beabsichtigen, mehrere WSUS-Server bereitzustellen (z. B. in Filialen). In diesem Fall sollten Sie die Verwendung der internen Windows-Datenbank für die sekundären Server erwägen (auch wenn Sie SQL Server für den WSUS-Stammserver verwenden). Da für jeden WSUS-Server eine separate Instanz von SQL Server erforderlich ist, können schnell Probleme mit der Datenbankleistung auftreten, wenn nur eine Instanz von SQL Server für mehrere WSUS-Server eingesetzt wird.

Die interne Windows-Datenbank stellt keine Benutzeroberfläche oder Tools zur Datenbankverwaltung bereit. Wenn Sie diese Datenbank für WSUS verwenden, müssen Sie sie mit externen Tools verwalten. Weitere Informationen finden Sie unter:

- [Sicherung und Wiederherstellung von WSUS-Daten und Sichern des Servers](#)
- [Neuindizieren der WSUS-Datenbank](#)

WSUS mit SQL Server

In den folgenden Fällen wird empfohlen, SQL Server mit WSUS zu verwenden:

1. Sie benötigen eine WSUS-Lösung mit Netzwerklastenausgleich (NLB).
2. Sie haben bereits mindestens eine Instanz von SQL Server installiert.
3. Sie können den SQL Server-Dienst nicht unter einem lokalen Konto, das kein Systemkonto ist, oder mit der SQL Server-Authentifizierung ausführen. WSUS unterstützt nur die Windows-Authentifizierung.

WSUS-Updatespeicher

Beim Synchronisieren von Updates auf den WSUS-Server werden die Metadaten- und Updatedateien an zwei separaten Speicherorten gespeichert. Metadaten werden in der WSUS-Datenbank gespeichert. Updatedateien können auf dem WSUS-Server oder auf Microsoft Update-Servern gespeichert werden, je nachdem, wie Sie Ihre Optionen für die Synchronisierung konfiguriert haben. Falls Sie sich dafür entscheiden, Updatedateien auf dem WSUS-Server zu speichern, laden Clientcomputer genehmigte Updates vom lokalen WSUS-Server herunter. Andernfalls laden Clientcomputer genehmigte Updates direkt von Microsoft Update herunter. Welche Option für Ihre Organisation am sinnvollsten ist, hängt von der Netzwerkbandbreite zum Internet, der Netzwerkbandbreite im Intranet und der lokalen Speicherverfügbarkeit ab.

Sie können für jeden bereitgestellten WSUS-Server eine andere Updatespeicherlösung verwenden.

Lokaler WSUS-Serverspeicher

Die lokale Speicherung von Updatedateien ist bei der Installation und Konfiguration von WSUS die Standardoption. Mit dieser Option können Sie Bandbreite auf der Internetverbindung des Unternehmens sparen, da Clientcomputer Updates direkt vom lokalen WSUS-Server herunterladen.

Diese Option setzt voraus, dass auf dem Server ausreichend Speicherplatz für alle erforderlichen Updates verfügbar ist. WSUS erfordert mindestens 20 GB zum lokalen Speichern von Updates. Basierend auf getesteten Variablen werden jedoch 30 GB empfohlen.

Remotespeicher auf Microsoft Update-Servern

Sie können Updates remote auf Microsoft Update-Servern speichern. Diese Option ist hilfreich, wenn die meisten Clientcomputer die Verbindung mit dem WSUS-Server über eine langsame WAN-Verbindung herstellen, für den Internetzugriff jedoch über eine Verbindung mit hoher Bandbreite verfügen.

In diesem Fall wird der WSUS-Stammserver mit Microsoft Update synchronisiert und empfängt die Updatemetadaten. Nachdem Sie die Updates genehmigt haben, laden die Clientcomputer die genehmigten Updates von Microsoft Update-Servern herunter.

1.4. Auswählen der WSUS-Updatesprachen

Wenn Sie eine WSUS-Serverhierarchie bereitstellen, sollten Sie bestimmen, für welche Sprachen Updates in der Organisation erforderlich sind. Konfigurieren Sie den WSUS-Stammserver zum Herunterladen von Updates in allen Sprachen, die in der Organisation verwendet werden.

Es kann z. B. vorkommen, dass die Hauptniederlassung Updates in Englisch und Französisch benötigt, für eine Filiale aber Updates in Englisch, Französisch und Deutsch und für eine weitere Filiale Updates in Englisch und Spanisch erforderlich sind. In dieser Situation konfigurieren Sie den WSUS-Stammserver zum Herunterladen von Updates in Englisch, Französisch, Deutsch und Spanisch. Anschließend konfigurieren Sie den WSUS-Server der

ersten Filiale zum Herunterladen von Updates in Englisch, Französisch und Deutsch und den WSUS-Server der zweiten Filiale zum Herunterladen von Updates in Englisch und Spanisch.

Auf der Seite **Sprachen auswählen** des WSUS-Konfigurations-Assistenten können Sie auswählen, ob Sie Updates für alle Sprachen oder eine Teilmenge von Sprachen wünschen. Durch die Auswahl einer Teilmenge von Sprachen sparen Sie Speicherplatz. Wählen Sie jedoch UNBEDINGT alle Sprachen aus, die für sämtliche Downstreamserver und Clientcomputer eines WSUS-Servers erforderlich sind.

Im Folgenden finden Sie einige WICHTIGE Hinweise zu Updatesprachen, die Sie vor dem Konfigurieren dieser Option bedenken sollten:

- Wählen Sie neben allen anderen Sprachen, die in der Organisation benötigt werden, immer Englisch aus.
Alle Updates basieren auf englischen Sprachpaketen.
- Downstreamserver und Clientcomputer empfangen nicht alle erforderlichen Updates, wenn Sie nicht alle benötigten Sprachen für den Upstreamserver auswählen. Achten Sie darauf, dass Sie alle erforderlichen Sprachen für alle zugeordneten Clientcomputer aller Downstreamserver auswählen.
- Auf dem WSUS-Stammserver, der mit Microsoft Update synchronisiert wird, sollten Sie generell Updates in allen Sprachen herunterladen. Dadurch stellen Sie sicher, dass alle Downstreamserver und Clientcomputer Updates in den für sie erforderlichen Sprachen empfangen.

Wenn Sie Updates lokal speichern und einen WSUS-Server zum Herunterladen von Updates in einer begrenzten Anzahl von Sprachen eingerichtet haben, werden Sie möglicherweise feststellen, dass Updates in Sprachen vorhanden sind, die Sie nicht angegeben haben. Bei vielen Updatedateien handelt es sich um Bündel mehrerer Sprachen, von denen Sie mindestens eine auf dem Server angegeben haben.

Upstreamserver

NOTE

Konfigurieren Sie Upstreamserver zum Synchronisieren von Updates in allen Sprachen, die für Downstreamserver im Replikatmodus erforderlich sind. Für nicht synchronisierte Sprachen erfolgt keine Benachrichtigung über erforderliche Updates.

Updates werden auf Clientcomputern, die diese Sprache erfordern, als **Nicht zutreffend** angezeigt. Um dies zu vermeiden, stellen Sie sicher, dass alle Betriebssystemsprachen in den Optionen für die Synchronisierung der WSUS-Server enthalten sind. Sie können alle Betriebssystemsprachen durch das Aufrufen der Ansicht **Computer** der WSUS-Verwaltungskonsole und Sortieren der Computer nach Betriebssystemsprache einsehen. Eventuell sollten jedoch weitere Sprachen berücksichtigt werden, wenn beispielsweise Microsoft-Anwendungen in mehr als einer Sprache verwendet werden (beispielsweise, wenn auf einigen Computern, die die englische Version von Windows 8 verwenden, die französische Version von Microsoft Word installiert ist).

Das Auswählen von Sprachen für einen Upstreamserver ist nicht dasselbe wie das Auswählen von Sprachen für einen Downstreamserver. Das folgende Verfahren macht die Unterschiede deutlich.

Auswählen von Updatesprachen für einen Server, der über Microsoft Update synchronisiert wird

1. Im WSUS-Konfigurationsassistenten:

- Um Updates in allen Sprachen zu erhalten, klicken Sie auf **Updates in allen Sprachen herunterladen, einschließlich neuer Sprachen**.
- Um Updates nur für bestimmte Sprachen zu erhalten, klicken Sie auf **Updates nur in folgenden Sprachen herunterladen**, und wählen Sie dann die gewünschten Sprachen aus.

Auswählen von Updatesprachen für einen Downstreamserver

1. Wenn der Upstreamserver zum Herunterladen von Updatedateien in einer Teilmenge von Sprachen

konfiguriert wurde: Klicken Sie im WSUS-Konfigurationsassistenten auf **Updates nur in folgenden Sprachen herunterladen** (nur die Sprachen, die mit einem Sternchen gekennzeichnet sind, werden vom Upstreamserver unterstützt), und wählen Sie dann die gewünschten Sprachen aus.

NOTE

Dies sollte geschehen, obwohl der Downstreamserver dieselben Sprachen wie der Upstreamserver herunterladen soll.

2. Wenn der Upstreamserver zum Herunterladen von Updatedateien in allen Sprachen konfiguriert wurde: Klicken Sie im WSUS-Konfigurationsassistenten auf **Updates in allen Sprachen herunterladen, die auf dem Upstreamserver unterstützt werden**.

NOTE

Dies sollte geschehen, obwohl der Downstreamserver dieselben Sprachen wie der Upstreamserver herunterladen soll. Diese Einstellung bewirkt, dass der Upstreamserver Updates in allen Sprachen herunterlädt, einschließlich der Sprachen, die ursprünglich nicht für den Upstreamserver konfiguriert wurden. Wenn Sie dem Upstreamserver Sprachen hinzufügen, sollten Sie die neuen Updates auf dessen Replikatserver kopieren.

Das Ändern der Sprachoptionen nur auf dem Upstreamserver könnte dazu führen, dass die Anzahl der Updates, die auf dem zentralen Server genehmigt sind, nicht mit der Anzahl der genehmigten Updates auf den Replikatservern übereinstimmt.

1.5. Planen der WSUS-Computergruppen

WSUS bietet Ihnen die Möglichkeit, Updates gezielt auf Gruppen von Clientcomputern anzuwenden, sodass Sie sicherstellen können, dass bestimmte Computer immer zum geeigneten Zeitpunkt die richtigen Updates erhalten. Wenn z. B. für alle Computer in einer Abteilung (z. B. im Buchhaltungsteam) eine bestimmte Konfiguration verwendet wird, können Sie eine Gruppe für das Team erstellen, entscheiden, welche Updates für die Computer erforderlich sind und wann sie installiert werden sollen, und anschließend mithilfe von WSUS-Berichten die Updates für das Team auswerten.

NOTE

Auf einem im Replikatmodus ausgeführten WSUS-Server können keine Computergruppen erstellt werden. Alle Computergruppen, die für Clientcomputer des Replikatservern erforderlich sind, müssen auf dem WSUS-Stammserver der WSUS-Serverhierarchie erstellt werden. Weitere Informationen zum Replikatmodus finden Sie unter [Verwalten von WSUS-Replikatservern](#) im Betriebshandbuch für WSUS 3.0 SP2.

Computer sind immer der Gruppe **Alle Computer** zugewiesen und bleiben in der Gruppe **Nicht zugewiesene Computer**, bis Sie sie einer anderen Gruppe zuweisen. Computer können mehreren Gruppen angehören.

Computergruppen können in Hierarchien eingerichtet werden (z. B. „Gehaltsabrechnung“ und „Kreditoren“, als untergeordnete Gruppen von „Buchhaltung“). Für eine übergeordnete Gruppe genehmigte Updates werden zusätzlich zur übergeordneten Gruppe automatisch für untergeordnete Gruppen bereitgestellt. Wenn Sie in diesem Beispiel Update1 für die Gruppe „Buchhaltung“ genehmigen, wird das Update auf allen Computern in der Gruppe „Buchhaltung“ und allen Computern in der Gruppe „Kreditoren“ bereitgestellt.

Da Computer mehreren Gruppen zugewiesen werden können, kann es passieren, dass ein Update mehrmals für einen Computer genehmigt wird. Das Update wird jedoch nur einmal bereitgestellt, und alle Konflikte werden vom WSUS-Server aufgelöst. Wenn im obigen Beispiel ComputerA der Gruppe „Gehaltsabrechnung“ und der Gruppe

„Kreditoren“ zugewiesen ist und Update1 für beide Gruppen genehmigt wird, wird es nur einmal bereitgestellt.

Für die Zuweisung von Computern zu Computergruppen stehen zwei Methoden zur Verfügung: serverseitige Zielgruppenadressierung und clientseitige Zielgruppenadressierung. Die Vorgehensweise bei diesen beiden Methoden ist wie folgt:

- **Serverseitige Zielgruppenadressierung:** Sie weisen manuell einen oder mehrere Clientcomputer gleichzeitig mehreren Gruppen zu.
- **Clientseitige Zielgruppenadressierung:** Sie verwenden Gruppenrichtlinien oder bearbeiten die Registrierungseinstellungen auf Clientcomputern so, dass diese Computer sich den zuvor erstellten Computergruppen selbst hinzufügen.

Konfliktauflösung

Vom Server werden die folgenden Regeln zum Lösen von Konflikten und Ermitteln der sich ergebenden Aktion auf Clients angewendet:

1. Priority
2. Installieren/Deinstallieren
3. Stichtag

Priority

Die der Gruppe mit der höchsten Priorität zugewiesenen Aktionen setzen die Aktionen der anderen Gruppen außer Kraft. Je tiefer sich eine Gruppe in der Hierarchie befindet, desto höher ist ihre Priorität. Die Priorität wird nur basierend auf der Tiefe zugewiesen. Alle Verzweigungen besitzen die gleiche Priorität. Beispielsweise hat eine Gruppe, die sich zwei Ebenen unterhalb des Desktops befindet, eine höhere Priorität als eine Gruppe eine Ebene unterhalb des Serverzweigs.

Im folgenden Textbeispiel aus dem Hierarchiebereich der Update Services-Konsole wurden für den WSUS-Server WSUS-01 die Computergruppen „Desktopcomputer“ und „Server“ der Standardgruppe **Alle Computer** hinzugefügt. Die Gruppen „Desktopcomputer“ und „Server“ befinden sich auf derselben Hierarchieebene.

- **Update Services**
 - **WSUS-01**
 - **Updates**
 - **Computer**
 - **Alle Computer**
 - **Nicht zugewiesene Computer**
 - **Desktopcomputer**
 - **Desktops-L1**
 - **Desktops-L2**
 - **Leistungsverlauf für Server**
 - **Servers-L1**
 - **Downstreamserver**
 - **Synchronisierungen**
 - **Berichte**
 - **Optionen**

In diesem Beispiel besitzt die Gruppe zwei Ebenen unterhalb der Verzweigung „Desktopcomputer“ (Desktops-L2) eine höhere Priorität als die Gruppe eine Ebene unterhalb der Verzweigung „Server“ (Servers-L1). Dementsprechend haben bei einem Computer, der sowohl Mitglied der Gruppe %amp;quot;Desktops-L2%amp;quot; als auch der Gruppe %amp;quot;Servers-L1%amp;quot; ist, alle Aktionen für die Gruppe %amp;quot;Desktops-L2%amp;quot; Priorität gegenüber den für die Gruppe %amp;quot;Servers-L1%amp;quot; angegebenen Aktionen.

Priorität der Installation und Deinstallation

Installationsaktionen setzen Deinstallationsaktionen außer Kraft. Erforderliche Installationen haben Vorrang vor optionalen Installationen. (Optionale Installationen sind nur über die API verfügbar, und durch das Ändern einer Genehmigung für ein Update mithilfe der WSUS-Verwaltungskonsole werden alle optionalen Genehmigungen gelöscht.)

Priorität von Terminen

Aktionen, die über einen Stichtag (eine Frist) verfügen, setzen Aktionen ohne Stichtag außer Kraft. Aktionen mit früheren Stichtagen setzen Aktionen mit späteren Stichtagen außer Kraft.

1.6. Planen der WSUS-Leistung

Einige Bereiche müssen vor der Bereitstellung von WSUS sorgfältig geplant werden, um eine optimale Leistung zu erhalten. Die wichtigsten Bereiche sind:

- Netzwerkeinrichtung
- Zurückgestellter Download
- Filter
- Installation
- Große Updatebereitstellungen
- Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)

Netzwerkeinrichtung

Anhand der folgenden Methoden kann die Leistung in WSUS-Netzwerken optimiert werden:

1. Richten Sie WSUS-Netzwerke nicht in einer hierarchischen Topologie, sondern in einer Hub-Spoke-Topologie ein.
2. Verwenden Sie die DNS-Netzwerkmaskenanforderung für Roamingclientcomputer, und konfigurieren Sie Roamingclientcomputer zum Herunterladen von Updates vom lokalen WSUS-Server.

Zurückgestellter Download

Sie können Updates genehmigen und die Updatemetadaten herunterladen, bevor Sie die Updatedateien herunterladen. Diese Methode wird als *zurückgestellter Download* bezeichnet. Wenn Sie Downloads zurückstellen, wird ein Update erst nach seiner Genehmigung heruntergeladen. Da bei dieser Methode die Netzwerkbandbreiten- und Speicherplatznutzung optimiert wird, wird empfohlen, Downloads zurückzustellen.

In einer Hierarchie von WSUS-Servern wird für alle Downstreamserver automatisch die auf dem WSUS-Stammserver festgelegte Einstellung für zurückgestellten Download verwendet. Diese Standardeinstellung kann geändert werden. Sie können z. B. einen Upstreamserver für vollständige, sofortige Synchronisierungen und anschließend einen Downstreamserver zum Zurückstellen der Downloads konfigurieren.

Es wird empfohlen, in einer Hierarchie verbundener WSUS-Server möglichst wenig Serverebenen zu verwenden. Wenn Sie zurückgestellte Downloads aktivieren und ein Downstreamserver ein Update anfordert, das auf dem Upstreamserver nicht genehmigt wurde, wird durch die Anforderung des Downstreamservers ein Download auf dem Upstreamserver erzwungen. Der Downstreamserver lädt das Update dann bei einer nachfolgenden

Synchronisierung herunter. In einer WSUS-Serverhierarchie mit vielen Ebenen, kann es zu Verzögerungen kommen, wenn Updates angefordert, heruntergeladen und dann durch die Serverhierarchie übertragen werden. Wenn Updates lokal gespeichert werden, sind zurückgestellte Downloads standardmäßig aktiviert. Sie können diese Option manuell ändern.

Filter

WSUS bietet Ihnen die Möglichkeit, Updatesynchronisierungen nach Sprache, Produkt und Klassifizierung zu filtern. In einer Hierarchie von WSUS-Servern werden für alle Downstreamserver automatisch die auf dem WSUS-Stammserver ausgewählten Updatefilteroptionen verwendet. Sie können Downloadserver neu konfigurieren, sodass sie nur eine Teilmenge von Sprachen empfangen.

Standardmäßig werden die Produkte Windows und Office aktualisiert, und die Standardklassifizierungen sind „Wichtige Updates“, „Sicherheitsupdates“ und „Definitionsupdates“. Um die Bandbreiten- und Speicherplatznutzung zu reduzieren, sollten Sie nur die Sprachen auswählen, die Sie tatsächlich verwenden.

Installation

Updates bestehen normalerweise aus neuen Versionen von Dateien, die bereits auf dem zu aktualisierenden Computer vorhanden sind. Auf binärer Ebene unterscheiden sich die vorhandenen Dateien möglicherweise nur wenig von den aktualisierten Versionen. Das Feature für Schnellinstallationsdateien ermittelt die genauen Byteunterschiede zwischen Versionen, erstellt und verteilt Updates nur für diese Unterschiede und führt die vorhandene Datei dann mit den aktualisierten Bytes zusammen.

Dieses Feature wird auch als „Deltaübermittlung“ bezeichnet, da es nur das Delta (die Differenz) zwischen zwei Versionen einer Datei herunterlädt. Schnellinstallationsdateien sind größer als die an Clientcomputer verteilten Updates, da sie alle möglichen Versionen jeder zu aktualisierenden Datei enthalten.

Schnellinstallationsdateien können zum Beschränken der Bandbreite im lokalen Netzwerk genutzt werden, da WSUS nur das Delta für eine bestimmte Version einer aktualisierten Komponente übermittelt. Allerdings erfordert dies zusätzliche Bandbreite zwischen dem WSUS-Server, eventuellen Upstream-WSUS-Server und Microsoft Update und zusätzlichen lokalen Speicherplatz. Standardmäßig verwendet WSUS keine Schnellinstallationsdateien.

Nicht alle Updates eignen sich für die Verteilung mittels Schnellinstallationsdateien. Wenn Sie diese Option aktivieren, erhalten Sie Schnellinstallationsdateien für alle Updates. Wenn Sie Updates nicht lokal speichern, entscheidet der Windows Update-Agent, ob die Dateien der Expressinstallation oder die Updatedistribution für das vollständige Update heruntergeladen werden.

Große Updatebereitstellung

Mithilfe der folgenden Methoden können Sie beim Bereitstellen großer Updates (z. B. Service Packs) eine Überlastung des Netzwerks verhindern:

1. Verwenden Sie die Bandbreiteneinschränkung des intelligenten Hintergrundübertragungsdiensts (BITS).
BITS-Bandbreiteneinschränkungen können nach Tageszeit gesteuert werden, sie gelten jedoch für alle Anwendungen, für die BITS verwendet wird. Informationen zur Steuerung der BITS-Drosselung finden Sie unter [Gruppenrichtlinien](#).
2. Verwenden Sie die Bandbreiteneinschränkung der Internetinformationsdienste (Internet Information Services, IIS), um die Einschränkung auf einen oder mehrere Webdienste zu beschränken.
3. Verwenden Sie Computergruppen, um das Rollout zu steuern. Ein Clientcomputer identifiziert sich selbst als Mitglied einer bestimmten Computergruppe, wenn er Informationen an den WSUS-Server sendet. Der WSUS-Server ermittelt anhand dieser Informationen, welche Updates auf dem Computer bereitgestellt werden müssen. Sie können mehrere Computergruppen einrichten und Downloads großer Service Packs nacheinander für eine Teilmenge dieser Gruppen genehmigen.

Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)

WSUS verwendet das BITS-Protokoll für alle Dateiübertragungsaufgaben. Dies beinhaltet Downloads auf Clientcomputer und Serversynchronisierungen. Mithilfe von BITS können Programme Dateien mit wenig Bandbreite herunterladen. BITS verwaltet Dateiübertragungen durch Trennen von Netzwerkverbindungen und Computerneustarts. Weitere Informationen finden Sie unter: [Intelligenter Hintergrundübertragungsdienst \(Background Intelligent Transfer Service, BITS\)](#).

1.7. Planen der Einstellungen für automatische Updates

Sie können einen Stichtag für die Genehmigung von Updates auf dem WSUS-Server festlegen. Der Stichtag führt dazu, dass Clientcomputer das Update zu einem bestimmten Zeitpunkt installieren. Abhängig davon, ob der Stichtag abgelaufen ist, andere zu installierende Updates für den Computer in der Warteschlange vorhanden sind und das Update (oder ein anderes Update in der Warteschlange) einen Neustart erfordert, können jedoch unterschiedliche Situationen auftreten.

Standardmäßig ruft das Feature „Automatische Updates“ alle 22 Stunden (minus einer zufälligen Verschiebung) Updates vom WSUS-Server ab. Wenn neue Updates installiert werden müssen, werden sie heruntergeladen. Die Zeit zwischen den einzelnen Ermittlungszyklen kann auf einen Wert zwischen 1 und 22 Stunden festgelegt werden.

Die Benachrichtigungsoptionen können wie folgt bearbeitet werden:

1. Wenn „Automatische Updates“ zur Benachrichtigung des Benutzers über Updates, die zur Installation bereit sind, konfiguriert ist, wird die Benachrichtigung an das Systemprotokoll und den Infobereich des Clientcomputers gesendet.
2. Klickt ein Benutzer mit entsprechenden Anmeldeinformationen auf das Symbol im Infobereich, zeigt „Automatische Updates“ die zur Installation verfügbaren Updates an. Der Benutzer muss auf **Installieren** klicken, um die Installation zu starten. Erfordert das Update einen Neustart des Computers, wird eine Meldung angezeigt. Wenn ein Neustart erforderlich ist, kann „Automatische Updates“ erst nach dem Neustart des Computers weitere Updates ermitteln.

Wenn „Automatische Updates“ zum Installieren von Updates nach einem festgelegten Zeitplan konfiguriert ist, werden die erforderlichen Updates heruntergeladen und als „Bereit für die Installation“ markiert. „Automatische Updates“ benachrichtigt Benutzer mit entsprechenden Anmeldeinformationen durch ein Symbol im Infobereich, und ein Ereignis wird im Systemprotokoll erfasst.

Zum geplanten Zeitpunkt installiert „Automatische Updates“ das Update und startet den Computer neu (sofern erforderlich) – auch, wenn kein lokaler Administrator angemeldet ist. Falls ein lokaler Administrator angemeldet ist und der Computer neu gestartet werden muss, zeigt „Automatische Updates“ eine Warnung und einen Countdown für den Neustart an. Andernfalls erfolgt die Installation im Hintergrund.

Wenn der Computer neu gestartet werden muss und ein Benutzer angemeldet ist, wird ein ähnliches Countdowndialogfeld angezeigt, um den Benutzer über den bevorstehenden Neustart zu informieren. Die Einstellungen für Computerneustarts können mit dem Feature „Gruppenrichtlinie“ bearbeitet werden.

Nachdem die neuen Updates heruntergeladen wurden, ruft „Automatische Updates“ die Liste genehmigter Pakete vom WSUS-Server ab, um zu überprüfen, ob die heruntergeladenen Pakete noch gültig und genehmigt sind. Entfernt ein WSUS-Administrator Updates aus der Liste genehmigter Updates, während Updates von „Automatische Updates“ heruntergeladen werden, werden somit nur die Updates installiert, die noch immer genehmigt sind.

Schritt 1: Installieren der WSUS-Serverrolle

24.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Der nächste Schritt zur Bereitstellung des WSUS-Servers ist die Installation der WSUS-Serverrolle. Anhand des folgenden Verfahrens wird die Installation der WSUS-Serverrolle mithilfe von Server-Manager beschrieben.

IMPORTANT

In diesem Installationsverfahren wird nur die Installation von WSUS mit der internen Windows-Datenbank (WID) behandelt. Die Verfahren zum Installieren von WSUS mithilfe von Microsoft SQL Server sind in [diesem Artikel](#) dokumentiert.

So installieren Sie die WSUS-Serverrolle

1. Melden Sie sich an dem Server, auf dem Sie die WSUS-Serverrolle installieren möchten, mit einem Konto an, das Mitglied der Gruppe "Lokale Administratoren" ist.
2. Klicken Sie im **Server-Manager** auf **Verwalten** und dann auf **Rollen und Features hinzufügen**.
3. Klicken Sie auf der Seite **Vorbereitung** auf **Weiter**.
4. Stellen Sie sicher, dass die Option **Rollenbasierte oder featurebasierte Installation** auf der Seite **Installationstyp auswählen** ausgewählt ist, und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Zielserver auswählen** aus, wo sich der Server befindet (in einem Serverpool oder auf einer virtuellen Festplatte). Wählen Sie nach der Auswahl des Orts den Server aus, auf dem Sie die WSUS-Serverrolle installieren möchten, und klicken Sie dann auf **Weiter**.
6. Wählen Sie **Windows Server Update Services** auf der Seite **Serverrollen auswählen** aus. Sollen für **Windows Server Update Services erforderliche Features hinzugefügt werden?** wird geöffnet. Klicken Sie auf **Features hinzufügen** und dann auf **Weiter**.
7. Behalten Sie auf der Seite **Features auswählen** die Standardeinstellungen bei, und klicken Sie dann auf **Weiter**.

IMPORTANT

Für WSUS ist nur die Standardkonfiguration der Webserverrolle erforderlich. Wenn Sie beim Einrichten von WSUS aufgefordert werden, die Webserverrolle weiter zu konfigurieren, können Sie ohne Bedenken die Standardeinstellungen akzeptieren und die WSUS-Einrichtung fortsetzen.

8. Klicken Sie auf der Seite **Windows Server Update Services** auf **Weiter**.
9. Behalten Sie auf der Seite **Rollendienste auswählen** die Standardauswahl bei, und klicken Sie auf **Weiter**.

TIP

Sie müssen einen Datenbanktyp auswählen. Wenn die Datenbankoptionen alle deaktiviert (nicht ausgewählt) sind, treten bei Aufgaben im Anschluss an die Installation Fehler auf.

10. Geben Sie auf der Seite **Auswahl des Inhaltsspeicherorts** einen gültigen Speicherort zum Speichern der Updates ein. Sie können z. B. einen Ordner mit dem Namen "WSUS_database" im Stammverzeichnis von Laufwerks K: speziell für diesen Zweck erstellen und k:\WSUS_database als gültigen Speicherort eingeben.
11. Klicken Sie auf **Weiter**. Die Seite **Webserverrolle (IIS)** wird geöffnet. Überprüfen Sie die Informationen, und klicken Sie dann auf **Weiter**. Behalten Sie die Standardeinstellungen in **select the role services to install for Web Server (IIS)** (Zu installierende Rollendienste für Webserver (IIS) auswählen) bei, und klicken Sie dann auf **Weiter**.
12. Überprüfen Sie die auf der Seite **Installationsauswahl** bestätigten ausgewählten Optionen, und klicken Sie dann auf **Installieren**. Der WSUS-Installations-Assistent ausgeführt wird. Dieser Vorgang kann einige Minuten dauern.
13. Klicken Sie nach Abschluss der WSUS-Installation im Fenster "Zusammenfassung" im Bereich **Installationsstatus** auf **Nachinstallationsaufgaben starten**. Der Text ändert sich und fordert Folgendes an: **Der Server wird konfiguriert. Bitte warten**. Wenn der Vorgang abgeschlossen ist, ändert sich der Text in: **Die Konfiguration wurde erfolgreich abgeschlossen**. Klicken Sie auf **Schließen**.
14. Überprüfen Sie, ob in **Server-Manager** eine Benachrichtigung erscheint, die Sie über einen erforderlichen Neustart informiert. Dies kann je nach installierter Serverrolle variieren. Falls ein Neustart erforderlich ist, starten Sie den Server neu, um die Installation abzuschließen.

IMPORTANT

Hiermit ist der Installationsvorgang abgeschlossen, jedoch müssen Sie mit [Schritt 2: Konfigurieren von WSUS](#) fortfahren, damit WSUS voll funktionsfähig ist.

Schritt 2: Konfigurieren von WSUS

24.04.2020 • 44 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Nachdem Sie die WSUS-Serverrolle auf dem Server installiert haben, müssen Sie sie korrekt konfigurieren. In der folgenden Prüfliste sind die Schritte für die Erstkonfiguration des WSUS-Servers zusammengefasst.

AUFGABE	BESCHREIBUNG
2.1. Konfigurieren der Netzwerkverbindungen	Konfigurieren Sie das Clusternetzwerk mithilfe des Netzwerkkonfigurations-Assistenten.
2.2. Konfigurieren von WSUS mit dem WSUS-Konfigurations-Assistenten	Verwenden Sie den WSUS-Konfigurations-Assistenten, um die WSUS-Basiskonfiguration auszuführen.
2.3. Konfigurieren von WSUS-Computergruppen	Erstellen Sie Computergruppen in der WSUS-Verwaltungskonsole zum Verwalten von Updates in Ihrer Organisation.
2.4. Konfigurieren von Clientupdates	Geben Sie an, wie und wann automatische Updates auf Clientcomputern angewendet werden.
2.5. Schützen von WSUS mit dem Secure Sockets Layer-Protokoll	Konfigurieren Sie das Secure Sockets Layer (SSL)-Protokoll zum Schutz von Windows Server Update Services (WSUS).

2.1. Konfigurieren der Netzwerkverbindungen

Bevor Sie mit der Konfiguration beginnen, müssen Sie sich die folgenden Fragen beantworten:

1. Ist die Firewall des Servers so konfiguriert, dass Clients auf den Server zugreifen können?
2. Kann dieser Computer eine Verbindung mit dem Upstreamserver herstellen (z. B. dem Server, der zum Herunterladen von Updates von Microsoft Update verwendet wird)?
3. Kennen Sie den Namen des Proxyservers und die Benutzeranmeldeinformationen für den Proxyserver, falls Sie sie benötigen?

In der Standardkonfiguration ruft WSUS Updates von Microsoft Update ab. Wenn du über einen Proxyserver im Netzwerk verfügst, kannst du WSUS für die Verwendung des Proxyservers konfigurieren. Falls eine Unternehmensfirewall zwischen WSUS und dem Internet vorhanden ist, musst du sie ggf. konfigurieren, um sicherzustellen, dass WSUS Updates abrufen kann.

TIP

Obwohl Internetkonnektivität erforderlich ist, um Updates von Microsoft Update herunterzuladen, bietet WSUS die Möglichkeit, Updates in Netzwerke zu importieren, die nicht mit dem Internet verbunden sind.

Wenn Sie die Antworten auf diese Fragen kennen, können Sie mit der Konfiguration der folgenden WSUS-Netzwerkeinstellungen beginnen:

- **Updates** Geben Sie an, wie dieser Server Updates abruft (von Microsoft Update oder von einem anderen WSUS-Server).
- **Proxy** Wenn WSUS einen Proxyserver für den Internetzugriff verwenden muss, musst du Proxeinstellungen im WSUS-Server konfigurieren.
- **Firewall** Wenn sich WSUS hinter einer Unternehmensfirewall befindet, müssen einige zusätzliche Schritte auf dem Edgegerät ausgeführt werden, um den WSUS-Datenverkehr auf richtige Weise zuzulassen.

2.1.1. Verbindung zwischen WSUS-Server und Internet

Falls eine Unternehmensfirewall zwischen WSUS und dem Internet vorhanden ist, müssen Sie sie ggf. konfigurieren, um sicherzustellen, dass WSUS Updates abrufen kann. Der WSUS-Server verwendet den Port 443 für das HTTPS-Protokoll, um Updates von Microsoft Update herunterzuladen. Die meisten Unternehmensfirewalls lassen diese Art von Datenverkehr zu. In einigen Unternehmen ist der Zugriff der Server aber aufgrund der unternehmensspezifischen Sicherheitsrichtlinien eingeschränkt. Falls dein Unternehmen den Zugriff einschränkt, benötigst du die Autorisierung zum Zulassen des Internetzugriffs von WSUS auf die folgenden URLs:

- <http://windowsupdate.microsoft.com>
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- <http://download.windowsupdate.com>
- <https://download.microsoft.com>
- http://*.download.windowsupdate.com
- <http://wustat.windows.com>
- <http://ntservicepack.microsoft.com>
- <http://go.microsoft.com>
- <http://dl.delivery.mp.microsoft.com>
- <https://dl.delivery.mp.microsoft.com>

IMPORTANT

Informationen zu einem Szenario, bei dem über WSUS aufgrund von Firewallkonfigurationen keine Updates abgerufen werden können, findest du in der Microsoft Knowledge Base unter [Artikel 885819](#).

Im folgenden Abschnitt wird beschrieben, wie eine Unternehmensfirewall zwischen WSUS und dem Internet konfiguriert wird. Da WSUS den gesamten Netzwerdatenverkehr initiiert, ist es nicht erforderlich, die Windows-Firewall auf dem WSUS-Server zu konfigurieren. Obwohl die Verbindung zwischen Microsoft Update und WSUS erfordert, dass die Ports 80 und 443 geöffnet sind, können Sie mehrere WSUS-Server zur Synchronisierung mit einem benutzerdefinierten Port konfigurieren.

2.1.2. Verbindung zwischen WSUS-Servern

Upstream- und Downstream-WSUS-Server werden auf dem Port synchronisiert, der vom WSUS-Administrator konfiguriert wurde. Diese Ports sind standardmäßig folgendermaßen konfiguriert:

- Bei WSUS 3.2 und früher: Port 80 für HTTP und 443 für HTTPS
- Unter WSUS 6.2 und höher (mindestens Windows Server 2012) werden Port 8530 für HTTP und 8531 für HTTPS verwendet.

Die Firewall auf dem WSUS-Server muss für das Zulassen von eingehendem Datenverkehr auf diesen Ports konfiguriert werden.

2.1.3. Verbindung zwischen Clients (Windows Update-Agent) und WSUS-Servern

Die Überwachungsschnittstellen und Ports werden auf den IIS-Websites für WSUS und in allen Gruppenrichtlinieneinstellungen zur Konfiguration von Clientcomputern konfiguriert. Die Standardports sind identisch mit denen im vorherigen Abschnitt **Verbindung zwischen WSUS-Servern**, und die Firewall auf dem WSUS-Server muss ebenfalls für eingehenden Datenverkehr über diese Ports konfiguriert werden.

Konfigurieren der Proxyserver

Wenn das Unternehmensnetzwerk Proxyserver verwendet, müssen die Proxyserver die Protokolle HTTP und SSL unterstützen und Standardauthentifizierung oder Windows-Authentifizierung verwenden. Diese Anforderungen können mithilfe einer der folgenden Konfigurationen erfüllt werden:

1. Ein einzelner Proxyserver, der zwei Protokollkanäle unterstützt. In diesem Fall legen Sie einen Kanal für die Verwendung von HTTP und den anderen Kanal für HTTPS fest.

NOTE

Sie können einen Proxyserver einrichten, der beide Protokolle für WSUS während der Installation der WSUS-Serversoftware verarbeitet.

2. Zwei Proxyserver, von denen jeder ein einzelnes Protokoll unterstützt. In diesem Fall ist ein Proxyserver für die Verwendung von HTTP und der andere Proxyserver zur Verwendung von HTTPS konfiguriert.

Verwenden Sie zum Einrichten von zwei Proxyservern, von denen jeder ein Protokoll für WSUS behandelt, das folgende Verfahren:

Einrichten von WSUS zur Verwendung der beiden Proxyserver

1. Melden Sie sich bei dem Computer, der als WSUS-Server verwendet wird, mit einem Konto an, das Mitglied der lokalen Administratorgruppe ist.
2. Installieren Sie die WSUS-Serverrolle. Geben Sie während der Ausführung des WSUS-Konfigurations-Assistenten (im nächsten Abschnitt erläutert) keinen Proxyserver an.
3. Öffnen Sie eine Eingabeaufforderung (Cmd.exe) als Administrator. Wählen Sie zum Öffnen einer Eingabeaufforderung als Administrator **Start** aus. Gib in **Suche starten** den Suchbegriff **Eingabeaufforderung** ein. Klicke am oberen Rand des Menüs „Start“ mit der rechten Maustaste auf **Eingabeaufforderung**, und klicke dann auf **Als Administrator ausführen**. Gehe wie folgt vor, wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird: Gib die entsprechenden Anmeldeinformationen ein (falls angefordert), vergewissere dich, dass die gewünschte Aktion angezeigt wird, und klicke dann auf **Weiter**.
4. Wechsele im Eingabeaufforderungsfenster zum Ordner „C:\Programme\Update Services\Tools“. Gib den folgenden Befehl ein:

wsusutil ConfigureSSlproxy [] -enable, wobei:
 - a. Proxyserver für den Namen des Proxyservers steht, der HTTPS unterstützt.
 - b. Proxyport die Portnummer des Proxyservers ist.

5. Schließe das Eingabeaufforderungsfenster.

Führen Sie das folgende Verfahren aus, um den Proxyserver hinzuzufügen, der das HTTP-Protokoll für die WSUS-Konfiguration verwendet:

Hinzufügen eines Proxyservers, der das HTTP-Protokoll verwendet

1. Öffnen Sie die WSUS-Verwaltungskonsole.
2. Erweitern Sie im linken Bereich den Servernamen, und klicken Sie dann auf **Optionen**.
3. Klicken Sie im Bereich **Optionen** auf **Updatequelle und Proxyserver** und anschließend auf die Registerkarte **Proxyserver**.
4. Verwenden Sie die folgenden Optionen, um die vorhandene Proxyserverkonfiguration zu ändern:

Ändern oder Hinzufügen eines Proxyservers zur WSUS-Konfiguration

- a. Aktivieren Sie das Kontrollkästchen für **Proxyserver für die Synchronisierung verwenden**.
- b. Geben Sie im Textfeld **Proxyservername** den Namen des Proxyservers ein.
- c. Geben Sie im Textfeld **Proxyportnummer** die Portnummer des Proxyservers ein. Die Standardportnummer ist 80.
- d. Wenn der Proxyserver erfordert, dass du ein bestimmtes Benutzerkonto verwendest, aktivierst du das Kontrollkästchen **Benutzeranmeldeinformationen für die Verbindungsherstellung mit dem Proxyserver verwenden**. Gib den erforderlichen Benutzernamen, die Domäne und das Kennwort in die entsprechenden Textfelder ein.
- e. Falls der Proxyserver Standardauthentifizierung unterstützt, aktivieren Sie das Kontrollkästchen **Standardauthentifizierung zulassen (Kennwort wird in Klartext gesendet)**.
- f. Klicken Sie auf **OK**.

Entfernen eines Proxyservers aus der WSUS-Konfiguration

- a. Um einen Proxyserver aus der WSUS-Konfiguration zu entfernen, deaktivieren Sie das Kontrollkästchen **Proxyserver für die Synchronisierung verwenden**.
- b. Klicken Sie auf **OK**.

2.2. Konfigurieren von WSUS mit dem WSUS-Konfigurations-Assistenten

Dieses Verfahren setzt voraus, dass Sie den WSUS-Konfigurations-Assistenten verwenden, der beim erstmaligen Starten der WSUS-Verwaltungskonsole angezeigt wird. Weiter unten in diesem Thema wird beschrieben, wie Sie diese Konfigurationen auf der Seite **Optionen** ausführen.

So konfigurieren Sie WSUS

1. Klicken Sie im Navigationsbereich des Server-Managers auf **Dashboard**, auf **Tools** und dann auf **Windows Server Update Services**.

NOTE

Klicke auf **Ausführen**, wenn das Dialogfeld **WSUS-Installation abschließen** angezeigt wird. Klicke im Dialogfeld **WSUS-Installation abschließen** auf **Schließen**, wenn die Installation erfolgreich abgeschlossen wurde.

2. Der WSUS-Konfigurations-Assistent wird geöffnet. Lesen Sie die Informationen auf der Seite **Vorbemerkungen**, und klicken Sie dann auf **Weiter**.
3. Lesen Sie die Anweisungen auf der Seite **Am Programm zur Verbesserung von Microsoft Update teilnehmen**, und entscheiden Sie, ob Sie am Programm teilnehmen möchten. Wenn Sie am Programm

teilnehmen möchten. Behalte die Standardauswahl bei, oder deaktiviere das Kontrollkästchen, und klicke dann auf **Weiter**.

4. Auf der Seite **Upstreamserver auswählen** stehen Ihnen zwei Optionen zur Verfügung:

- a. Updates mit Microsoft Update synchronisieren
- b. Von einem anderen Windows Server Update Services-Server synchronisieren
 - Wenn du dich für die Synchronisierung mit einem anderen WSUS-Server entscheidest, gibst du den Servernamen und den Port an, über den der Server mit dem Upstreamserver kommuniziert.
 - Wenn Sie SSL verwenden möchten, aktivieren Sie das Kontrollkästchen **SSL beim Synchronisieren der Updateinformationen verwenden**. Die Server verwenden den Port 443 für die Synchronisierung. (Stellen Sie sicher, dass dieser Server und der Upstreamserver SSL unterstützen).
 - Falls es sich um einen Replikatserver handelt, aktivierst du das Kontrollkästchen **Dies ist ein Replikat des Upstreamservers**.

5. Nachdem Sie die entsprechenden Optionen für Ihre Bereitstellung ausgewählt haben, klicken Sie auf **Weiter**, um fortzufahren.

6. Aktivieren Sie auf der Seite **Proxyserver angeben** das Kontrollkästchen **Proxyserver für die Synchronisierung verwenden**, und geben Sie dann den Namen des Proxyservers und die Portnummer (standardmäßig Port 80) in die entsprechenden Felder ein.

IMPORTANT

Dieser Schritt muss ausgeführt werden, wenn WSUS einen Proxyserver für den Internetzugriff benötigt.

7. Wenn für die Verbindung mit dem Proxyserver bestimmte Benutzeranmeldeinformationen verwendet werden sollen, aktivierst du das Kontrollkästchen **Benutzeranmeldeinformationen verwenden, um Verbindung mit dem Proxyserver herzustellen**. Gib anschließend den Benutzernamen, die Domäne und das Kennwort des Benutzers in die entsprechenden Felder ein. Falls du für den Benutzer, der die Verbindung mit dem Proxyserver herstellt, die Standardauthentifizierung aktivieren möchtest, aktivierst du das Kontrollkästchen **Standardauthentifizierung zulassen (Kennwort wird in Klartext gesendet)**.

8. Klicken Sie auf **Weiter**. Klicke auf der Seite **Mit Upstreamserver verbinden** auf **Verbindung starten**.

9. Wenn die Verbindung hergestellt wurde, klicken Sie auf **Weiter**, um fortzufahren.

10. Auf der Seite **Sprachen auswählen** kannst du die Sprachen auswählen, für die WSUS Updates empfängt (alle Sprachen oder eine Teilmenge von Sprachen). Wenn du eine Teilmenge von Sprachen auswählst, sparst du Speicherplatz. Es ist aber WICHTIG, alle Sprachen auszuwählen, die für sämtliche Clients des WSUS-Servers erforderlich sind. Falls du nur für bestimmte Sprachen Updates abrufen möchtest, aktivierst du **Updates nur in folgenden Sprachen herunterladen**. Wähle anschließend die gewünschten Sprachen aus. Andernfalls kannst du die Standardeinstellung übernehmen.

WARNING

Wenn Sie die Option **Updates nur in folgenden Sprachen herunterladen** auswählen und ein WSUS-Downstreamserver mit dem Server verbunden ist, werden für den Downstreamserver ebenfalls nur die ausgewählten Sprachen verwendet.

11. Nachdem Sie die entsprechenden Sprachoptionen für Ihre Bereitstellung ausgewählt haben, klicken Sie auf

Weiter , um fortzufahren.

12. Auf der Seite **Produkte auswählen** können Sie die Produkte angeben, für die Sie Updates herunterladen möchten. Wähle Produktkategorien wie Windows oder bestimmte Produkte wie Windows Server 2008 aus. Durch die Auswahl einer Produktkategorie werden alle Produkte in der Kategorie ausgewählt.
13. Wähle die entsprechenden Produktoptionen für deine Bereitstellung aus, und klicke dann auf **Weiter**.
14. Wählen Sie auf der Seite **Klassifizierungen auswählen** die gewünschten Updateklassifizierungen aus. Sie können alle Klassifizierungen oder eine Teilmenge auswählen. Klicken Sie anschließend auf **Weiter**.
15. Auf der Seite **Synchronisierungszeitplan festlegen** können Sie auswählen, ob die Synchronisierung manuell oder automatisch ausgeführt werden soll.
 - Bei Auswahl von **Manuell synchronisieren** musst du die Synchronisierung über die WSUS-Verwaltungskonsole starten.
 - Bei Auswahl von **Automatisch synchronisieren** führt der WSUS-Server die Synchronisierung in festgelegten Intervallen aus.

Legen Sie die Zeit für **Erste Synchronisierung** fest, und geben Sie die Anzahl von **Synchronisierungen pro Tag** an, die dieser Server ausführen soll. Wenn Sie z. B. vier Synchronisierungen pro Tag mit der ersten Synchronisierung um 3:00 Uhr festlegen, finden um 3:00 Uhr, 9:00 Uhr, 15:00 Uhr und 21:00 Uhr Synchronisierungen statt

16. Nachdem Sie die entsprechenden Synchronisierungsoptionen für Ihre Bereitstellung ausgewählt haben, klicken Sie auf **Weiter** , um fortzufahren.
17. Auf der Seite **Fertig gestellt** haben Sie die Möglichkeit, die Synchronisierung direkt zu starten, indem Sie das Kontrollkästchen **Erstsynchronisierung starten** aktivieren. Wenn du diese Option nicht auswählst, musst du die Erstsynchronisierung über die WSUS-Verwaltungskonsole ausführen. Klicken Sie auf **Weiter** , wenn Sie mehr über zusätzliche Einstellungen erfahren möchten, oder auf **Fertig stellen** , um den Assistenten zu beenden und die WSUS-Erstkonfiguration abzuschließen.
18. Nach dem Klicken auf **Fertig stellen** wird die WSUS-Verwaltungskonsole angezeigt.

Damit ist die grundlegende WSUS-Konfiguration abgeschlossen. Lesen Sie jetzt die nächsten Abschnitte, um mehr über das Ändern der Einstellungen mithilfe der WSUS-Verwaltungskonsole zu erfahren.

2.3. Konfigurieren von WSUS-Computergruppen

Computergruppen sind ein WICHTIGER Bestandteil von WSUS-Bereitstellungen (Windows Server Update Services). Mithilfe von Computergruppen können Sie Updates testen und gezielt für bestimmte Computer anwenden. Es gibt die folgenden zwei Standardcomputergruppen: „Alle Computer“ und „Nicht zugewiesene Computer“. Standardmäßig fügt der WSUS-Server jeden Clientcomputer bei der ersten Verbindungsherstellung mit dem Server einer dieser beiden Gruppen hinzu.

Sie können beliebig viele benutzerdefinierte Computergruppen erstellen, um Updates in Ihrer Organisation zu verwalten. Es wird empfohlen, mindestens eine Computergruppe zu erstellen, mit der Updates getestet werden können, bevor sie auf anderen Computern in der Organisation bereitgestellt werden.

Gehen Sie wie im Folgenden beschrieben vor, um eine neue Gruppe zu erstellen und ihr einen Computer zuzuweisen:

So erstellen Sie eine Computergruppe

1. Erweitere in der WSUS-Verwaltungskonsole unter **Update Services** den Eintrag **Computer**, klicke mit der rechten Maustaste auf **Alle Computer**, und klicke dann auf **Computergruppe hinzufügen**.
2. Gib im Dialogfeld **Computergruppe hinzufügen** den Namen der neuen Gruppe in das Feld **Name** ein,

und klicke dann auf **Hinzufügen**.

3. Klicke auf **Computer**, und wähle anschließend die Computer aus, die du der neuen Gruppe zuweisen möchtest.
4. Klicke mit der rechten Maustaste auf die im vorherigen Schritt ausgewählten Computernamen, und klicke dann auf **Mitgliedschaft ändern**.
5. Wähle im Dialogfeld **Gruppenmitgliedschaft für Computer** festlegen die erstellte Testgruppe aus, und klicke dann auf **OK**.

2.4. Konfigurieren von Clientupdates

Beim WSUS-Setup wird IIS automatisch so konfiguriert, dass die aktuelle Version von „Automatische Updates“ an jeden Clientcomputer verteilt wird, der eine Verbindung mit dem WSUS-Server herstellt. Die für „Automatische Updates“ am besten geeignete Konfiguration hängt von der Netzwerkumgebung ab.

- In einer Umgebung, in der der Active Directory-Verzeichnisdienst verwendet wird, kannst du ein vorhandenes domänenbasiertes Gruppenrichtlinienobjekt (Group Policy Object, GPO) verwenden oder ein neues GPO erstellen.
- In einer Umgebung ohne Active Directory konfigurierst du „Automatische Updates“ mit dem Editor für lokale Gruppenrichtlinien und verweist anschließend auf den Clientcomputern auf den WSUS-Server.

IMPORTANT

Die folgenden Verfahren gelten für Netzwerke, in denen Active Directory ausgeführt wird. Zudem wird vorausgesetzt, dass Sie mit dem Feature „Gruppenrichtlinie“ vertraut sind und es zum Verwalten des Netzwerks verwenden.

Verwenden Sie die folgenden Verfahren, um „Automatische Updates“ für Clientcomputer zu konfigurieren:

- [Schritt 4: Konfigurieren von Gruppenrichtlinien für automatische Updates](#)
- [2.3. Konfigurieren von Computergruppen](#) in diesem Thema

Konfigurieren von „Automatische Updates“ in „Gruppenrichtlinie“;

Wenn du Active Directory in deinem Netzwerk eingerichtet hast, kannst du mehrere Computer gleichzeitig konfigurieren, indem du sie in ein GPO einfügst und dieses GPO anschließend mit WSUS-Einstellungen konfigurierst. Es wird empfohlen, ein neues GPO zu erstellen, das nur WSUS-Einstellungen enthält.

Verknüpfen Sie dieses WSUS-GPO mit einem für die Umgebung geeigneten Active Directory-Container. In einer einfachen Umgebung reicht es u. U. aus, ein WSUS-GPO mit der Domäne zu verknüpfen. In einer komplexeren Umgebung müssen Sie möglicherweise mehrere WSUS-GPOs mit mehreren Organisationseinheiten (Organizational Unit, OU) verknüpfen, sodass Sie unterschiedliche WSUS-Richtlinieneinstellungen für verschiedene Computertypen anwenden können.

So aktivieren Sie WSUS über ein Domänen-GPO

1. Navigiere in der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) zu dem GPO, in dem du WSUS konfigurieren möchtest, und klicke dann auf **Bearbeiten**.
2. Erweitere in der GPMC nacheinander **Computerkonfiguration**, **Richtlinien**, **Administrative Vorlagen** und **Windows-Komponenten**, und klicke dann auf **Windows Update**.
3. Doppelklicken Sie im Detailbereich auf **Automatische Updates konfigurieren**. Die Richtlinie

Automatische Updates konfigurieren wird geöffnet.

4. Klicken Sie auf **Aktiviert**, und wählen Sie anschließend eine der folgenden Optionen unter der Einstellung **Automatische Updates konfigurieren** aus:

- **Vor Herunterladen und Installation benachrichtigen.** Bei Auswahl dieser Option wird ein angemeldeter Administrator vor dem Herunterladen und Installieren der Updates benachrichtigt.
- **Autom. Herunterladen, aber vor Installation benachrichtigen.** Bei Auswahl dieser Option wird der Download von Updates automatisch gestartet, und anschließend wird ein angemeldeter Administrator benachrichtigt, bevor die Updates installiert werden. Diese Option ist standardmäßig ausgewählt.
- **Autom. Herunterladen und laut Zeitplan installieren.** Bei Auswahl dieser Option wird der Download von Updates automatisch gestartet, und anschließend werden die Updates zu dem von Ihnen angegebenen Zeitpunkt installiert.
- **Lokalen Administrator ermöglichen, Einstellung auszuwählen.** Bei Auswahl dieser Option können lokale Administratoren den Bereich **Automatische Updates** in der Systemsteuerung verwenden, um eine Konfigurationsoption auszuwählen. Sie können z. B. einen geplanten Installationszeitpunkt auswählen. Lokale Administratoren können **Automatische Updates** nicht deaktivieren.

5. Wähle **Clientseitige Zielzuordnung aktivieren** und dann **Aktiviert** aus. Gib anschließend den Namen der WSUS-Computergruppe, der du diesen Computer hinzufügen möchtest, im Feld **Zielgruppenname für diesen Computer** ein.

NOTE

Durch die Option **Clientseitige Zielzuordnung aktivieren** können Clientcomputer sich selbst Zielcomputergruppen auf dem WSUS-Server hinzufügen, wenn automatische Updates auf einen WSUS-Server umgeleitet werden. Falls der Status „Aktiviert“ lautet, identifiziert sich dieser Computer selbst als Mitglied einer bestimmten Computergruppe, wenn er Informationen an den WSUS-Server sendet, mit denen ermittelt wird, welche Updates auf diesem Computer bereitgestellt werden. Diese Einstellung zeigt dem WSUS-Server an, welche Gruppe der Clientcomputer verwendet. Sie müssen die Gruppe auf dem WSUS-Server erstellen und ihr Domänenmitgliedscomputer hinzufügen.

6. Klicken Sie auf **OK**, um die Richtlinie **Clientseitige Zielzuordnung aktivieren** zu schließen und zum Detailfenster „Windows Update“ zurückzukehren.

7. Klicken Sie auf **OK**, um die Richtlinie **Automatische Updates konfigurieren** zu schließen und zum Detailfenster „Windows Update“ zurückzukehren.

8. Doppelklicken Sie im Detailbereich **Windows Update auf Internen Pfad für den Microsoft Updatedienst angeben**.

9. Klicken Sie auf **Aktiviert**, und geben Sie dann die URL des gleichen WSUS-Servers in die Felder **Interner Updatedienst zum Ermitteln von Updates** und **Intranetserver für die Statistik** ein. Gib beispielsweise <http://servername> in beide Felder ein (wobei *servername* der Name des WSUS-Servers ist).

WARNING

Beim Eingeben der Intranetadresse des WSUS-Servers muss der zu verwendende Port angegeben werden. Standardmäßig verwendet WSUS den Port 8530 für HTTP und den Port 8531 für HTTPS. Wenn du HTTP verwendest, musst du beispielsweise <http://servername:8530> eingeben.

10. Klicken Sie auf OK.

Nach dem Einrichten eines Clientcomputers dauert es einige Minuten, bis der Computer auf der Seite **Computer** in der WSUS-Verwaltungskonsole angezeigt wird. Bei Clientcomputern, die mit einem domänenbasierten GPO konfiguriert werden, kann es bis zu 20 Minuten dauern, bis die neuen Richtlinieneinstellungen von der Gruppenrichtlinie auf den Clientcomputer angewendet werden. Standardmäßig wird die Gruppenrichtlinienaktualisierung alle 90 Minuten mit einer Verschiebung von 0 bis 30 Minuten im Hintergrund ausgeführt. Wenn du die Gruppenrichtlinienaktualisierung früher ausführen möchtest, kannst du auf dem Clientcomputer ein Eingabeaufforderungsfenster öffnen und „gpupdate /force“ eingeben.

Bei Clientcomputern, die mit dem Editor für lokale Gruppenrichtlinien konfiguriert werden, wird das GPO direkt angewendet, und die Aktualisierung dauert ca. 20 Minuten. Wenn du die Ermittlung manuell startest, musst du nicht 20 Minuten warten, bis der Clientcomputer eine Verbindung mit WSUS herstellt.

Da das Warten auf den Start der Ermittlung zeitaufwändig sein kann, können Sie ggf. das folgende Verfahren verwenden, um die Ermittlung sofort zu initiieren.

So starten Sie die WSUS-Ermittlung

1. Öffne auf dem Clientcomputer ein Eingabeaufforderungsfenster mit erhöhten Rechten.
2. Gib „wuauctl.exe /detectnow“ ein, und drücke dann die EINGABETASTE.

2.5. Schützen von WSUS mit dem Secure Sockets Layer-Protokoll

Sie können das Secure Sockets Layer (SSL)-Protokoll zum Sichern der WSUS-Bereitstellung verwenden. SSL wird von WSUS zur Authentifizierung von Clientcomputern und WSUS-Downstreamservern gegenüber dem WSUS-Server verwendet. SSL wird von WSUS auch zum Verschlüsseln von Metadaten für Updates verwendet.

IMPORTANT

Clients und Downstreamserver, die für die Verwendung von Transport Layer Security (TLS) oder HTTPS konfiguriert werden, müssen auch zur Verwendung eines vollqualifizierten Domänenamens (FQDN) für WSUS-Upstreamserver konfiguriert werden.

SSL wird von WSUS nur für Metadaten und nicht für Updatedateien verwendet. Auf diese Weise verteilt auch Microsoft Update die Updates. Microsoft reduziert das Risiko beim Senden von Updatedateien über einen unverschlüsselten Kanal, indem jedes Update signiert wird. Darüber hinaus wird ein Hashwert berechnet und zusammen mit den Metadaten für jedes Update gesendet. Wenn ein Update heruntergeladen wird, überprüft WSUS die digitale Signatur und den Hashwert. Wenn das Update geändert wurde, wird es nicht installiert.

Einschränkungen von WSUS-SSL-Bereitstellungen

Berücksichtigen Sie bei Verwendung von SSL zum Sichern der WSUS-Bereitstellung die folgenden Einschränkungen:

1. Die Verwendung von SSL erhöht die Auslastung des Servers. Sie sollten aufgrund des Aufwands zur Verschlüsselung aller Metadaten, die über das Netzwerk gesendet wird, von einem Leistungsverlust von 10 % ausgehen.
2. Wenn Sie WSUS mit einer SQL Server-Remotedatenbank verwenden, wird die Verbindung zwischen dem WSUS-Server und dem Datenbankserver nicht durch SSL gesichert. Wenn die Verbindung mit der Datenbank gesichert werden muss, sollten Sie folgende Empfehlungen berücksichtigen:
 - Verschiebe die WSUS-Datenbank auf den WSUS-Server.
 - Verschiebe den Remotedatenbankserver und den WSUS-Server in ein privates Netzwerk.
 - Stelle Internet Protocol Security (IPsec) bereit, um den Netzwerkverkehr zu schützen. Weitere

Informationen zu IPsec finden Sie unter [Creating and Using IPsec Policies](#).

Konfigurieren von SSL auf dem WSUS-Server

WSUS erfordert zwei Ports für SSL: einen Port, der HTTPS für das Senden verschlüsselter Metadaten verwendet, und einen Port, der HTTP für das Senden der Updates verwendet. Beachten Sie beim Konfigurieren von WSUS für SSL Folgendes:

- Sie können nicht die gesamte WSUS-Website so konfigurieren, dass SSL erforderlich ist, da der gesamte Datenverkehr an die WSUS-Website verschlüsselt werden müsste. WSUS verschlüsselt nur Updatemetadaten. Wenn ein Computer versucht, Updatedateien auf dem HTTPS-Port abzurufen, schlägt die Übertragung fehl.

Sie sollten SSL nur für die folgenden virtuellen Stammverzeichnisse erfordern:

- **SimpleAuthWebService**
- **DSSAuthWebService**
- **ServerSyncWebService**
- **APIremoting30**
- **ClientWebService**

Sie sollten SSL nicht für die folgenden virtuellen Stammverzeichnisse erfordern:

- **Inhalt**
- **Inventory**
- **ReportingWebService**
- **SelfUpdate**
- Das Zertifikat der Zertifizierungsstelle (CA) muss in den vertrauenswürdigen Stamm-CA-Speicher des lokalen Computerspeichers oder in den vertrauenswürdigen Stamm-CA-Speicher von Windows Server Update Service auf WSUS-Downstreamservern importiert werden. Wenn das Zertifikat nur in den vertrauenswürdigen Stamm-CA-Speicher des lokalen Benutzers importiert wird, wird der Downstream-WSUS-Server nicht auf dem Upstreamserver authentifiziert.

Weitere Informationen zur Verwendung von SSL-Zertifikaten in IIS findest du unter [Require Secure Sockets Layer \(IIS 7\)](#).

- Sie müssen das Zertifikat auf allen Computern importieren, die mit dem WSUS-Server kommunizieren. Dies umfasst alle Clientcomputer, Downstreamserver und Computer, auf denen die WSUS-Verwaltungskonsole ausgeführt wird. Das Zertifikat sollte in den vertrauenswürdigen Stamm-CA-Speicher des lokalen Computers oder in den vertrauenswürdigen Stamm-CA-Speicher von Windows Server Update Service importiert werden.
- Sie können einen beliebigen Port für SSL verwenden. Der Port, den Sie für SSL eingerichtet haben, bestimmt jedoch auch den Port, über den WSUS unverschlüsselt den HTTP-Datenverkehr sendet. Betrachten Sie die folgenden Beispiele:
 - Bei Verwendung des Branchenstandardports 443 für HTTPS-Datenverkehr verwendet WSUS den Branchenstandardport 80 für unverschlüsselten HTTP-Datenverkehr.
 - Wenn du einen anderen Port als 443 für HTTPS-Datenverkehr verwendest, sendet WSUS unverschlüsselten HTTP-Datenverkehr über den Port, der von der Zahl gesehen vor dem Port für HTTPS liegt. Wenn Sie beispielsweise Port 8531 für HTTPS verwenden, wird WSUS Port 8530 für HTTP verwendet.

- Sie müssen *ClientServicingProxy* erneut initialisieren, wenn der Servername, die SSL-Konfiguration oder die Portnummer geändert wird.

So konfigurieren Sie SSL auf dem WSUS-Server

1. Melden Sie sich bei dem WSUS-Server mit einem Konto an, das Mitglied der WSUS-Administratorgruppe oder der lokalen Administratorgruppe ist.
2. Wechsel zu **Start**, gib **CMD** ein, klicke mit der rechten Maustaste auf **Eingabeaufforderung**, und klicke dann auf **Als Administrator ausführen**.
3. Navigiere zum Ordner **%ProgramFiles%\Update Services\Tools**.
4. Gib in der Eingabeaufforderung den folgenden Befehl ein:

Wsusutil configuessl certificateName

Dabei gilt Folgendes:

certificateName ist der DNS-Name des WSUS-Servers.

Konfigurieren von SSL auf Clientcomputern

Wenn Sie SSL auf Clientcomputern konfigurieren, sollten Sie Folgendes berücksichtigen:

- Sie müssen eine URL für einen sicheren Port auf dem WSUS-Server einschließen. Da SSL auf dem Server nicht erzwungen werden kann, können Sie nur sicherstellen, dass der Clientcomputer einen sicheren Kanal verwenden kann, indem eine URL genutzt wird, die HTTPS angibt. Wenn du einen anderen Port als 443 für SSL verwendest, musst du auch diesen Port in die URL einfügen.
- Das Zertifikat muss in den vertrauenswürdigen Stamm-CA-Speicher des lokalen Computers oder in den vertrauenswürdigen Stamm-CA-Speicher des Diensts für automatische Updates importiert werden. Wenn das Zertifikat nur in den vertrauenswürdigen Stamm-CA-Speicher des lokalen Benutzers importiert wird, schlägt die Serverauthentifizierung für automatische Updates fehl.
- Die Clientcomputer müssen dem Zertifikat vertrauen, das Sie an den WSUS-Server binden. Je nach verwendetem Zertifikattyp müssen Sie möglicherweise einen Dienst einrichten, sodass die Clientcomputer dem an den WSUS-Server gebundenen Zertifikat vertrauen.

Konfigurieren von SSL für WSUS-Downstreamserver

Die folgenden Anweisungen dienen der Konfiguration der Synchronisierung eines Downstreamservers mit einem Upstreamserver, der SSL verwendet.

So synchronisieren Sie einen Downstreamserver mit einem Upstreamserver, der SSL verwendet

1. Melden Sie sich mit einem Konto beim Computer an, das Mitglied der WSUS-Administratorgruppe oder der lokalen Administratorgruppe ist.
2. Klicke auf **Start, Alle Programme, Verwaltung** und dann auf **Windows Server Update Service**.
3. Erweitern Sie im rechten Bereich den Namen des Servers.
4. Klicken Sie auf **Optionen** und dann auf **Updatequelle und Proxyserver**.
5. Wählen Sie auf der Seite **Updatequelle** die Option **Von einem Windows Server Update Services-Server synchronisieren** aus.
6. Gib den Namen des Upstreamservers in das Textfeld **Servername** ein. Gib die Portnummer, die der Server für SSL-Verbindungen verwendet, in das Textfeld **Portnummer** ein.
7. Aktiviere das Kontrollkästchen **SSL beim Synchronisieren der Updateinformationen verwenden**, und klicke auf **OK**.

Zusätzliche SSL-Ressourcen

Die Schritte zum Einrichten einer Zertifizierungsstelle, zum Binden des Zertifikats an die WSUS-Website und zum Einrichten einer Vertrauensstellung zwischen Clientcomputern und Zertifikat gehen über den Rahmen dieses Handbuchs hinaus. Weitere Informationen und eine Anleitung zum Installieren von Zertifikaten sowie zum Einrichten der Umgebung finden Sie in den folgenden Themen:

- [Suite B-PKI: Schritt-für-Schritt-Anleitung](#)
- [Implementieren und Verwalten von Zertifikatvorlagen](#)
- [Active Directory-Zertifikatdienste: Leitfaden zu Upgrades und zur Migration](#)
- [Konfigurieren der automatischen Registrierung von Zertifikaten](#)

2.6. Abschluss der IIS-Konfiguration

Standardmäßig ist der anonyme Lesezugriff für die Standardwebsite und alle neuen IIS-Sites aktiviert. Einige Programme, vor allem Windows SharePoint Services, können den anonymen Zugriff entfernen. Ist dies der Fall, musst du den anonymen Lesezugriff erneut aktivieren, bevor du WSUS erfolgreich installieren und ausführen kannst.

Führen Sie die Schritte für die entsprechende Version von IIS aus, um anonymen Lesezugriff zu aktivieren:

1. [Enable Anonymous Authentication \(IIS 7\)](#) – IIS 7-Handbuch.
2. [Enabling Anonymous Authentication \(IIS 6.0\)](#) – IIS 6.0-Handbuch.

2.7. Konfigurieren eines Signaturzertifikats

WSUS bietet die Möglichkeit, benutzerdefinierte Updatepakete für Produkte von Microsoft und andere Produkte zu veröffentlichen. WSUS kann diese benutzerdefinierten Updatepakete für Sie automatisch mit einem Authenticode-Zertifikat signieren. Um die Signatur von benutzerdefinierten Updates zu aktivieren, müssen Sie ein Paketsignaturzertifikat auf dem WSUS-Server installieren. Bei der Signatur benutzerdefinierter Updates sind verschiedene Aspekte zu beachten.

1. **Zertifikatverteilung.** Der private Schlüssel muss auf dem WSUS-Server installiert sein, und der öffentliche Schlüssel muss explizit im Speicher für vertrauenswürdige Zertifikate auf allen Client-PCs und Servern installiert werden, die benutzerdefinierte signierte Updates erhalten sollen.
2. **Ablaufdatum.** Wenn das selbstsignierte Zertifikat abläuft oder sich das Ablaufdatum nähert, protokolliert WSUS entsprechende Ereignisse im Ereignisprotokoll.
3. **Zertifikatupdates/Zertifikatsperre.** Wenn du versucht hast, ein Zertifikat zu aktualisieren oder zu sperren (d. h. nach Erkennung des Ablaufdatums), hat WSUS keine Funktionalität zur Ermöglichung dieses Vorgangs angeboten. Dafür mussten manuelle Aufgaben ausgeführt werden, die entweder sehr schwierig manuell auszuführen waren oder sich schlecht automatisieren ließen.

Schritt 3: Genehmigen und Bereitstellen von Updates in WSUS

24.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Computer in einer Computergruppe kontaktieren innerhalb der nächsten 24 Stunden automatisch den WSUS-Server, um Updates abzurufen. Mithilfe des WSUS-Berichtsfeatures können Sie feststellen, ob diese Updates auf den Testcomputern bereitgestellt wurden. Nach dem erfolgreichen Abschließen der Tests können Sie die Updates für die entsprechenden Computergruppen in Ihrer Organisation genehmigen. In der folgenden Prüfliste sind die Schritte zum Genehmigen und Bereitstellen von Updates mithilfe der WSUS-Verwaltungskonsole beschrieben.

AUFGABE	BESCHREIBUNG
3.1. Genehmigen und Bereitstellen von WSUS-Updates	Verwenden Sie die WSUS-Verwaltungskonsole zum Genehmigen und Bereitstellen von WSUS-Updates.
3.2. Konfigurieren von Regeln für die automatische Genehmigung	Konfigurieren Sie WSUS für die automatische Genehmigung der Installation von Updates für ausgewählte Gruppen sowie die Art der Genehmigung von Revisionen für vorhandene Updates.
3.3. Überprüfen von installierten Updates anhand von WSUS-Berichten	Verwenden Sie das WSUS-Berichtsfeature zum Überprüfen von installierten Updates, der Computer auf denen sie installiert wurden sowie weiterer Details.

3.1. Genehmigen und Bereitstellen von WSUS-Updates

Verwenden Sie das folgende Verfahren, um Updates zu genehmigen und bereitzustellen.

So genehmigen Sie WSUS-Updates und stellen sie bereit

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**. Im rechten Bereich wird eine Zusammenfassung der Updatestatus für **Alle Updates**, **Wichtige Updates**, **Sicherheitsupdates** und **WSUS-Updates** angezeigt.
2. Klicken Sie im Bereich **Alle Updates** auf **Für Computer erforderliche Updates**.
3. Wählen Sie in der Liste mit Updates jene aus, die Sie für die Installation in Ihrer Testcomputergruppe genehmigen möchten. Informationen zu einem ausgewählten Update sind unten im Bereich **Updates** verfügbar. Zum Auswählen mehrerer zusammenhängender Updates hältst du die **UMSCHALTTASTE** gedrückt, während du auf den Updatenamen klickst. Zum Auswählen mehrerer nicht zusammenhängender Updates halten Sie die **STRG**-Taste gedrückt, während Sie auf die Updatenamen klicken.
4. Klicken Sie mit der rechten Maustaste auf das die ausgewählten Updates, und klicken Sie anschließend auf **Genehmigen**.
5. Wählen Sie im Dialogfeld **Updates genehmigen** Ihre Testgruppe aus, und klicken Sie dann auf den Pfeil nach unten.
6. Klicken Sie auf **Für die Installation genehmigt** und anschließend auf **OK**.

7. Das Fenster **Status der Genehmigung** wird angezeigt. Darin wird der Fortschritt der Aufgaben angezeigt, die sich auf die Updategenehmigung auswirken. Klicken Sie nach Abschluss des Genehmigungsprozesses auf **Schließen**.

3.2. Konfigurieren von Regeln für die automatische Genehmigung

Mit automatischen Genehmigungen können Sie angeben, wie die automatische Genehmigung der Installation von Updates für ausgewählte Gruppen erfolgen soll und wie vorhandene Updates genehmigt werden sollen.

So konfigurieren Sie die automatische Genehmigung

1. Erweitern Sie in der WSUS-Verwaltungskonsole unter **Update Services** den WSUS-Server, und klicken Sie dann auf **Optionen**. Das Fenster **Optionen** wird geöffnet.
2. Klicken Sie in **Optionen** auf **Automatische Genehmigungen**. Das Dialogfeld „**Automatische Genehmigungen**“ wird geöffnet.
3. Klicken Sie in **Updateregeln** auf **Neue Regel**. Das Dialogfeld **Regel hinzufügen** wird geöffnet.
4. Wähle unter **Regel hinzufügen** in **Schritt 1: Eigenschaften auswählen** jede einzelne Option oder eine Kombination von Optionen aus den folgenden Möglichkeiten aus:
 - Wenn ein Update in einer bestimmten Klassifizierung enthalten ist
 - Wenn ein Update in einem bestimmten Produkt enthalten ist
 - Stichtag für die Genehmigung festlegen
5. Klicke in **Schritt 2: Eigenschaften bearbeiten** auf jede der aufgeführten Optionen, und wähle dann jeweils die gewünschten Optionen aus.
6. Gib in **Schritt 3: Namen angeben** einen Namen für die Regel ein, und klicke dann auf **OK**.
7. Klicken Sie auf **OK**, um das Dialogfeld „**Automatische Genehmigungen**“ zu schließen.

3.3. Überprüfen von installierten Updates anhand von WSUS-Berichten

24 Stunden nach dem Genehmigen der Updates können Sie mithilfe des WSUS-Berichtsfeatures feststellen, ob die Updates auf den Testgruppencomputern bereitgestellt wurden. Verwenden Sie das WSUS-Berichtsfeature folgendermaßen, um den Status eines Updates zu überprüfen.

So überprüfen Sie Updates

1. Klicken Sie im Navigationsbereich der WSUS-Verwaltungskonsole auf **Berichte**.
2. Klicken Sie auf der Seite mit den **Berichten** auf den Bericht **Updatestatus-Zusammenfassung**. Das Fenster **Updatebericht** wird geöffnet.
3. Wenn Sie die Updateliste filtern möchten, wählen Sie die zu verwendenden Kriterien aus, z. B. **Updates in folgenden Klassifizierungen einbeziehen**, und klicken Sie anschließend auf **Bericht ausführen**.
4. Der Bereich **Updatebericht** wird angezeigt. Sie können den Status einzelner Updates überprüfen, indem Sie im linken Abschnitt des Bereichs das gewünschte Update auswählen. Im letzten Abschnitt des Berichtsbereichs wird die Statuszusammenfassung des Updates angezeigt.
5. Sie können diesen Bericht speichern oder drucken, indem Sie auf der Symbolleiste auf das entsprechende Symbol klicken.
6. Nach dem Prüfen der Updates können Sie diese für die Installation in den entsprechenden Computergruppen in Ihrer Organisation genehmigen.

Schritt 4: Konfigurieren von Gruppenrichtlinien für „Automatische Updates“

24.04.2020 • 75 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In einer Active Directory-Umgebung können Sie mithilfe von Gruppenrichtlinien definieren, wie Computer und Benutzer (in diesem Dokument als WSUS-Clients bezeichnet) mit Windows-Updates interagieren können, um automatische Updates von Windows Server Update Services (WSUS) zu beziehen.

Dieses Thema enthält zwei Hauptabschnitte:

Gruppenrichtlinieneinstellungen für WSUS-Clientupdates. Hier finden Sie vorgeschriebene Vorgehensweisen und Verhaltendetails zu den Gruppenrichtlinieneinstellungen für Windows Update und „Wartungszeitplan“, die steuern, wie WSUS-Clients mit Windows Update interagieren können, um automatische Updates zu erhalten.

Zusätzliche Informationen enthält die folgenden Abschnitte:

- **Zugreifen auf die Windows Update-Einstellungen in Gruppenrichtlinien.** Hier finden Sie allgemeine Hinweise zur Verwendung des Gruppenrichtlinienverwaltungs-Editors und Informationen zum Zugriff auf die Richtlinienerweiterungen „Updatedienste“ und Einstellungen für „Wartungszeitplan“ in Gruppenrichtlinien.
- **Für diese Anleitung relevante Änderungen an WSUS:** Für Administratoren, die mit WSUS 3.2 und früheren Versionen vertraut sind, enthält dieser Abschnitt eine kurze Zusammenfassung der wichtigsten Unterschiede zwischen der aktuellen und früheren Versionen von WSUS, die für diesen Leitfaden relevant sind.
- **Begriffe und Definitionen:** Definitionen für verschiedene Begriffe im Zusammenhang mit WSUS und Updatediensten, die in diesem Leitfaden verwendet werden.

Gruppenrichtlinieneinstellungen für WSUS-Clientupdates

Dieser Abschnitt enthält Informationen zu drei Gruppenrichtlinienerweiterungen. In diesen Erweiterungen finden Sie die Einstellungen, die Sie verwenden können, um zu konfigurieren, wie WSUS-Clients mit Windows Update interagieren können, um automatische Updates zu erhalten.

- [Computerkonfiguration > Windows Update \(Richtlinieneinstellungen\)](#)
- [Computerkonfiguration > Wartungszeitplan \(Richtlinieneinstellungen\)](#)
- [Benutzerkonfiguration > Windows Update \(Richtlinieneinstellungen\)](#)

NOTE

In diesem Thema wird davon ausgegangen, dass Sie bereits mit Gruppenrichtlinien vertraut sind und damit arbeiten. Wenn Sie mit Gruppenrichtlinien nicht vertraut sind, wird empfohlen, die Informationen im Abschnitt [Zusätzliche Informationen](#) in diesem Dokument zu lesen, bevor Sie versuchen, Richtlinieneinstellungen für WSUS zu konfigurieren.

Computerkonfiguration > Windows Update (Richtlinieneinstellungen)

Dieser Abschnitt enthält Details zu den folgenden computerbasierten Richtlinieneinstellungen:

- Automatische Updates sofort installieren
- Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten
- Signierte Updates aus einem Intranetspeicherort für Microsoft-Updatedienste zulassen
- Suchhäufigkeit für automatische Updates
- Automatische Updates konfigurieren
- Neustart für geplante Installationen verzögern
- Die Standardoption „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anpassen
- Option „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anzeigen
- Clientseitige Zielzuordnung aktivieren
- Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivieren
- Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind
- Erneut zu einem Neustart für geplante Installationen auffordern
- Geplante Installationen automatischer Updates erneut planen
- Internen Pfad für den Microsoft Updatedienst angeben
- Empfohlene Updates über automatische Updates aktivieren
- Softwarebenachrichtigungen aktivieren

Im Gruppenrichtlinienverwaltungs-Editor befinden sich Windows Update-Richtlinien für die computerbasierte Konfiguration im folgenden Pfad: **Richtliniename > Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows Update.**

NOTE

Standardmäßig sind diese Einstellungen nicht konfiguriert.

Automatische Updates sofort installieren

Gibt an, ob das Feature „Automatische Updates“ Updates automatisch installiert, die Windows-Dienste nicht unterbrechen oder Windows neu starten.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ auf **Deaktiviert** festgelegt ist, hat diese Richtlinie keine Auswirkung.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass Updates nicht sofort installiert werden. Lokale Administratoren können diese Einstellung mithilfe des Editors für lokale Gruppenrichtlinien ändern.
Aktiviert	Gibt an, dass das Feature „Automatische Updates“ Updates sofort installiert, nachdem Sie heruntergeladen wurden und für die Installation bereit sind.
Deaktiviert	Gibt an, dass Updates nicht sofort installiert werden.

Optionen: Es gibt keine Optionen für diese Einstellung.

Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten

Gibt an, ob Benutzer, die keine Administratoren sind, Updatebenachrichtigungen auf Grundlage der Richtlinieneinstellung „Automatische Updates konfigurieren“ erhalten.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	Weitere Informationen finden Sie in der folgenden Tabelle.

NOTE

Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert oder nicht konfiguriert ist, hat diese Richtlinieneinstellung keine Auswirkung.

IMPORTANT

Ab Windows 8 und Windows RT ist diese Richtlinieneinstellung standardmäßig aktiviert. In allen früheren Versionen von Windows ist sie standardmäßig deaktiviert.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass Benutzern immer das Fenster zur Kontensteuerung angezeigt wird und erhöhte Berechtigungen für diese Aufgaben erforderlich sind. Lokale Administratoren können diese Einstellung mithilfe des Editors für lokale Gruppenrichtlinien ändern.

<p>Aktiviert</p>	<p>Gibt an, dass für „Windows Update – automatische Updates“ und „Microsoft Update“ Nichtadministratoren einbezogen werden, wenn festgelegt wird, welcher angemeldete Benutzer Updatebenachrichtigungen empfängt. Benutzer, die keine Administratoren sind, können alle optionalen, empfohlenen und WICHTIGEN Update-Inhalte installieren, für die sie eine Benachrichtigung empfangen haben. Benutzern wird das Fenster „Benutzerkontensteuerung“ nicht angezeigt, und sie benötigen keine erhöhten Berechtigungen zum Installieren dieser Updates. Ausnahmen sind Updates, die Änderungen an den Einstellungen für Benutzeroberfläche, Endbenutzer-Lizenzvertrag oder Windows Update enthalten.</p> <p>Es gibt zwei Situationen, in denen die Auswirkung dieser Einstellung vom ausgeführten Computer abhängt:</p> <ol style="list-style-type: none"> 1. Ausblenden oder Wiederherstellen von Updates 2. Abbrechen der Installation eines Updates <p>Wenn diese Richtlinieneinstellung unter Windows Vista oder Windows XP aktiviert ist, wird Benutzern das Fenster „Benutzerkontensteuerung“ nicht angezeigt. Sie benötigen keine erhöhten Berechtigungen zum Ausblenden, Wiederherstellen oder Abbrechen von Updates.</p> <p>Wenn diese Richtlinieneinstellung unter Windows Vista aktiviert ist, wird Benutzern das Fenster „Benutzerkontensteuerung“ nicht angezeigt. Sie benötigen keine erhöhten Berechtigungen zum Ausblenden, Wiederherstellen oder Abbrechen von Updates. Wenn diese Richtlinieneinstellung nicht aktiviert ist, wird Benutzern das Fenster „Benutzerkontensteuerung“ stets angezeigt. Sie benötigen erhöhte Berechtigungen zum Ausblenden, Wiederherstellen oder Abbrechen von Updates.</p> <p>Unter Windows 7 hat diese Richtlinieneinstellung keine Auswirkungen. Benutzern wird immer das Fenster zur Kontensteuerung angezeigt, und sie benötigen erhöhte Berechtigungen für diese Aufgaben.</p> <p>Unter Windows 8 und Windows RT hat diese Richtlinieneinstellung keine Auswirkungen.</p>
<p>Deaktiviert</p>	<p>Gibt an, dass nur angemeldete Administratoren Updatebenachrichtigungen erhalten. Hinweis: Unter Windows 8 und Windows RT ist diese Richtlinieneinstellung standardmäßig aktiviert. In allen früheren Versionen von Windows ist sie standardmäßig deaktiviert.</p>

Optionen: Es gibt keine Optionen für diese Einstellung.

Signierte Updates aus einem Intranetspeicherort für Microsoft-Updatedienste zulassen

Gibt an, ob das Feature „Automatische Updates“ Updates akzeptiert, die von anderen Entitäten als Microsoft signiert wurden, wenn das Update an einem Speicherort des Microsoft Update-Diensts im Intranet gefunden wird.

UNTERSTÜTZT FÜR:	AUSNAHME:
<p>Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.</p>	<p>Windows RT</p>

NOTE

Updates von einem anderen Dienst als dem Microsoft Update-Dienst im Intranet müssen immer von Microsoft signiert sein und sind von dieser Richtlinieneinstellung nicht betroffen.

NOTE

Unter Windows RT wird diese Richtlinie nicht unterstützt. Die Aktivierung dieser Richtlinie wirkt sich nicht auf Computer aus, auf denen Windows RT ausgeführt wird.

Optionen: Es gibt keine Optionen für diese Einstellung.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass Updates aus einem Speicherort für den Microsoft Update-Dienst im Intranet von Microsoft signiert werden müssen.
Aktiviert	Gibt an, dass das Feature „Automatische Updates“ Updates akzeptiert, die über einen Speicherort für den Microsoft Update-Dienst im Intranet empfangen wurden, wenn sie durch ein Zertifikat signiert sind, das sich im Zertifikatspeicher „Vertrauenswürdige Herausgeber“ des lokalen Computers befindet.
Deaktiviert	Gibt an, dass Updates aus einem Speicherort für den Microsoft Update-Dienst im Intranet von Microsoft signiert werden müssen.

Optionen: Es gibt keine Optionen für diese Einstellung.

Neustart immer automatisch zur geplanten Zeit durchführen

Gibt an, ob ein Neustartzeitgeber immer sofort beginnt, nachdem Windows Update wichtige Updates installiert hat, anstatt zuerst die Benutzer für mindestens zwei Tage auf dem Anmeldebildschirm zu benachrichtigen.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Wenn die Richtlinieneinstellung „Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind“ aktiviert ist, hat diese Richtlinie keine Auswirkungen.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass Windows Update das Neustartverhalten des Computers nicht ändert.

Aktiviert	Gibt an, dass ein Neustartzeitgeber immer sofort beginnt, nachdem Windows Update wichtige Updates installiert hat, anstatt zuerst die Benutzer für mindestens zwei Tage auf dem Anmeldebildschirm zu benachrichtigen. Der Neustartzeitgeber kann so konfiguriert werden, dass er mit einem beliebigen Wert von 15 bis 180 Minuten beginnt. Wenn der Zeitgeber ausgeführt wird, wird der Neustart auch dann fortgesetzt, wenn Benutzer am Computer angemeldet sind.
Deaktiviert	Gibt an, dass Windows Update das Neustartverhalten des Computers nicht ändert.

Optionen: Wenn diese Einstellung aktiviert ist, können Sie den Zeitraum angeben, nach dem Updates installiert werden, bevor ein Computerneustart erzwungen wird.

Suchhäufigkeit für automatische Updates

Gibt die Stunden an, die Windows wartet, bis es nach verfügbaren Updates sucht. Die genaue Wartezeit wird festgelegt, indem die hier angegebenen Stunden minus 0 bis 20 % der angegebenen Stunden verwendet werden. Wenn diese Richtlinie beispielsweise verwendet wird, um eine Suchhäufigkeit von 20 Stunden anzugeben, suchen alle Clients, für die diese Richtlinie angewendet wird, in einer beliebigen Häufigkeit von 16 bis 20 Stunden nach Updates.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	Windows RT

NOTE

Die Einstellung „Internen Pfad für den Microsoft Updatedienst angeben“ muss aktiviert sein, damit diese Richtlinie wirksam wird.

Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert ist, hat diese Richtlinie keine Auswirkung.

NOTE

Unter Windows RT wird diese Richtlinie nicht unterstützt. Die Aktivierung dieser Richtlinie wirkt sich nicht auf Computer aus, auf denen Windows RT ausgeführt wird.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass Windows im Standardintervall von 22 Stunden auf verfügbare Updates prüfen soll.
Aktiviert	Gibt an, dass Windows im angegebenen Intervall auf verfügbare Updates prüfen soll.
Deaktiviert	Gibt an, dass Windows im Standardintervall von 22 Stunden auf verfügbare Updates prüfen soll.

Optionen: Wenn diese Einstellung aktiviert ist, können Sie das Zeitintervall (in Stunden) festlegen, das Windows Update wartet, bevor nach Updates gesucht wird.

Automatische Updates konfigurieren

Gibt an, ob automatische Updates auf diesem Computer aktiviert sind.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	Windows RT

Wenn diese Option aktiviert ist, müssen Sie eine der vier Optionen auswählen, die in dieser Gruppenrichtlinieneinstellung angegeben sind.

Um diese Einstellung zu verwenden, wählen Sie **Aktiviert** und dann unter **Optionen** unter **Automatische Updates konfigurieren** eine der Optionen (2, 3, 4 oder 5) aus.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass die Verwendung automatischer Updates nicht auf Gruppenrichtlinienebene angegeben ist. Ein Computeradministrator kann jedoch weiterhin in der Systemsteuerung automatische Updates konfigurieren.
Aktiviert	Gibt an, dass Windows erkennt, wann der Computer online ist, und verwendet seine Internetverbindung, um Windows Update nach verfügbaren Updates zu durchsuchen. Wenn diese Option aktiviert ist, können lokale Administratoren mithilfe der Windows Update-Systemsteuerung eine Konfigurationsoption ihrer Wahl auswählen. Lokale Administratoren dürfen jedoch die Konfiguration für das Feature „Automatische Updates“ nicht deaktivieren. - 2: Vor Herunterladen und Installation benachrichtigen Wenn Windows Update Updates findet, die für den Computer gelten, werden Benutzer darüber informiert, dass Updates zum Download bereit stehen. Benutzer können dann Windows Update ausführen, um alle verfügbaren Updates herunterzuladen und zu installieren. - 3: Autom. Herunterladen, aber vor Installation benachrichtigen (Standardeinstellung) Windows Update findet anwendbare Updates und lädt sie im Hintergrund herunter. Der Benutzer wird während des Vorgangs nicht benachrichtigt oder unterbrochen. Wenn die Downloads abgeschlossen sind, werden Benutzer benachrichtigt, dass Updates zur Installation bereit stehen. Benutzer können dann Windows Update ausführen, um die heruntergeladenen Updates zu installieren. - 4: Autom. Herunterladen und laut Zeitplan installieren Sie können den Zeitplan mithilfe der Optionen in dieser Gruppenrichtlinieneinstellung angeben. Wenn kein Zeitplan angegeben ist, sieht der Standardzeitplan für alle Installationen täglich 03:00 Uhr vor. Wenn für Updates ein Neustart erforderlich ist, um die Installation abzuschließen, startet Windows den Computer

	<p>automatisch neu. (Falls ein Benutzer beim Computer angemeldet ist, wenn Windows neu gestartet werden kann, wird der Benutzer benachrichtigt und erhält die Möglichkeit, den Neustart zu verzögern.) Hinweis: Ab Windows 8 können Sie Updates so festlegen, dass sie während der automatischen Wartung installiert werden, anstatt einen bestimmten an Windows Update gekoppelten Zeitplan zu verwenden. Bei der automatischen Wartung werden Updates installiert, wenn der Computer nicht verwendet wird. Es wird vermieden, dass Updates installiert werden, wenn der Computer im Akkubetrieb ist. Wenn die automatische Wartung innerhalb weniger Tage keine Updates installieren kann, installiert Windows Update die Updates sofort. Benutzer werden dann über einen anstehenden Neustart benachrichtigt. Ein anstehender Neustart erfolgt nur dann, wenn kein Potenzial für einen versehentlichen Datenverlust besteht. Sie können Zeitplanoptionen in den Einstellungen unter „Wartungszeitplan“ im Gruppenrichtlinienverwaltungs-Editor angeben. Diese befinden sich im Pfad Richtlinienname > Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Wartungszeitplan > Aktivierungsgrenze für automatische Wartung. Weitere Informationen zu Einstellungsdetails findest du im Abschnitt des folgenden Verweises: Einstellungen für den Wartungszeitplan.</p> <p>5: Lokalem Administrator ermöglichen, Einstellung auszuwählen</p> <p>Gibt an, ob lokale Administratoren die Systemsteuerung für „Automatische Updates“ verwenden dürfen, um eine Konfigurationsoption ihrer Wahl auszuwählen, z. B. ob lokale Administratoren eine geplante Installationsuhrzeit wählen können.</p> <p>Lokalen Administratoren wird nicht gestattet, die Konfiguration für „Automatische Updates“ zu deaktivieren.</p>
Deaktiviert	Gibt an, dass alle Clientupdates, die über den öffentlichen Windows Update-Dienst verfügbar sind, manuell aus dem Internet heruntergeladen und installiert werden müssen.

Neustart für geplante Installationen verzögern

Gibt die Zeitspanne an, die „Automatische Updates“ warten soll, bis mit einem geplanten Neustart fortgefahrt wird.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinie gilt nur, wenn „Automatische Updates“ für die Ausführung geplanter Installationen von Updates konfiguriert ist. Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert ist, hat diese Richtlinie keine Auswirkung.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass nach der Installation von Updates die Standardwartezeit von 15 Minuten abläuft, bevor ein geplanter Neustart stattfindet.
Aktiviert	Gibt an, dass nach Abschluss der Installation ein geplanter Neustart erfolgt, nachdem die angegebene Anzahl von Minuten abgelaufen ist.
Deaktiviert	Gibt an, dass nach der Installation von Updates die Standardwartezeit von 15 Minuten abläuft, bevor ein geplanter Neustart stattfindet.

Optionen: Wenn diese Einstellung aktiviert ist, können Sie diese Option verwenden, um die Zeitspanne (in Minuten) anzugeben, die „Automatische Updates“ warten soll, bevor mit einem geplanten Neustart fortgefahrt wird.

Die Standardoption „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anpassen

Mit dieser Richtlinieneinstellung können Sie festlegen, ob die Option **Updates installieren und herunterfahren** als Standardoption im Dialogfeld **Windows herunterfahren** zulässig ist.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinieneinstellung hat keine Auswirkung, wenn die Richtlinieneinstellung *Richtlinienname* > **Computerkonfiguration** > **Richtlinien** > **Administrative Vorlagen** > **Windows-Komponenten** > **Windows Update** > Option „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anzeigen aktiviert ist.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass Updates installieren und herunterfahren die Standardoption im Dialogfeld Windows herunterfahren wird, wenn Updates für die Installation zu dem Zeitpunkt verfügbar sind, zu dem der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
Aktiviert	Wenn Sie diese Richtlinieneinstellung aktivieren, ist die letzte Option des Benutzers zum Herunterfahren (z. B. „Ruhezustand“ oder „Neu starten“) die Standardoption im Dialogfeld Windows herunterfahren , und zwar unabhängig davon, ob die Option Updates installieren und herunterfahren im Menü Wählen Sie einen Vorgang aus verfügbar ist.

Deaktiviert	Gibt an, dass Updates installieren und herunterfahren die Standardoption im Dialogfeld Windows herunterfahren wird, wenn Updates für die Installation zu dem Zeitpunkt verfügbar sind, zu dem der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
--------------------	---

Optionen: Es gibt keine Optionen für diese Einstellung.

Keine Verbindungen mit Windows Update-Internetadressen herstellen

Auch wenn Windows Update für das Empfangen von Updates von einem internen Updatedienst konfiguriert ist, wird es in regelmäßigen Abständen Informationen vom öffentlichen Windows Update-Dienst abrufen, um zukünftige Verbindungen mit Windows Update und anderen Diensten wie Microsoft Update oder Microsoft Store zu ermöglichen.

Wenn Sie diese Richtlinie aktivieren, wird die Funktionalität zum regelmäßigen Abrufen von Informationen aus den öffentlichen Windows Server Update Services deaktiviert. Dies kann dazu führen, dass die Verbindung mit öffentlichen Diensten wie Microsoft Store nicht mehr funktioniert.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme ab Windows Server 2012 R2 , Windows 8.1 oder Windows RT 8.1, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinie gilt nur, wenn der Computer so konfiguriert ist, dass eine Verbindung mit einem internen Updatedienst über die Richtlinieneinstellung „Internen Pfad für den Microsoft Updatedienst angeben“ hergestellt wird.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Das Standardverhalten zum Abrufen von Informationen aus den öffentlichen Windows Server Update Services bleibt erhalten.
Aktiviert	Gibt an, dass Computer keine Informationen aus den öffentlichen Windows Server Update Services abrufen.
Deaktiviert	Das Standardverhalten zum Abrufen von Informationen aus den öffentlichen Windows Server Update Services bleibt erhalten.

Optionen: Es gibt keine Optionen für diese Einstellung.

Option "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anzeigen

Gibt an, ob die Option **Updates installieren und herunterfahren** im Dialogfeld **Windows herunterfahren** angezeigt wird.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig
Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass die Option Updates installieren und herunterfahren im Dialogfeld Windows herunterfahren verfügbar ist, wenn Updates verfügbar sind, wenn der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt. Ein lokaler Administrator kann diese Einstellung mithilfe einer lokalen Richtlinie ändern.
Aktiviert	Gibt an, dass Updates installieren und herunterfahren nicht als Option im Dialogfeld Windows herunterfahren angezeigt wird, selbst wenn Updates für die Installation verfügbar sind, wenn der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
Deaktiviert	Gibt an, dass die Option Updates installieren und herunterfahren die Standardoption im Dialogfeld Windows herunterfahren wird, wenn Updates für die Installation zu dem Zeitpunkt verfügbar sind, zu dem der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.

Optionen: Es gibt keine Optionen für diese Einstellung.

Clientseitige Zielzuordnung aktivieren

Gibt die Namen der Zielgruppen an, die in der WSUS-Konsole konfiguriert werden und die Updates von WSUS empfangen sollen.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	Windows RT

NOTE

Diese Richtlinie gilt nur, wenn dieser Computer so konfiguriert ist, dass er die angegebenen Zielgruppennamen im WSUS unterstützt. Wenn der Zielgruppenname im WSUS nicht vorhanden ist, wird er bis zur Erstellung ignoriert. Wenn die Richtlinieneinstellung „Internen Pfad für den Microsoft Updatedienst angeben“ deaktiviert oder nicht konfiguriert ist, hat diese Richtlinie keine Auswirkung.

NOTE

Unter Windows RT wird diese Richtlinie nicht unterstützt. Die Aktivierung dieser Richtlinie wirkt sich nicht auf Computer aus, auf denen Windows RT ausgeführt wird.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass keine Zielgruppeninformationen an WSUS gesendet werden. Ein lokaler Administrator kann diese Einstellung mithilfe einer lokalen Richtlinie ändern.
Aktiviert	Gibt an, dass die angegebenen Zielgruppeninformationen an WSUS gesendet werden. Sie dienen zum Bestimmen, welche Updates auf diesem Computer bereitgestellt werden sollen. Wenn WSUS mehrere Zielgruppen unterstützt, können Sie mit dieser Richtlinie mehrere durch Semikolon getrennte Gruppennamen angeben, sofern Sie die Zielgruppennamen der Computergruppenliste in WSUS hinzugefügt haben. Andernfalls muss eine einzelne Gruppe angegeben werden.
Deaktiviert	Gibt an, dass keine Zielgruppeninformationen an WSUS gesendet werden.

Optionen: Verwenden Sie diesen Bereich, um einen oder mehrere Zielgruppennamen anzugeben.

Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivieren
Gibt an, ob Windows Update die Features „Windows-Energieverwaltung“ oder „Energieoptionen“ verwendet, um den Computer automatisch aus dem Ruhezustand zu aktivieren, wenn Updates für die Installation geplant sind.

Der Computer wird nur dann automatisch aktiviert, wenn Windows Update für die automatische Installation von Updates konfiguriert ist. Wenn sich der Computer im Ruhezustand befindet, während die geplante Installationszeit eintritt, und es Updates gibt, die angewendet werden müssen, verwendet Windows Update die Features „Windows-Energieverwaltung“ oder „Energieoptionen“, um den Computer automatisch zu aktivieren und die Updates zu installieren. Windows Update aktiviert auch den Computer und installiert ein Update, wenn eine Installationsfrist festgelegt ist.

Der Computer wird nur aktiviert, wenn es zu installierende Updates gibt. Wenn der Computer im Akkubetrieb ist und Windows Update ihn aktiviert, werden keine Updates installiert, und der Computer kehrt nach zwei Minuten automatisch in den Ruhezustand zurück.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme ab Windows Vista und Windows Server 2008 (Windows 7), die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Windows Update aktiviert den Computer nicht aus dem Ruhezustand, um Updates zu installieren. Ein lokaler Administrator kann diese Einstellung mithilfe einer lokalen Richtlinie ändern.
Aktiviert	Windows Update aktiviert den Computer aus dem Ruhezustand, um unter den zuvor genannten Bedingungen Updates zu installieren.

Deaktiviert	Windows Update aktiviert den Computer nicht aus dem Ruhezustand, um Updates zu installieren.
--------------------	--

Optionen: Es gibt keine Optionen für diese Einstellung.

Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind

Gibt an, dass „Automatische Updates“ zum Abschluss einer geplanten Installation darauf wartet, dass der Computer von einem angemeldeten Benutzer neu gestartet wird, anstatt einen automatischen Neustart des Computers zu bewirken.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinie gilt nur, wenn „Automatische Updates“ für die Ausführung geplanter Installationen von Updates konfiguriert ist. Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert ist, hat diese Richtlinie keine Auswirkung.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass „Automatische Updates“ den Benutzer benachrichtigt, dass der Computer zum Abschließen der Installation in fünf Minuten automatisch neu gestartet wird.
Aktiviert	Einige Updates erfordern einen Neustart des Computers, bevor die Updates wirksam werden. Wenn der Status auf „Aktiviert“ festgelegt ist, startet „Automatische Updates“ einen Computer während einer geplanten Installation nicht automatisch neu, wenn ein Benutzer am Computer angemeldet ist. Stattdessen benachrichtigt „Automatische Updates“ den Benutzer, dass er den Computer neu starten soll.
Deaktiviert	Gibt an, dass „Automatische Updates“ den Benutzer benachrichtigt, dass der Computer zum Abschließen der Installation in fünf Minuten automatisch neu gestartet wird.

Optionen: Es gibt keine Optionen für diese Einstellung.

Erneut zu einem Neustart für geplante Installationen auffordern

Gibt die Zeitspanne an, die „Automatische Updates“ warten soll, ehe der Benutzer zu einem geplanten Neustart aufgefordert wird.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	Windows RT

IMPORTANT

Diese Richtlinie gilt nur, wenn „Automatische Updates“ für die Ausführung geplanter Installationen von Updates konfiguriert ist. Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert ist, hat diese Richtlinie keine Auswirkung.

NOTE

Diese Richtlinie hat keine Auswirkungen auf Computer, auf denen Windows RT ausgeführt wird.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Ein geplanter Neustart erfolgt zehn Minuten, nachdem die Aufforderung zum Neustart der Nachricht verworfen wurde. Ein lokaler Administrator kann diese Einstellung mithilfe einer lokalen Richtlinie ändern.
Aktiviert	Gibt an, dass nach der Verschiebung der vorherigen Aufforderung zum Neustart ein geplanter Neustart nach Ablauf der angegebenen Anzahl von Minuten erfolgt.
Deaktiviert	Ein geplanter Neustart erfolgt zehn Minuten, nachdem die Aufforderung zum Neustart der Nachricht verworfen wurde.

Optionen: Falls aktiviert, können Sie mit dieser Einstellungsoption die Zeitspanne (in Minuten) angeben, die vergeht, bis Benutzer erneut zu einem geplanten Neustart aufgefordert werden.

Geplante Installationen automatischer Updates erneut planen

Gibt die Zeitspanne an, die „Automatische Updates“ nach dem Start des Computers warten muss, bevor mit einer geplanten Installation fortgefahrene wird, die zuvor ausgelassen wurde.

Wenn der Status auf **Nicht konfiguriert** festgelegt ist, wird eine ausgelassene geplante Installation eine Minute nach dem nächsten Start des Computers ausgeführt.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinie gilt nur, wenn „Automatische Updates“ für die Ausführung geplanter Installationen von Updates konfiguriert ist. Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert ist, hat diese Richtlinie keine Auswirkung.

Status der Richtlinieneinstellung	Verhalten
-----------------------------------	-----------

Nicht konfiguriert	Gibt an, dass eine ausgelassene geplante Installation eine Minute nach dem nächsten Start des Computers ausgeführt wird.
Aktiviert	Gibt an, dass eine geplante Installation, die nicht früher erfolgt ist, in der angegebenen Anzahl von Minuten nach dem nächsten Start des Computers erfolgt.
Deaktiviert	Gibt an, dass bei der nächsten geplanten Installation eine ausgelassene geplante Installation durchgeführt wird.

Optionen: Wenn diese Richtlinieneinstellung aktiviert ist, können Sie damit eine Anzahl von Minuten nach dem nächsten Start des Computers festlegen, damit eine geplante Installation, die zuvor nicht stattgefunden hat, durchgeführt wird.

Internen Pfad für den Microsoft Updatedienst angeben

Gibt einen alternativen Intranetserver zum Hosten von Updates von Microsoft Update an. Sie können dann WSUS verwenden, um Computer in Ihrem Netzwerk automatisch zu aktualisieren.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	Windows RT.

Mit dieser Einstellung können Sie einen WSUS-Server in Ihrem Netzwerk angeben, der als interner Updatedienst fungiert. Anstatt Microsoft Updates im Internet zu verwenden, durchsuchen WSUS-Clients diesen Dienst nach geeigneten Updates.

Zum Verwenden dieser Einstellung müssen Sie zwei Servernamenwerte festlegen: den Server, auf dem der Client Updates erkennt und herunterlädt, und den Server, auf den aktualisierte Arbeitsstationen Statistiken hochladen. Die Werte müssen nicht unterschiedlich sein, wenn beide Dienste auf demselben Server konfiguriert sind.

NOTE

Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert ist, hat diese Richtlinie keine Auswirkung.

NOTE

Unter Windows RT wird diese Richtlinie nicht unterstützt. Die Aktivierung dieser Richtlinie wirkt sich nicht auf Computer aus, auf denen Windows RT ausgeführt wird.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Wenn „Automatische Updates“ nicht per Richtlinie oder Benutzervoreinstellung deaktiviert sind, stellt der Client eine direkte Verbindung mit der Windows Update-Website im Internet her.

Aktiviert	Gibt an, dass sich der Client anstatt mit Windows Update mit dem angegebenen WSUS-Server verbindet, um Updates zu suchen und herunterzuladen. Die Aktivierung dieser Einstellung bedeutet, dass Endbenutzer in Ihrer Organisation zum Abrufen von Updates keine Firewall überwinden müssen. Außerdem erhalten Sie die Möglichkeit, Updates vor deren Bereitstellung zu testen.
Deaktiviert	Wenn „Automatische Updates“ nicht per Richtlinie oder Benutzervoreinstellung deaktiviert sind, stellt der Client eine direkte Verbindung mit der Windows Update-Website im Internet her.

Optionen: Wenn diese Richtlinieneinstellung aktiviert ist, müssen Sie den Updatedienst im Intranet angeben, den WSUS-Clients zum Auffinden von Updates verwenden, und den Statistikserver im Internet, auf den aktualisierte WSUS-Clients Statistiken hochladen. Beispielwerte:

EINSTELLUNGSOPTION:	BEISPIELWERT:
Interner Updatedienst zum Ermitteln von Updates	http://wsus01:8530
Intranetserver für die Statistik	http://IntranetUpd01

Empfohlene Updates über automatische Updates aktivieren

Gibt an, ob „Automatische Updates“ WICHTIGE und empfohlene Updates von WSUS bereitstellt.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme ab Windows Vista, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig
Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, dass „Automatische Updates“ weiterhin WICHTIGE Updates bereitstellt, sofern das Feature bereits dafür konfiguriert sind.
Aktiviert	Gibt an, dass „Automatische Updates“ empfohlene und WICHTIGE Updates von WSUS bereitstellt.
Deaktiviert	Gibt an, dass „Automatische Updates“ weiterhin WICHTIGE Updates bereitstellt, sofern das Feature bereits dafür konfiguriert sind.

Optionen: Es gibt keine Optionen für diese Einstellung.

Softwarebenachrichtigungen aktivieren

Mit dieser Richtlinieneinstellung können Sie steuern, ob Benutzer detaillierte optimierte Benachrichtigungen über vom Microsoft Update-Dienst vorgestellte Software angezeigt bekommen. Optimierte Benachrichtigungen vermitteln den Nutzen und fördern die Installation und Verwendung von optionaler Software. Diese Richtlinieneinstellung ist für die Verwendung in nicht so streng verwalteten Umgebungen vorgesehen, in denen Sie dem Endbenutzer den Zugriff auf den Microsoft Update-Dienst ermöglichen.

Wenn Sie den Microsoft Update-Dienst nicht verwenden, hat die Richtlinieneinstellung „Softwarebenachrichtigungen“ keine Auswirkung.

Wenn die Richtlinieneinstellung „Automatische Updates konfigurieren“ deaktiviert oder nicht konfiguriert ist, hat die Richtlinieneinstellung „Softwarebenachrichtigungen“ keine Auswirkung.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme ab Windows Server 2008 (Windows Vista) und Windows 7, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinieneinstellung ist standardmäßig deaktiviert.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Benutzern auf Computern mit Windows 7 werden keine Benachrichtigungen zu optionalen Anwendungen angeboten. Benutzern auf Computern mit Windows Vista werden keine Benachrichtigungen zu optionalen Anwendungen oder Updates angeboten. Ein lokaler Administrator kann diese Einstellung in der Systemsteuerung oder mithilfe einer lokalen Richtlinie ändern.
Aktiviert	Wenn Sie diese Richtlinieneinstellung aktivieren, wird eine Benachrichtigung auf dem Computer des Benutzers angezeigt, sobald die vorgestellte Software verfügbar ist. Der Benutzer kann auf die Benachrichtigung klicken, um Windows Update zu öffnen und weitere Informationen über die Software zu erhalten oder sie zu installieren. Der Benutzer kann auch auf Diese Nachricht schließen oder Später anzeigen klicken, um die Benachrichtigung entsprechend zurückzustellen. Unter Windows 7 werden von dieser Richtlinieneinstellung nur detaillierte Benachrichtigungen für optionale Anwendungen gesteuert. Unter Windows Vista werden von dieser Richtlinieneinstellung detaillierte Benachrichtigungen für optionale Anwendungen und Updates gesteuert.
Deaktiviert	Gibt an, dass Benutzern von Windows 7 keine detaillierten Benachrichtigungen für optionale Anwendungen und Benutzern von Windows Vista keine detaillierten Benachrichtigungen zu optionalen Anwendungen oder optionalen Updates angeboten werden.

Optionen: Es gibt keine Optionen für diese Einstellung.

Computerkonfiguration > Wartungszeitplan (Richtlinieneinstellungen)

In der Einstellung „Automatische Updates konfigurieren“ haben Sie die Option **4: Autom. Herunterladen und laut Zeitplan installieren** ausgewählt. Sie können die Einstellungen für den Wartungszeitplan auf Computern mit Windows 8 und Windows RT in der Gruppenrichtlinien-Verwaltungskonsole angeben. Wenn Sie in der Einstellung „Automatische Updates konfigurieren“ nicht Option 4 ausgewählt haben, müssen Sie diese

Einstellungen nicht für automatische Updates konfigurieren. Die Einstellungen für den Wartungszeitplan befinden sich in folgendem Pfad: **Richtlinienname** > **Computerkonfiguration** > **Richtlinien** > **Administrative Vorlagen** > **Windows-Komponenten** > **Wartungszeitplan**. Die Gruppenrichtlinienerweiterung „Wartungszeitplan“ enthält die folgenden Einstellungen:

- [Aktivierungsgrenze für automatische Wartung](#)
- [Zufällige Verzögerung für automatische Wartung](#)
- [Richtlinie für die Aktivierung der automatischen Wartung](#)

Aktivierungsgrenze für automatische Wartung

Mit dieser Richtlinie können Sie die Einstellung „Aktivierungsgrenze für automatische Wartung“ konfigurieren.

Die Aktivierungsgrenze für die Wartung ist die täglich geplante Uhrzeit des Starts der automatischen Wartung.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Einstellung bezieht sich auf Option 4 in **Automatische Updates konfigurieren**. Wenn Sie in **Automatische Updates konfigurieren** Option 4 nicht ausgewählt haben, müssen Sie diese Einstellung nicht konfigurieren.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Wenn diese Richtlinieneinstellung nicht konfiguriert ist, gilt für Clientcomputer die in der Systemsteuerung unter Info-Center > Automatische Wartung angegebene tägliche geplante Uhrzeit.
Aktiviert	Wenn Sie diese Richtlinieneinstellung aktivieren, werden alle Standard- oder geänderten Einstellungen überschrieben, die auf Clientcomputern in Systemsteuerung > Info-Center > Automatische Wartung (oder bei einigen Clientversionen Wartung) konfiguriert sind.
Deaktiviert	Wenn Sie diese Richtlinieneinstellung auf Deaktiviert festlegen, gilt für Clientcomputer die in der Systemsteuerung unter Info-Center > Automatische Wartung angegebene tägliche geplante Uhrzeit.

Zufällige Verzögerung für automatische Wartung

Mit dieser Richtlinie können Sie die Einstellung „Zufällige Verzögerung für automatische Wartung“ konfigurieren.

Die zufällige Verzögerung der Wartung ist die Zeitspanne, bis zu der die automatische Wartung ab ihrer Aktivierungsgrenze verzögert wird. Diese Einstellung ist nützlich für virtuelle Computer, bei denen eine zufällige Wartung eine Leistungsanforderung sein kann.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Einstellung bezieht sich auf Option 4 in **Automatische Updates konfigurieren**. Wenn Sie in **Automatische Updates konfigurieren** Option 4 nicht ausgewählt haben, müssen Sie diese Einstellung nicht konfigurieren.

Falls aktiviert, wird die regelmäßige Wartungsverzögerung standardmäßig auf **PT4H** festgelegt.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Eine vierstündige zufällige Verzögerung wird Automatische Wartung zugeordnet.
Aktiviert	Die automatische Wartung verzögert den Start ab ihrer Aktivierungsgrenze bis um die angegebene Zeitspanne.
Deaktiviert	„Automatische Wartung“ wird keine zufällige Verzögerung zugeordnet.

Richtlinie für die Aktivierung der automatischen Wartung

Mit dieser Richtlinie können Sie die Einstellung „Richtlinie für die Aktivierung der automatischen Wartung“ konfigurieren.

Die Richtlinie für die Aktivierung der Wartung gibt an, ob „Automatische Wartung“ eine Aktivierungsanforderung an den ausgeführten Computer für die tägliche geplante Wartung richten soll.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Wenn die Aktivierungsrichtlinie des ausgeführten Computers explizit deaktiviert ist, hat diese Einstellung keine Auswirkung.

NOTE

Diese Einstellung bezieht sich auf Option 4 in **Automatische Updates konfigurieren**. Wenn Sie in **Automatische Updates konfigurieren** Option 4 nicht ausgewählt haben, müssen Sie diese Einstellung nicht konfigurieren.

Status der Richtlinieneinstellung	Verhalten

Nicht konfiguriert	Wenn Sie diese Richtlinieneinstellung auf nicht konfigurieren, gilt die in der Systemsteuerung unter Info-Center > Automatische Wartung angegebene Aktivierungseinstellung.
Aktiviert	Wenn Sie diese Richtlinieneinstellung aktivieren, versucht „Automatische Wartung“, eine Aktivierungsrichtlinie für das Betriebssystem festzulegen und bei Bedarf eine Aktivierungsanforderung für die tägliche geplante Uhrzeit zu stellen.
Deaktiviert	Wenn Sie diese Richtlinieneinstellung deaktivieren, gilt die in der Systemsteuerung unter Info-Center > Automatische Wartung angegebene Aktivierungseinstellung.

Benutzerkonfiguration > Windows Update (Richtlinieneinstellungen)

Dieser Abschnitt enthält Details zu den folgenden benutzerbasierten Richtlinieneinstellungen:

- Option „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anzeigen
- Die Standardoption „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anpassen
- Zugriff auf alle Windows Update-Funktionen entfernen

In der Gruppenrichtlinien-Verwaltungskonsole befinden sich die Benutzereinstellungen für automatische Computerupdates im folgenden Pfad: **Richtliniename > Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows Update**. Die Einstellungen werden in der gleichen Reihenfolge aufgelistet, in der sie in den Gruppenrichtlinienerweiterungen „Computerkonfiguration“ und „Benutzerkonfiguration“ angezeigt werden, wenn die Registerkarte **Einstellungen** der Windows Update-Richtlinie so ausgewählt ist, dass die Einstellungen alphabetisch sortiert werden.

NOTE

Standardmäßig sind diese Einstellungen, sofern nicht anders angegeben, nicht konfiguriert.

TIP

Für jede dieser Einstellungen können Sie die folgenden Schritte ausführen, um die Einstellungen zu aktivieren, zu deaktivieren oder zwischen ihnen zu wechseln:

Option „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anzeigen

Gibt an, ob die Option **Updates installieren und herunterfahren** im Dialogfeld **Windows herunterfahren** angezeigt wird.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig
Status der Richtlinieneinstellung	Verhalten

Nicht konfiguriert	Gibt an, dass die Option Updates installieren und herunterfahren im Dialogfeld Windows herunterfahren angezeigt wird, wenn Updates verfügbar sind, wenn der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
Aktiviert	Das Aktivieren dieser Richtlinieneinstellung bewirkt, dass Updates installieren und herunterfahren nicht als Option im Dialogfeld Windows herunterfahren angezeigt wird, selbst wenn Updates für die Installation verfügbar sind, wenn der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
Deaktiviert	Gibt an, dass die Option Updates installieren und herunterfahren im Dialogfeld Windows herunterfahren angezeigt wird, wenn Updates verfügbar sind, wenn der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.

Optionen: Es gibt keine Optionen für diese Einstellung.

Die Standardoption „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anpassen

Gibt an, ob die Option **Updates installieren und herunterfahren** im Dialogfeld **Windows herunterfahren** als Standardoption zulässig ist.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig

NOTE

Diese Richtlinieneinstellung hat keine Auswirkung, wenn *Richtlinienname > Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows Update > Option „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anzeigen* aktiviert ist.

Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Gibt an, ob die Option Updates installieren und herunterfahren die Standardoption im Dialogfeld Windows herunterfahren wird, wenn Updates für die Installation zu dem Zeitpunkt verfügbar sind, zu dem der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
Aktiviert	Gibt an, ob die letzte Option des Benutzers zum Herunterfahren (z. B. „Ruhezustand“ oder „Neu starten“) die Standardoption im Dialogfeld Windows herunterfahren ist, und zwar unabhängig davon, ob die Option Updates installieren und herunterfahren im Menü Wählen Sie einen Vorgang aus verfügbar ist.

Deaktiviert	Gibt an, ob die Option Updates installieren und herunterfahren die Standardoption im Dialogfeld Windows herunterfahren wird, wenn Updates für die Installation zu dem Zeitpunkt verfügbar sind, zu dem der Benutzer die Option „Herunterfahren“ zum Herunterfahren des Computers auswählt.
--------------------	--

Optionen: Es gibt keine Optionen für diese Einstellung.

Zugriff auf alle Windows Update-Funktionen entfernen

Mit dieser Einstellung können Sie den WSUS-Clientzugriff auf Windows Update aufheben.

UNTERSTÜTZT FÜR:	AUSNAHME:
Windows-Betriebssysteme, die sich noch innerhalb ihres Lebenszyklus für den Support von Microsoft-Produkten befinden.	ungültig
Status der Richtlinieneinstellung	Verhalten
Nicht konfiguriert	Benutzer können eine Verbindung mit der Windows Update-Website herstellen.
Aktiviert	<p>WICHTIG: Falls aktiviert, werden alle Windows Update-Features entfernt. Dazu gehört das Blockieren des Zugriffs auf die Windows Update-Website unter https://windowsupdate.microsoft.com, über den Windows Update-Link im Startmenü oder auf dem Startbildschirm und auch das Menü Extras in Internet Explorer. Die automatische Aktualisierung von Windows ist ebenfalls deaktiviert. Der Benutzer wird weder über wichtige Updates von Windows Update informiert noch erhält er diese. Diese Einstellung verhindert auch, dass der Geräte-Manager automatisch Treiberupdates von der Windows Update-Website installiert. Falls aktiviert, können Sie eine der folgenden Benachrichtigungsoptionen konfigurieren:</p> <ul style="list-style-type: none"> - 0: Keine Benachrichtigungen anzeigen Durch diese Einstellung wird der gesamte Zugriff auf Windows Update-Features entfernt, und es werden keine Benachrichtigungen angezeigt. - 1: Benachrichtigungen über erforderlichen Neustart anzeigen Diese Einstellung zeigt Benachrichtigungen zu Neustarts an, die zum Abschluss einer Installation erforderlich sind. Hinweis: Auf Computern mit Windows 8 und Windows RT werden bei aktiverter Richtlinie nur Benachrichtigungen über Neustarts und zur Tatsache angezeigt, dass Updates nicht erkannt werden können. Die Benachrichtigungsoptionen werden nicht unterstützt. Benachrichtigungen auf dem Anmeldebildschirm werden immer angezeigt.
Deaktiviert	Benutzer können eine Verbindung mit der Windows Update-Website herstellen.

Optionen: Siehe **Aktiviert** in der Tabelle für diese Einstellung.

Zusätzliche Informationen

Dieser Abschnitt bietet zusätzliche Informationen zum Öffnen und Speichern von WSUS-Einstellungen in Gruppenrichtlinien sowie Definitionen für die in diesem Leitfaden verwendeten Begriffe. Für Administratoren, die mit früheren Versionen von WSUS (3.2 und früher) vertraut sind, gibt es eine Tabelle, in der die Unterschiede zwischen WSUS-Versionen kurz zusammengefasst sind.

Zugriff auf die Windows Update-Einstellungen in Gruppenrichtlinien

Nachfolgend wird beschrieben, wie Sie die Gruppenrichtlinien-Verwaltungskonsole auf Ihrem Domänencontroller öffnen. Anschließend wird beschrieben, wie Sie entweder ein bestehendes Gruppenrichtlinienobjekt auf Domänenebene zur Bearbeitung öffnen oder ein neues Gruppenrichtlinienobjekt auf Domänenebene erstellen und zur Bearbeitung öffnen.

NOTE

Sie müssen Mitglied der Gruppe **Domänen-Admins** o. ä. sein, um diese Schritte ausführen zu können.

So können Sie ein Gruppenrichtlinienobjekt öffnen oder hinzufügen

1. Wechseln Sie auf Ihrem Domänencontroller zu **Server-Manager > Tools > Gruppenrichtlinienverwaltung**. Die Gruppenrichtlinien-Verwaltungskonsole wird geöffnet.
2. Erweitern Sie im linken Bereich Ihre Gesamtstruktur. Doppelklicken Sie beispielsweise auf **Gesamtstruktur: example.com**.
3. Doppelklicken Sie im linken Bereich auf **Domänen** und dann auf die Domäne, für die Sie ein Gruppenrichtlinienobjekt verwalten möchten. Doppelklicken Sie beispielsweise auf **example.com**.
4. Führen Sie eines der folgenden Verfahren aus:
 - Um ein bestehendes Gruppenrichtlinienobjekt auf Domänenebene zur Bearbeitung zu öffnen, doppelklicken Sie auf die Domäne, die das zu verwaltende Gruppenrichtlinienobjekt enthält. Klicken Sie mit der rechten Maustaste auf die zu verwaltende Domänenrichtlinie, und klicken Sie dann auf **Bearbeiten**. Der Gruppenrichtlinienverwaltungs-Editor wird geöffnet.
 - So können Sie ein neues Gruppenrichtlinienobjekt erstellen und zur Bearbeitung öffnen
 - a. Klicken Sie mit der rechten Maustaste auf die Domäne, für die Sie ein neues Gruppenrichtlinienobjekt erstellen möchten, und klicken Sie dann auf **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**.
 - b. Geben Sie in **Neues Gruppenrichtlinienobjekt** in das Feld **Name** den Namen des neuen Gruppenrichtlinienobjekts ein, und klicken Sie dann auf **OK**.
 - c. Klicken Sie mit der rechten Maustaste auf Ihr neues Gruppenrichtlinienobjekt, und klicken Sie dann auf **Bearbeiten**. Der Gruppenrichtlinienverwaltungs-Editor wird geöffnet.

So öffnen Sie die Gruppenrichtlinienerweiterungen „Windows Update“ oder „Wartungszeitplan“

1. Führen Sie im Gruppenrichtlinienverwaltungs-Editor eine der folgenden Aktionen aus:
 - Öffnen Sie die Gruppenrichtlinienerweiterung „Computerkonfiguration > Windows Update“. Navigieren Sie zu: **Richtliniename > Computerkonfiguration > Richtlinien / Administrative Vorlagen > Windows-Komponenten > Windows Update**.
 - Öffnen Sie die Gruppenrichtlinienerweiterung „Benutzerkonfiguration > Windows Update“. Navigieren Sie zu: **Richtliniename > Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows Update**.
 - Öffnen Sie die Gruppenrichtlinienerweiterung „Computerkonfiguration >

Wartungszeitplan". Navigieren Sie im Gruppenrichtlinienobjekt-Editor zu **Richtliniename > Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Wartungszeitplan**.

Weitere Informationen zu Gruppenrichtlinien finden Sie unter [Übersicht über Gruppenrichtlinien](#).

TIP

Nachdem Sie die gewünschte Gruppenrichtlinienerweiterung geöffnet haben, können Sie mit den folgenden Schritten die Einstellungen aktivieren, deaktivieren oder zwischen ihnen wechseln:

So konfigurieren Sie Gruppenrichtlinieneinstellungen

1. Doppelklicken Sie in *ExtensionOfGroupPolicy* auf die Einstellung, die Sie anzeigen oder ändern möchten.
2. Führen Sie zum Konfigurieren der Einstellung einen der folgenden Schritte aus:
 - Um den standardmäßig nicht angegebenen Status der Einstellung beizubehalten, wählen Sie **Nicht konfiguriert** aus.
 - Um die Einstellung zu aktivieren, wählen Sie **Aktiviert** aus.
 - Um die Einstellung zu deaktivieren, wählen Sie **Deaktiviert** aus.
3. Wenn unter **Optionen** Optionen aufgeführt sind, behalten Sie die Standardwerte bei, oder ändern Sie sie nach Bedarf.
4. Führen Sie eines der folgenden Verfahren aus:
 - Um Ihre Änderungen zu speichern und mit der nächsten Einstellung fortfahren, klicken Sie auf **Übernehmen** und dann auf **Nächste Einstellung**.
 - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen.
 - Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen.

Für diesen Leitfaden relevante Änderungen an WSUS

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen der aktuellen und früheren Version von WSUS zusammengefasst, die für diesen Leitfaden relevant sind.

WINDOWS SERVER- UND WSUS-VERSIONEN	BESCHREIBUNG
Windows Server 2012 R2 mit WSUS 6.0 und nachfolgende Versionen	Ab Windows Server 2012 ist die Serverrolle „WSUS“ in das Betriebssystem integriert, und die zugehörigen Gruppenrichtlinieneinstellungen für WSUS-Clients sind standardmäßig in Gruppenrichtlinien enthalten.
Windows Server 2008 (und frühere Versionen von Windows Server) mit WSUS 3.2 und früher	Unter Windows Server 2008 (und früheren Versionen von Windows Server) mit WSUS-Versionen 3.2 (und früher) sind die Gruppenrichtlinieneinstellungen zum Steuern von WSUS-Clients in diesen Windows Server-Betriebssystemen nicht enthalten. Die Richtlinieneinstellungen befinden sich in der administrativen WSUS-Vorlage wuau.adm . Bei diesen Serverversionen muss die administrative WSUS-Vorlage zunächst der Gruppenrichtlinien-Verwaltungskonsole hinzugefügt werden, bevor die WSUS-Clienteinstellungen konfiguriert werden können.

Begriffe und Definitionen

Es folgt eine Liste der in diesem Leitfaden verwendeten Begriffe.

BEGRIFF	DEFINITION
Automatische Updates	<p>Ein Dienst, der auf Windows-Computern ausgeführt wird (Automatische Updates): Die Clientcomputerkomponente, die in die Microsoft-Betriebssysteme Windows Vista, Windows Server 2003, Windows XP und Windows 2000 mit SP3 integriert ist, um Updates von Microsoft Update oder Windows Update zu beziehen.</p> <p>Modern (Automatische Updates): Der Begriff wird verwendet, um zu beschreiben, dass der Windows Update-Agent Updates automatisch plant und herunterlädt.</p>
Autonomer Server	Ein Downstreamserver mit Windows Server Update Services (WSUS), auf dem Administratoren WSUS-Komponenten verwalten können.
Downstreamserver	Ein Server mit Windows Server Update Services (WSUS), der Updates von einem anderen WSUS-Server anstatt von Microsoft Update oder Windows Update bezieht.
Gruppenrichtlinienerweiterung (und: Erweiterung von Gruppenrichtlinie)	<p>Eine Sammlung von Einstellungen in Gruppenrichtlinien, mit denen gesteuert wird, wie Benutzer und Computer (für die die Richtlinien gelten) verschiedene Windows-Dienste und -Funktionen konfigurieren und nutzen können.</p> <p>Administratoren können WSUS mit Gruppenrichtlinien für die clientseitige Konfiguration des Clients für „Automatische Updates“ verwenden, um sicherzustellen, dass Endbenutzer unternehmensweite Updaterichtlinien nicht deaktivieren oder umgehen können.</p> <p>WSUS erfordert nicht den Einsatz von Active Directory oder Gruppenrichtlinien. Die Clientkonfiguration kann auch über eine lokale Gruppenrichtlinie oder durch Ändern der Windows-Registrierung angewendet werden.</p>
Interner Updatedienst	Eine Netzwerkinfrastruktur, in der Updates mithilfe eines oder mehrerer WSUS-Server verteilt werden.
Replikatserver	Ein Downstreamserver mit Windows Server Update Services (WSUS), der die Genehmigungen und Einstellungen auf dem Upstreamserver spiegelt, mit dem er verbunden ist. Sie können WSUS nicht auf einem Replikatserver verwalten.
Microsoft Update	Eine Microsoft-Downloadwebsite im Internet: Eine Microsoft-Website im Internet, die Updates für Windows-Computer (Gerätetreiber), Windows-Betriebssysteme und andere Microsoft-Softwareprodukte speichert und verteilt.
Software Update Services (SUS)	SUS war das Vorgängerprodukt von Windows Server Update Services (WSUS).
Aktualisierungen	Eine Sammlung von Softwarerevisionen, Hotfixes, Service Packs, Feature Packs und Gerätetreibern, die auf einem Computer installiert werden können, um die Funktionalität zu erweitern oder Leistung und Sicherheit zu verbessern.

BEGRIFF	DEFINITION
Updatedateien	Die Dateien, die zur Installation eines Updates auf einem Computer erforderlich sind.
Updateinformationen (auch als Metadaten für Updates bezeichnet):	Die Informationen über ein Update im Gegensatz zu dessen Binärdateien in einem Updatepaket. Metadaten bieten beispielsweise Informationen über die Eigenschaften eines Updates und ermöglichen es Ihnen so herauszufinden, wofür das Update nützlich ist. Zu den Metadaten gehören auch die Microsoft-Software-Lizenzbedingungen. Das Metadatenpaket, das für ein Update heruntergeladen wird, ist in der Regel wesentlich kleiner als das eigentliche Updatedateipaket.
Updatequelle	Der Speicherort, mit dem ein WSUS-Server (Windows Server Update Services) synchronisiert wird, um Updatedateien abzurufen. Dieser Speicherort kann entweder Microsoft Update oder ein Upstreamserver mit WSUS sein.
Upstreamserver	Ein WSUS-Server (Windows Server Update Services), der Updatedateien für einen anderen WSUS-Server bereitstellt, der wiederum als Downstreamserver bezeichnet wird.
Windows Server Update Services (WSUS)	<p>Ein Serverrollenprogramm, das auf einem oder mehreren Windows Server-Computern in einem Unternehmensnetzwerk ausgeführt wird. Eine WSUS-Infrastruktur ermöglicht Ihnen, die Installation von Updates für Computer in Ihrem Netzwerk zu verwalten.</p> <p>Mit WSUS können Sie Updates vor der Freigabe genehmigen oder ablehnen, die Installation von Updates bis zu einem bestimmten Datum erzwingen und umfangreiche Berichte darüber erhalten, welche Updates die einzelnen Computer in Ihrem Netzwerk benötigen. Sie können WSUS so konfigurieren, dass bestimmte Updateklassen automatisch genehmigt werden (kritische Updates, Sicherheitsupdates, Service Packs, Treiber usw.). WSUS ermöglicht Ihnen auch, Updates nur für die „Erkennung“ zu genehmigen, sodass Sie sehen können, welche Computer ein bestimmtes Update benötigen, ohne die Updates installieren zu müssen.</p> <p>Bei einer WSUS-Implementierung muss mindestens ein WSUS-Server im Netzwerk eine Verbindung mit Microsoft Update herstellen, um verfügbare Updates herunterladen zu können. Basierend auf der Netzwerksicherheit und -konfiguration kann der Administrator bestimmen, wie viele andere Server sich direkt mit Microsoft Update verbinden.</p> <p>Sie können einen WSUS-Server so konfigurieren, dass Updates über das Internet aus folgenden Quellen abgerufen werden können:</p> <ul style="list-style-type: none"> • öffentliches Microsoft Update • öffentliches Windows Update • Microsoft Store

BEGRIFF	DEFINITION
Windows Update	<p>Eine Microsoft-Downloadwebsite im Internet: Eine Microsoft-Website im Internet, die Updates für Windows-Computer (Gerätekopplungen) und Windows-Betriebssysteme speichert und verteilt.</p> <p>Computerdienst: Der Name des Windows Update-Diensts, der auf Computern ausgeführt wird. Windows Update erkennt, lädt und installiert Updates auf Windows-Computern.</p> <p>Je nach Computer- und Richtlinienkonfiguration kann der Windows Update-Agent Updates aus folgenden Quellen herunterladen:</p> <ul style="list-style-type: none"> Microsoft Update Windows Update Microsoft Store Einem Updatedienst (WSUS) im Internet (Netzwerk) <p>Computer, die nicht in einer WSUS-basierten Umgebung verwaltet werden, verwenden in der Regel Windows Update, um sich direkt (über das Internet) mit Windows Update, Microsoft Update oder Microsoft Store zu verbinden und Updates zu beziehen.</p>
WSUS-Client	<p>Ein Computer, der Updates von einem WSUS-Updatedienst im Intranet erhält.</p> <p>Bei Gruppenrichtlinieneinstellungen, die die Interaktion des Endbenutzers mit „Automatische Updates“ steuern: ein Benutzer eines Computers in einer WSUS-Umgebung.</p>

Verwalten von Updates mit Windows Server Update Services

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

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Überprüfen Sie regelmäßig die Startseite der WSUS-Konsole, um die allgemeine Updatekompatibilität und die Netzwerkintegrität anzuzeigen. Überprüfen Sie Anwendungsprotokolle häufig, wenn Sie Probleme vermuten, wie z. B. Fehler beim Herunterladen oder wenn Clientcomputer keine Berichte an den WSUS-Server senden können. Diese Anleitung enthält Informationen zum Verwalten des Windows Server Update Services.

In diesem Handbuch

In diese Anleitung finden Sie Informationen zu folgenden Themen:

- [Einrichten von Updatesynchronisierungen](#)
- [Verwalten von WSUS-Clientcomputern und WSUS-Computergruppen](#)
- [Anzeigen und Verwalten von Updates](#)
- [WSUS und die Katalogwebsite](#)
- [Vorgänge für Updates](#)
- [Assistent für die Serverbereinigung](#)
- [Ausführen des WSUS-Replikatmodus](#)
- [WSUS-Nachrichten und Tipps zur Problembehandlung](#)

Einrichten von Updatesynchronisierungen

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Während der Synchronisierung werden von einem WSUS-Server Updates (Aktualisieren von Metadaten und Dateien) aus einer Update Quelle heruntergeladen. Außerdem werden neue Produkt Klassifizierungen und-Kategorien heruntergeladen, sofern vorhanden. Wenn der WSUS-Server zum ersten Mal synchronisiert wird, werden alle Updates heruntergeladen, die Sie beim Konfigurieren der Synchronisierungs Optionen angegeben haben. Nach der ersten Synchronisierung lädt Ihr WSUS-Server nur Updates von der Update Quelle sowie Revisionen der Metadaten für vorhandene Updates und Ablauf Aktualisierungen für Updates herunter.

Das erste Mal, wenn ein WSUS-Server Updates herunterlädt, kann einige Zeit in Anspruch nehmen. Wenn Sie mehrere WSUS-Server einrichten, können Sie den Prozess bis zu einem gewissen Grad beschleunigen, indem Sie alle Updates auf einem WSUS-Server herunterladen und dann die Updates in die Inhaltsverzeichnisse der anderen WSUS-Server kopieren.

Sie können Inhalt aus dem Inhaltsverzeichnis eines WSUS-Servers in einen anderen kopieren. Der Speicherort des Inhaltsverzeichnisses wird angegeben, wenn Sie die WSUS-Installationsprozedur nach der Installation ausführen. Sie können das Tool "WSUSUtil.exe" verwenden, um Update Metadaten von einem WSUS-Server in eine Datei zu exportieren. Anschließend können Sie diese Datei in andere WSUS-Server importieren.

Einrichten von Updatesynchronisierungen

Die Seite **Optionen** ist der zentrale Zugriffspunkt in der WSUS-Verwaltungskonsole, mit dem Sie die Synchronisierung von Updates durch den WSUS-Server anpassen. Sie können angeben, welche Updates automatisch synchronisiert werden sollen, wo der Server Updates, Verbindungseinstellungen und der Synchronisierungs Zeitplan erhält. Sie können den Konfigurations-Assistenten auch über die Seite **Optionen** verwenden, um den WSUS-Server zu einem beliebigen Zeitpunkt zu konfigurieren oder neu zu konfigurieren.

Synchronisieren von Updates nach Produkt und Klassifizierung

Ein WSUS-Server lädt Updates basierend auf den Produkten oder Produktfamilien (z. b. Windows oder Windows Server 2008, Datacenter Edition) und Klassifizierungen (z. b. kritische Updates oder Sicherheitsupdates) herunter, die Sie angeben. bei der ersten Synchronisierung werden vom WSUS-Server alle in den angegebenen Kategorien verfügbaren Updates heruntergeladen. In nachfolgenden synchronierungen werden von Ihrem WSUS-Server nur die neuesten Updates (oder Änderungen an den bereits auf dem WSUS-Server verfügbaren Updates) für die von Ihnen angegebenen Kategorien heruntergeladen.

Sie können auf der Seite **Optionen** unter **Produkte und Klassifizierungen** Update-Produkte und-Klassifizierungen angeben. Produkte werden in einer Hierarchie gruppiert nach Produktfamilie aufgelistet. Wenn Sie Windows auswählen, wählen Sie automatisch alle Produkte aus, die dieser Produkt Hierarchie unterliegen. Wenn Sie das übergeordnete Kontrollkästchen aktivieren, wählen Sie alle untergeordneten Elemente und alle zukünftigen Versionen aus. Wenn Sie die untergeordneten Kontrollkästchen aktivieren, werden die übergeordneten Kontrollkästchen nicht ausgewählt. Die Standardeinstellung für Produkte ist alle Windows-Produkte, und die Standardeinstellung für Klassifizierungen ist kritisch und Sicherheitsupdates.

Wenn ein WSUS-Server im Replikat Modus ausgeführt wird, sind Sie nicht in der Lage, diese Aufgabe auszuführen. Weitere Informationen zum Replikat Modus finden Sie unter [Ausführen des WSUS-Replikat Modus](#) und [Schritt 1: Vorbereiten der WSUS-Bereitstellung](#).

So geben Sie Update Produkte und Klassifizierungen für die Synchronisierung an

1. Klicken Sie in der WSUS-Verwaltungskonsole auf den Knoten **Optionen** .
2. Klicken Sie auf **Produkte und Klassifizierungen**, und klicken Sie dann auf die Registerkarte **Produkte** .
3. Aktivieren Sie die Kontrollkästchen für die Produkte oder Produktfamilien, die Sie mit WSUS aktualisieren möchten, und klicken Sie dann auf **OK**.
4. Aktivieren Sie auf der Registerkarte **Klassifizierungen** die Kontrollkästchen der Update Klassifizierungen, die vom WSUS-Server synchronisiert werden sollen, und klicken Sie dann auf **OK**.

NOTE

Produkte oder Klassifizierungen können auf die gleiche Weise entfernt werden. Der WSUS-Server beendet die Synchronisierung neuer Updates für die gelöschten Produkte. Updates, die für diese Produkte synchronisiert wurden, bevor Sie sie löschen, verbleiben jedoch auf dem WSUS-Server und werden als verfügbar aufgeführt.

Um diese Produkte zu entfernen, lehnen Sie das Update ab, wie unter [Update Operations \(Updates\)](#) beschrieben, und entfernen Sie sie dann mithilfe des [Assistenten zum Bereinigen von Servern](#) .

Synchronisieren von Updates nach Sprache

Der WSUS-Server lädt Updates basierend auf den von Ihnen angegebenen Sprachen herunter. Sie können Updates in allen Sprachen synchronisieren, in denen Sie verfügbar sind, oder Sie können eine Teilmenge von Sprachen angeben. Wenn Sie über eine Hierarchie von WSUS-Servern verfügen und Updates in verschiedenen Sprachen herunterladen müssen, stellen Sie sicher, dass Sie alle erforderlichen Sprachen auf dem Upstreamserver angegeben haben. Auf einem Downstream-Server können Sie eine Teilmenge der Sprachen angeben, die Sie auf dem Upstreamserver angegeben haben.

Synchronisieren von Updates aus dem Microsoft Update-Katalog

Ausführliche Informationen zum Synchronisieren von Updates vom Microsoft Update-Katalog Standort finden Sie unter [WSUS und der Katalog Website](#).

Konfigurieren von Proxy Server Einstellungen

Sie können den WSUS-Server für die Verwendung eines Proxy Servers während der Synchronisierung mit einem Upstreamserver oder Microsoft Update konfigurieren. Diese Einstellung gilt nur, wenn die Synchronisierung auf dem WSUS-Server ausgeführt wird. Standardmäßig wird vom WSUS-Server versucht, eine direkte Verbindung mit dem Upstreamserver oder Microsoft Update herzustellen.

So geben Sie einen Proxy Server für die Synchronisierung an

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Optionen**, und klicken Sie dann auf **Update Quelle und Proxy Server**.
2. Aktivieren Sie auf der Registerkarte **Proxy Server** das Kontrollkästchen **Proxy Server beim Synchronisieren verwenden**, und geben Sie dann den Server Namen und die Portnummer des Proxy Servers ein.

NOTE

Konfigurieren Sie WSUS mit der Portnummer, für deren Verwendung der Proxy Server konfiguriert ist.

- Wenn Sie eine Verbindung mit dem Proxy Server mit bestimmten Benutzer Anmelde Informationen herstellen möchten, aktivieren Sie das Kontrollkästchen **Benutzer Anmelde Informationen zum Herstellen einer Verbindung mit dem Proxy Server verwenden**, und geben Sie dann den Benutzernamen, die Domäne und das Kennwort des Benutzers in die entsprechenden Felder ein.

- Wenn Sie für den Benutzer, der eine Verbindung mit dem Proxy Server herstellt, die Standard Authentifizierung aktivieren möchten, aktivieren Sie das Kontrollkästchen Standard Authentifizierung zulassen (Kennwort wird in Klartext gesendet) .
3. Klicken Sie auf OK.

NOTE

Da WSUS den gesamten Netzwerk Datenverkehr initiiert, ist es nicht erforderlich, die Windows-Firewall auf einem WSUS-Server zu konfigurieren, der direkt mit Microsoft Update verbunden ist.

Konfigurieren der Update Quelle

Die Update Quelle ist der Speicherort, von dem der WSUS-Server seine Updates abruft und Metadaten aktualisiert. Sie können angeben, dass die Update Quelle entweder Microsoft Update oder ein anderer WSUS-Server sein soll (der WSUS-Server, der als Update Quelle fungiert, ist der Upstream-Server, und der Server ist der Downstream-Server).

Zum Anpassen der Synchronisierung des WSUS-Servers mit der Update Quelle stehen folgende Optionen zur Verfügung:

- Sie können einen benutzerdefinierten Port für die Synchronisierung angeben. Weitere Informationen zum Konfigurieren von Ports finden Sie unter [Schritt 3: Konfigurieren von WSUS](#) im WSUS-Bereitstellungs Handbuch.
- Sie können Secure Socket Layer (SSL) verwenden, um die Synchronisierung von Update Informationen zwischen WSUS-Servern zu sichern. Weitere Informationen zur Verwendung von SSL finden Sie im Abschnitt 3.5. Sichern Sie WSUS mit dem Secure Sockets Layer-Protokoll von [Schritt 3: Konfigurieren von WSUS](#) im WSUS-Bereitstellungs Handbuch.

Manuelles oder Automatisches Synchronisieren

Sie können entweder den WSUS-Server manuell synchronisieren oder eine Uhrzeit für die automatische Synchronisierung angeben.

So synchronisieren Sie den WSUS-Server manuell

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Optionen**, und klicken Sie dann auf **Synchronisierungs Zeitplan**.
2. Klicken Sie auf **manuell synchronisieren**, und klicken Sie dann auf OK.

So richten Sie einen Zeitplan für die automatische Synchronisierung ein

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Optionen**, und klicken Sie dann auf **Synchronisierungs Zeitplan**.
2. Klicken Sie auf **automatisch synchronisieren**.
3. Wählen Sie bei der ersten Synchronisierung die Uhrzeit aus, zu der die Synchronisierung jeden Tag gestartet werden soll.
4. Wählen Sie für **Synchronisierung pro Tag** die Anzahl der Synchronitäten aus, die Sie jeden Tag ausführen möchten. Wenn Sie z. B. vier Synchronisierungen täglich um 3:00 Uhr morgens durchführen möchten, erfolgt die Synchronisierung um 3:00 Uhr, 9:00 Uhr, 3:00 Uhr und 9:00 Uhr jeden Tag. (Beachten Sie, dass ein zufälliger Zeit Offset der geplanten Synchronisierungs Zeit hinzugefügt wird, um die Serververbindungen auf Microsoft Update zu versetzen.)
5. Klicken Sie auf OK.

So synchronisieren Sie den WSUS-Server sofort

1. Wählen Sie in der WSUS-Verwaltungskonsole den obersten Server Knoten aus.
2. Klicken Sie im Bereich **Übersicht** unter **Synchronisierungs Status** auf **Jetzt synchronisieren**.

NOTE

Die Synchronisierung wird vom Downstreamserver initiiert.

Verwalten von WSUS-Clientcomputern und WSUS-Computergruppen

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

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Der Knoten Computer ist der zentrale Zugriffspunkt in der WSUS-Verwaltungskonsole zum Verwalten von WSUS-Client Computern und-Geräten. Unter diesem Knoten finden Sie die verschiedenen Gruppen, die Sie eingerichtet haben (zuzüglich der Standardgruppe "nicht zugewiesene Computer").

Verwalten von Client Computern

Wenn Sie eine der Computer Gruppen im Knoten Computer unter **Optionen** auswählen, werden die Computer in dieser Gruppe im Detailbereich angezeigt. Wenn ein Computer mehreren Gruppen zugewiesen ist, wird er in den Listen beider Gruppen angezeigt. Wenn Sie einen Computer in der Liste auswählen, werden die zugehörigen Eigenschaften angezeigt. Hierzu gehören allgemeine Details zum Computer und der Status der Updates, wie z. b. die Installation oder der Erkennungs Status eines Updates für einen bestimmten Computer. Sie können die Liste der Computer unter einer bestimmten Computergruppe nach dem Status filtern. In der Standardeinstellung werden nur Computer angezeigt, für die Updates erforderlich sind oder bei denen Installationsfehler aufgetreten sind. Allerdings können Sie die Anzeige nach beliebigen Status filtern. Klicken Sie nach dem Ändern des Status Filters auf **Aktualisieren**.

Sie können Computer Gruppen auch auf der Seite Computer verwalten. dazu gehören das Erstellen der Gruppen und das Zuweisen von Computern. Weitere Informationen zum Verwalten von Computer Gruppen finden Sie im Abschnitt Verwalten von Computer Gruppen im nächsten Abschnitt dieses Handbuchs und Abschnitt [1.5. Planen der WSUS-Computer Gruppen](#) in Schritt 1: Vorbereiten der WSUS-Bereitstellung des WSUS-Bereitstellungs Handbuchs.

NOTE

Sie müssen die Client Computer zunächst so konfigurieren, dass Sie den WSUS-Server kontaktieren, bevor Sie Sie von diesem Server aus verwalten können. Bis Sie diese Aufgabe ausführen, erkennt der WSUS-Server Ihre Client Computer nicht und wird nicht in der Liste auf der Seite Computer angezeigt. Weitere Informationen zum Einrichten von Client Computern finden Sie unter [1.5. Planen Sie WSUS-Computer Gruppen](#) von Schritt 1: Vorbereiten der WSUS-Bereitstellung und Schritt 3: Konfigurieren von WSUS im WSUS-Bereitstellungs Handbuch.

Steuern, wann Updates von WSUS-Client Computern installiert werden

Es gibt zwei Methoden, um zu steuern, wann Updates von WSUS-Client Computern installiert werden:

- Genehmigung mit Terminen: Stichtage erzwingen strikt, wenn ein Update installiert wird.
- WSUS-Gruppenrichtlinien: Gruppenrichtlinien steuern, wann Updates durch den Windows Update-Agent überprüft und installiert werden

Weitere Informationen finden Sie im WSUS-Bereitstellungs Handbuch unter [Step 5: Configure Gruppenrichtlinie Settings for automatische Updates](#).

Verwalten von Computer Gruppen

WSUS bietet Ihnen die Möglichkeit, Updates gezielt auf Gruppen von Clientcomputern anzuwenden, sodass Sie sicherstellen können, dass bestimmte Computer immer zum geeigneten Zeitpunkt die richtigen Updates erhalten. Wenn z. B. für alle Computer in einer Abteilung (z. B. im Buchhaltungsteam) eine bestimmte Konfiguration verwendet wird, können Sie eine Gruppe für das Team erstellen, entscheiden, welche Updates für die Computer erforderlich sind und wann sie installiert werden sollen, und anschließend mithilfe von WSUS-Berichten die Updates für das Team auswerten.

Computer werden immer der Gruppe **alle Computer** zugewiesen und bleiben der Gruppe **nicht zugewiesene Computer** zugewiesen, bis Sie sie einer anderen Gruppe zuweisen. Computer können mehreren Gruppen angehören.

Computergruppen können in Hierarchien eingerichtet werden (z. B. "Gehaltsabrechnung" und "Kreditoren" als untergeordnete Gruppen von "Buchhaltung"). Updates, die für eine höhere Gruppe genehmigt werden, werden automatisch für niedrigere Gruppen und für die höhere Gruppe bereitgestellt. Wenn Sie Update1 für die Gruppe "Buchhaltung" genehmigen, wird das Update auf allen Computern in der Gruppe "Buchhaltung", auf allen Computern in der Gehaltsgruppe und auf allen Computern in der Gruppe "Konten ist" bereitgestellt.

Da Computer mehreren Gruppen zugewiesen werden können, kann es passieren, dass ein Update mehrmals für einen Computer genehmigt wird. Das Update wird jedoch nur einmal bereitgestellt, und alle Konflikte werden vom WSUS-Server aufgelöst. Wenn Sie das obige Beispiel fortsetzen möchten, wenn ComputerA sowohl dem Abrechnungs- als auch dem Konto für die kontozuweisung zugewiesen ist und Update1 für beide Gruppen genehmigt wird, wird es nur einmal bereitgestellt.

Für die Zuweisung von Computern zu Computergruppen stehen zwei Methoden zur Verfügung: serverseitige Zielgruppenadressierung und clientseitige Zielgruppenadressierung. Bei der serverseitigen Ausrichtung müssen Sie mindestens einen Client Computer manuell in eine Computergruppe verschieben. Bei der clientseitigen Zielzuordnung richten Sie Clientcomputer mithilfe von Gruppenrichtlinien oder durch entsprechende Bearbeitung der Registrierungseinstellungen so ein, dass sie sich zuvor erstellten Computergruppen selbst hinzufügen können. Bei diesem Prozess kann ein Skript erstellt und auf mehreren Computern gleichzeitig bereitgestellt werden. Sie müssen die Ziel Methode angeben, die auf dem WSUS-Server verwendet werden soll, indem Sie eine der beiden Optionen im Abschnitt **Computer** der Seite **Optionen** auswählen.

NOTE

Auf einem im Replikatmodus ausgeführten WSUS-Server können keine Computergruppen erstellt werden. Alle Computer Gruppen, die für Clients des Replikat Servers erforderlich sind, müssen auf dem WSUS-Server erstellt werden, der das Stammverzeichnis der WSUS-Server Hierarchie ist. Weitere Informationen zum Replikat Modus finden Sie unter [Ausführen des WSUS-Replikat Modus](#). Weitere Informationen zur serverseitigen und Client seitigen Zielgruppe finden Sie im Abschnitt [1.5. Planen der WSUS-Computer Gruppen](#) von Schritt 1: Vorbereiten der WSUS-Bereitstellung im WSUS-Bereitstellungs Handbuch.

Anzeigen und Verwalten von Updates

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sie können die WSUS-Konsole verwenden, um Updates anzuzeigen und zu verwalten.

Anzeigen von Updates

Auf der Seite **Updates** können Sie folgende Aufgaben ausführen:

- Anzeigen von Updates. In der Update Übersicht werden Updates angezeigt, die von der Update Quelle mit dem WSUS-Server synchronisiert wurden und für die Genehmigung verfügbar sind.
- Updates filtern. In der Standardansicht können Sie Updates nach Genehmigungs Status und Installationsstatus filtern. Die Standardeinstellung ist für nicht genehmigte Updates, die von einigen Clients benötigt werden oder bei denen bei einigen Clients Installationsfehler aufgetreten sind. Sie können diese Ansicht ändern, indem Sie die Filter für den Genehmigungs Status und den Installationsstatus ändern und dann auf **Aktualisierenklicken**.
- Erstellen Sie neue Update Sichten. Klicken Sie im **Aktions** Bereich auf **neue Update Ansicht**. Sie können Updates nach Klassifizierung, Produkt, der Gruppe, für die Sie genehmigt wurden, und dem Synchronisierungs Datum filtern. Sie können die Liste sortieren, indem Sie in der Titelleiste auf die entsprechende Spaltenüberschrift klicken.
- Suchen Sie nach Updates. Sie können nach einem einzelnen Update oder Satz von Updates nach Titel, Beschreibung, Knowledge Base-Artikel oder der Microsoft Security Response Center-Nummer für das Update suchen.
- Details, Status und Revisions Verlauf für jedes Update anzeigen.
- Genehmigen und ablehnen von Updates.

Anzeigen von Updates

1. Erweitern Sie in der WSUS-Verwaltungskonsole den Knoten **Updates**, und klicken Sie dann auf **alle Updates**.
2. Standardmäßig werden Updates mit dem Titel, der Klassifizierung, dem installierten/nicht anwendbaren Prozentsatz und dem Genehmigungs Status angezeigt. Wenn Sie weitere oder andere Update Eigenschaften anzeigen möchten, klicken Sie mit der rechten Maustaste auf die Spaltenüberschriften Leiste, und wählen Sie die entsprechenden Spalten aus.
3. Klicken Sie auf die entsprechende Spaltenüberschrift, um nach verschiedenen Kriterien zu sortieren, z. b. Download Status, Titel, Klassifizierung, Veröffentlichungsdatum oder Genehmigungs Status.

So filtern Sie die Liste der Updates, die auf der Seite **Updates** angezeigt werden

1. Erweitern Sie in der WSUS-Verwaltungskonsole den Knoten **Updates**, und klicken Sie dann auf **alle Updates**.
2. Wählen Sie im mittleren Bereich neben **Genehmigung** den gewünschten Genehmigungs Status aus, und wählen Sie neben **Status** den gewünschten Installationsstatus aus. Klicken Sie auf **Refresh**.

So erstellen Sie eine neue Update Ansicht in WSUS

1. Erweitern Sie in der WSUS-Verwaltungskonsole den Knoten **Updates**, und klicken Sie dann auf **alle**

Updates.

2. Klicken Sie im **Aktions** Bereich auf **neue Update Ansicht**.
3. Wählen Sie im Fenster " **Update Ansicht hinzufügen** " unter **Schritt 1: Eigenschaften auswählendie** Eigenschaften aus, die zum Filtern der Update Ansicht erforderlich sind:
 - SELECT-Updates sind in einer bestimmten Klassifizierung, um nach Updates zu filtern, die zu einer oder mehreren Update Klassifizierungen gehören.
 - SELECT-Updates sind für ein bestimmtes Produkt, das nach Updates für ein oder mehrere Produkte oder Produktfamilien gefiltert werden soll.
 - SELECT Updates werden für eine bestimmte Gruppe genehmigt, um nach Updates zu filtern, die für mindestens eine Computergruppe genehmigt wurden.
 - SELECT-Updates wurden innerhalb eines bestimmten Zeitraums synchronisiert, um nach Updates zu filtern, die zu einem bestimmten Zeitpunkt synchronisiert wurden.
 - SELECT Updates sind WSUS-Updates zum Filtern von WSUS-Updates.
4. Klicken Sie unter **Schritt 2: Bearbeiten der Eigenschaften** auf die unterstrichenen Wörter, um die gewünschten Werte auszuwählen.
5. Geben Sie unter **Schritt 3: Namen angeben** einen Namen für die neue Sicht ein.
6. Klicken Sie auf **OK**.

Die neue Ansicht wird im Struktur Ansichts Bereich unter Updates angezeigt. Sie wird wie die Standardansichten im mittleren Bereich angezeigt, wenn Sie Sie auswählen.

So suchen Sie nach einem Update

1. Wählen Sie den Knoten **Updates** aus (oder einen beliebigen Knoten darunter).
2. Klicken Sie im Bereich **Aktionen** auf **Suchen**.
3. Geben Sie im **Such** Fenster auf der Registerkarte **Updates** Ihre Suchkriterien ein. Sie können Text aus den Feldern **Titel, Beschreibung und Artikelnummer der Microsoft Knowledge Base (KB)** verwenden. Jedes dieser Elemente ist eine Eigenschaft, die in den Update Eigenschaften auf der Registerkarte **Details** aufgeführt ist.

So zeigen Sie die Eigenschaften für ein Update an

1. Erweitern Sie in der WSUS-Verwaltungskonsole den Knoten **Updates**, und klicken Sie dann auf **alle Updates**.
2. Klicken Sie in der Liste der Updates auf das Update, das Sie anzeigen möchten.
3. Im unteren Bereich werden die unterschiedlichen Eigenschaften Abschnitte angezeigt:
 - In der Titelleiste wird der Titel des Updates angezeigt. Beispiel: Sicherheits Update für Windows Media Player 9 (KB911565).
 - Der Abschnitt "Status" zeigt den Installationsstatus des Updates an (die Computer, auf denen er installiert werden muss, Computer, auf denen er mit Fehlern installiert wurde, Computer, auf denen er installiert wurde oder die nicht anwendbar sind, sowie Computer, auf denen der Status für das Update nicht gemeldet wurde) sowie allgemeine Informationen (KB-und MSRC-Versions Datum usw.).
 - Im Abschnitt Beschreibung wird eine kurze Beschreibung des Updates angezeigt.
 - Im Abschnitt Weitere Details werden die folgenden Informationen angezeigt:
 - Das Installations Verhalten des Updates (unabhängig davon, ob es sich um einen Wechsel

handelt, fordert einen Neustart an, erfordert eine Benutzereingabe oder muss exklusiv installiert werden).

- Gibt an, ob das Update Microsoft-Software-Lizenzbedingungen enthält.
- Die Produkte, für die das Update gilt
- Updates, durch die dieses Update abgelöst wird
- Die Updates, die durch dieses Update abgelöst werden
- Die vom Update unterstützten Sprachen
- Die Update-ID

Beachten Sie, dass Sie diese Prozedur nur auf jeweils einem Update ausführen können. Wenn Sie mehrere Updates auswählen, wird nur das erste Update in der Liste im Bereich "Eigenschaften" angezeigt.

Verwalten von Updates mit WSUS

Updates werden für die Aktualisierung oder die Bereitstellung einer vollständigen Datei Ersetzung für Software verwendet, die auf einem Computer installiert ist. Jedes Update, das auf Microsoft Update verfügbar ist, besteht aus zwei Komponenten:

- Metadaten: stellt Informationen zum Update bereit. Metadaten bieten beispielsweise Informationen über die Eigenschaften eines Updates und ermöglichen es Ihnen so herauszufinden, wofür das Update nützlich ist. Zu den Metadaten gehören auch die Microsoft-Software-Lizenzbedingungen. Das Metadatenpaket, das für ein Update heruntergeladen wird, ist in der Regel wesentlich kleiner als das eigentliche Updatedateipaket.
- Update Dateien: die eigentlichen Dateien, die zum Installieren eines Updates auf einem Computer erforderlich sind.

Beim Synchronisieren von Updates auf den WSUS-Server werden die Metadaten- und Updatedateien an zwei separaten Speicherorten gespeichert. Metadaten werden in der WSUS-Datenbank gespeichert. Update Dateien können entweder auf dem WSUS-Server oder auf Microsoft Update Servern gespeichert werden, je nachdem, wie Sie die Synchronisierungs Optionen konfiguriert haben. Wenn Sie Update Dateien auf Microsoft Update Servern speichern möchten, werden zum Zeitpunkt der Synchronisierung nur Metadaten heruntergeladen. die Updates werden über die WSUS-Konsole genehmigt, und die Update Dateien werden von den Client Computern zum Zeitpunkt der Installation direkt aus dem Microsoft Update. Weitere Informationen zu den Optionen zum Speichern von Updates finden Sie im Abschnitt [1.3. Wählen Sie](#) im WSUS-Bereitstellungs Handbuch eine WSUS-Speicherstrategie von Schritt 1: Vorbereiten der WSUS-Bereitstellung aus.

Sie werden die Synchronisierung einrichten und ausführen, Computer und Computer Gruppen hinzufügen und Updates regelmäßig bereitstellen. Die folgende Liste enthält Beispiele für allgemeine Aufgaben, die Sie beim Aktualisieren von Computern mit WSUS durchführen können.

- Bestimmen Sie einen allgemeinen Update Verwaltungsplan basierend auf der Netzwerktopologie und Bandbreite, den Unternehmensanforderungen und der Organisationsstruktur.
 - Gibt an, ob eine Hierarchie von WSUS-Servern eingerichtet werden soll und wie die Hierarchie strukturiert werden soll.
 - Welche Computer Gruppen erstellt werden sollen, und wie Sie Ihnen Computer zuweisen (serverseitige oder Client seitige Zielgruppen).
 - Welche Datenbank für Update Metadaten verwendet werden soll (z. b. interne Windows-Datenbank, SQL Server).
 - Gibt an, ob Updates automatisch und zu welchem Zeitpunkt synchronisiert werden sollen.

- Legen Sie Synchronisierungs Optionen wie Update Quelle, Produkt-und Update Klassifizierung, Sprache, Verbindungseinstellungen, Speicherort und Synchronisierungs Zeitplan fest.
- Sie erhalten die Updates und zugeordneten Metadaten auf dem WSUS-Server, indem Sie die Synchronisierung von Microsoft Update oder einem WSUS-Upstream-Server ausführen.
- Genehmigen oder ablehnen von Updates. Sie haben die Möglichkeit, Benutzern die Installation der Updates selbst zu gestatten (wenn es sich um lokale Administratoren auf Ihren Client Computern handelt).
- Konfigurieren Sie automatische Genehmigungen. Sie können auch konfigurieren, ob Sie die automatische Genehmigung von Revisionen vorhandener Updates aktivieren oder Revisionen manuell genehmigen möchten. Wenn Sie Änderungen manuell genehmigen möchten, verwendet der WSUS-Server weiterhin die ältere Version, bis Sie die neue Revision manuell genehmigen.
- Überprüfen Sie den Status von Updates. Sie können den Update Status anzeigen, einen Statusbericht drucken oder e-Mail für reguläre Statusberichte konfigurieren.

Aktualisieren von Produkten und Klassifizierungen

Die auf Microsoft Update verfügbaren Updates unterscheiden sich anhand des Produkts (oder der Produktfamilie) und der Klassifizierung.

Ein Produkt ist eine bestimmte Edition eines Betriebssystems oder einer Anwendung, z. b. Windows Server 2012. Eine Produktfamilie ist das Basis Betriebssystem bzw. die Basisanwendung, von dem die einzelnen Produkte abgeleitet werden. Ein Beispiel für eine Produktfamilie ist Microsoft Windows, von dem Windows Server 2012 ein Mitglied ist. Sie können die Produkte oder Produktfamilien auswählen, für die der Server Updates synchronisieren soll. Sie können eine Produktfamilie oder einzelne Produkte innerhalb der Familie angeben. Wenn Sie ein Produkt oder eine Produktfamilie auswählen, erhalten Sie Updates für die aktuelle und zukünftige Version des Produkts.

Update Klassifizierungen stellen den Typ des Updates dar. Für ein bestimmtes Produkt oder eine Produktfamilie können Updates unter mehreren Update Klassifizierungen verfügbar sein (z. b. wichtige Updates und Sicherheitsupdates der Windows 7-Familie). In der folgenden Tabelle sind die Update Klassifizierungen aufgeführt.

UPDATEKLASSIFIZIERUNGEN	BESCHREIBUNG
Kritische Updates	Im großen und ganzen finden Sie Korrekturen für bestimmte Probleme, die kritische, nicht sicherheitsrelevante Fehler behandeln.
Definitionsupdates	Updates für Viren-oder andere Definitions Dateien.
Treiber	Software Komponenten, die zur Unterstützung neuer Hardware entwickelt wurden.
Feature Packs	Neue featurereleases, die normalerweise in der nächsten Version in Produkte eingeführt werden.
Sicherheitsupdates	Allgemein veröffentlichte Korrekturen für bestimmte Produkte, die Sicherheitsprobleme behandeln.
Service Packs	Kumulative Sätze aller Hotfixes, Sicherheitsupdates, kritischer Updates und Updates, die seit der Veröffentlichung des Produkts erstellt wurden. Service Packs können auch eine begrenzte Anzahl von vom Kunden angeforderten Entwurfs Änderungen oder-Features enthalten.

UPDATEKLASSIFIZIERUNGEN	BESCHREIBUNG
Tools	Hilfsprogramme oder Funktionen, die bei der Ausführung einer Aufgabe oder einer Gruppe von Aufgaben helfen.
Updaterollups	Einen kumulativen Satz von Hotfixes, Sicherheitsupdates, kritischen Updates und anderen Updates, die zur einfachen Bereitstellung zusammengepackt werden. Ein Rollup bezieht sich in der Regel auf einen bestimmten Bereich, z. B. Sicherheit oder eine bestimmte Komponente, wie z. B. Internetinformationsdienste (IIS).
Updates	Allgemein veröffentlichte Korrekturen für bestimmte Probleme, die auf nicht kritische, nicht sicherheitsrelevante Fehler hinweisen.

Symbole, die für Updates in Windows Server Update Services verwendet werden

Updates in WSUS werden durch eines der folgenden Symbole dargestellt.

Um diese Symbole anzuzeigen, müssen Sie die ablösungs Spalte in der Update Services-Konsole aktivieren.

Kein Symbol

Das Update hat keine ablösungs Beziehung zu anderen Updates.

Betriebliche Bedenken:

Keine Einsatzbedenken.

Symbol "abgelöst"



Dieses Update ersetzt andere Updates.

Betriebliche Bedenken:

Keine Einsatzbedenken.

Abgelöst & abgelöst-Symbol



Dieses Update wird durch ein anderes Update abgelöst und ersetzt andere Updates.

Betriebliche Bedenken:

Ersetzen Sie diese Updates, wenn möglich, durch die ersetzenen Updates.

Symbol „Abgelöst“



Dieses Update wird durch ein anderes Update abgelöst.

Betriebliche Bedenken:

Ersetzen Sie diese Updates, wenn möglich, durch die ersetzenen Updates.

WSUS und die Katalogwebsite

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Die Katalog Site ist der Microsoft-Speicherort, von dem Sie Hotfixes und Hardwaretreiber importieren können.

Die Microsoft Update Katalog-Website

Um Hotfixes in WSUS zu importieren, müssen Sie von einem WSUS-Computer aus auf den Microsoft Update-Katalog Standort zugreifen. Alle Computer, auf denen die WSUS-Verwaltungskonsole installiert ist, unabhängig davon, ob es sich um einen WSUS-Server handelt, können zum Importieren von Hotfixes vom Katalog Standort verwendet werden. Sie müssen als Administrator auf dem Computer angemeldet sein, um die Hotfixes zu importieren.

So greifen Sie auf die Microsoft Update Katalog-Website zu

1. Wählen Sie in der WSUS-Verwaltungskonsole entweder den obersten Server Knoten oder **Updatesaus**, und klicken Sie im **Aktions** Bereich auf **Updates importieren**. Ein Browserfenster wird auf der Microsoft Update Katalog-Website geöffnet.
2. Um auf die Updates an diesem Standort zuzugreifen, müssen Sie das Microsoft Update Catalog-ActiveX-Steuerelement installieren.
3. Sie können diese Website nach Windows-Hotfixes und Hardware Treibern durchsuchen. Wenn Sie die gewünschten gefunden haben, fügen Sie Sie Ihrem Warenkorb hinzu.
4. Wenn Sie das Durchsuchen abgeschlossen haben, wechseln Sie zum Warenkorb, und klicken Sie auf Importieren, um Ihre Updates zu importieren. Deaktivieren Sie das Kontrollkästchen **direkt in Windows Server Update Services importieren**, um die Updates herunterzuladen, ohne Sie zu importieren.

Genehmigte Updates, die von der Microsoft Update Katalog-Website importiert werden, werden bei der nächsten Synchronisierung des WSUS-Servers heruntergeladen. Sie werden nicht zum Zeitpunkt des Imports von der Microsoft Update Katalog-Website heruntergeladen.

Beachten Sie, dass Sie über die WSUS-Konsole auf die Microsoft Update Katalog-Website zugreifen müssen, um sicherzustellen, dass die Updates in einem WSUS-kompatiblen Format importiert werden. Wenn Sie manuell auf die Microsoft Update Katalog-Website zugreifen, werden alle Updates, die Sie herunterladen, nicht in den WSUS-Server importiert, sondern als Einzelperson * heruntergeladen. MSU-Dateien. WSUS verfügt zurzeit nicht über einen unterstützten Mechanismus zum Importieren von Dateien in der *. MSU-Format.

Wenn Sie den-Server Bereinigungs-Assistenten ausführen, werden Updates, die aus dem Microsoft Update Katalog importiert wurden und als nicht genehmigt oder abgelehnt festgelegt wurden, möglicherweise vom WSUS-Server entfernt. Wenn Sie entfernt werden, können Sie aus dem Microsoft Update Katalog neu importiert werden.

NOTE

Sie können Updates entfernen, die aus dem Microsoft Update Katalog importiert werden, die entweder als nicht genehmigt oder abgelehnt festgelegt wurden, indem Sie den WSUS-Server Bereinigungs-Assistenten ausführen. Sie können Updates, die zuvor aus ihren WSUS-Systemen entfernt wurden, über den Microsoft Update Katalog erneut importieren.

Einschränken des Zugriffs auf Hotfixes

WSUS-Administratoren können den Zugriff auf die Hotfixes beschränken, die Sie von der Microsoft Update Katalog-Website heruntergeladen haben. Führen Sie die folgenden Schritte aus, um diese Einschränkung vorzunehmen:

So schränken Sie den Zugriff auf Hotfixes ein

1. Aktivieren Sie die Windows-Authentifizierung für den IIS-Inhalts-vroot.
 - Starten Sie den IIS-Manager.
 - Navigieren Sie unter WSUS-Verwaltungs Website zum Knoten Inhalt.
 - Doppelklicken Sie im **Inhalts** Startbereich auf die Option **Authentifizierung**.
 - Wählen Sie **anonyme Authentifizierung** aus, und klicken Sie im **Aktions** Bereich auf der rechten Seite auf **Deaktivieren**.
 - Wählen Sie **Windows-Authentifizierung** aus, und klicken Sie im **Aktions** Bereich auf der rechten Seite auf **aktivieren**.
2. Erstellen Sie eine WSUS-Zielgruppe für die Computer, für die der Hotfix erforderlich ist, und fügen Sie Sie der Gruppe hinzu. Weitere Informationen zu Computern und Gruppen finden Sie unter [Verwalten von WSUS-Client Computern und WSUS-Computer Gruppen](#) in diesem Handbuch und Abschnitt 3,3. [Konfigurieren Sie WSUS-Computer Gruppen](#) von Schritt 3: Konfigurieren von WSUS im WSUS-Bereitstellungs Handbuch.
3. Laden Sie die Dateien für den Hotfix herunter.
4. Legen Sie die Berechtigungen für diese Dateien so fest, dass Sie nur von Computer Konten dieser Computer gelesen werden können. Außerdem müssen Sie dem Netzwerkdienst Konto Vollzugriff auf die Dateien gestatten.
5. Genehmigen Sie den Hotfix für die WSUS-Zielgruppe, die Sie in Schritt 2 erstellt haben.

Importieren von Updates in verschiedenen Sprachen

Die Microsoft Update Catalog-Website enthält Updates, die mehrere Sprachen unterstützen. Es ist sehr **wichtig**, die vom WSUS-Server unterstützten Sprachen mit den von diesen Updates unterstützten Sprachen abzulegen. Wenn der WSUS-Server nicht alle Sprachen unterstützt, die im Update enthalten sind, wird das Update nicht auf Client Computern bereitgestellt. Ebenso gilt: Wenn ein Update, das mehrere Sprachen unterstützt, auf den WSUS-Server heruntergeladen, aber noch nicht auf Client Computern bereitgestellt wurde und ein Administrator eine der in diesem Update enthaltenen Sprachen deaktiviert, wird das Update nicht auf den Clients bereitgestellt.

Vorgänge für Updates

09.04.2020 • 28 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Nachdem Updates mit dem WSUS-Server synchronisiert wurden, werden Sie automatisch auf die für die Client Computer des Servers relevanten Kriterien überprüft. Sie müssen jedoch die Updates genehmigen, bevor Sie auf den Computern in Ihrem Netzwerk bereitgestellt werden. Wenn Sie ein Update genehmigen, weisen Sie WSUS im Grunde zu, was damit zu tun ist (Ihre Auswahl ist für ein neues Update " **install** " oder " **ablehnen** "). Sie können Updates für die Gruppe **alle Computer** oder für Untergruppen genehmigen. Wenn Sie ein Update nicht genehmigen, wird der Genehmigungs Status **nicht genehmigt** angezeigt, und der WSUS-Server ermöglicht Clients, zu prüfen, ob das Update benötigt wird.

Wenn Ihr WSUS-Server im Replikat Modus ausgeführt wird, können Sie keine Updates auf dem WSUS-Server genehmigen. Weitere Informationen zum Replikat Modus finden Sie unter [Ausführen des WSUS-Replikat Modus](#).

Genehmigen von Updates

Sie können die Installation von Updates für alle Computer in Ihrem WSUS-Netzwerk oder für verschiedene Computer Gruppen genehmigen. Nach der Genehmigung eines Updates können Sie eine oder mehrere der folgenden Aktionen ausführen:

- Wenden Sie diese Genehmigung ggf. auf untergeordnete Gruppen an.
- Legen Sie einen Stichtag für die automatische Installation fest. Wenn Sie diese Option auswählen, legen Sie bestimmte Uhrzeiten und Datumsangaben fest, um Updates zu installieren, und überschreiben alle Einstellungen auf den Client Computern. Außerdem können Sie ein letztes Datum für den Stichtag angeben, wenn Sie ein Update sofort genehmigen möchten (das installiert werden soll, wenn Client Computer das nächste Mal mit dem WSUS-Server in Verbindung treten).
- Entfernt ein installiertes Update, wenn dieses Update das Entfernen unterstützt.

Es gibt zwei wichtige Überlegungen, die Sie beachten sollten:

- Erstens können Sie keinen Stichtag für die automatische Installation eines Updates festlegen, wenn eine Benutzereingabe erforderlich ist (z. b. die Angabe einer für das Update relevanten Einstellung). Um zu ermitteln, ob ein Update Benutzereingaben erfordert, sehen Sie sich das Feld **möglicherweise Benutzereingabe anfordern** in den Update Eigenschaften für ein Update an, das auf der Seite **Updates** angezeigt wird. Überprüfen Sie im Feld **Updates genehmigen** auch, ob für das ausgewählte Update **Benutzereingaben erforderlich sind** und ein **Installations Stichtag nicht unterstützt** wird.
- Wenn Updates für die WSUS-Serverkomponente vorliegen, können Sie andere Updates für Client Systeme erst genehmigen, wenn das WSUS-Update genehmigt wurde. Diese Warnmeldung wird im Dialogfeld "Updates genehmigen" angezeigt: Es sind WSUS-Updates vorhanden, die nicht genehmigt wurden. Sie sollten die WSUS-Updates genehmigen, bevor Sie dieses Update genehmigen. In diesem Fall sollten Sie auf den Knoten WSUS-Updates klicken und sicherstellen, dass alle Updates in dieser Ansicht vor der Rückkehr zu den allgemeinen Updates genehmigt wurden.

So genehmigen Sie Updates

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**, und klicken Sie dann auf **alle Updates**.

2. Wählen Sie in der Liste der Updates das Update aus, das Sie genehmigen möchten, und klicken Sie mit der rechten Maustaste (oder wechseln Sie zum Bereich Aktionen). Wählen Sie dann im Dialogfeld **Updates genehmigen** die Computergruppe aus, für die Sie das Update genehmigen möchten, und klicken Sie auf den Pfeil daneben.
3. Wählen Sie **für die Installation genehmigt aus**, und klicken Sie dann auf **genehmigen**.
4. Im Fenster **Genehmigungs Status** wird der Fortschritt im Hinblick auf das Abschließen der Genehmigung angezeigt. Wenn der Prozess abgeschlossen ist, wird die Schaltfläche **Schließen** angezeigt. Klicken Sie auf **Schließen**.
5. Wenn Sie einen Stichtag auswählen, klicken Sie mit der rechten Maustaste auf das Update, wählen Sie die entsprechende Computergruppe aus, klicken Sie auf den Pfeil daneben, und klicken Sie dann auf **Stichtag**.
 - Sie können einen der Standard Termine (eine Woche, zwei Wochen, einen Monat) auswählen, oder Sie können auf **Benutzer** definiert klicken, um ein Datum und eine Uhrzeit anzugeben.
 - Wenn Sie ein Update installieren möchten, sobald die Client Computer mit dem Server in Kontakt treten, klicken Sie auf **Benutzerdefiniert**, und legen Sie dann ein Datum und eine Uhrzeit auf das aktuelle Datum und die Uhrzeit bzw. auf das aktuelle Datum fest.

So genehmigen Sie mehrere Updates

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**, und klicken Sie dann auf **alle Updates**.
2. Zum Auswählen mehrerer zusammenhängender Updates drücken Sie während der Auswahl von Updates die **UMSCHALT** Taste. Zum Auswählen mehrerer nicht zusammenhängender Updates halten Sie die **STRG**-Taste gedrückt, während Sie Updates auswählen.
3. Klicken Sie mit der rechten Maustaste auf die Auswahl und dann auf **genehmigen**. Das Dialogfeld **Updates genehmigen** wird geöffnet, und der **Genehmigungs Status** ist auf **vorhandene Genehmigungen beibehalten** und die Schaltfläche **OK** deaktiviert.
4. Sie können die Genehmigungen für die einzelnen Gruppen ändern, dies wirkt sich jedoch nicht auf die untergeordneten Genehmigungen aus. Wählen Sie die Gruppe aus, für die Sie die Genehmigung ändern möchten, und klicken Sie auf den Pfeil auf der linken Seite. Klicken Sie im Kontextmenü auf **für die Installation genehmigt**.
5. Die Genehmigung für die ausgewählte Gruppe wird in **installgeändert**. Wenn untergeordnete Gruppen vorhanden sind, bleibt die Genehmigung weiterhin **bestehen**. Um die Genehmigung für die untergeordneten Gruppen zu ändern, klicken Sie auf die Gruppe, und klicken Sie auf den Pfeil auf der linken Seite. Klicken Sie im Kontextmenü auf **auf auf untergeordnete Elemente anwenden**.
6. Klicken Sie auf das untergeordnete Element, und klicken Sie auf den Pfeil auf der linken Seite, um ein bestimmtes untergeordnetes Element festzulegen. Klicken Sie im Kontextmenü auf **identisch als übergeordnetes Element**. Wenn Sie ein untergeordnetes Element für das Erben von Genehmigungen festlegen, aber die übergeordneten Genehmigungen nicht ändern, erbt das untergeordnete Objekt die vorhandenen Genehmigungen des übergeordneten Elements.
7. Wenn Sie das Genehmigungs Verhalten für alle untergeordneten Elemente ändern möchten, genehmigen Sie **alle Computer**, und wählen Sie dann **auf untergeordnete Elemente anwenden** aus.
8. Klicken Sie auf **OK**, nachdem Sie alle Genehmigungen eingerichtet haben. Im Fenster **Genehmigungs Status** wird der Fortschritt im Hinblick auf das Abschließen der Genehmigung angezeigt. Wenn der Prozess abgeschlossen ist, ist die Schaltfläche **Schließen** verfügbar. Klicken Sie auf **Schließen**.

Abnehmende Updates

Wenn Sie diese Option auswählen, wird das Update aus der Standardliste der verfügbaren Updates entfernt, und

der WSUS-Server bietet das Update für Clients weder für die Evaluierung noch für die Installation. Sie können diese Option erreichen, indem Sie ein Update oder eine Gruppe von Updates auswählen und mit der rechten Maustaste klicken oder zum Bereich Aktionen wechseln. Abgelehnte Updates werden nur dann in der Liste Updates angezeigt, wenn Sie in der Liste Genehmigung die Option **abgelehnt** ausgewählt haben, wenn Sie den Filter für die Update Liste unter **Ansicht**angeben.

Ablehnen von Updates

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**, und klicken Sie dann auf **alle Updates**.
2. Wählen Sie in der Liste der Updates mindestens ein Update aus, das Sie ablehnen möchten.
3. Wählen Sie **ablehnenaus**, und klicken Sie dann in der Bestätigungsmeldung auf **Ja**.

Bereinigen abgelehnter Updates

Abgelehnte Updates verbrauchen weiterhin einige WSUS-Server Ressourcen. Sie sollten den Server Bereinigungs-Assistenten ausführen, um Abgelehnte Updates aus der WSUS-Datenbank zu entfernen. Weitere Informationen finden Sie [unter dem Server Bereinigungs-Assistenten](#).

Abgelehnte Updates werden erneut eingefügt.

Nachdem ein Update abgelehnt wurde, können Sie es weiterhin wiederherstellen.

So setzen Sie Abgelehnte Updates wieder

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**, und klicken Sie dann auf **alle Updates**.
2. Ändern Sie **Genehmigung** in **abgelehnt**, und klicken Sie auf **Aktualisieren**. Die Liste der abgelehnten Updates wird geladen.
3. Wählen Sie in der Liste der Updates mindestens ein abgelehntes Update aus, das Sie wiederherstellen möchten.
4. Klicken Sie zum Wiederherstellen eines bestimmten Updates mit der rechten Maustaste auf das Update, und wählen Sie **genehmigenaus**. Klicken Sie im Dialogfeld **Updates genehmigen** auf **OK**, um den Standardstatus nicht genehmigte Genehmigung erneut anzuwenden. Das Update wird in der Liste als **nicht genehmigt**, sondern nicht als abgelehnt angezeigt.

Nachdem ein abgelehntes Update mit dem WSUS-Server Bereinigungs-Assistenten bereinigt wurde, wird es auf dem WSUS-Server gelöscht und in der Ansicht alle Updates nicht mehr angezeigt. Sie können abgelehnte, bereinigte Updates aus dem Microsoft Update Katalog neu importieren. Weitere Informationen finden Sie unter [WSUS und die-Katalog Website](#).

Ändern eines genehmigten Updates in "nicht genehmigt"

Wenn ein Update genehmigt wurde und Sie es nicht zu diesem Zeitpunkt installieren möchten, sondern es für einen späteren Zeitpunkt speichern möchten, können Sie das Update in den Status nicht genehmigt ändern. Dies bedeutet, dass das Update in der Standardliste der verfügbaren Updates verbleibt und die Client Konformität meldet, aber nicht auf Clients installiert wird.

So ändern Sie ein Update von "genehmigt" in "nicht genehmigt"

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**, und klicken Sie dann auf **alle Updates**.
2. Wählen Sie in der Liste der Updates mindestens ein genehmigtes Update aus, das Sie in nicht genehmigt ändern möchten.
3. Wählen Sie im Kontextmenü oder im Bereich **Aktionen** die Option **nicht genehmigtaus**, und klicken Sie dann in der Bestätigungsmeldung auf **Ja**.

Genehmigen von Updates zum Entfernen

Sie können ein Update zum Entfernen genehmigen (d. h., ein bereits installiertes Update zu deinstallieren). Diese Option ist nur verfügbar, wenn das Update bereits installiert ist und das Entfernen unterstützt. Sie können einen Stichtag für die Installation des Updates angeben, oder Sie können ein letztes Datum für den Stichtag angeben, wenn Sie das Update sofort entfernen möchten (wenn Client Computer das nächste Mal mit dem WSUS-Server in Verbindung treten).

Es ist wichtig zu erwähnen, dass nicht alle Updates entfernt werden. Sie können sehen, ob ein Update das Entfernen unterstützt, indem Sie ein einzelnes Update auswählen und sich im **Detail** Bereich ansehen. Unter **Weitere Details** wird die Wechsel Kategorie angezeigt. Wenn das Update nicht durch WSUS entfernt werden kann, kann es in einigen Fällen mithilfe der Option Software in der Systemsteuerung entfernt werden.

So genehmigen Sie Updates zum Entfernen

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Updates**, und klicken Sie dann auf **alle Updates**.
2. Wählen Sie in der Liste der Updates mindestens ein Update aus, das Sie zum Entfernen genehmigen möchten, und klicken Sie mit der rechten Maustaste darauf (oder wechseln Sie zum **Aktions** Bereich).
3. Wählen Sie im Dialogfeld **Updates genehmigen** die Computergruppe aus, von der Sie das Update entfernen möchten, und klicken Sie auf den Pfeil daneben.
4. Wählen Sie **genehmigte zum Entfernen aus**, und klicken Sie dann auf die Schaltfläche **Entfernen**.
5. Nachdem die Genehmigung entfernen abgeschlossen ist, können Sie einen Stichtag auswählen, indem Sie mit der rechten Maustaste auf das Update klicken, die entsprechende Computergruppe auswählen und dann auf den Pfeil daneben klicken. Wählen Sie dann **Stichtag aus**. Sie können einen der Standard Termine (eine Woche, zwei Wochen, einen Monat) auswählen, oder Sie können auf **Benutzer** definiert klicken, um ein bestimmtes Datum und eine bestimmte Uhrzeit auszuwählen.
6. Wenn Sie ein Update entfernen möchten, sobald die Client Computer den Server kontaktieren, klicken Sie auf **Benutzerdefiniert**, und legen Sie ein Datum in der Vergangenheit fest.

Automatisches genehmigen von Updates

Sie können den WSUS-Server für die automatische Genehmigung bestimmter Updates konfigurieren. Sie können auch die automatische Genehmigung von Revisionen vorhandener Updates angeben, sobald diese verfügbar sind. Diese Option ist standardmäßig ausgewählt. Eine Revision ist eine Version eines Updates, bei der Änderungen vorgenommen wurden (z. b. Wenn Sie abgelaufen ist oder die Anwendbarkeits Regeln geändert wurden). Wenn Sie die überarbeitete Version eines Updates nicht automatisch genehmigen, wird die ältere Version von WSUS verwendet, und Sie müssen die Update Revision manuell genehmigen.

Sie können Regeln erstellen, die auf dem WSUS-Server automatisch während der Synchronisierung angewendet werden. Sie geben an, welche Updates Sie automatisch für die Installation genehmigen möchten, indem Sie die Update Klassifizierung, das Produkt und die Computergruppe durchsuchen. Dies gilt nur für neue Updates und nicht für überarbeitete Updates. Sie können auch einen Stichtag für die Genehmigung von Updates angeben, mit dem eine Anzahl von Tagen und eine bestimmte Zeitspanne festgelegt wird, bevor das genehmigte Update Stichtag installiert wird. Diese Einstellungen sind im Bereich **Optionen** unter **Automatische Genehmigungen** verfügbar.

So genehmigen Sie Updates automatisch

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Optionen**, und klicken Sie dann auf **Automatische Genehmigungen**.
2. Klicken Sie in **Updateregeln** auf **Neue Regel**.
3. Wählen Sie im Dialogfeld **Regel hinzufügen** unter **Schritt 1: Eigenschaften auswählen** aus, ob

verwendet werden soll, **Wenn ein Update in einer bestimmten Klassifizierung oder ein Update in einem bestimmten Produkt** (oder beiden) als Kriterium verwendet wird. Wählen Sie optional aus, ob Sie **einen Stichtag** für die Genehmigung festlegen möchten.

4. Klicken Sie in **Schritt 2: Bearbeiten der Eigenschaften** auf die unterstrichenen Eigenschaften, um die Klassifizierungen, Produkte und Computer Gruppen auszuwählen, für die Sie ggf. automatische Genehmigungen benötigen. Wählen Sie optional den Tag und die Uhrzeit der Update Genehmigung aus.
5. Geben Sie in **Schritt 3: Geben Sie einen Namen** ein den eindeutigen Namen für die Regel ein.
6. Klicken Sie auf **OK**.

Regeln für automatische Genehmigungen gelten nicht für Updates, für die ein Endbenutzer-Lizenzvertrag (EULA) erforderlich ist, der auf dem Server noch nicht akzeptiert wurde. Wenn Sie feststellen, dass das Anwenden einer automatischen Genehmigungs Regel nicht dazu führt, dass alle relevanten Updates genehmigt werden, sollten Sie diese Updates manuell genehmigen.

Automatisches genehmigen von Revisionen von Updates und abnehmenden abgelaufenen Updates

Der Abschnitt Automatische Genehmigungen des Bereichs Optionen enthält eine Standardoption zum automatischen genehmigen von Revisionen genehmigter Updates. Sie können auch festlegen, dass der WSUS-Server abgelaufene Updates automatisch ablehnen soll. Wenn Sie die überarbeitete Version eines Updates nicht automatisch genehmigen möchten, wird auf dem WSUS-Server die ältere Revision verwendet, und Sie müssen die Update Revision manuell genehmigen.

NOTE

Eine Revision ist eine Version eines Updates, die geändert wurde (z. b. ob Sie abgelaufen ist oder über aktualisierte Anwendbarkeits Regeln verfügt).

So genehmigen Sie Aktualisierungen von Updates automatisch und lehnen abgelaufene Updates ab

1. Klicken Sie in der WSUS-Verwaltungskonsole auf **Optionen**, und klicken Sie dann auf **Automatische Genehmigungen**.
2. Vergewissern Sie sich, dass auf der Registerkarte **erweitert** sowohl **neue Revisionen genehmigter Updates automatisch genehmigen** als auch **Updates automatisch ablehnen, wenn eine neue Revision das ablaufen** der Änderungen bewirkt.
3. Klicken Sie auf **OK**.

NOTE

Wenn Sie die Standardwerte für diese Optionen behalten, können Sie eine gute Leistung in Ihrem WSUS-Netzwerk gewährleisten. Wenn Sie nicht möchten, dass abgelaufene Updates automatisch abgelehnt werden, sollten Sie Sie in regelmäßigen Abständen manuell ablehnen.

Automatisch abnehmende abgelösten Updates

Wenn Sie ein neues Update genehmigen, das ein vorhandenes Update ersetzt, das automatisch genehmigt wird, gilt das ersetzte Update nicht mehr für einen Computer oder ein Gerät, sobald das neuere Update installiert wurde. Sie können in der WSUS-Konsole überprüfen, ob ein Update für alle Computer nicht anwendbar ist. Wenn dies der Fall ist, kann das Update sicher abgelehnt werden. Außerdem wird das Update möglicherweise automatisch abgelehnt, wenn Sie den WSUS-Server Bereinigungs-Assistenten ausführen.

Wenn Sie nach abgelösten Updates suchen möchten, können Sie die Spalte "abgelösten Flag" in der Ansicht "alle Updates" auswählen und nach dieser Spalte sortieren. Es gibt vier Gruppen:

- Updates, die noch nie abgelöst wurden (ein leeres Symbol).
- Updates, die abgelöst wurden, aber noch nie ein anderes Update abgelöst haben (ein Symbol mit einem blauen Quadrat unten).
- Updates, die abgelöst wurden und ein anderes Update abgelöst haben (ein Symbol mit einem blauen Quadrat in der Mitte).
- Updates, die ein anderes Update abgelöst haben (ein Symbol mit einem blauen Quadrat oben).

Es gibt keine Funktion in Windows Server Update Services, die bei der Genehmigung eines neueren Updates automatisch ersetzte Updates ablehnt. Es wird empfohlen, zuerst die Genehmigung auf "nicht genehmigt" festzulegen und dann mit dem Assistenten für die Server Bereinigung das Update automatisch abzulehnen, wenn alle relevanten Bedingungen erfüllt sind. Weitere Informationen finden Sie unter [dem Server Bereinigungs-Assistenten](#).

Genehmigen von ersetzen oder abgelösten Updates

In der Regel führt ein Update, das andere Updates ersetzt, eine oder mehrere der folgenden Aktionen aus:

- Erweiterung, Verbesserung oder Ergänzung der Korrekturen, die von früher herausgegebenen Updates bereitgestellt wurden
- Steigerung der Effizienz des Updatedateipakets, das auf Clientcomputern installiert wird, sofern die Installation des Updates genehmigt wird. Beispielsweise könnte das abgelöste Update Dateien enthalten, die für die Korrektur oder die jetzt vom neuen Update unterstützten Betriebssysteme nicht mehr relevant sind. Diese Dateien sind dann im Dateipaket des abgelösten Updates nicht enthalten.
- Aktualisiert neuere Versionen von Betriebssystemen. Es ist auch wichtig zu beachten, dass das ersetzende Update möglicherweise keine früheren Versionen von Betriebssystemen unterstützt.

Umgekehrt führt ein Update, das durch ein anderes Update abgelöst wird, Folgendes aus:

- Korrigiert eines Problems ähnlich dem des Updates, das es ersetzt. Das Update, durch das es ersetzt wird, kann jedoch die Behebung verbessern, die das ersetzte Update bereitstellt.
- Aktualisiert frühere Versionen von Betriebssystemen. In einigen Fällen werden diese Versionen von Betriebssystemen nicht mehr durch das ersetzende Update aktualisiert.

Im Detailbereich eines einzelnen Updates weist ein Informationssymbol und eine Meldung oben darauf hin, dass es entweder ersetzt oder durch ein anderes Update abgelöst wird. Außerdem können Sie ermitteln, welche Updates durch das Update abgelöst oder ersetzt werden, indem Sie sich die Updates, die **dieses Update ersetzen**, und die Updates, die **durch diese Update Einträge ersetzt** wurden, im Abschnitt **zusätzliche Details** der **Eigenschaften** ansehen. Der Detailbereich eines Updates wird unterhalb der Liste der Updates angezeigt.

WSUS lehnt ersetzte Updates nicht automatisch ab, und es wird empfohlen, dass Sie nicht davon ausgehen, dass abgelösten Updates zugunsten des neuen, ersetzenden Updates abgelehnt werden sollen. Stellen Sie vor dem ablehnen eines abgelösten Updates sicher, dass es von keinem Ihrer Client Computer mehr benötigt wird. Im folgenden finden Sie Beispiele für Szenarien, in denen Sie möglicherweise ein erabgelösten Update installieren müssen:

- Wenn ein ersetzendes Update nur neuere Versionen eines Betriebssystems unterstützt und auf einigen Client Computern frühere Versionen des Betriebssystems ausgeführt werden.
- Wenn ein ersetzendes Update die Anwendbarkeit stärker einschränkt als das Update, das es ersetzt, ist es

für einige Client Computer ungeeignet.

- Wenn ein Update aufgrund neuer Änderungen nicht mehr von einem zuvor veröffentlichten Update abgelöst wird. Es ist möglich, dass durch Änderungen in jeder Version ein Update nicht mehr ein Update ersetzt, das zuvor in einer früheren Version abgelöst wurde. In diesem Szenario wird weiterhin eine Meldung über das ersetzte Update angezeigt, auch wenn das Update, durch das es ersetzt wird, durch ein Update ersetzt wurde, das dies nicht getan hat.

Assistent für die Serverbereinigung

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Der Server Bereinigung-Assistent ist in die Benutzeroberfläche integriert und kann verwendet werden, um Ihnen bei der Verwaltung des Speicherplatzes zu helfen. Mit diesem Assistenten können die folgenden Vorgänge ausgeführt werden:

- Entfernen nicht verwendeter Updates und Update Revisionen entfernen Sie alle älteren Updates, und aktualisieren Sie Revisionen, die nicht genehmigt wurden.
- Löschen Sie Computer, die keine Verbindung mit dem Server herstellen, löschen Sie alle Client Computer, die den Server innerhalb von dreißig Tagen oder mehr nicht kontaktiert haben
- Nicht benötigte Update Dateien löschen löscht alle Update Dateien, die nicht von Updates oder Downstreamservern benötigt werden.
- Abgelaufene Updates ablehnen ablehnen alle Updates, die von Microsoft abgelaufen sind.
- Ablehnen von abgelösten Updates ablehnen alle Updates, die alle folgenden Kriterien erfüllen:
 - Das ersetzte Update ist nicht obligatorisch.
 - Das ersetzte Update befindet sich seit dreißig Tagen oder länger auf dem Server.
 - Das ersetzte Update wird zurzeit von keinem Client als erforderlich gemeldet.
 - Das abgelöste Update wurde mindestens 90 Tage lang nicht explizit für eine Computergruppe bereitgestellt.
 - Das ersetzende Update muss für die Installation in einer Computergruppe genehmigt werden.

WARNING

In einer WSUS-Hierarchie wird dringend empfohlen, zuerst den Bereinigungs Prozess auf dem untersten, Downstream/Replikat-WSUS-Server auszuführen und dann die Hierarchie nach oben zu verschieben. Eine nicht ordnungsgemäße Ausführung der Bereinigung auf einem Upstream-Server vor dem Ausführen der Bereinigung auf jedem Downstreamserver kann zu einem Konflikt zwischen den Daten in upstreamdatenbanken und downstreamdatenbanken führen. Der Daten Konflikt kann zu Synchronisierungs Fehlern zwischen den Upstream- und Downstreamservern führen.

IMPORTANT

Wenn Sie unnötige Inhalte mit dem Server Bereinigungs-Assistenten entfernen, werden alle privaten Update Dateien, die Sie von der Microsoft Update Katalog-Website heruntergeladen haben, ebenfalls entfernt. Sie müssen diese Dateien nach dem Ausführen des Server Bereinigungs-Assistenten erneut importieren.

Wenn Updates mithilfe einer Regel für die automatische Genehmigung genehmigt werden, sind Sie möglicherweise immer noch im genehmigten Zustand und werden nicht durch den Server Bereinigungs-Assistenten entfernt. Zum Entfernen automatisch genehmigter Updates, die den Status "genehmigt" aufweisen,

muss der WSUS-Administrator mindestens manuell den Genehmigungs Status der abgelösten Updates auf "nicht genehmigt" festlegen, damit Sie vom Server Bereinigungs-Assistenten zum Entschlüsseln berechtigt werden. Der Server Bereinigung-Assistent stellt sicher, dass ein neueres Update genehmigt wird und dass das Update von keinem Client System nach Bedarf gemeldet wird, bevor das Update als abgelehnt gekennzeichnet wird.

Ausführen des WSUS-Replikatmodus

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

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ein WSUS-Server im Replikat Modus erbt die Update Genehmigungen und Computer Gruppen, die auf einem Verwaltungs Server erstellt wurden. In einem Szenario, in dem der Replikat Modus verwendet wird, verfügen Sie in der Regel über einen einzelnen Verwaltungs Server, und ein oder mehrere untergeordnete WSUS-Replikat Server werden in der gesamten Organisation basierend auf der Standort-oder Organisations Sie genehmigen Updates und erstellen Computer Gruppen auf dem Verwaltungs Server, auf dem die Replikat Modus-Server dann gespiegelt werden. Server im Replikat Modus können nur während der WSUS-Installation eingerichtet werden. Wenn Sie dieses Szenario implementiert haben, ist es wahrscheinlich, dass es in Ihrer Organisation wichtig ist, dass Update Genehmigungen und Computer Gruppen zentral verwaltet werden.

Wenn Ihr WSUS-Server im Replikat Modus ausgeführt wird, können Sie nur eingeschränkte Verwaltungsfunktionen auf dem Server ausführen, die hauptsächlich aus folgenden Elementen bestehen:

- Hinzufügen und Entfernen von Computern zu Computer Gruppen. Die Mitgliedschaft in der Computergruppe wird nicht an Replikat Server verteilt, sondern nur Computer Gruppen selbst. Auf einem Replikat Modus-Server erben Sie daher die Computer Gruppen, die Sie auf dem Verwaltungs Server erstellt haben. Die Computer Gruppen sind jedoch leer. Anschließend müssen Sie die Client Computer, die eine Verbindung mit dem Replikat Server herstellen, den Computer Gruppen zuweisen.
- Festlegen eines Synchronisierungszeitplans
- Angeben von Proxy/Server-Einstellungen
- Angeben der Update Quelle. Dabei kann es sich um einen anderen Server als den Verwaltungs Server handeln.
- Aufrufen verfügbarer Updates
- Überwachen der Update-, Synchronisierungs-, Computer Status-und WSUS-Einstellungen auf dem Server
- Ausführen aller standardmäßigen WSUS-Berichte auf Replikat Modus-Servern

WSUS-Nachrichten und Tipps zur Problembehandlung

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Dieses Thema enthält Informationen zu den folgenden WSUS-Meldungen:

- Der Computer hat den Status nicht gemeldet.
- Meldungs-ID 6703-Fehler beim Synchronisieren der WSUS
- Fehler 0x80070643: Schwerwiegender Fehler bei der Installation.
- Einige Dienste werden nicht ausgeführt. Überprüfen Sie die folgenden Dienste [...]

Der Computer hat den Status nicht gemeldet.

Diese Meldung wird in der WSUS-Konsole generiert, wenn ein WSUS-Client Computer keine Informationen an den WSUS-Server sendet, um den aktuellen Aktualisierungs Status anzugeben. Dieses Problem tritt normalerweise durch den WSUS-Client Computer und nicht durch den WSUS-Server auf.

Die häufigsten Gründe sind:

- Die Konnektivität des Computers mit dem Netzwerk wurde unterbrochen:
 - Das Netzwerkkabel ist nicht verbunden.
 - Ein dazwischenliegende Netzwerkkabel ist fehlerhaft.
 - Der Computer verfügt über einen fehlerhaften Netzwerkadapter.
 - Der Netzwerkport, mit dem der Computer verbunden ist, wurde deaktiviert.
 - Der drahtlose Adapter kann keine Verbindung mit dem drahtlosen Zugriffspunkt des Unternehmens herstellen und eine Verbindung mit ihm herstellen.
- Der Computer ist ausgeschaltet. (Es wurde heruntergefahren oder befindet sich im Standbymodus oder im Ruhezustand.)

Meldungs-ID 6703-Fehler beim Synchronisieren der WSUS

Meldung: Fehler bei der Anforderung mit HTTP-Status 503: Dienst nicht verfügbar.

Quelle: Microsoft. updateservices. Administration. AdminProxy. kreateupdateserver.

Wenn Sie versuchen, Update Services auf dem WSUS-Server zu öffnen, erhalten Sie die folgende Fehlermeldung:

Fehler: Verbindungsfehler

Fehler beim Herstellen einer Verbindung mit dem WSUS-Server. Dieser Fehler kann aus verschiedenen Gründen auftreten. Wenden Sie sich an Ihren Netzwerkadministrator, falls das Problem weiterhin besteht. Klicken Sie auf den Server Knoten zurücksetzen, um erneut eine Verbindung mit dem Server herzustellen.

Zusätzlich zu den obigen Schritten schlägt der Zugriff auf die URL für die WSUS-Verwaltungs Website (d. h.

<http://CM12CAS:8530>) mit dem folgenden Fehler fehl:

HTTP-Fehler 503. Der Dienst ist nicht verfügbar.

In dieser Situation ist die wahrscheinlichste Ursache, dass sich der WsusPool-Anwendungs Pool in IIS im beendeten Zustand befindet.

Außerdem wird der Standardwert für das Limit für den privaten Speicher (KB) für den Anwendungs Pool wahrscheinlich auf den Standardwert von 1843200 KB festgelegt. Wenn dieses Problem auftritt, erhöhen Sie das Limit für den privaten Speicher auf 4 GB (4 Millionen KB), und starten Sie den Anwendungs Pool neu. Um das Limit für den privaten Speicher zu erhöhen, wählen Sie den Anwendungs Pool WsusPool aus, und klicken Sie unter Anwendungs Pool bearbeiten auf Erweiterte Einstellungen. Legen Sie dann das Limit für den privaten Speicher auf 4 GB (4 Millionen KB) fest. Nachdem der Anwendungs Pool neu gestartet wurde, überwachen Sie den Status der SMS_WSUS_SYNC_Manager-Komponente, "WCM.log" und "wsyncmgr.log" auf Fehler. Beachten Sie, dass es möglicherweise erforderlich ist, den Grenzwert für den privaten Arbeitsspeicher je nach Umgebung auf 8 GB (8 Millionen KB) oder höher zu erhöhen.

Weitere Informationen finden Sie unter: die [WSUS-Synchronisierung in ConfigMgr 2012 schlägt mit HTTP 503-Fehlern fehl](#).

Fehler 0x80070643: Schwerwiegender Fehler bei der Installation.

Das WSUS-Setup verwendet Microsoft SQL Server, um die Installation auszuführen. Dieses Problem tritt auf, weil der Benutzer, der das WSUS-Setup ausgeführt hat, nicht über System Administrator Berechtigungen in SQL Server verfügt.

Um dieses Problem zu beheben, erteilen Sie System Administrator Berechtigungen für ein Benutzerkonto oder ein Gruppenkonto in SQL Server, und führen Sie dann das WSUS-Setup erneut aus.

Einige Dienste werden nicht ausgeführt. Überprüfen Sie die folgenden Dienste:

- **SelfUpdate:** Weitere Informationen zur Problembehandlung beim SelfUpdate-Dienst finden Sie unter [Automatische Updates muss aktualisiert werden](#).
- **Wssuservice.exe:** Dieser Dienst vereinfacht die Synchronisierung. Wenn bei der Synchronisierung Probleme auftreten, greifen Sie auf "wssuservice.exe" zu, indem Sie auf **Start**, zeigen Sie auf **Verwaltung**, klicken Sie auf **Dienste**, und suchen Sie dann in der Liste der Dienste nach **Windows Server Update Service**. Gehen Sie wie folgt vor:
 - Überprüfen Sie, ob dieser Dienst ausgeführt wird. Klicken Sie auf **starten**, wenn es beendet oder **neu gestartet** wird, um den Dienst zu aktualisieren.
 - Verwenden Sie Ereignisanzeige, um die **Anwendungs-, SECURIT-und System** Ereignisprotokolle zu überprüfen, um festzustellen, ob Ereignisse vorhanden sind, die möglicherweise auf ein Problem hinweisen.
 - Sie können auch die Datei "SoftwareDistribution.log" überprüfen, um festzustellen, ob Ereignisse vorhanden sind, die auf ein Problem hinweisen können.
- **Webservicesql-Dienst:** Webdienste werden in IIS gehostet. Wenn Sie nicht ausgeführt werden, stellen Sie sicher, dass IIS ausgeführt wird (oder gestartet). Sie können auch versuchen, den Webdienst zurückzusetzen, indem Sie an einer Eingabeaufforderung **iisreset** eingeben.
- **SQL-Dienst:** Jeder Dienst mit Ausnahme des selbst Aktualisierungs-Dienstanbieter erfordert, dass der SQL-Dienst ausgeführt wird. Wenn eine der Protokolldateien SQL-Verbindungsprobleme anzeigt, überprüfen Sie

zuerst den SQL-Dienst. Um auf den SQL-Dienst zuzugreifen, klicken Sie auf **Start**, zeigen Sie auf **Verwaltung**, klicken Sie auf **Dienste**, und suchen Sie dann nach einem der folgenden Informationen:

- **MSSQLSERVER** (wenn Sie WMSDE oder MSDE verwenden, oder wenn Sie SQL Server verwenden und den Standardinstanznamen für den Instanznamen verwenden)
- **MSSQL \$ WSUS** (wenn Sie eine SQL Server Datenbank verwenden und die WSUS-Daten Bank Instanz benannt haben)

Klicken Sie mit der rechten Maustaste auf den Dienst, und klicken Sie dann auf **starten** , wenn der Dienst nicht ausgeführt wird, oder **neu starten** , um den Dienst zu aktualisieren, falls er ausgeführt wird

ISV-Unterstützung für Express-Updatebereitstellung

24.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Windows Server 2016

Windows 10-Updatedownloads können groß sein, da jedes Paket alle zuvor veröffentlichten Korrekturen enthält, um Konsistenz und Einfachheit sicherzustellen.

Seit Version 7 konnte für Windows die Größe von Downloads mit Windows-Updates mit dem Feature **Express** reduziert werden. Dieses Feature wird von Verbrauchergeräten zwar standardmäßig unterstützt, aber für Windows 10 Enterprise-Geräte muss Windows Server Update Services (WSUS) verwendet werden, um Express nutzen zu können.

Unterstützung von Express durch Microsoft

- **Express für eigenständiges WSUS**

Die Express-Updatebereitstellung ist **für alle unterstützten Versionen von WSUS bereits verfügbar**.

- **Express auf Geräten, die direkt mit Windows Update verbunden sind**

Für Verbrauchergeräte wird der Express-Download unterstützt: Der Windows Update-Client (WU) wird zum Überprüfen, Herunterladen und Installieren von Updates verwendet. Während der Downloadphase fordert der WU-Client Express-Pakete an und lädt die entsprechenden Bytebereiche herunter.

- **Enterprise-Geräte, die mit Windows Update for Business verwaltet werden, profitieren ebenfalls von der Unterstützung der Express-Updatebereitstellung ohne Änderung der Konfiguration.**

Nutzen von Express durch ISVs

ISVs können WSUS und den WU-Client verwenden, um die Express-Updatebereitstellung zu unterstützen.

Microsoft empfiehlt die folgenden drei Schritte, die in den folgenden Abschnitten ausführlicher erläutert werden:

1. **Konfigurieren von WSUS**

WSUS-Server ist für Überprüfungs- und Updatesynchronisierungen erforderlich (weitere Informationen [hier](#))

2. **Angeben und Füllen eines ISV-Dateicaches**

Die Verwendung eines ISV-Dateicaches wird empfohlen, um den Updateinhalt zu hosten, also die CABINET-Dateien(.cab) des Updates und die Express-Pakete (.psf).

3. **Einrichten eines ISV-Client-Agents zum Steuern von WU-Clientvorgängen**

NOTE

Das kumulative Update für Windows 10 Version 1607 vom Januar 2017 ([KB3213986 \(Betriebssystembuild 14393.693\)](#)) muss installiert sein.

- Mit dem ISV-Client-Agent wird festgelegt, welche Updates genehmigt und wann Updates heruntergeladen und installiert werden.
- Mit dem WU-Client werden die herunterzuladenden Bytebereiche ermittelt, und die Downloadanforderung

wird initiiert.

Schritt 1: Konfigurieren von WSUS

WSUS dient als Schnittstelle für Windows Update und zum Verwalten aller Metadaten zur Beschreibung von Express-Paketen, die heruntergeladen werden müssen. Informationen zur Bereitstellung findest du unter [Übersicht über Windows Server Update Services 3.0 SP2](#). Nachdem WSUS bereitgestellt wurde, musst du zunächst die Entscheidung treffen, ob Updateinhalte lokal auf dem WSUS-Server gespeichert werden sollen. Beim Konfigurieren von WSUS empfehlen wir, Updates nicht lokal zu speichern. Hierbei wird angenommen, dass du bereits über Software verfügst, mit der die Bereitstellung dieser Pakete in deiner Umgebung gesteuert wird. Weitere Informationen zur Konfiguration des lokalen WSUS-Speichers findest du unter [Festlegen des Speicherorts für Updates](#).

Schritt 2: Angeben und Füllen des ISV-Dateicaches

Angeben des ISV-Dateicaches

Mit neuen clientseitigen Einstellungen für die Gruppenrichtlinie und die Verwaltung mobiler Geräte (Mobile Device Management, MDM), die in der [Referenz zum Konfigurationsdienstanbieter](#) ausführlich beschrieben sind, wird der Speicherort des ISV-Dateicaches beschrieben.

NAME	BESCHREIBUNG
Konfiguriere einen anderen Downloadspeicherort für Updates.	Gibt einen alternativen Intranetserver zum Hosten von Updates von Microsoft Update an. Du kannst diesen Updatedienst dann verwenden, um Computer in deinem Netzwerk automatisch zu aktualisieren.

Beim Einrichten des alternativen Downloadspeicherorts für den ISV-Dateicache hast du zwei Optionen:

1. Gib einen ISV-HTTP-Serverhostnamen an. Dies ist der ISV-Dateicache.

Bei diesem Ansatz wird der WU-Client so konfiguriert, dass Downloadanforderungen an den HTTP-Server gesendet werden, der in der Richtlinie angegeben ist.

2. Angeben von „localhost“

Bei diesem Ansatz wird der WU-Client so konfiguriert, dass Downloadanforderungen an „localhost“ gesendet werden. Der ISV-Client-Agent kann diese Anforderungen dann verarbeiten und entsprechend weiterleiten, um die Downloadanforderung zu erfüllen.

IMPORTANT

Für den ISV-Dateicache ist Folgendes erforderlich:

- Der Server muss HTTP 1.1-konform gemäß RFC sein: <http://www.w3.org/Protocols/rfc2616/rfc2616.html>
Der Webserver muss **HEAD**- und **GET**-Anforderungen unterstützen.
 - Teilbereichsanforderungen
 - Keep-Alive
 - „Transfer-Encoding:chunked“ nicht verwenden

Füllen des ISV-Dateicaches

Der ISV-Dateicache muss mit Dateien gefüllt werden, die den auf verwalteten Clients zu installierenden Updates zugeordnet sind.

Fülle den ISV-Dateicache wie folgt auf:

- Verwende [WSUS-APIs](#), um auf den Dateipfad des Updates und den Dateinamen für den MU-Dienst zuzugreifen.

Die Metadaten für jedes Update auf dem WSUS-Server enthalten den Dateipfad des Updates und den Dateinamen unter Microsoft Update wie folgt (Microsoft Update-Hostname in Fettdruck, gefolgt von Dateipfad und -name): <http://download.windowsupdate.com>

/c/msdownload/update/software/updt/2016/09/windows10.0-kb3195781-x64_0c06079bcc35cba35a48bd2b1ec46f818bd2e74.msu

2. Lade Dateien von Microsoft Update herunter, und speichere sie mit einem dieser beiden Verfahren im ISV-Dateicache:

- Speichern der Dateien, indem du **den gleichen Ordnerpfad wie für den MU-Dienst verwendest**
- Speichern der Dateien mit einem **vom ISV definierten Ordnerpfad**

Der HTTP-Server (bzw. „localhost“) sollte so eingerichtet werden, dass **HTTP GET-Anforderungen**, in denen auf den MU-Ordnerpfad und den zugehörigen Dateinamen verwiesen wird, an den Speicherort der ISV-Datei umgeleitet werden.

Schritt 3: Einrichten eines ISV-Client-Agents zum Steuern von WU-Clientvorgängen

Der ISV-Client-Agent orchestriert den Download und die Installation von genehmigten Updates, indem der folgende Workflow verwendet wird:

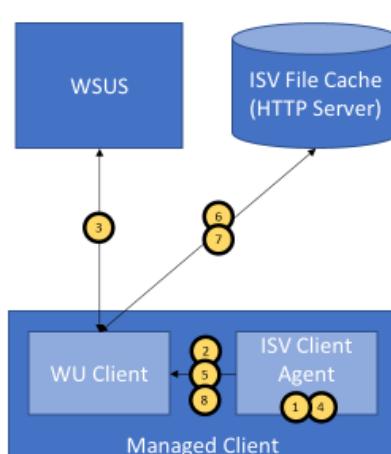
1. Der ISV-Client-Agent ruft den WU-Client auf, um einen Überprüfungsvorgang für den WSUS-Server auszuführen.
2. Beim Überprüfungsvorgang werden die jeweiligen Updates für den WU-Client zurückgegeben.
3. Der ISV-Client bestimmt, welche Updates genehmigt, heruntergeladen und installiert werden.
4. Der ISV-Client-Agent ruft den WU-Client auf, um die genehmigten Updates herunterzuladen.
5. Nachdem die Updates heruntergeladen wurden, ruft der ISV-Client-Agent den WU-Client auf, um die genehmigten Updates zu installieren.

Weitere Informationen zur Nutzung des WU-Clients zum Überprüfen, Herunterladen und Installieren von Updates findest du unter [Suchen, Herunterladen und Installieren von Updates](#).

Optionen des Workflows für den Download

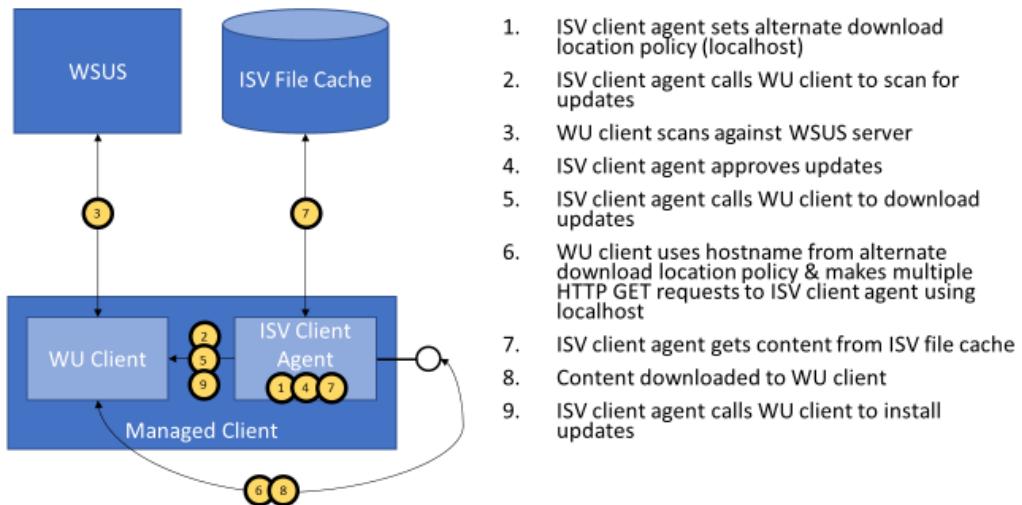
Hier sind zwei Abbildungen mit den Optionen des Workflows für den Download eines ISV-Dateicaches angegeben:

Download from ISV file cache using HTTP server



1. ISV client agent sets alternate download location policy
2. ISV client agent calls WU client to scan for updates
3. WU client scans against WSUS server
4. ISV client agent approves updates
5. ISV client agent calls WU client to download updates
6. WU client uses hostname from alternate download location policy & makes multiple HTTP GET requests to ISV file cache
7. Content downloaded to WU client
8. ISV client agent calls WU client to install updates

Download from ISV file cache using localhost & ISV client agent



Funktionsweise des Express-Downloads

- Für Betriebssystemupdates, die Express unterstützen, sind zwei Versionen der Dateinutzlast im Dienst gespeichert:
 - **Vollständige Dateiversion:** Ersetzt im Wesentlichen die lokalen Versionen der Updatebinärdateien.
 - **Express-Version:** Enthält die Deltas, die zum Patchen der vorhandenen Binärdateien auf dem Gerät erforderlich sind.

Sowohl auf die vollständige Dateiversion als auch auf die Express-Version wird in den Metadaten des Updates verwiesen, die im Rahmen der Überprüfungsphase auf den Client heruntergeladen wurden.

Der Express-Download funktioniert wie folgt:

Der WU-Client versucht zuerst, Express herunterzuladen. Unter bestimmten Umständen wird bei Bedarf auf die vollständige Dateiversion zurückgegriffen (z. B. bei Verwendung eines Proxys, der Bytebereichsanforderungen nicht unterstützt).

1. Wenn der WU-Client einen Express-Download initiiert, lädt der WU-Client zuerst einen Stub herunter, der Teil des Express-Pakets ist.
2. Der WU-Client sendet diesen Stub an Windows Installer, der den Stub für eine lokale Inventur verwendet. Hierbei werden die Deltas der Datei auf dem Gerät damit verglichen, was erforderlich ist, um die neueste Version der bereitgestellten Datei abzurufen.
3. Windows Installer fordert dann den WU-Client zum Herunterladen der Bereiche auf, die als erforderlich bestimmt wurden.
4. Der WU-Client lädt diese Bereiche herunter und leitet sie an Windows Installer weiter, der die Bereiche anwendet und dann bestimmt, ob weitere Bereiche erforderlich sind. Dies wird wiederholt, bis Windows Installer den WU-Client informiert, dass alle erforderlichen Bereiche heruntergeladen wurden.

Der Download ist dann abgeschlossen, und das Update kann installiert werden.

Reduzierung der Bandbreitennutzung durch Übermittlungsoptimierung

Die Übermittlungsoptimierung ist eine selbstorganisierende Lösung für verteilten Cache für Unternehmen, die die Bandbreitennutzung für Updates bzw. Upgrades von Betriebssystemen und Anwendungen reduzieren möchten.

Dank der Übermittlungsoptimierung können Clients diese Elemente basierend auf dem angegebenen Downloadspeicherort (in diesem Fall der ISV-Dateicache) von alternativen Quellen (z. B. andere Peers im Netzwerk) herunterladen.

Standardmäßig ermöglicht die Übermittlungsoptimierung in Windows 10 Enterprise und Education die Peer-to-Peer-Freigabe nur innerhalb des Netzwerks der Organisation. Du kannst dies über die Gruppenrichtlinie und in den Einstellungen der Verwaltung mobiler Geräte (Mobile Device Management, MDM) aber abweichend konfigurieren.

Weitere Informationen zur Übermittlungsoptimierung findest du unter [Übermittlungsoptimierung für Windows 10-Updates](#).

ISV-Unterstützung für monatliche Delta-Updates ohne WSUS

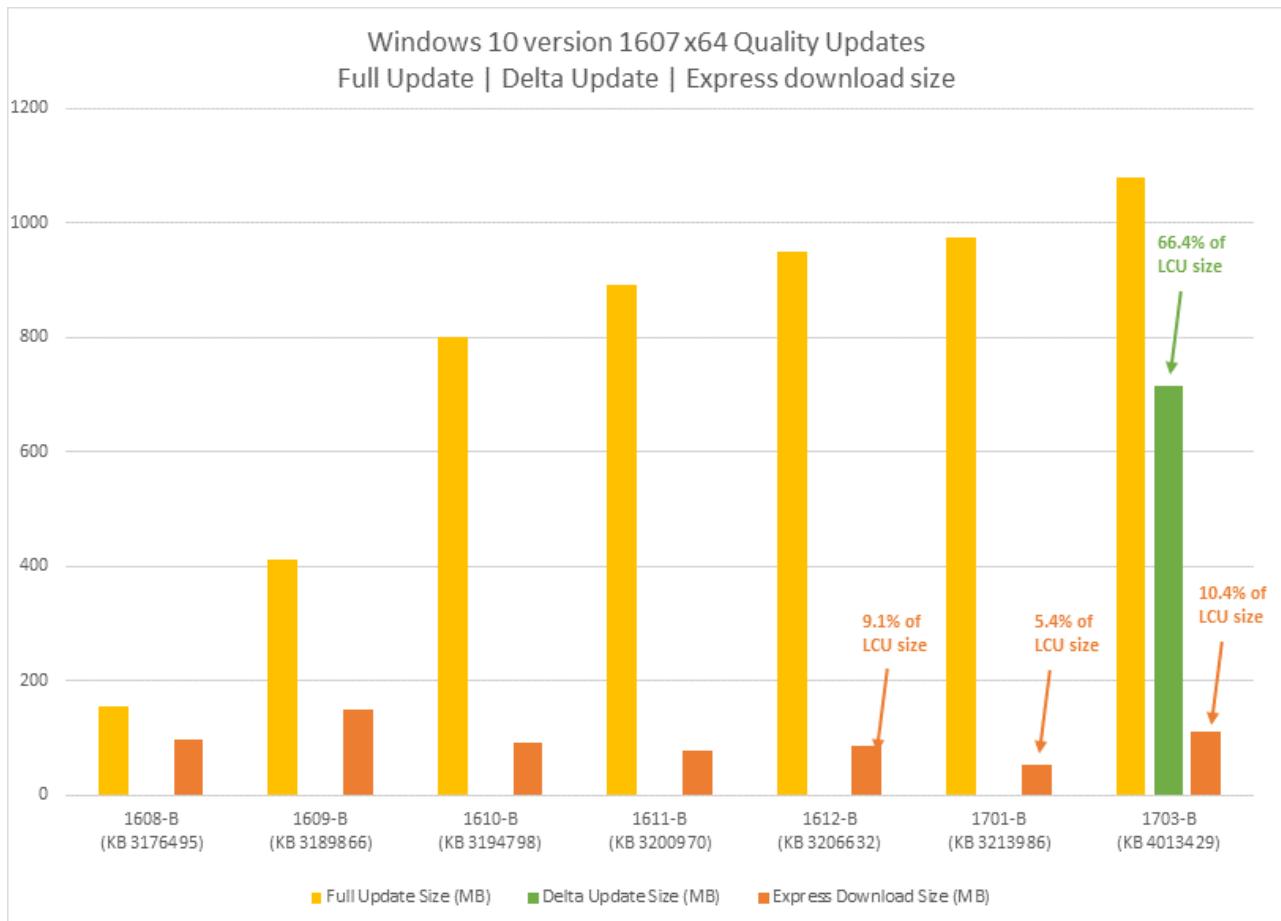
24.04.2020 • 7 minutes to read • [Edit Online](#)

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

Windows 10-Updatedownloads können groß sein, da jedes Paket alle zuvor veröffentlichten Korrekturen enthält, um Konsistenz und Einfachheit sicherzustellen.

Seit Version 7 kann Windows mithilfe des [Express](#)-Features die Größe von Windows Update-Downloads reduzieren. Obwohl Verbrauchergeräte dieses Feature standardmäßig unterstützen, erfordern Windows 10 Enterprise-Geräte Windows Server Update Services (WSUS), um Express nutzen zu können. Wenn Sie über WSUS verfügen, finden Sie weitere Informationen unter [ISV-Unterstützung für die Express-Updatebereitstellung](#). Wir empfehlen die Verwendung zum Aktivieren der Express-Updatebereitstellung.

Wenn WSUS derzeit nicht installiert ist, Sie vorläufig jedoch kleinere Updatepaketgrößen benötigen, können Sie ein monatliches Delta-Update verwenden. Durch das Delta-Update werden die Paketgrößen zwar erheblich reduziert, jedoch nicht so sehr wie bei der WSUS-Express-Updatebereitstellung. Es wird empfohlen, nach Möglichkeit ein WSUS-Express-Update bereitzustellen, um die Paketgrößen maximal zu verringern. Im folgenden Diagramm werden Downloadgrößen für Delta-Updates, kumulative Updates und Express-Updates für Windows 10 Version 1607 verglichen:



Was ist ein monatliches Delta-Update?

Es gibt zwei Varianten des monatlichen Sicherheitsupdates: Delta-Updates und kumulative Updates.

Das monatliche Delta-Update ist neu und eine vorläufige Lösung für unabhängige Softwarehersteller, die nicht über WSUS verfügen, um die Paketgrößen zu verringern.

IMPORTANT

Das Delta-Update ist für die Wartung von Windows 10 Version 1607 (Anniversary Update), Version 1703 (Creators Update) und Version 1709 (Fall Creators Update) verfügbar. Für Releases nach Version 1709 müssen Sie eine Bereitstellungsinfrastruktur implementieren, die die [Express-Updatebereitstellung](#) unterstützt, um weiterhin inkrementelle Updates nutzen zu können.

Bei Verwendung des monatlichen Delta-Updates enthalten Pakete nur die Updates eines Monats. Ein monatliches kumulatives Update enthält alle Updates bis zu diesem Update, was zu einer umfangreichen Datei führt, die jeden Monat vergrößert wird. Sowohl Delta als auch monatliche Updates werden am zweiten Dienstag eines jeden Monats veröffentlicht (auch bekannt als „Update-Dienstag“ bekannt). In der folgenden Tabelle werden Delta-Updates und kumulative Updates verglichen:

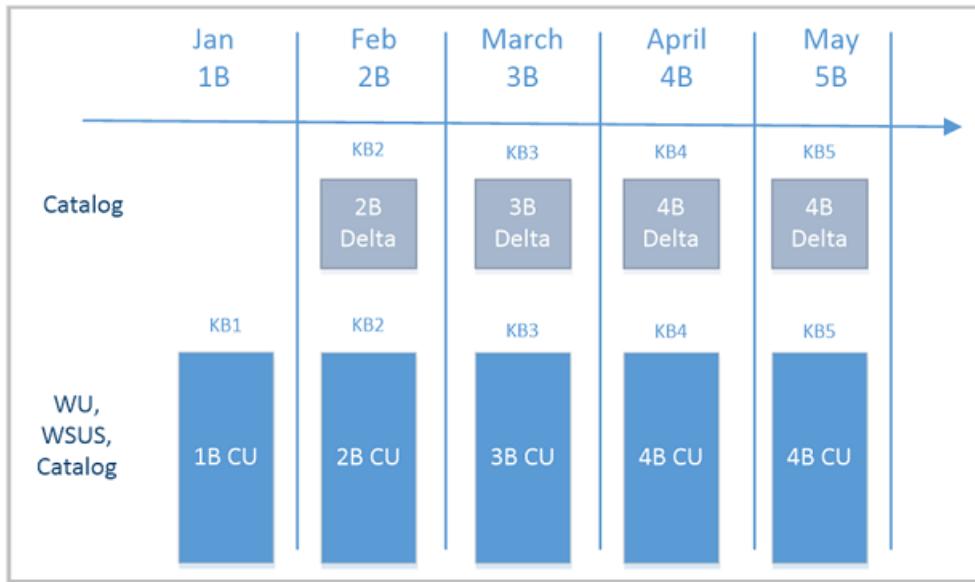
	MONATLICHES DELTA-UPDATE	MONATLICHES KUMULATIVES UPDATE
Scope	einzelnes Update nur mit neuen Fehlerbehebungen für diesen Monat	einzelnes Update mit allen neuen Fehlerbehebungen für diesen und die vorherigen Monate
Application	kann nur angewendet werden, wenn das Update des vorherigen Monats angewendet wurde (kumulatives Update oder Delta-Update)	kann jederzeit angewendet werden
Bereitstellung	wird nur im Windows Update-Katalog veröffentlicht, wo es zur Verwendung mit anderen Tools oder Prozessen heruntergeladen werden kann; wird nicht für PCs angeboten, die mit Windows Update verbunden sind	wird in Windows Update (wo es von allen Verbrauchercomputern installiert wird), WSUS und dem Windows Update-Katalog veröffentlicht

Delta-Updates und kumulative Updates verfügen über die gleiche KB-Nummer, die gleiche Klassifizierung und werden zur gleichen Zeit veröffentlicht. Updates können entweder durch den Updatetitel im Katalog oder durch den Namen der MSU unterschieden werden:

- 02/2017 ***Delta-Update*** für Windows 10 Version 1607 für x64-basierte Systeme (KB1234567)
- 02/2017 ***Kumulatives Update*** für Windows 10 Version 1607 für x86-basierte Systeme (KB1234567)

Verwendung des monatlichen Delta-Updates

Wenn die Größe eines Updates für das Clientgerät von Bedeutung ist, werden für Geräte, auf denen das Update des Vormonats installiert wurde, Delta-Updates und für Geräte, auf denen diese Updates nicht installiert wurden, kumulative Updates empfohlen. Auf diese Weise benötigen alle Geräte nur ein einzelnes Update, um sie auf den neuesten Stand zu bringen. Dies erfordert eine geringfügige Anpassung des gesamten Updateverwaltungsprozesses, da Sie basierend auf der Aktualität der Geräte in der Organisation unterschiedliche Updates bereitstellen müssen:



Verhindern der Bereitstellung von Delta-Updates und kumulativen Updates im selben Monat

Da das Delta-Update und das kumulative Update gleichzeitig verfügbar sind, ist es wichtig zu verstehen, was geschieht, wenn Sie beide Updates im selben Monat bereitstellen.

Wenn Sie die gleiche Version des Delta-Updates und des kumulativen Updates genehmigen und bereitstellen, generieren Sie nicht nur zusätzlichen Netzwerkspaceverbrauch, da beide auf den PC heruntergeladen werden, sondern Sie können Ihren Computer nach dem Neustart möglicherweise nicht mit Windows neu starten.

Wenn versehentlich Delta-Updates und kumulative Updates installiert sind und der Computer nicht mehr gestartet wird, können Sie diesen mit den folgenden Schritten wiederherstellen:

1. Starten Sie den Computer über die WinRE-Eingabeaufforderung.
2. Listen Sie die Pakete mit dem Status „Ausstehend“ auf:

```
x:\windows\system32\dism.exe /image:<drive letter for windows directory> /Get-Packages >> <path to text file>
```

Beispiel: x:\windows\system32\dism.exe /image:c:\ /Get-Packages >> c:\temp\packages.txt

3. Öffnen Sie die Textdatei, in die Sie **get-packages** weitergeleitet haben. Führen Sie **remove-package** für jeden Paketnamen aus, wenn für die Installation ausstehende Patches angezeigt werden:

```
dism.exe /image:<drive letter for windows directory> /remove-package /packagename:<package name>
```

Beispiel:

```
x:\windows\system32\dism.exe /image:c:\ /remove-package /packagename:Package_for_KB4014329~31bf3856ad364e35~amd64~~10.0.1.0
```

NOTE

Entfernen Sie keine für die Deinstallation ausstehenden Patches.

IMPORTANT

Das Delta-Update ist für die Wartung von Windows 10 Version 1607 (Anniversary Update), Version 1703 (Creators Update) und Version 1709 (Fall Creators Update) verfügbar. Für Releases nach Version 1709 müssen Sie eine Bereitstellungsinfrastruktur implementieren, die die [Express-Updatebereitstellung](#) unterstützt, um weiterhin inkrementelle Updates nutzen zu können.

Migrieren der WSUS-Datenbank von wid zu SQL

21.05.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Führen Sie die folgenden Schritte aus, um die WSUS-Datenbank (SUSDB) von einer internen Windows-Daten Bank Instanz zu einer lokalen oder Remote Instanz von SQL Server zu migrieren.

Voraussetzungen

- SQL-Instanz. Hierbei kann es sich um den **MSSQLSERVER** -Standard Server oder um eine benutzerdefinierte Instanz handeln.
- SQL Server Management Studio
- WSUS mit installierter **wid**-Rolle
- IIS (Dies ist normalerweise der Fall, wenn Sie WSUS über Server-Manager installieren). Er ist noch nicht installiert. er muss sein.

Migrieren der WSUS-Datenbank

IIS-und WSUS-Dienste auf dem WSUS-Server abbrechen

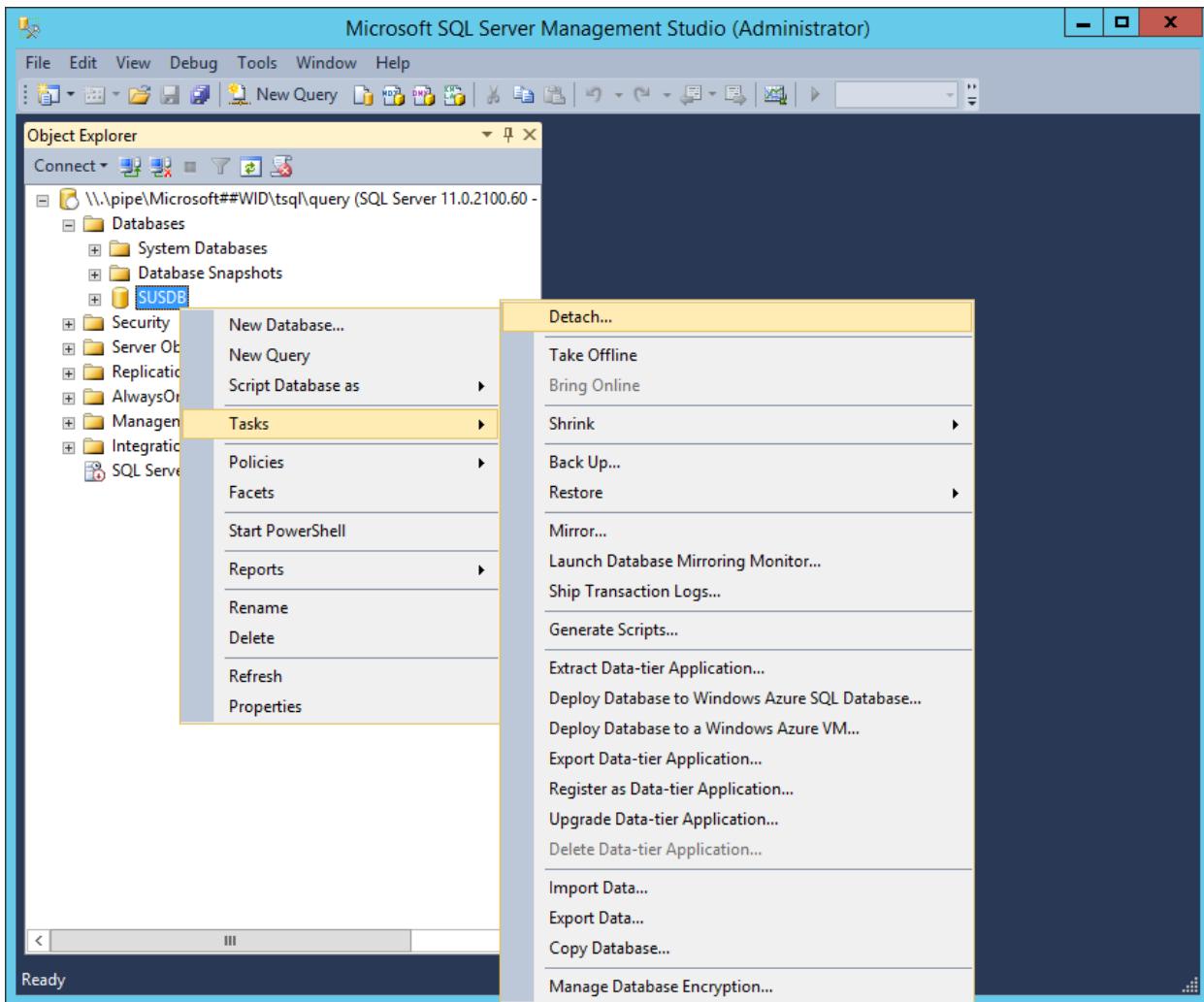
Führen Sie in PowerShell (mit erhöhten Rechten) Folgendes aus:

```
Stop-Service IISADMIN  
Stop-Service WsusService
```

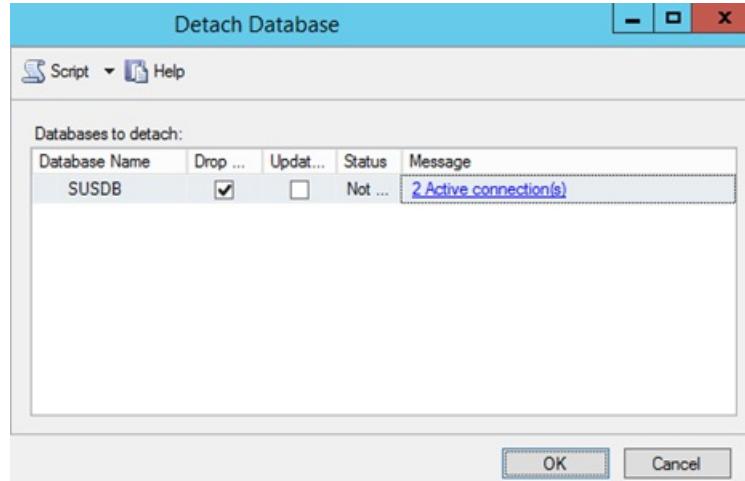
Trennen von SUSDB von der internen Windows-Datenbank

Verwenden von SQL Management Studio

1. Klicken Sie mit der rechten Maustaste auf **SUSDB** --> **Tasks** , - > Klicken Sie auf **trennen**:



2. Aktivieren Sie vorhandene Verbindungen löschen , und klicken Sie auf OK (optional, wenn aktive



Verbindungen vorhanden sind).

Verwenden der Eingabeaufforderung

IMPORTANT

Diese Schritte zeigen, wie Sie die WSUS-Datenbank (SUSDB) mit dem Hilfsprogramm **sqlcmd** von der internen Windows-Daten Bank Instanz trennen. Weitere Informationen zum **sqlcmd** -Hilfsprogramm finden Sie unter [sqlcmd Utility](#).

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten
2. Führen Sie den folgenden SQL-Befehl aus, um die WSUS-Datenbank (SUSDB) von der internen Windows-Daten Bank Instanz mit dem **sqlcmd** -Hilfsprogramm zu trennen:

```

sqlcmd -S \\.\pipe\Microsoft##WID\tsql\query
use master
GO
alter database SUSDB set single_user with rollback immediate
GO
sp_detach_db SUSDB
GO

```

Kopieren Sie die SUSDB-Dateien in die SQL Server

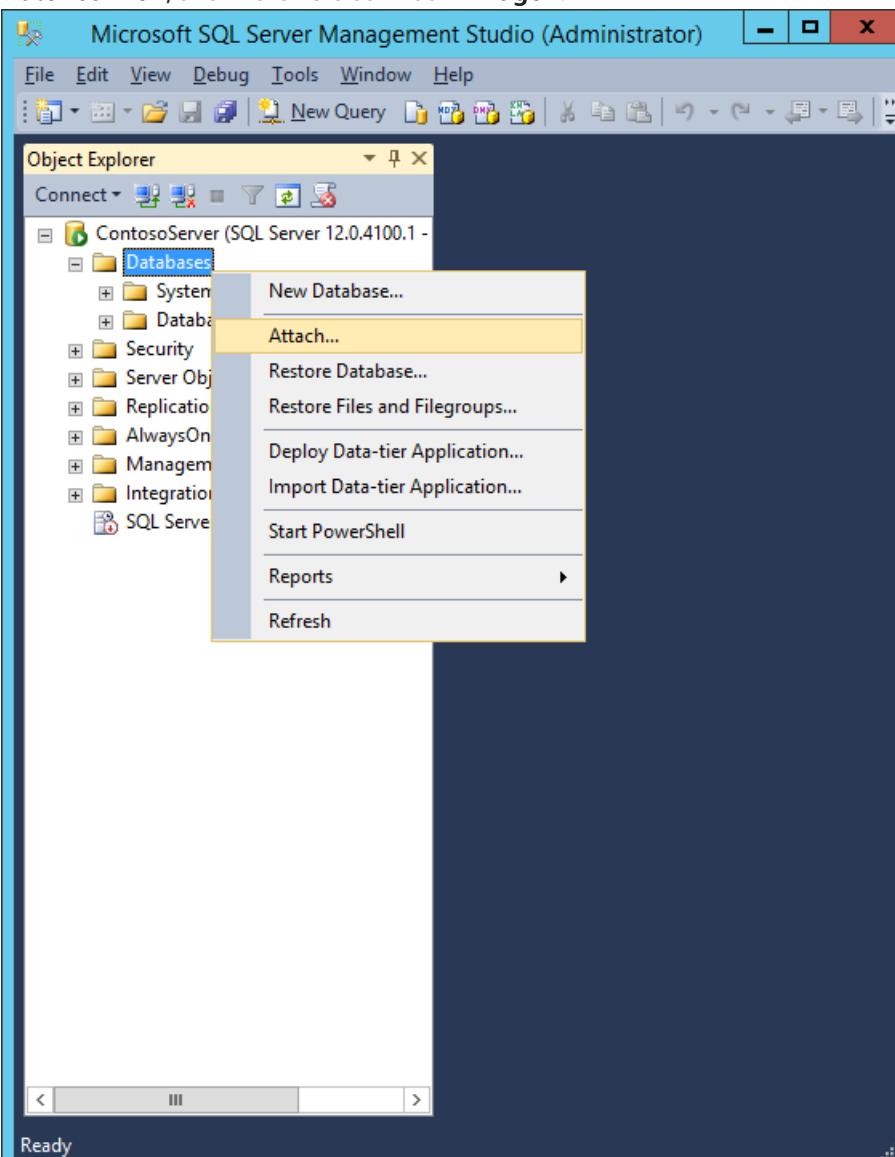
1. Kopieren Sie SUSDB.mdf und SUSDB_Log.ldf aus dem Ordner "wid Data" (% System Drive% \ Windows \ wid \ Data) in den SQL-instanzdatenordner.

TIP

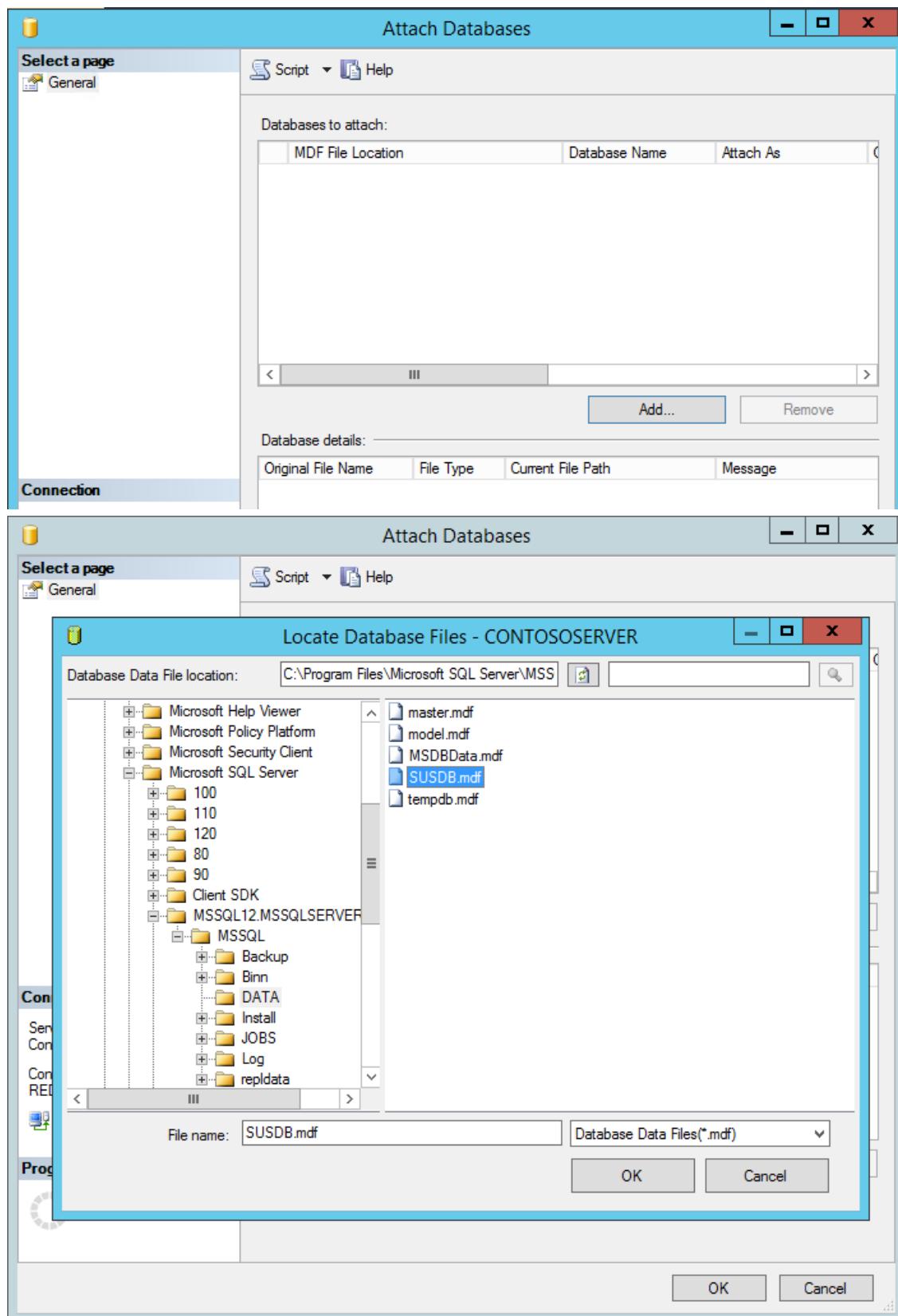
Wenn der SQL-instanzordner z. B. "c:\Programme\Microsoft SQL server\mssql12." lautet, Mssqlserver\mssql und der Ordner "wid Data" lautet "c:\windows\wid\data". Kopieren Sie die SUSDB-Dateien aus "c:\windows\wid\data" in "c:\Programme\Microsoft SQL server\mssql12.". MSSQLSERVER\MSSQL\Data

Anfügen von SUSDB an die SQL-Instanz

1. Klicken Sie in SQL Server Management Studio unter dem Instanzknoten mit der rechten Maustaste auf Datenbanken, und klicken Sie dann auf Anfügen.



2. Klicken Sie im Feld Datenbanken anfügen unter anzufügende Datenbanken auf die Schaltfläche Hinzufügen, suchen Sie nach der Datei SUSDB.mdf (aus dem Ordner wid kopiert), und klicken Sie dann auf OK.



TIP

Dies kann auch mithilfe von Transact-SQL durchgeführt werden. Anweisungen zum Anfügen einer Datenbank finden Sie in der SQL-Dokumentation.

Beispiel (Verwenden von Pfaden aus dem vorherigen Beispiel):

```
USE master;
GO
CREATE DATABASE SUSDB
ON
    (FILENAME = 'C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Data\SUSDB.mdf'),
    (FILENAME = 'C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Log\SUSDB_Log.ldf')
FOR ATTACH;
GO
```

Überprüfen von SQL Server und Daten Bank Anmeldungen und-Berechtigungen

Anmelde Berechtigungen SQL Server

Überprüfen Sie nach dem Anfügen der SUSDB, ob NT-Autorität \ Netzwerkdienst über Anmelde Berechtigungen für die Instanz von SQL Server verfügt, indem Sie folgende Schritte ausführen:

1. Gehe zu SQL Server Management Studio
2. Öffnen der Instanz
3. Klicken Sie auf Sicherheit
4. Klicken Sie auf Anmeldungen .

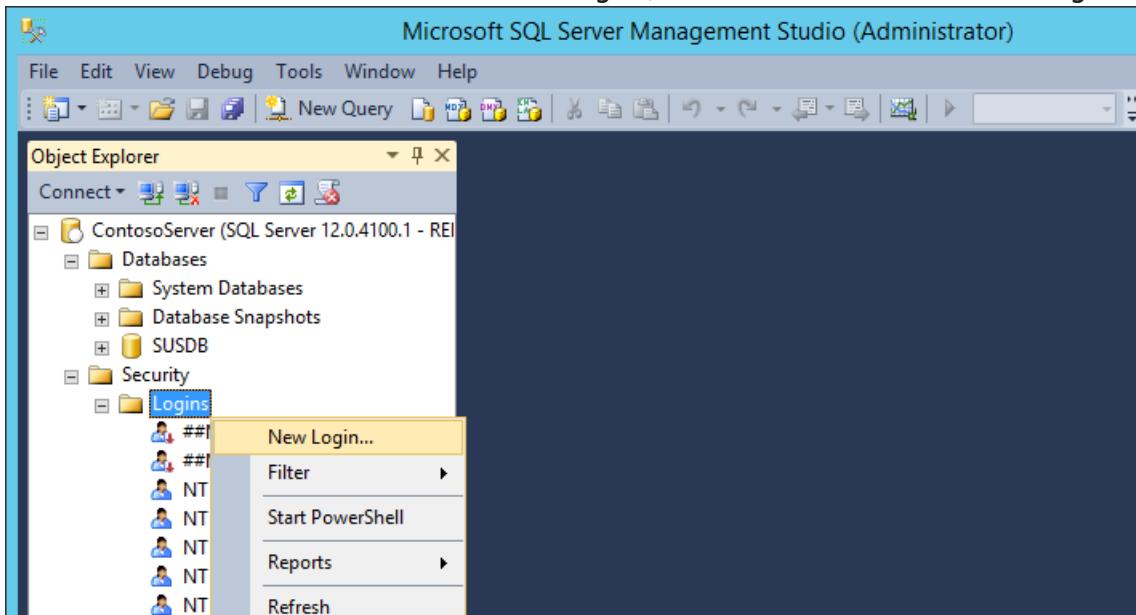
Das Konto NT-Autorität \ Netzwerkdienst sollte aufgeführt werden. Wenn dies nicht der Fall ist, müssen Sie diese hinzufügen, indem Sie einen neuen Anmelde Namen hinzufügen.

IMPORTANT

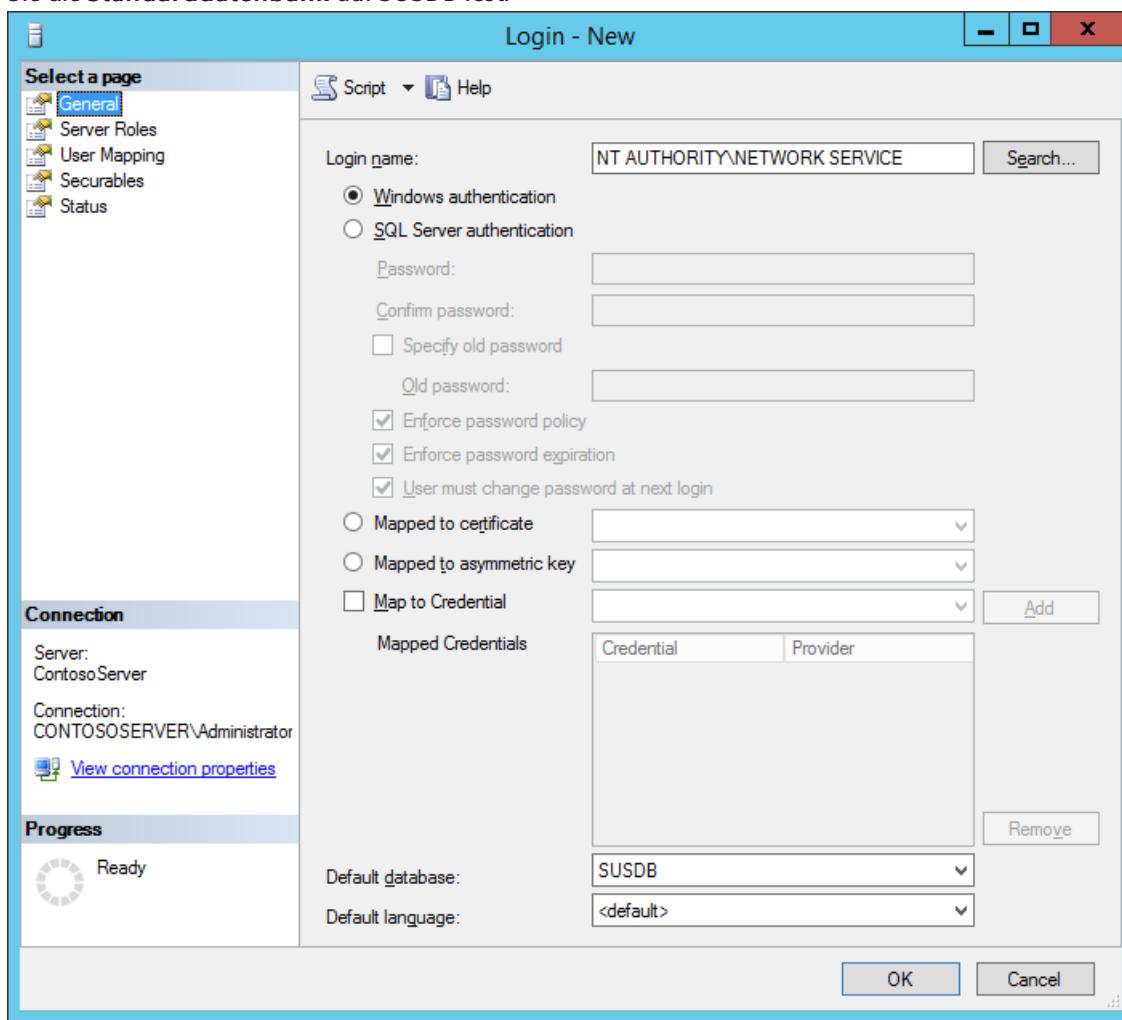
Wenn sich die SQL-Instanz auf einem anderen Computer als WSUS befindet, muss das Computer Konto des WSUS-Servers im Format [FQDN] \ [wsuscomputername] \\$ aufgeführt werden. Wenn dies nicht der Fall ist, können Sie mit den folgenden Schritten hinzugefügt werden, indem Sie NT-Autorität \ Netzwerkdienst durch das Computer Konto des WSUS-Servers ([FQDN] \ [wsuscomputername] \\$) ersetzen. Dies gilt zusätzlich zum erteilen von Berechtigungen für NT-Autorität \ Netzwerkdienst .

Hinzufügen von NT-Autorität \ Netzwerkdienst und erteilen von Berechtigungen

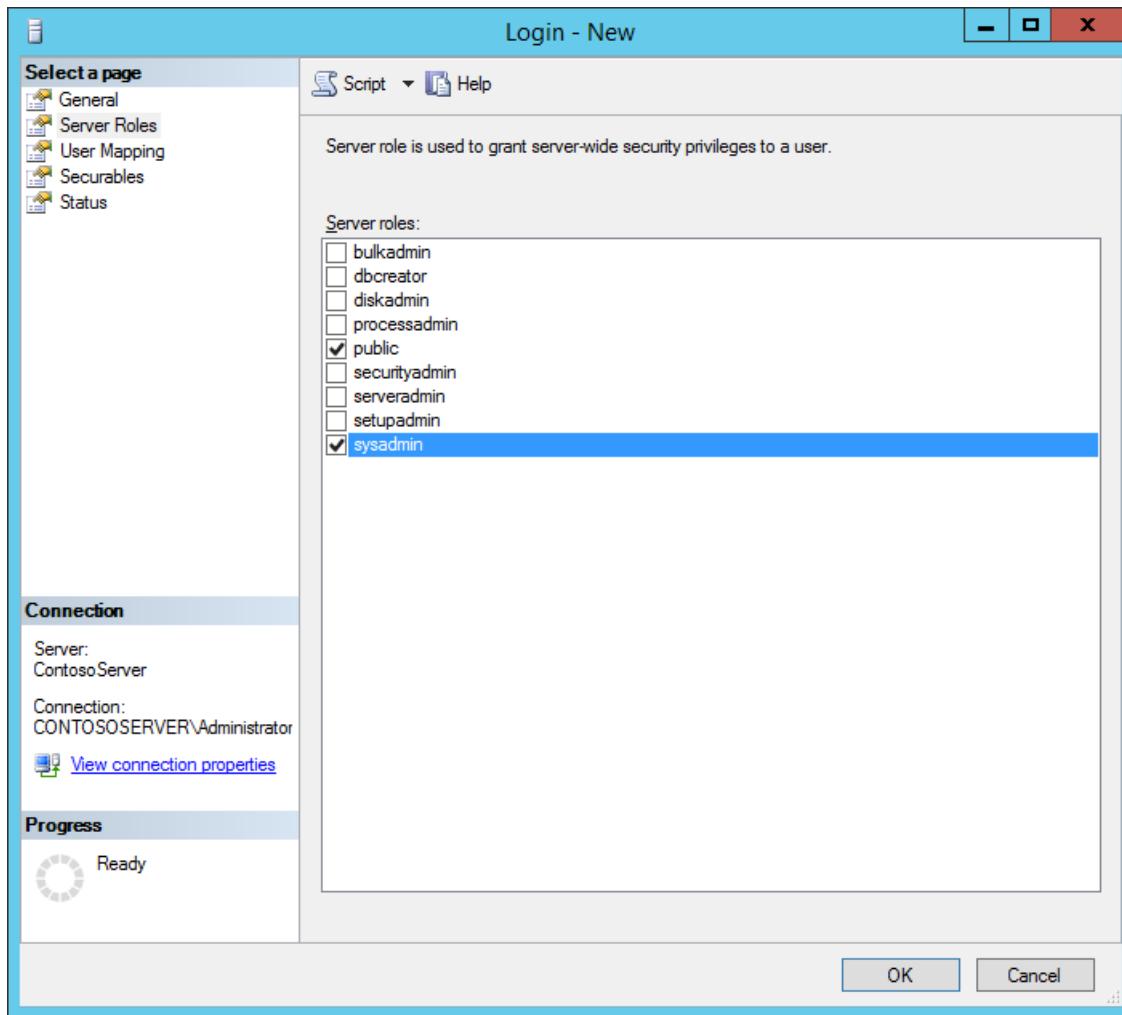
1. Klicken Sie mit der rechten Maustaste auf Anmeldungen , und klicken Sie auf neue Anmeldung.



2. Geben Sie auf der Seite Allgemein den Anmelde Namen (NT-Autorität \ Netzwerkdienst) ein, und legen Sie die Standarddatenbank auf SUSDB fest.

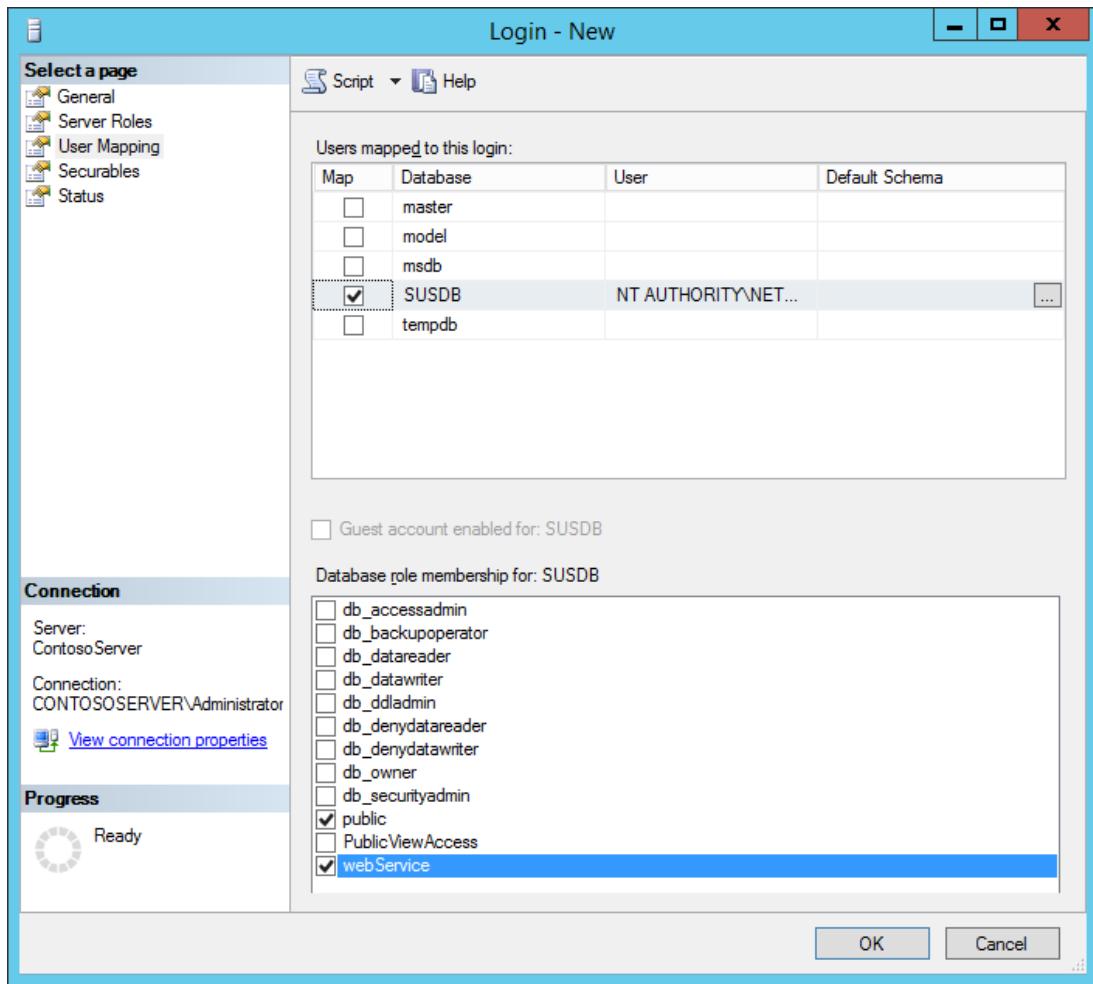


3. Vergewissern Sie sich, dass auf der Seite Server Rollen die Option Public und sysadmin ausgewählt ist.



4. Auf der Seite Benutzer Zuordnung :

- Unter **Benutzer**, die dieser Anmeldung zugeordnet sind: Wählen Sie **SUSDB** aus.
- Stellen Sie sicher, dass unter **Mitgliedschaft in Daten Bank Rolle für:** **SUSDB** Folgendes aktiviert ist:
 - **public**
 - **Webdienst**



5. Klicken Sie auf OK

Nun sollte NT-Autorität \ Netzwerkdienst unter Anmeldungen angezeigt werden.

Datenbankberechtigungen

1. Klicken Sie mit der rechten Maustaste auf die SUSDB.
2. Eigenschaften auswählen
3. Klicken Sie auf Berechtigungen

Das Konto NT-Autorität \ Netzwerkdienst sollte aufgeführt werden.

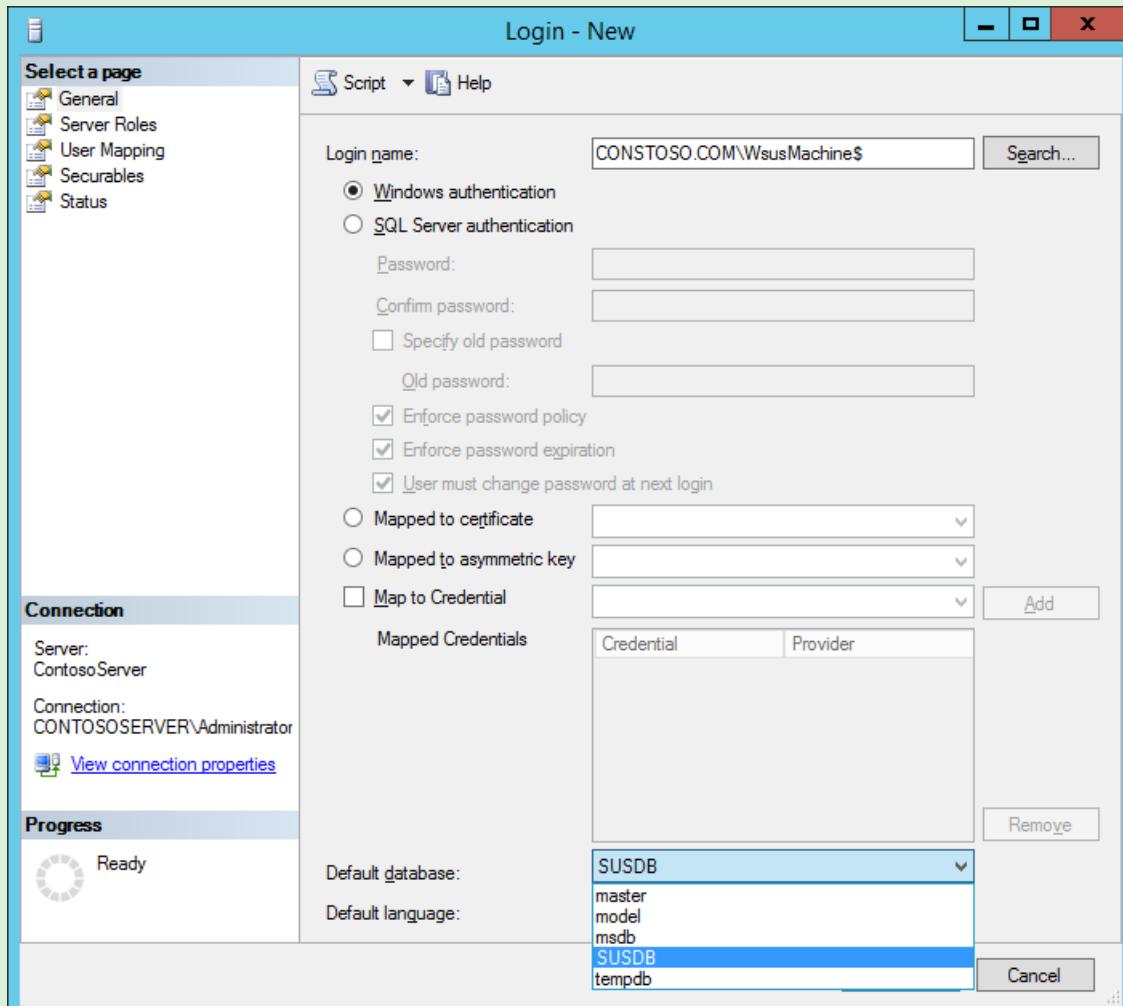
1. Wenn dies nicht der Fall ist, fügen Sie das Konto hinzu.
2. Geben Sie im Textfeld Anmelde Name den WSUS-Computer im folgenden Format ein:

[Vollständig verfügbar] \ [Wsuscomputername] \$

3. Vergewissern Sie sich, dass die Standarddatenbank auf SUSDB festgelegt ist.

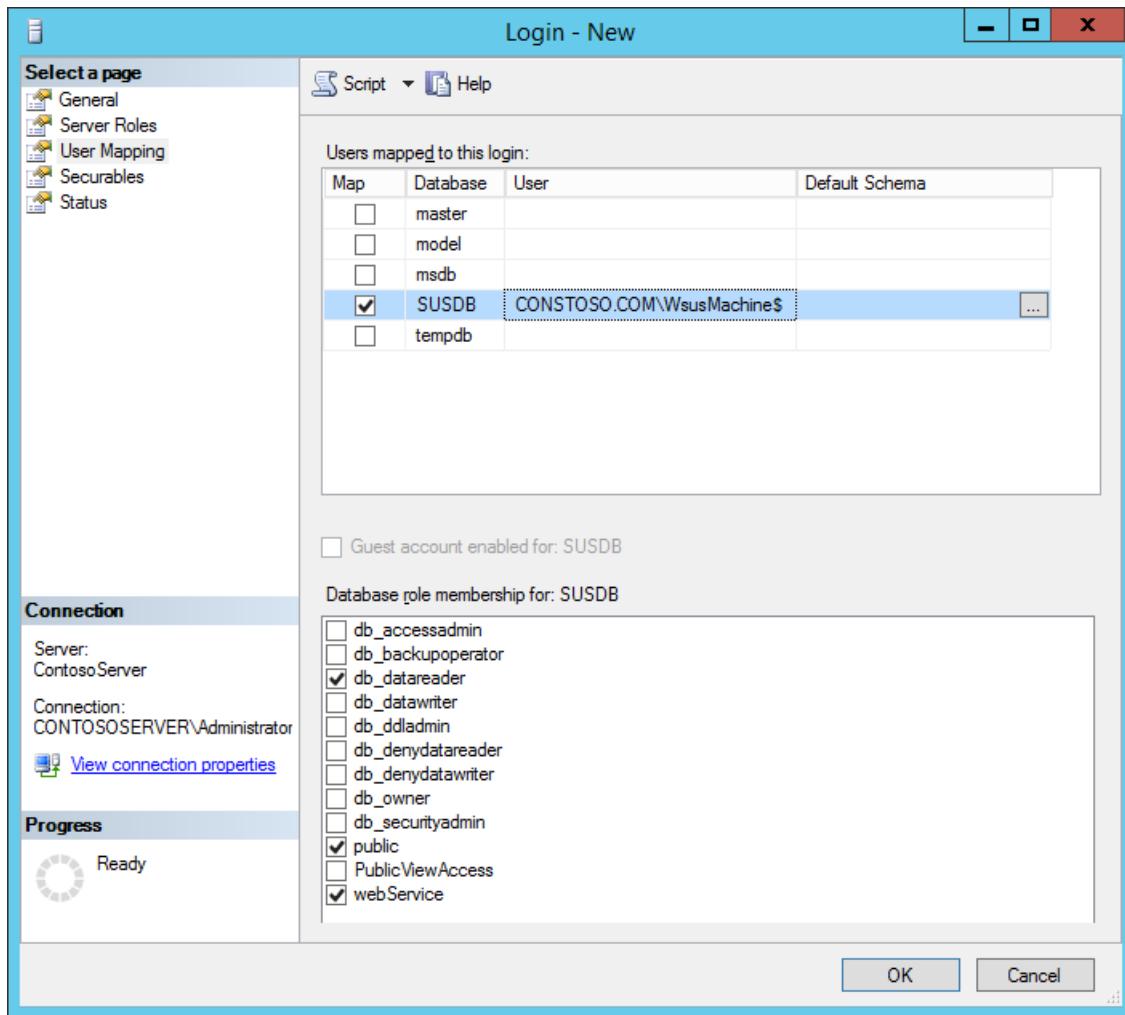
TIP

Im folgenden Beispiel lautet der FQDN "Contoso.com", und der WSUS-Computername lautet "wsusmachine":



4. Wählen Sie auf der Seite Benutzer Zuordnung unter Benutzer, die dieser Anmeldung zugeordnet sind die SUSDB -Datenbank aus.

5. Überprüfen Sie den Webdienst unter der Mitgliedschaft in Daten Bank Rolle für: SUSDB:



6. Klicken Sie auf **OK**, um Einstellungen zu speichern.

NOTE

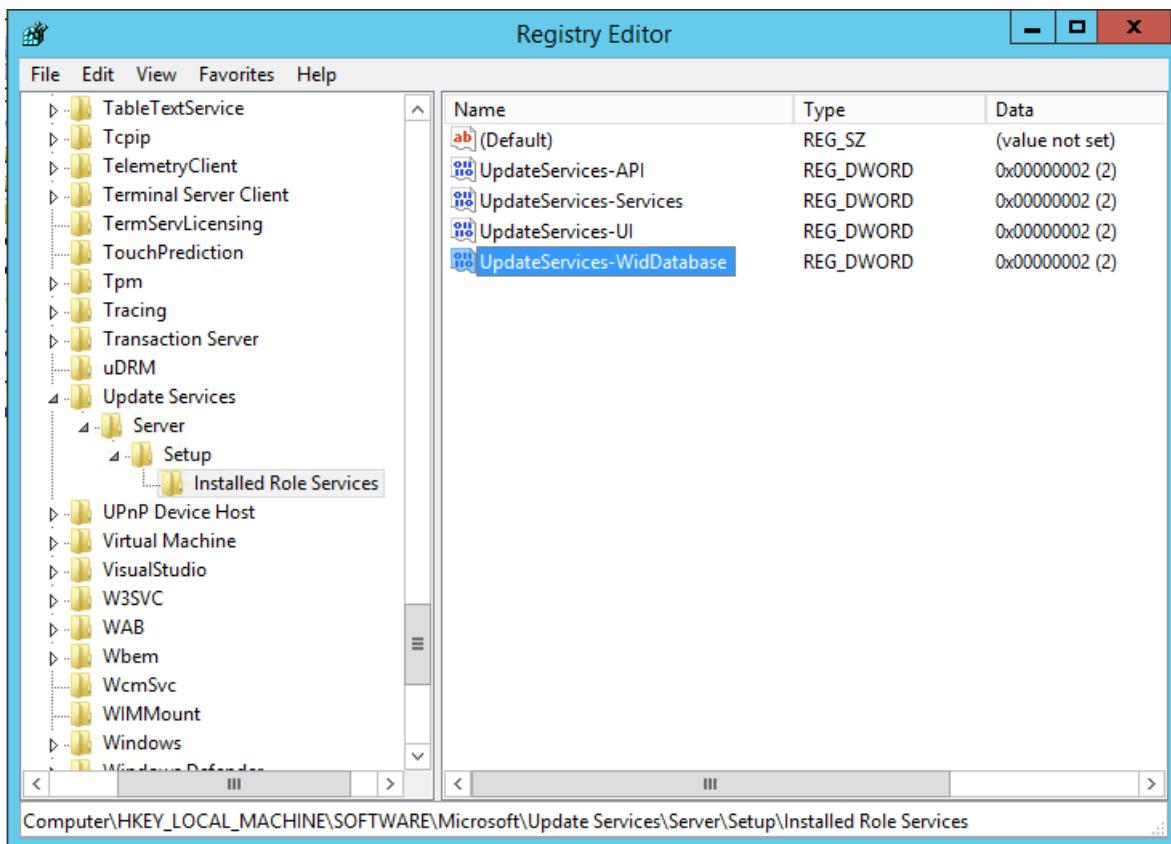
Möglicherweise müssen Sie den SQL-Dienst neu starten, damit die Änderungen wirksam werden.

Bearbeiten Sie die Registrierung, um WSUS auf die SQL Server Instanz zu verweisen.

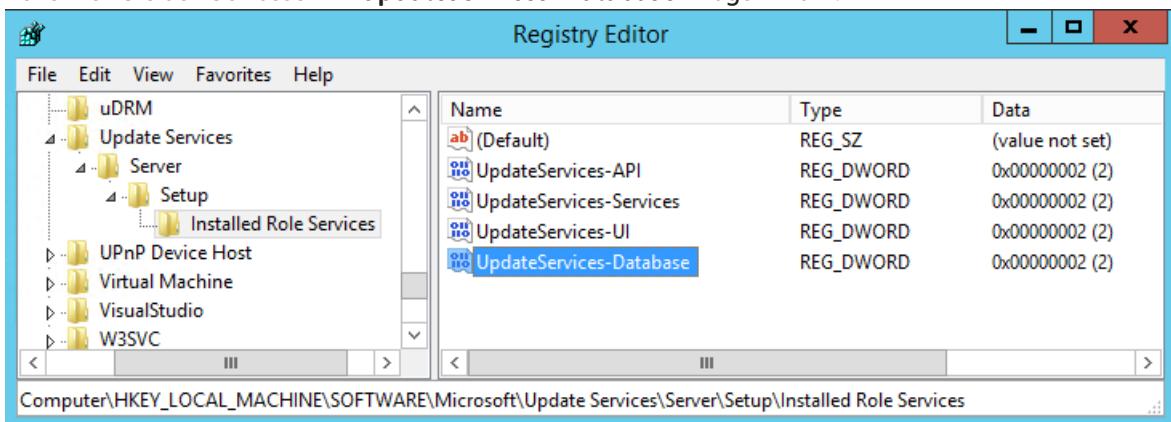
IMPORTANT

Folgen Sie den Schritten in diesem Abschnitt sorgfältig. Wird die Registrierung falsch angepasst, können schwerwiegende Probleme auftreten. Bevor Sie sie ändern, [sichern Sie die Registrierung zwecks Wiederherstellung](#) für den Fall, dass Probleme auftreten.

1. Klicken Sie auf **Start** und dann auf **Ausführen**. Geben Sie **regedit&** ein, und klicken Sie auf **OK**.
2. Suchen Sie den folgenden Schlüssel: **HKEY_LOCAL_MACHINE\software\microsoft\updateservices\server\setup\sqlservername**
3. Geben Sie im Textfeld **Wert** den Wert **[Servername] \ [InstanceName]** ein, und klicken Sie dann auf **OK**. Wenn der Instanzname die Standard Instanz ist, geben Sie **[Servername]** ein.
4. Suchen Sie den folgenden Schlüssel: **HKEY_LOCAL_MACHINE\software\microsoft\update services\server\setup\installierte Rolle services\updateservices-widdatabase**



5. Benennen Sie den Schlüssel in "updateservices-Database image41" um.



NOTE

Wenn Sie diesen Schlüssel nicht aktualisieren, versucht **WSUSUtil**, die wid anstelle der SQL-Instanz zu bedienen, zu der Sie migriert haben.

Starten der IIS-und WSUS-Dienste auf dem WSUS-Server

Führen Sie in PowerShell (mit erhöhten Rechten) Folgendes aus:

```
Start-Service IISADMIN
Start-Service WsusService
```

NOTE

Wenn Sie die WSUS-Konsole verwenden, schließen Sie sie, und starten Sie sie neu.

Deinstallieren der wid-Rolle (nicht empfohlen)

WARNING

Durch das Entfernen der wid-Rolle wird auch ein Daten Bank Ordner (%systemdrive%\Programme\Update services\database) entfernt, der Skripts enthält, die von "WSUSUtil.exe" für Aufgaben nach der Installation benötigt werden. Wenn Sie die wid-Rolle deinstallieren möchten, stellen Sie sicher, dass Sie den Ordner %systemdrive%\Programme\Update services\database vorab sichern.

Mithilfe von PowerShell:

```
Uninstall-WindowsFeature -Name 'Windows-Internal-Database'
```

Nachdem die wid-Rolle entfernt wurde, überprüfen Sie, ob der folgende Registrierungsschlüssel vorhanden ist:

HKEY_LOCAL_MACHINE\software\microsoft\update services\server\setup\installierte Rolle services\updateservices-Database

Systemdaten: Übersicht

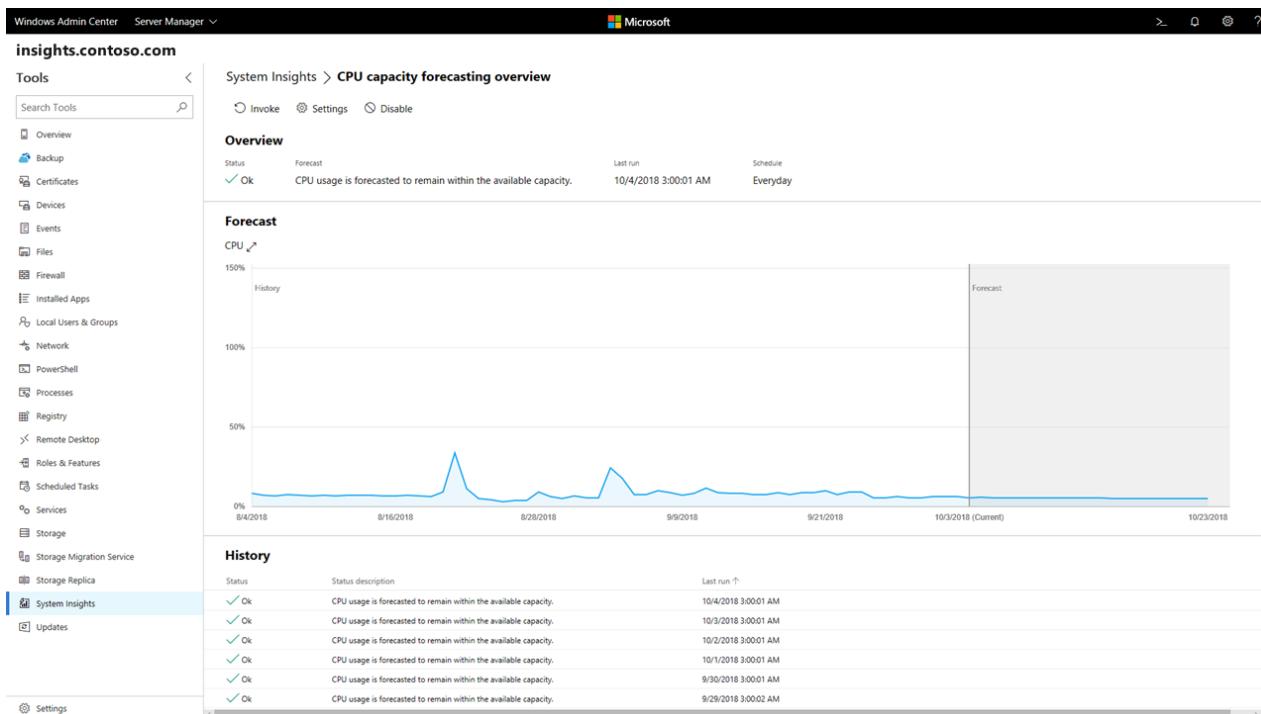
09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

System Insights ist ein neues Predictive Analytics Feature in Windows Server 2019. Die Vorhersagefunktionen von System Insights, die jeweils durch ein Machine Learning-Modell unterstützt werden, analysieren lokal Windows Server-System Daten (z. B. Leistungsindikatoren und Ereignisse), um Einblicke in die Funktionsweise Ihrer Server zu erhalten und die Betriebskosten zu reduzieren, die mit der reaktiven Verwaltung von Problemen in ihren bereit Stellungen einhergehen.

In Windows Server 2019 wird System Insights mit vier Standardfunktionen ausgeliefert, die sich auf die Kapazitäts Vorhersage konzentrieren, und zukünftige Ressourcen für Compute-, Netzwerk- und Speicherressourcen basierend auf Ihren vorherigen Verwendungs Mustern Vorhersagen. System Insights ist auch mit einer [erweiterbaren Infrastruktur](#)ausgeliefert, sodass von Microsoft und Drittanbietern neue Vorhersagefunktionen zu System Insights hinzugefügt werden können, ohne das Betriebs System zu aktualisieren.

Sie können System Einblicke über eine intuitive [Windows Admin Center](#) -Erweiterung oder [direkt über PowerShell](#)verwalten. mit System Insights können Sie jede Vorhersagefunktion separat entsprechend den Anforderungen Ihrer Bereitstellung konfigurieren. Alle Vorhersage Ergebnisse werden im Ereignisprotokoll veröffentlicht, sodass Sie [Azure Monitor](#) oder [System Center Operations Manager](#) verwenden können, um auf einfache Weise Vorhersagen für eine Gruppe von Computern zu aggregieren und anzuzeigen.



Lokale Funktionalität

System Insights wird vollständig lokal unter Windows Server ausgeführt. Mithilfe der neuen Funktionen, die in Windows Server 2019 eingeführt wurden, werden alle Ihre Daten direkt auf Ihrem Computer gesammelt, gespeichert und analysiert, sodass Sie Predictive Analytics Funktionen ohne cloudkonnektivität umsetzen können.

Die Systemdaten werden auf dem Computer gespeichert, und diese Daten werden anhand von Vorhersagefunktionen analysiert, die in der Cloud nicht umgeschult werden müssen. Mit System Insights können

Sie Ihre Daten auf Ihrem Computer speichern und weiterhin von Predictive Analytics Funktionen profitieren.

Erste Schritte

<https://www.youtube-nocookie.com/embed/AJxQkx5WSaA>

TIP

Sehen Sie sich diese kurzen Videos an, um die Informationen zu erhalten, die Sie für die ersten Schritte und die zuverlässige Verwaltung von System Insights benötigen: [Getting Started with System Insights in 10](#)

Voraussetzungen

System Insights ist auf jeder Windows Server 2019-Instanz verfügbar. Es wird auf Host- und Gast Computern, auf jedem Hypervisor und in jeder Cloud ausgeführt.

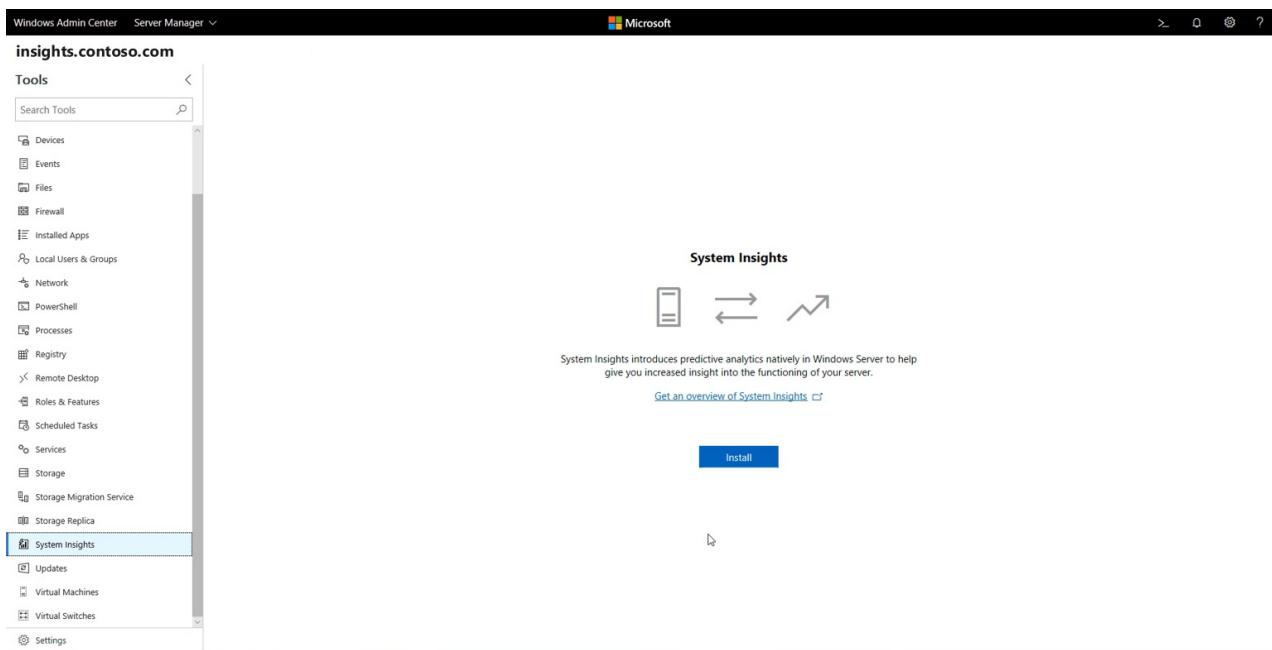
Installieren von System Insights

IMPORTANT

System Insights sammelt und speichert die Daten in einem Jahr vor einem Jahr. Wenn Sie Ihre Daten beim Upgrade Ihres Betriebssystems beibehalten möchten, Stellen Sie sicher, dass Sie ein direktes Upgrade verwenden.

Installieren des Features

Sie können System Insights mit der Erweiterung im Windows Admin Center installieren:



Sie können System Insights auch direkt über Server-Manager installieren, indem Sie das **System-Insights**-Feature hinzufügen oder PowerShell verwenden:

```
Add-WindowsFeature System-Insights -IncludeManagementTools
```

Feedback bereitstellen

Wir freuen uns über Ihr Feedback, um uns bei der Verbesserung dieses Features zu unterstützen. Sie können die folgenden Kanäle verwenden, um Feedback zu senden:

- **Feedback-Hub:** Verwenden Sie das Feedback-Hub-Tool in Windows 10, um einen Fehler oder ein Feedback zu

melden. Geben Sie dabei Folgendes an:

- **Kategorie:** Server
- **SubCategory:** System Insights
- **UserVoice:** übermitteln Sie Featureanforderungen über unsere [UserVoice-Seite](#). Teilen Sie den Kollegen mit, dass Sie die für Sie wichtigen Elemente upstimmen.
- **E-Mail:** Wenn Sie Ihr Feedback privat an das Featureteam senden möchten, senden Sie eine e-Mail an system-insights-feed@microsoft.com. Beachten Sie, dass wir Sie möglicherweise bitten, Feedback-Hub oder UserVoice zu verwenden.

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Grundlegendes zu Funktionen](#)
- [Verwalten von Funktionen](#)
- [Hinzufügen und Entwickeln von Funktionen](#)
- [FAQ zu System Insights](#)

Grundlegendes zu Funktionen

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

Gilt für: Windows Server 2019

In diesem Thema wird das Konzept der Funktionen in System Insights definiert und die in Windows Server 2019 verfügbaren Standardfunktionen vorgestellt.

In diesem Thema werden auch die Datenquellen, Vorhersagezeit Achsen und Vorhersage Status beschrieben, die für die Standardfunktionen verwendet werden.

Übersicht über die Funktionen

Eine System Insights-Funktion ist ein Machine Learning-oder Statistik Modell, das Systemdaten analysiert, um Ihnen einen besseren Einblick in die Funktionsweise Ihrer Bereitstellung zu verschaffen. System Insights führt einen anfänglichen Satz von Standardfunktionen ein und ermöglicht das dynamische Hinzufügen neuer Funktionen, ohne dass das Betriebssystem aktualisiert werden muss.

NOTE

Ausführliche Informationen zum Erstellen, hinzufügen und Aktualisieren von Funktionen finden Sie [hier](#). Das Dokument zur [Verwaltung von Funktionen](#) bietet weitere allgemeine Informationen zu dieser Funktionalität.

Außerdem wird jede Funktion lokal auf einer Windows Server-Instanz ausgeführt, und jede Funktion kann einzeln verwaltet werden.

Funktions Ausgaben

Wenn eine Funktion aufgerufen wird, stellt Sie eine Ausgabe bereit, um das Ergebnis der Analyse oder Vorhersage zu erläutern. Jede Ausgabe muss einen **Status** und eine **Statusbeschreibung** enthalten, um die Vorhersage zu beschreiben, und jedes Ergebnis kann optional Funktions spezifische Daten enthalten, die mit der Vorhersage verknüpft sind. Die **Statusbeschreibung** enthält eine Kontext Erklärung für den **Status**, und die Funktion meldet entweder den Status "OK", "Warnung" oder "kritisch". Außerdem kann eine Funktion einen **Fehler** oder **keinen** Status verwenden, wenn keine Vorhersage erstellt wurde. Im folgenden finden Sie die Funktionsstatus und ihre grundlegende Bedeutung:

- **OK** : alles sieht gut aus.
- **Warnung** : Es ist keine sofortige Beachtung erforderlich, aber Sie sollten sich einen Blick darauf machen.
- **Kritisch** : Sie sollten sich bald einen Einblick machen.
- **Fehler** : ein unbekanntes Problem hat dazu geführt, dass die Funktion fehlgeschlagen ist.
- **None** : Es wurde keine Vorhersage erstellt. Dies kann auf fehlende oder andere Funktions spezifische Gründe zurückzuführen sein, die keine Vorhersage treffen.

Außerdem werden alle Funktions spezifischen Daten, die im Ergebnis enthalten sind, in einer vom Benutzer zugänglichen JSON-Datei platziert, und der Dateipfad [kann mithilfe von PowerShell gefunden werden](#).

Standardfunktionen

In Windows Server 2019 werden mit System Insights vier Standardfunktionen eingeführt, die sich auf die Kapazitäts Vorhersage konzentrieren:

- **CPU-Kapazitäts Vorhersage** : prognostiziert CPU-Auslastung.
- **Netzwerk Kapazitäts Vorhersage** : prognostiziert die Netzwerk Auslastung für jeden Netzwerkadapter.
- **Prognose zur Gesamtspeicher Auslastung**: prognostiziert den gesamten Speicherverbrauch auf allen lokalen Laufwerken.
- **Prognose für den Volumenverbrauch** : prognostiziert den Speicherverbrauch für jedes Volume.

Jede Funktion analysiert Vergangenheits Daten, um die zukünftige Verwendung vorherzusagen. **alle Vorhersagefunktionen sind so konzipiert, dass Sie langfristige Trends und nicht das kurzfristige Verhalten prognostizieren.** Dadurch können Administratoren die Hardware ordnungsgemäß bereitstellen und ihre Workloads optimieren, um zukünftige Ressourcenkonflikte zu vermeiden. Da diese Funktionen sich auf die langfristige Verwendung konzentrieren, analysieren diese Funktionen tägliche Daten.

Vorhersagemodell

Die Standardfunktionen verwenden ein Planungsmodell, um die zukünftige Verwendung vorherzusagen, und für jede Vorhersage wird das Modell lokal auf den Daten des Computers trainiert. Dieses Modell ist so konzipiert, dass langfristige Trends erkannt werden, und das erneute trainieren auf jeder Windows Server-Instanz ermöglicht die Anpassung an das spezifische Verhalten und die benutzerspezifischen Aspekte der einzelnen Computer.

NOTE

Wenn Sie bestimmen, welcher Modelltyp verwendet werden muss, testen Sie viele Modelle mithilfe eines Datasets, das Zehntausende von Computern enthält. Nachdem Sie diese Modelle analysiert und optimiert haben, haben wir uns entschieden, ein Modell für die automatische Regression zu verwenden, da es hochgradig präzise und visuell intuitive Vorhersagen erzeugt, ohne zu viel Zeit zum trainieren zu benötigen. Dieses Modell erfordert jedoch drei Wochen Trainingsdaten, sodass jede Funktion einen grundlegenden linearen Trend verwendet, bis drei Wochen Daten verfügbar sind.

Vorhersagezeit Achsen

Die Standardfunktionen prognostizieren eine bestimmte Anzahl von Tagen in der Zukunft, basierend auf der Anzahl der Tage, für die Daten erfasst wurden. In der folgenden Tabelle werden die vorhersagbaren Zeitachsen dieser Funktionen angezeigt:

GRÖSSE DER EINGABEDATEN	PROGNOSIS LÄNGE
0-5 Tage	Es erfolgt keine Vorhersage.
6-180 Tage	1/3 * Größe der Eingabedaten
180-365 Tage	60 Tage

Prognoseredaten

Jede Funktion analysiert tägliche Daten, um die zukünftige Nutzung zu prognostizieren. CPU, Netzwerk und sogar die Speicherauslastung können sich jedoch im Laufe des Tages ändern und dynamisch an die Arbeits Auslastungen auf dem Computer angepasst werden. Da die Nutzung im Laufe des Tages nicht konstant ist, ist es wichtig, die tägliche Nutzung in einem einzelnen Datenpunkt ordnungsgemäß darzustellen. In der folgenden Tabelle werden die spezifischen Datenpunkte und die Art der Datenverarbeitung ausführlich erläutert:

FUNKTIONSSNAME	DATENQUELLE (N)	FILTER LOGIK
Prognose des Volumen Verbrauchs	Volumegröße	Maximale tägliche Nutzung
Prognose der Speichernutzung Gesamt	Summe der Volumegrößen, Summe der Datenträger Größen	Maximale tägliche Nutzung

FUNKTIONSNAMEN	DATENQUELLE (N)	FILTER LOGIK
Prognose der CPU-Kapazität	Prozessorzeit (%)	Maximal 2 Stunden Durchschnitt pro Tag
Prognose zur Netzwerkkapazität	Gesamtanzahl Bytes/Sek.	Maximal 2 Stunden Durchschnitt pro Tag

Wenn Sie die oben beschriebene Filter Logik auswerten, ist es wichtig zu beachten, dass jede Funktion Administratoren informieren möchte, wenn die zukünftige Verwendung die verfügbare Kapazität überschreitet – auch wenn die CPU-Zeitüberschreitung eine Auslastung von 100% erreicht hat, kann die CPU-Auslastung nicht zu einer sinnvollen Leistungsminderung oder Ressourcenkonflikten führen. Bei CPU- und Netzwerkverbindungen sollte die hohe Nutzung statt der momentanen Spitzen unterstützt werden. Eine Durchschnitts Auslastung der CPU- und Netzwerk Auslastung im ganzen Tag würde jedoch wichtige Verwendungs Informationen verlieren, weil eine hohe CPU-Auslastung oder Netzwerk Auslastung eine erhebliche Auswirkung auf die Leistung Ihrer kritischen Workloads haben könnte. Der maximale Wert von 2 Stunden pro Tag vermeidet diese extreme und erzeugt nach wie vor sinnvolle Daten für jede zu analysierende Funktion.

Bei der Volume- und Gesamtspeicher Auslastung kann die Speicherauslastung jedoch die verfügbare Kapazität nicht überschreiten, auch wenn dies nicht der Fall ist, sodass die maximale tägliche Nutzung für diese Funktionen verwendet wird.

Vorhersage Status

Alle System Insights-Funktionen müssen einen Status ausgeben, der mit jeder Vorhersage verknüpft ist. Jede Standardfunktion verwendet die folgende Logik zum Definieren der einzelnen Vorhersage Status:

- **OK:** die Vorhersage überschreitet die verfügbare Kapazität nicht.
- **Warnung:** die Vorhersage überschreitet die verfügbare Kapazität in den nächsten 30 Tagen.
- **Kritisch:** die Vorhersage überschreitet die verfügbare Kapazität in den nächsten 7 Tagen.
- **Fehler:** bei der Funktion ist ein unerwarteter Fehler aufgetreten.
- **None:** Es sind nicht genügend Daten vorhanden, um eine Vorhersage zu treffen. Dies kann auf fehlende Daten zurückzuführen sein oder daran, dass in jüngster Zeit keine Daten gemeldet wurden.

NOTE

Wenn eine Funktions Vorhersage für mehrere Instanzen ist (z. B. mehrere Volumes oder Netzwerkadapter), gibt der Status den schwerwiegenderen Status für alle Instanzen an. Einzelne Statuswerte für jedes Volume oder jeden Netzwerkadapter werden im Windows Admin Center oder innerhalb der Daten angezeigt, die in der Ausgabe der einzelnen Funktionen enthalten sind. Anweisungen zum Analysieren der JSON-Ausgabe der Standardfunktionen finden Sie in [diesem Blog](#).

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Übersicht über System Einblicke](#)
- [Verwalten von Funktionen](#)
- [Hinzufügen und Entwickeln von Funktionen](#)
- [FAQ zu System Insights](#)

Verwalten von Funktionen

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

Gilt für: Windows Server 2019

In Windows Server 2019 bietet System Insights eine Reihe von Einstellungen, die für jede Funktion konfiguriert werden können. Diese Einstellungen können angepasst werden, um den spezifischen Anforderungen Ihrer Bereitstellung gerecht zu werden. In diesem Thema wird beschrieben, wie die verschiedenen Einstellungen für jede Funktion über das Windows Admin Center oder PowerShell verwaltet werden, und es werden grundlegende PowerShell-Beispiele und Windows Admin Center-Screenshots bereitgestellt, um die Anpassung dieser Einstellungen zu veranschaulichen.

TIP

Sie können diese kurzen Videos auch verwenden, um Sie bei den ersten Schritten und der Verwaltung von System Insights zu unterstützen: Einstieg in die ersten Schritte [mit System Insights in 10 Minuten](#)

Obwohl dieser Abschnitt PowerShell-Beispiele enthält, können Sie die [Dokumentation zu System Insights PowerShell](#) verwenden, um alle Cmdlets, Parameter und Parametersätze in System Insights anzuzeigen.

Anzeigen von Funktionen

Zum Einstieg können Sie alle verfügbaren Funktionen mithilfe des Cmdlets `Get-insightscapability` auflisten:

```
Get-InsightsCapability
```

Diese Funktionen sind auch in der System Insights-Erweiterung sichtbar:

The screenshot shows the Windows Admin Center interface with the 'insights.contoso.com' server selected. The left sidebar has a 'Tools' section with various icons for Overview, Certificates, Devices, Events, Files, Firewall, Local Users & Groups, Network, PowerShell, Processes, Registry, Remote Desktop, Roles & Features, Scheduled Tasks, Services, Storage, Storage Replica, and Updates. The 'System Insights' icon is highlighted with a blue bar at the bottom. The main content area is titled 'System Insights' with a 'PREVIEW' button. It features four radio buttons: 'Invoke', 'Settings', 'Enable', and 'Disable'. Below this is a table with four rows of data:

Capability name	State	Status	Status description	Last run
CPU capacity forecasting	Enabled	✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/14/2018, 3:00:01 AM
Networking capacity forecasting	Enabled	✓ Ok	Network usage is forecasted to remain within the available capacity.	6/14/2018, 3:00:01 AM
Total storage consumption forecasting	Enabled	✓ Ok	Disk usage is forecasted to remain within the available capacity.	6/14/2018, 3:00:01 AM
Volume consumption forecasting	Enabled	✓ Ok	Volume usage is forecasted to remain within the available capacity.	6/14/2018, 3:00:01 AM

Aktivieren und Deaktivieren einer Funktion

Jede Funktion kann aktiviert oder deaktiviert werden. Durch das Deaktivieren einer Funktion wird verhindert, dass diese Funktion aufgerufen wird, und bei nicht standardmäßigen Funktionen wird durch das Deaktivieren einer Funktion die gesamte Datensammlung für diese Funktion beendet. Standardmäßig sind alle Funktionen aktiviert, und Sie können den Status einer Funktion mithilfe des Cmdlets **Get-insightscapability** überprüfen.

Um eine Funktion zu aktivieren oder zu deaktivieren, verwenden Sie die Cmdlets **enable-insightscapability** und **Deaktivieren-insightscapability** :

```
Enable-InsightsCapability -Name "CPU capacity forecasting"  
Disable-InsightsCapability -Name "Networking capacity forecasting"
```

Diese Einstellungen können auch durch Auswahl einer Funktion im Windows Admin Center ein-/ausgeschaltet werden, indem Sie auf die Schaltflächen **aktivieren** oder **Deaktivieren** klicken.

Aufrufen einer Funktion

Wenn Sie eine Funktion aufrufen, wird die Funktion zum Abrufen einer Vorhersage sofort ausgeführt.

Administratoren können jederzeit eine Funktion aufrufen, indem Sie im Windows Admin Center auf die Schaltfläche "aufrufen" oder das Cmdlet "Aufruf-insightscapability" klicken:

```
Invoke-InsightsCapability -Name "CPU capacity forecasting"
```

TIP

Um sicherzustellen, dass der Aufruf einer Funktion nicht mit kritischen Vorgängen auf dem Computer in Konflikt steht, sollten Sie Vorhersagen außerhalb der Geschäftszeiten planen.

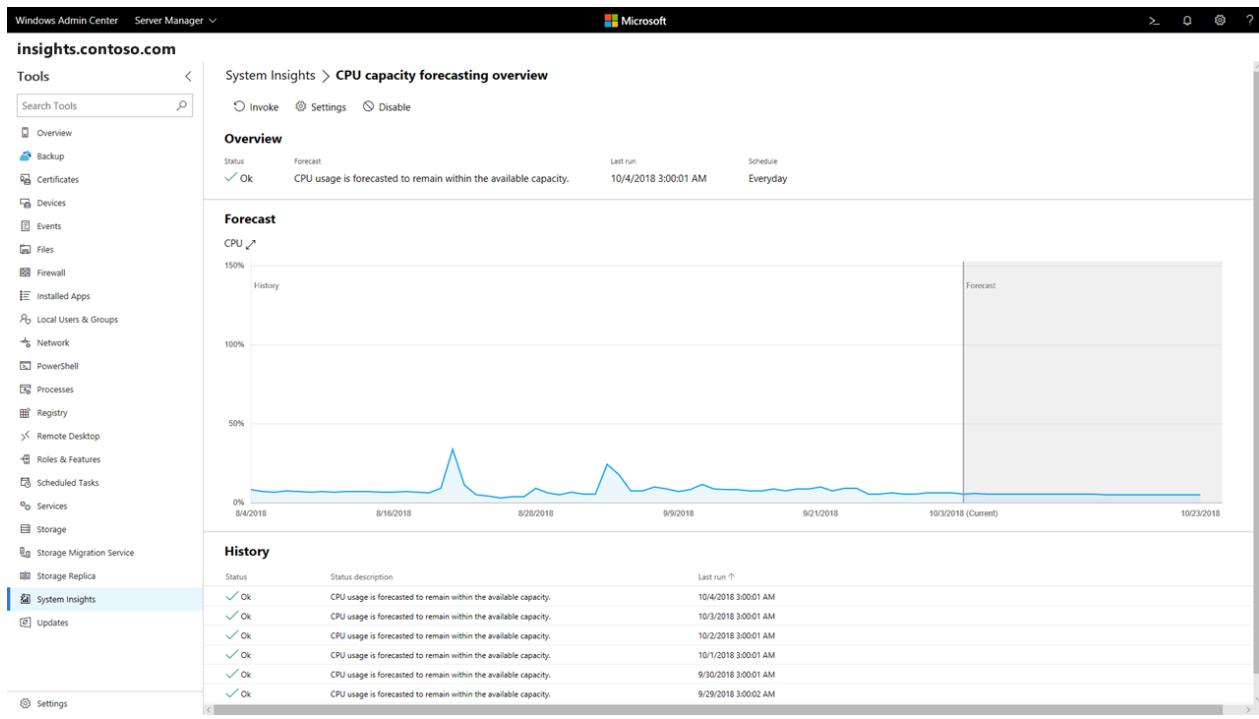
Abrufen von Funktions Ergebnissen

Nachdem eine Funktion aufgerufen wurde, werden die neuesten Ergebnisse mithilfe von "Get-insightscapability" oder "Get-insightscapabilityresult" angezeigt. Mit diesen Cmdlets werden die neuesten Status -und Status Beschreibungen der einzelnen Funktionen ausgegeben, die das Ergebnis der einzelnen Vorhersagen beschreiben. Die Felder **Status** und **Statusbeschreibung** werden weiter unten im Dokument mit den Grundlagen von [Funktionen](#) beschrieben.

Darüber hinaus können Sie das Cmdlet **Get-insightscapabilityresult** verwenden, um die letzten 30 Vorhersage Ergebnisse anzuzeigen und die der Vorhersage zugeordneten Daten abzurufen:

```
# Specify the History parameter to see the last 30 prediction results.  
Get-InsightsCapabilityResult -Name "CPU capacity forecasting" -History  
  
# Use the Output field to locate and then show the results of "CPU capacity forecasting."  
# Specify the encoding as UTF8, so that Get-Content correctly parses non-English characters.  
$Output = Get-Content (Get-InsightsCapabilityResult -Name "CPU capacity forecasting").Output -Encoding UTF8 |  
ConvertFrom-Json  
$Output.ForecastingResults
```

Die System Insights-Erweiterung zeigt automatisch den Vorhersage Verlauf an und analysiert die Ergebnisse des JSON-Ergebnisses, sodass Sie ein intuitives, qualitativ hoch gefasstes Diagramm der einzelnen Vorhersagen erhalten:



Verwenden des Ereignis Protokolls zum Abrufen von Funktions Ergebnissen

System Insights protokolliert jedes Mal ein Ereignis, wenn eine Funktion eine Vorhersage abschließt. Diese Ereignisse werden im Channel " **Microsoft-Windows-System-Insights/admin** " angezeigt, und System Insights veröffentlicht eine andere Ereignis-ID für jeden Status:

VORHERSAGE STATUS	EREIGNIS-ID
OK	151
Warnung	148
Wichtige Warnungen	150
Error	149
Keine	132

TIP

Verwenden Sie [Azure Monitor](#) oder [System Center Operations Manager](#), um diese Ereignisse zu aggregieren und die Vorhersage Ergebnisse für eine Gruppe von Computern anzuzeigen.

Festlegen eines Funktions Zeitplans

Zusätzlich zu on-Demand-Vorhersagen können Sie regelmäßige Vorhersagen für jede Funktion konfigurieren, sodass die angegebene Funktion automatisch nach einem vordefinierten Zeitplan aufgerufen wird. Verwenden Sie das Cmdlet **Get-insightscapabilitieschedule**, um Funktions Zeitpläne anzuzeigen:

TIP

Verwenden Sie den Pipeline-Operator in PowerShell, um Informationen zu allen Funktionen anzuzeigen, die vom Cmdlet "**Get-insightscapability**" zurückgegeben werden.

Periodische Vorhersagen sind standardmäßig aktiviert, aber Sie können jederzeit mithilfe der Cmdlets "enable-insightscapabilitieschedule" und "Deaktivieren-insightscapabilitieschedule" deaktiviert werden:

```
Enable-InsightsCapabilitySchedule -Name "Total storage consumption forecasting"  
Disable-InsightsCapabilitySchedule -Name "Volume consumption forecasting"
```

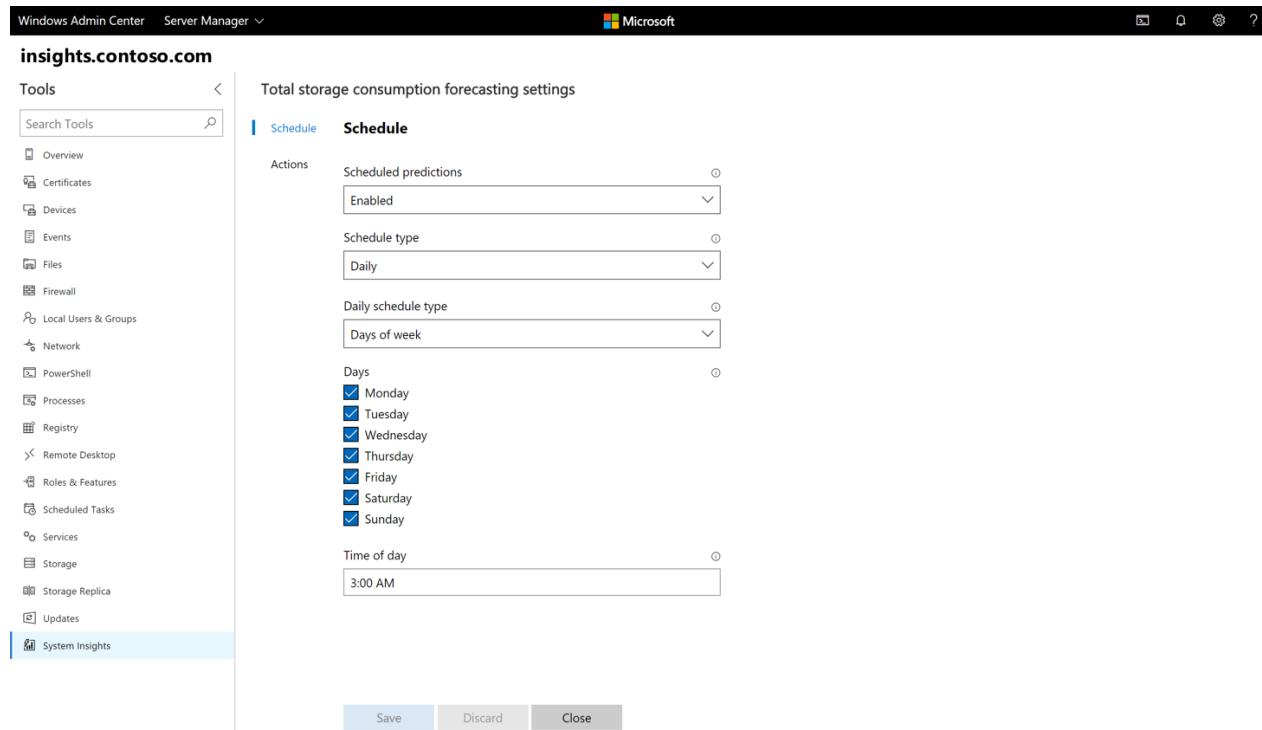
Jede Standardfunktion wird für jeden Tag um 3 Uhr geplant. Sie können jedoch benutzerdefinierte Zeitpläne für jede Funktion erstellen, und System Insights unterstützt eine Vielzahl von Zeit Plan Typen, die mithilfe des Cmdlets Set-insightscapabilitieschedule konfiguriert werden können:

```
Set-InsightsCapabilitySchedule -Name "CPU capacity forecasting" -Daily -DaysInterval 2 -At 4:00PM  
Set-InsightsCapabilitySchedule -Name "Networking capacity forecasting" -Daily -DaysOfWeek Saturday, Sunday -  
At 2:30AM  
Set-InsightsCapabilitySchedule -Name "Total storage consumption forecasting" -Hourly -HoursInterval 2 -  
DaysOfWeek Monday, Wednesday, Friday  
Set-InsightsCapabilitySchedule -Name "Volume consumption forecasting" -Minute -MinutesInterval 30
```

NOTE

Da die Standardfunktionen tägliche Daten analysieren, empfiehlt es sich, tägliche Zeitpläne für diese Funktionen zu verwenden. Weitere Informationen zu den Standardfunktionen [finden Sie hier](#).

Sie können auch das Windows Admin Center verwenden, um Zeitpläne für jede Funktion anzuzeigen und festzulegen, indem Sie auf Einstellungen klicken. Der aktuelle Zeitplan wird auf der Registerkarte Zeitplan angezeigt, und Sie können die GUI-Tools verwenden, um einen neuen Zeitplan zu erstellen:



Erstellen von Wiederherstellungs Aktionen

Mit System Insights können Sie benutzerdefinierte Wiederherstellungs Skripts basierend auf dem Ergebnis einer Funktion starten. Für jede Funktion können Sie ein benutzerdefiniertes PowerShell-Skript für jeden Vorhersage

Status konfigurieren, sodass Administratoren automatisch Korrekturmaßnahmen ergreifen können, anstatt einen manuellen Eingriff zu erfordern.

Beispiele für Wiederherstellungs Aktionen sind das Ausführen der Datenträger Bereinigung, das Erweitern eines Volumes, das Ausführen der Deduplizierung, das Live migrieren von VMS und das Einrichten Azure-Dateisynchronisierung

Sie können die Aktionen für jede Funktion mithilfe des Cmdlets **Get-insightscapabilityaction** anzeigen:

```
Get-InsightsCapability | Get-InsightsCapabilityAction
```

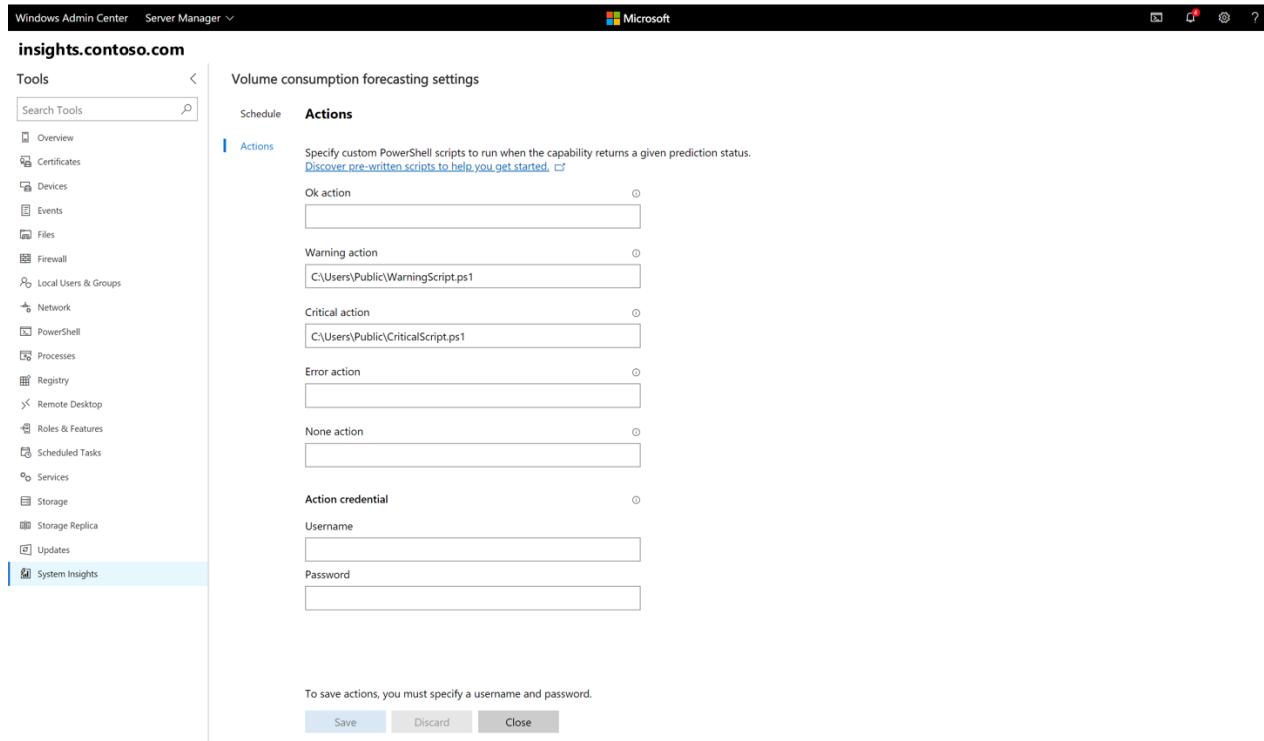
Mithilfe der Cmdlets " **Set-insightscapabilityaction** " und " **Remove-insightscapabilityaction** " können Sie neue Aktionen erstellen oder vorhandene Aktionen löschen. Jede Aktion wird mit Anmelde Informationen ausgeführt, die im **Action Credential** -Parameter angegeben sind.

NOTE

In der ersten System Insights-Version müssen Sie Wiederherstellungs Skripts außerhalb der Benutzerverzeichnisse angeben. Dies wird in einer zukünftigen Version korrigiert.

```
$Cred = Get-Credential  
Set-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Warning -Action  
"C:\Users\Public\WarningScript.ps1" -ActionCredential $Cred  
Set-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Critical -Action  
"C:\Users\Public\CriticalScript.ps1" -ActionCredential $Cred  
  
Remove-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Warning
```

Mithilfe der Registerkarte **Aktionen** auf der Seite **Einstellungen** können Sie auch Wiederherstellungs Aktionen mithilfe des Windows Admin Centers festlegen:



The screenshot shows the Windows Admin Center interface for managing system insights. On the left, there's a navigation sidebar with various tools like Overview, Certificates, Devices, Events, Files, Firewall, Local Users & Groups, Network, PowerShell, Processes, Registry, Remote Desktop, Roles & Features, Scheduled Tasks, Services, Storage, Storage Replica, and Updates. The 'System Insights' option is currently selected. The main content area has a title 'Volume consumption forecasting settings'. Below it, there are two tabs: 'Schedule' and 'Actions'. The 'Actions' tab is active, displaying a form to define PowerShell scripts for different prediction status levels: Ok action, Warning action (set to 'C:\Users\Public\WarningScript.ps1'), Critical action (set to 'C:\Users\Public\CriticalScript.ps1'), Error action, and None action. There's also a section for 'Action credential' with 'Username' and 'Password' fields. At the bottom, a note says 'To save actions, you must specify a username and password.' followed by 'Save', 'Discard', and 'Close' buttons.

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Übersicht über System Einblicke](#)
- [Grundlegendes zu Funktionen](#)
- [Hinzufügen und Entwickeln von Funktionen](#)
- [FAQ zu System Insights](#)

Hinzufügen und Entwickeln neuer Funktionen

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

Gilt für: Windows Server 2019

System Insights ermöglicht Ihnen das Hinzufügen neuer Vorhersagefunktionen zu System Insights, ohne dass Betriebssystemupdates erforderlich sind. Dadurch können Entwickler, einschließlich Microsoft und Drittanbietern, neue Funktionen in der Mitte der Veröffentlichung erstellen und bereitstellen, um die Szenarios zu berücksichtigen, die Sie interessieren.

Jede neue Funktion kann in die vorhandene System Insights-Infrastruktur integriert und erweitert werden:

- Neue Funktionen können **jeden Leistungs- oder System Ereignis Wert angeben**, der gesammelt, lokal gespeichert und an die Analysefunktion zurückgegeben wird, wenn die Funktion aufgerufen wird.
- Neue Funktionen können **die vorhandene Windows Admin Center und die PowerShell-Verwaltungsebenen nutzen**. In System Insights können nicht nur neue Funktionen erkannt werden, sondern Sie profitieren auch von benutzerdefinierten Zeitplänen und Wiederherstellungs Aktionen.

Verwalten neuer Funktionen

- [Erfahren Sie](#), wie Sie Funktionen mithilfe von PowerShell hinzufügen, entfernen und aktualisieren.

Entwickeln einer Funktion

Verwenden Sie die folgenden Ressourcen, um Ihnen den Einstieg in die Erstellung eigener benutzerdefinierter Funktionen zu erleichtern:

- [Erfahren Sie mehr](#) über die Datenquellen, die Sie erfassen können.
- [Laden](#) Sie das System Insights-nuget-Paket herunter, das die Klassen und Schnittstellen enthält, die Sie zum Schreiben einer Funktion benötigen.
- Weitere Informationen zu den Klassen und Schnittstellen von System Insights [finden Sie](#) in der API-Dokumentation.
- [Verwenden](#) Sie die System Insights-Beispiel Funktion, um Ihnen den Einstieg zu erleichtern. Dadurch wird gezeigt, wie Sie eine Funktion registrieren, die zu sammelnden Datenquellen angeben und mit der Analyse der Systemdaten beginnen.

NOTE

Dies ist eine vorab Funktionalität. Es kann geändert werden, da wir neue Funktionen hinzufügen und Feedback integrieren.

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Übersicht über System Einblicke](#)
- [Grundlegendes zu Funktionen](#)
- [Verwalten von Funktionen](#)
- [Hinzufügen, Entfernen und Aktualisieren von Funktionen](#)
- [FAQ zu System Insights](#)

Hinzufügen, Entfernen und Aktualisieren von Funktionen

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

Mit System Insights können Sie neue Funktionen erstellen, die die vorhandene Daten Sammlungs- und Verwaltungs Funktionalität nutzen. Nachdem diese Funktionen erstellt wurden, ist es ebenso wichtig, dass Sie auch über die Platt Form Unterstützung verfügen, um das Hinzufügen, entfernen und Aktualisieren dieser Funktionen zu verwalten.

In diesem Thema werden die Funktionen auf hoher Ebene zum Hinzufügen, entfernen und Aktualisieren von Funktionen in System Insights beschrieben.

Hinzufügen einer Funktion

Mit System Insights können Sie jederzeit neue Funktionen mithilfe des **Add-insightscapability** -Cmdlets hinzufügen. Die **Add-insightscapability** erfordert, dass Sie einen Funktionsnamen und die Funktionsbibliothek angeben. Die Funktionsbibliothek enthält die Beschreibung, Datenquellen und Vorhersage Logik der Funktion.

```
Add-InsightsCapability -Name Sample capability -Library C:\SampleCapability.dll
```

Nachdem Sie System Insights eine Funktion hinzugefügt haben, können Sie die Funktion sofort mithilfe von PowerShell oder Windows Admin Center aufrufen und verwalten.

Aktualisieren einer Funktion

System Insights ermöglicht Ihnen außerdem, eine Funktion mithilfe des Cmdlets " **Update-insightscapability** " zu aktualisieren.

```
Update-InsightsCapability -Name Sample capability -Library C:\SampleCapabilityv2.dll
```

Durch das Aktualisieren einer Funktion können Sie eine neue Funktionsbibliothek angeben, die es Ihnen ermöglicht, die Funktionsbeschreibung, die Datenquellen und die dieser Funktion zugeordnete Vorhersage Logik zu ändern. Wichtig ist, dass das Aktualisieren einer Funktion alle Konfigurations- und Verlaufs Informationen zu dieser Funktion beibehält, einschließlich benutzerdefinierter Zeitpläne, Aktionen und Verlaufs Vorhersage Ergebnisse.

Entfernen einer Funktion

Mithilfe des Cmdlets **Remove-insightscapability** können Sie auch Funktionen in System Insights entfernen.

```
Remove-InsightsCapability -Name Sample capability
```

NOTE

Die standardmäßigen Vorhersagefunktionen können nicht entfernt werden.

Durch das Entfernen einer Funktion werden die Funktionen und alle zugehörigen Informationen, einschließlich des Zeitplans, der Wiederherstellungs Aktionen und der bisherigen Vorhersage Ergebnisse, dauerhaft gelöscht.

TIP

Deaktivieren Sie ggf. eine Funktion, anstatt Sie zu entfernen, wenn Sie sich Sorgen machen, dass alle der Funktion zugeordneten Informationen dauerhaft gelöscht werden.

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Übersicht über System Einblicke](#)
- [Grundlegendes zu Funktionen](#)
- [Verwalten von Funktionen](#)
- [Hinzufügen und Entwickeln von Funktionen](#)
- [FAQ zu System Insights](#)

System Insights-Datenquellen

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

Gilt für: Windows Server 2019

Mit System Insights werden erweiterbare Funktionen für die Datensammlung eingeführt. Wenn Sie eine neue Funktion schreiben, können Sie vorhandene oder neue Datenquellen angeben, die lokal erfasst und analysiert werden sollen. In diesem Thema werden die Datenquellen beschrieben, die Sie auswählen können, wenn Sie eine neue Funktion registrieren.

Datenquellen

Wenn Sie eine neue Funktion schreiben, müssen Sie die spezifischen Datenquellen identifizieren, die für jede Funktion erfasst werden sollen. Die von Ihnen angegebenen Datenquellen werden gesammelt und direkt auf Ihrem Computer gespeichert, und Sie können drei Arten von Datenquellen auswählen:

- **Leistungsindikatoren:**

- Geben Sie den Indikator Pfad, den Namen und die Instanzen an, und System Insights sammelt die relevanten Daten, die von diesen Leistungsindikatoren gemeldet werden.

- **System Ereignisse:**

- Geben Sie den Channelnamen und die Ereignis-ID an, und mit System Insights wird aufgezeichnet, wie oft das Ereignis aufgetreten ist.

- **Bekannte Reihe**

- System Insights sammelt einige grundlegende Informationen auf Ihrem Computer für einige klar definierte Ressourcen. Diese Reihen werden für die Standardfunktionen verwendet, Sie können aber auch von jeder benutzerdefinierten Funktion verwendet werden. Folgende Informationen werden gesammelt:

- **Daten Träger:**

- *Eigenschaften:* GUID
 - *Daten:* Größe

- **Volume:**

- *Eigenschaften:* UniqueId, DriveLetter, filesystemlabel, size
 - *Daten:* verwendete Größe

- **Netzwerk Adapter:**

- *Eigenschaften:* interfaceguid, interfacedescription, Speed
 - *Daten:* empfangene Bytes/Sek., gesendete Bytes/Sek., Bytes gesamt/Sek.

- **CPU:**

- *Eigenschaften:*-
 - *Daten:* Prozessorzeit (%)

- Geben Sie eine bekannte Reihe an, und System Insights gibt die Daten zurück, die von dieser Reihe gesammelt werden.

Beibehaltungs Zeitachsen und Sammlungs Intervalle

Die oben aufgeführten Datenquellen haben unterschiedliche Beibehaltungs Zeiträume und Sammlungs Intervalle.

Die folgende Tabelle zeigt, wie lange und wie oft die einzelnen Datenquellen gesammelt werden:

DATENQUELLE	AUFBEWAHRUNGS ZEITACHSE	SAMMLUNGS INTERVALL
Leistungsindikatoren	3 Monate	15 Minuten
System Ereignisse	3 Monate	15 Minuten
Bekannte Reihe	1 Jahr	1 Stunde

Aggregations Typen

Da jede Reihe nur einen Datenpunkt für jedes Sammlungs Intervall aufzeichnen, verfügt jede Reihe über einen Aggregationstyp. In der folgenden Tabelle werden die Datenquelle und der zugehörige Aggregationstyp beschrieben:

NOTE

Für Leistungsindikatoren können Sie aus einigen unterschiedlichen Aggregations Typen auswählen.

DATENQUELLE	AGGREGATIONS TYPEN
Leistungsindikatoren	Sum, Average, Max, min
System Ereignisse	Anzahl
Bekannte Reihe zu Datenträgern	Last (aktueller Wert im Sammlungs Intervall)
Well-Known-Reihe von Volumes	Last (aktueller Wert im Sammlungs Intervall)
Well-Known-Serie (CPU)	Durchschnitt
Bekannte Serie zu Netzwerken	Durchschnitt

Daten Bedarf

System Insights sammelt alle Daten lokal auf Ihrem Laufwerk c (c:). Im Allgemeinen ist der Daten Speicherbedarf der System Insights gering. Dies hängt direkt vom Typ und der Anzahl der Datenquellen ab, die jede Funktion angibt, und in der folgenden Tabelle wird die Speicherauslastung für die einzelnen Datentypen ausführlich erläutert:

DATENQUELLE	MAXIMALER SPEICHERBEDARF
Leistungsindikatoren	240 KB
System Ereignisse	200 KB
Bekannte Reihe zu Datenträgern	200 KB pro Datenträger
Well-Known-Reihe von Volumes	300 KB pro Volume
Well-Known-Serie (CPU)	100 KB

DATENQUELLE	MAXIMALER SPEICHERBEDARF
Bekannte Serie zu Netzwerken	300 KB pro Netzwerkadapter

NOTE

Bei den standardmäßigen Vorhersagefunktionen muss der maximale Speicherplatz für die meisten eigenständigen Computer weniger als 10 MB betragen.

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Übersicht über System Einblicke](#)
- [Grundlegendes zu Funktionen](#)
- [Verwalten von Funktionen](#)
- [Hinzufügen und Entwickeln von Funktionen](#)
- [FAQ zu System Insights](#)

FAQ zu System Insights

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019

Wie können Sie System Einblicke mit Azure Monitor oder System Center Operations Manager verwenden?

In [Azure Monitor](#) und [System Center Operations Manager](#) werden Betriebsinformationen für Ihre bereit Stellungen bereitgestellt, um Ihnen die Verwaltung Ihrer Infrastruktur zu erleichtern. System Insights ist dagegen eine Windows Server-Funktion, die lokale Predictive Analytics Funktionen einführt. Mithilfe von System Insights und Azure Monitor oder SCOM können Sie die Vorhersagen über eine Population von Geräten hinweg ermitteln:

Azure Monitor oder SCOM können die von System Insights erstellten Ereignisse als Schlüssel ausgeben, da System Einblicke das Ergebnis jeder Vorhersage an das Ereignisprotokoll übergibt. Diese computerspezifischen Vorhersagen können über eine Flotte von Windows-Servern hinweg angezeigt werden, sodass Sie über eine einheitliche Ansicht dieser Vorhersagen für eine Gruppe von Server Instanzen verfügen.

Sehen Sie sich die Kanal-und Ereignis-IDs für [jede Vorhersage](#)an.

Wie verhält sich System Insights mit Windows ml?

[Windows ml](#) ist eine Plattform, die es Entwicklern ermöglicht, vorab trainierte Machine Learning-Modelle auf Windows-Geräten zu importieren und zu bewerten. Diese Modelle profitieren von der Hardwarebeschleunigung und können lokal bewertet werden.

System Insights ist ein Feature in Windows Server 2019, das lokale Vorhersagefunktionen sowie eine komplette Verwaltungs Umgebung bietet, einschließlich der PowerShell-und Windows Admin Center-Integration.

Kann ich für meinen Cluster System Einblicke verwenden?

Ja. System Insights kann unabhängig voneinander auf jedem einzelnen Failoverclusterknoten ausgeführt werden, und das Standardverhalten von System Insights prognostiziert die Verwendung von lokalem Speicher, Volume, CPU und Netzwerk. **Sie können auch die Vorhersage für Cluster Speicher aktivieren**, sodass die Speicher Prognose Funktionen die Nutzung für gruppierte Volumes und Speicher Vorhersagen.

Sie können diese Einstellungen im Windows Admin Center oder PowerShell verwalten. ausführlichere Informationen zu dieser Funktionalität finden Sie [hier](#).

Wie teuer ist das Ausführen der Standardfunktionen?

Jede Standardfunktion ist für die Durchführung von kostengünstiger. Die Ausführung der Funktionen dauert länger, wenn Sie mehr Daten sammeln, aber Sie sollten in der Regel in wenigen Sekunden fertiggestellt werden.

Siehe auch

Weitere Informationen zu System Insights finden Sie in den folgenden Ressourcen:

- [Übersicht über System Einblicke](#)
- [Grundlegendes zu Funktionen](#)
- [Verwalten von Funktionen](#)

- Hinzufügen und Entwickeln von Funktionen

Erste Schritte mit der Ereignissammlung für Setup und Start

09.04.2020 • 42 minutes to read • [Edit Online](#)

Gilt für: Windows Server

Übersicht

Die Setup-und Start Ereignis Sammlung ist ein neues Feature in Windows Server 2016, mit dem Sie einen Collector-Computer festlegen können, der eine Vielzahl wichtiger Ereignisse sammelt, die auf anderen Computern beim Starten oder durchlaufen des Setup Vorgangs auftreten. Die erfassten Ereignisse können Sie später mit der Ereignisanzeige, Message Analyzer, WEvtUtil oder Windows PowerShell-Cmdlets analysieren.

Diese Ereignisse konnten bisher nicht überwacht werden, da die erforderliche Infrastruktur, um diese zu sammeln, nicht vorhanden war, bis ein Computer eingerichtet wurde. Die Arten von Ereignissammlung für Setup und Start umfassen:

- Laden von Kernel-Modulen und Treibern
- Enumeration von Geräten und Initialisierung Ihrer Treiber (einschließlich Geräte wie z. B. CPU-Typ)
- Überprüfung und Bereitstellung von Dateisystemen
- Starten der ausführbaren Dateien
- Starten und Fertigstellen von System-Updates
- Die Punkte, wenn das System für die Anmeldung verfügbar wird, eine Verbindung mit einem Domänencontroller herstellt, der Abschluss der Dienstbeginne und die Verfügbarkeit der Netzwerkspeicherfreigaben

Der Sammelcomputer muss Windows Server 2016 ausführen (es kann ein Server mit Desktop Experience oder Server Core-Modus sein). Der Computer muss Windows 10 oder Windows Server 2016 ausführen. Sie können auch diesen Dienst auf einem virtuellen Computer ausführen, der auf einem Computer gehostet wird und nicht Windows Server 2016 ausführt. Die folgenden Kombinationen von virtualisierten Sammel- und Zielcomputern funktionieren:

VIRTUALISIERUNGSHOST	VIRTUELLE SAMMELCOMPUTER	VIRTUELLE ZIELCOMPUTER
Windows 8.1	Ja	Ja
Windows 10	Ja	Ja
Windows Server 2016	Ja	Ja
Windows Server 2012 R2	Ja	no

Installieren des Sammeldiensts

Ab Windows Server 2016 ist der Ereignissammlungsdienst eine optionale Funktion. In dieser Version können Sie ihn mit DISM.exe mit diesem Befehl an einer Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten installieren:

```
dism /online /enable-feature /featurename:SetupAndBootEventCollection
```

Dieser Befehl erstellt einen Dienst namens BootEventCollector und eine leere Konfigurationsdatei wird gestartet.

Vergewissern Sie sich durch `get-service -displayname *boot*`, dass die Installation erfolgreich war. Der Boot Event Collector sollte ausgeführt werden. Er wird unter dem Netzwerkdienstkonto ausgeführt und erstellt eine leere Konfigurationsdatei (Active.xml) unter
`%SystemDrive%\ProgramData\Microsoft\BootEventCollector\Config`.

Sie können auch den Ereignissammlungsdienst für Setup und Start mit dem Assistenten "Rollen und Funktionen hinzufügen" im Server-Manager installieren.

Konfiguration

Sie müssen zwei Elemente zum Erfassen von Setup- und Start-Ereignissen konfigurieren.

- Auf den Zielcomputern, die die Ereignisse senden (d. h. der Computer, dessen Setup und Start Sie überwachen möchten), aktivieren Sie das Transportprotokoll KDNET/EVENT-NET und aktivieren Sie die Weiterleitung von Ereignissen.
- Geben Sie auf dem Sammelcomputer an, von welchen Computern Ereignisse erfasst werden sollen und wo Sie gespeichert werden.

NOTE

Sie können keinen Computer konfigurieren, um Startereignisse an sich selbst zu senden. Wenn Sie zwei Computern überwachen möchten, können Sie diese so konfigurieren, dass sie die Ereignisse zu einander senden.

Konfigurieren des Zielcomputers

Aktivieren Sie auf jedem Zielcomputer zunächst den KDNET/EVENT-NET-Transport und klicken Sie dann auf Aktivieren des Sendens von ETW-Ereignissen über das Transportprotokoll und starten Sie den Zielcomputer neu.

EVENT-NET ist ein Transportprotokoll im Kernelmodus ähnlich wie KDNET (Kernel-Debugger-Protokoll). EVENT-NET überträgt nur Ereignisse und nicht den Debuggerzugriff. Diese beiden Protokolle schließen sich gegenseitig aus; Sie können nur eine der Adressen zu einem Zeitpunkt aktivieren.

Sie können den Ereignistransport (mit Windows PowerShell) remote oder lokal aktivieren.

So aktivieren Sie den Ereignistransport remote

1. Wenn Sie bereits Windows PowerShell-Remoting auf dem Zielcomputer festgelegt haben, fahren Sie mit Schritt 3 fort. Wenn dies nicht der Fall ist, öffnen Sie auf dem Zielcomputer ein Eingabeaufforderungsfenster, und führen Sie folgenden Befehl aus:

```
winrm quickconfig
```

2. Folgen Sie den Aufforderungen, und starten Sie den Zielcomputer neu. Wenn der Zielcomputer nicht in derselben Domäne wie der Sammelcomputer ist, müssen Sie ihn als vertrauenswürdigen Host definieren. Dazu gehen Sie folgendermaßen vor:

3. Führen Sie auf dem Sammelcomputer einen der folgenden Befehle aus:

- An einer Windows PowerShell-Eingabeaufforderung:

```
Set-Item -Force WSMan:\localhost\Client\TrustedHosts <target1>,<target2>,... , gefolgt von
```

```
Set-Item -Force WSMan:\localhost\Client\AllowUnencrypted true , wo <target1> usw. die Namen oder IP-Adressen der Zielcomputer sind.
```

- Oder an einer Eingabeaufforderung: `WinRM Set WinRM/config/Client @ {Treuhänder dhosts = <target1>,<TARGET2>,...; "Zuweisung" = true}`

IMPORTANT

Dies richtet eine unverschlüsselte Kommunikation ein, führen Sie dies also nicht außerhalb einer Lab-Umgebung durch.

4. Testen Sie die Verbindung auf dem Sammelcomputer mit einem der folgenden Windows PowerShell-Befehle:

Wenn sich der Zielcomputer in derselben Domäne wie der Collector-Computer befindet, führen Sie

```
New-PSSession -Computer <target> | Remove-PSSession
```

Wenn der Zielcomputer nicht in derselben Domäne ist, führen Sie

```
New-PSSession -Computer <target> -Credential Administrator | Remove-PSSession
```

 aus, was die Anmeldeinformationen aufruft.

Wenn der Befehl keine Suchzeichenfolge zurückgibt, war Remoting erfolgreich.

5. Öffnen Sie auf dem Zielcomputer eine Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten, und führen Sie diesen Befehl aus:

```
Enable-SbecBcd -ComputerName <target_name> -CollectorIP <ip> -CollectorPort <port> -Key <a.b.c.d>
```

Hier < target_name > der Name des Ziel Computers ist <IP> die IP-Adresse des Collector-Computers. <Port> ist die Portnummer, an der der Collector ausgeführt wird. Der Schlüssel <a.b.c.d> ist ein erforderlicher Verschlüsselungsschlüssel für die Kommunikation mit vier alphanumerischen Zeichenfolgen, die durch Punkte getrennt sind. Dieser Schlüssel wird auf dem Sammelcomputer verwendet. Wenn Sie einen Schlüssel eingeben, wird ein zufälliger Schlüssel generiert; Sie benötigen diesen für den Sammelcomputer, notieren Sie diese.

6. Wenn Sie bereits einen Sammelcomputer eingerichtet haben, aktualisieren Sie die Konfigurationsdatei auf dem Sammelcomputer mit den Informationen für den neuen Zielcomputer. Weitere Informationen finden Sie im Abschnitt Konfigurieren des Collector-Computers.

So aktivieren Sie den Ereignistransport lokal auf dem Zielcomputer

1. Starten Sie eine Eingabeaufforderung mit erhöhten Rechten, und führen Sie diese Befehle aus:

bcdedit/Event ja

bcdedit/eventsettings net HostIP: 1.2.3.4 Port: 50000 Key: a. b. c. d

Hier ist 1.2.3.4 ein Beispiel: Ersetzen Sie dies durch die IP-Adresse des Collector-Computers. Ersetzen Sie 50000 auch durch die Portnummer, in der der Collector ausgeführt wird, und a. b. c. d mit dem erforderlichen Verschlüsselungsschlüssel für die Kommunikation. Dieser Schlüssel wird auf dem Sammelcomputer verwendet. Wenn Sie einen Schlüssel eingeben, wird ein zufälliger Schlüssel generiert; Sie benötigen diesen für den Sammelcomputer, notieren Sie diese.

2. Wenn Sie bereits einen Sammelcomputer eingerichtet haben, aktualisieren Sie die Konfigurationsdatei auf dem Sammelcomputer mit den Informationen für den neuen Zielcomputer. Weitere Informationen finden Sie im Abschnitt Konfigurieren des Collector-Computers.

Nachdem der Ereignis Transport selbst aktiviert ist, müssen Sie das System aktivieren, um etw-Ereignisse über diesen Transport tatsächlich zu senden.

So aktivieren Sie das Sendens von ETW-Ereignissen durch den Transport Remote

1. Öffnen Sie auf dem Sammelcomputer eine Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten.**2. Führen Sie `Enable-SbecAutologger -ComputerName <target_name>` aus, wobei <target_name> der Name des Zielcomputers ist.**

Wenn Sie Windows PowerShell-Remoting nicht einrichten können, können Sie Ereignisse direkt an den Zielcomputer senden.

So aktivieren Sie das Senden von ETW-Ereignissen durch den Transport lokal

1. Starten Sie auf dem Zielcomputer Regedit.exe, und suchen Sie nach dem Registrierungsschlüssel:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger. Verschiedene Protokoll-Sitzungen werden als Unterschlüssel unter diesem Schlüssel aufgelistet. **Setup-Plattform, NT Kernel-Protokollierung und Einrichten von Microsoft Windows** sind Auswahlmöglichkeiten für die Verwendung der Setup und Start-Ereignissammlung, die empfohlene Option ist **EventLog-System**. Diese Schlüssel werden in [Configuring and Starting an AutoLogger Session](#) beschrieben.

2. Im Schlüssel EventLog-System ändern Sie den Wert der **LogFileMode** von **0x10000180** auf **0x10080180**. Weitere Informationen zu den Details dieser Einstellungen finden Sie unter [Logging Mode Constants](#).
3. Optional können Sie auch das Senden von Fehlerüberprüfungsdaten an den Sammelcomputer aktivieren. Suchen Sie nach dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager, und erstellen Sie den Schlüssel **Debug Print Filter** mit dem Wert **0x1**.
4. Starten Sie den Zielcomputer neu.

Auswählen des Netzwerkadapters

Wenn auf dem Zielcomputer mehr als ein Netzwerkadapter vorhanden ist, wählt der Treiber KDNET den ersten unterstützten aus der Liste aus. Sie können einen speziellen Netzwerkadapter zum Weiterleiten des Setups von Ereignissen mit folgenden Schritten angeben:

Angabe des Netzwerkadapters

1. Öffnen Sie auf dem Zielcomputer den Geräte-Manager, erweitern Sie **Netzwerkadapter**, suchen Sie nach dem Netzwerkadapter, den Sie verwenden möchten und klicken Sie mit der rechten Maustaste darauf.
2. Klicken Sie im Menü, das geöffnet wird auf **Eigenschaften**, und klicken Sie dann auf die Registerkarte **Details**, erweitern Sie im Menü das Feld **Eigenschaft** und scrollen Sie zu **Standortinformationen** (die Liste ist wahrscheinlich nicht in alphabetischer Reihenfolge), und klicken Sie dann auf. Der Wert ist eine Zeichenfolge des Formulars **PCI-Bus X, Y, Funktion Z Gerätsein**. Notieren Sie sich X.Y.Z; Dies sind die Bus-Parameter, die Sie für den folgenden Befehl benötigen.
3. Führen Sie einen der folgenden Befehle aus:

An einer Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten:

```
Enable-SbecBcd -ComputerName <target_name> -CollectorIP <ip> -CollectorPort <port> -Key <a.b.c.d> -BusParams <X.Y.Z>
```

Von einer Eingabeaufforderung mit erhöhten Rechten: **bcdedit /eventsettings net hostip:aaa port:50000 key:bbb busparams:X.Y.Z**

Überprüfen der Konfiguration des Zielcomputers

Zum Überprüfen der Einstellungen auf dem Zielcomputer: Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, und führen Sie **bcdedit /enum** aus. Wenn dieser Schritt abgeschlossen ist, führen Sie **bcdedit /eventsettings** aus. Überprüfen Sie die folgenden Werte:

- Key
- Debugtyp = NET
- HostIP = <IP-Adresse des Sammlers >
- Port = <Portnummer, die Sie für den zu verwendenden Collector angegeben haben >

- DHCP = Ja

Überprüfen Sie auch, dass **bcdedit /event** aktiviert ist, da **/debug** und **/event** sich gegenseitig ausschließen. Sie können nur eine oder die andere ausführen. Sie können auch nicht **/eventsettings** mit **/debug** oder **/dbgsettings** mit **/event** verwenden.

Beachten Sie außerdem, dass die Ereignissammlung nicht funktioniert, wenn Sie sie auf einem seriellen Anschluss festlegen.

Konfigurieren des Sammelcomputers

Der Sammlungsdienst empfängt die Ereignisse und speichert sie in ETL-Dateien. Diese ETL-Dateien können dann von anderen Tools, wie beispielsweise der Ereignisanzeige, Nachrichtenanalyse, Wevtutil und Windows PowerShell-Cmdlets gelesen werden.

Da Sie im ETW-Format den Namen des Zielcomputers nicht angeben können, müssen die Ereignisse für jeden Zielcomputer als separate Datei gespeichert werden. Die Anzeigetools zeigen möglicherweise einen Computernamen an, aber es ist der Name des Computers, auf dem das Tool ausgeführt wird.

Genauer gesagt, wird jeder Zielcomputer einem Ring von ETL-Dateien zugewiesen. Jeder Dateiname enthält einen Index von 000 bis zu einem Höchstwert, den Sie konfigurieren können (bis zu 999). Wenn die Datei die konfigurierte maximale Größe erreicht, werden Ereignisse in die nächste Datei geschrieben. Nach der höchsten möglichen Datei wird der Dateiindex erneut auf 000 zurückgesetzt. Auf diese Weise werden die Dateien automatisch wiederverwendet, was weniger Speicherplatz erfordert. Sie können auch zusätzliche externe Aufbewahrungsrichtlinien für die Datenträgerverwendung festgelegt. Beispielsweise können Sie Dateien, die älter als eine festgelegte Anzahl von Tagen haben, löschen.

Gesammelte ETL-Dateien werden in der Regel im Verzeichnis

c:\ProgramData\Microsoft\BootEventCollector\Etl gespeichert (dies hat möglicherweise zusätzliche Unterverzeichnisse). Finden Sie die aktuelle Protokolldatei, indem Sie diese dem Zeitpunkt der letzten Änderung sortieren. Es gibt auch ein Statusprotokoll (normalerweise unter **c:\ProgramData\Microsoft\BootEventCollector\Logs**), das aufzeichnet, wenn der Sammelcomputer in eine neue Datei schreibt.

Es gibt auch ein Sammelprotokoll, das Informationen über den Sammelcomputer selbst aufzeichnet. Sie können dieses Protokoll im ETW-Format speichern (in dem Windows-Protokollierungsdienstereignisse berichtet werden; dies ist die Standardeinstellung) oder in einer Datei (normalerweise unter **c:\ProgramData\Microsoft\BootEventCollector\Logs**). Eine Datei ist möglicherweise nützlich, wenn Sie ausführliche Modi aktivieren, die eine große Datenmenge erzeugen. Sie können auch das Protokoll so festlegen, dass es in eine Standardausgabe durch Ausführen des Sammelcomputers über die Befehlszeile schreibt.

Erstellen der sammlerkonfigurationsdatei

Wenn Sie den Dienst aktivieren, werden drei XML-Konfigurationsdateien erstellt und in "
c:\programdata\microsoft\booteventcollector\config" gespeichert:

- **Active.XML** diese Datei enthält die derzeit aktive Konfiguration des Sammeldiensts. Nach der Installation hat diese Datei den gleichen Inhalt wie **Empty.xml**. Wenn Sie eine neue Konfiguration für die Sammlung festlegen, speichern Sie diese in dieser Datei.
- **Empty.XML** diese Datei enthält die Mindestkonfigurationselemente, die ihre Standardwerte erfordern. Eine Sammlung ist nicht möglich; es kann nur den Sammlungsdienst im Leerlaufmodus starten.
- **Example.XML** diese Datei enthält Beispiele und Erklärungen möglicher Konfigurationselemente.

Auswählen einer Dateigrößen Beschränkung

Eine Entscheidung ist das Festlegen der Größe der Datei. Die beste maximale Dateigröße hängt von der erwarteten Menge der Ereignisse und dem verfügbaren Speicherplatz ab. Kleinere Dateien sind zum Löschen der

alten Daten besser geeignet. Allerdings enthält jede Datei den Aufwand für einen Header mit 64 KB, und das Lesen vieler Dateien, um den kombinierten Verlauf zu erhalten, kann unpraktisch sein. Die absolute Mindestgröße für die Dateigröße beträgt 256 KB. Angemessene praktische Begrenzung für die Dateigröße sollte über 1 MB und 10 MB ist wahrscheinlich einen guten normalen Wert. Eine höhere Grenze ist möglicherweise sinnvoll, wenn Sie viele Ereignisse erwarten.

Hier sind einige wichtige Punkte bezüglich der Konfigurationsdatei:

- Die Zielcomputeradresse. Sie können seine IPv4-Adresse, MAC-Adresse oder SMBIOS-GUID verwenden. Berücksichtigen Sie diese Faktoren bei der Auswahl der zu verwendenden Adresse:
 - Die IPv4-Adresse funktioniert am besten mit statischen Zuweisungen von IP-Adressen. Allerdings müssen auch statische IP-Adressen über DHCP verfügbar sein.
 - Eine MAC-Adresse oder SMBIOS-GUID ist komfortabel, wenn sie im Voraus bekannt sind, aber die IP-Adressen dynamisch zugewiesen werden.
 - IPv6-Adressen werden vom EVENT-NET-Protokoll nicht unterstützt.
 - Es ist möglich, mehrere Arten zum Identifizieren des Computers anzugeben. Wenn z. B. die physische Hardware ersetzt werden soll, können Sie die alte und neue MAC-Adresse eingeben und beide werden akzeptiert.
- Der Schlüssel für die Kommunikation mit dem Sammelcomputer
- Name des Zielcomputers. Sie können IP-Adresse, Hostname oder einen beliebigen anderen Namen als Name für den Computer verwenden.
- Der Name der verwendeten ETL-Datei und die Konfiguration der Ringgröße

So erstellen Sie die Konfigurationsdatei

1. Öffnen Sie eine Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten, und wechseln Sie zu %SystemDrive%\ProgramData\Microsoft\BootEventCollector\Config.
2. Geben Sie `notepad .\newconfig.xml` ein und drücken Sie die EINGABETASTE.
3. Kopieren Sie diese Konfiguration in das Editor-Fenster:

```
<collector configVersionMajor=1
statuslog=c:\ProgramData\Microsoft\BootEventCollector\Logs\statuslog.xml>
<common>
    <collectorport value=50000/>
    <forwarder type=etl>
        <set name=file value=c:\ProgramData\Microsoft\BootEventCollector\Etl\{computer}\{computer}_{#3}.etl/>
        <set name=size value=10mb/>
        <set name=nfiles value=10/>
        <set name=toxml value=none/>
    </forwarder>
    <target>
        <ipv4 value=192.168.1.1/>
        <key value=a.b.c.d/>
        <computer value=computer1/>
    </target>
    <target>
        <ipv4 value=192.168.1.2/>
        <key value=d1.e2.f3.g4/>
        <computer value=computer2/>
    </target>
</common>
</collector>
```

NOTE

Der Stamm Knoten ist <Collector>. Dessen Attribute geben die Version der Syntax für die Konfiguration und den Namen der Statusprotokolldatei an.

Das <common>-Element gruppiert mehrere Ziele und gibt dabei die allgemeinen Konfigurationselemente an. ähnlich wie eine Benutzergruppe kann verwendet werden, um die allgemeinen Berechtigungen für mehrere Benutzer anzugeben.

Das <collectorport>-Element definiert die UDP-Portnummer, an der der Collector auf eingehende Daten lauscht. Dies ist der Port, der im Zielkonfigurationsschritt für Bcdedit angegeben wurde. Die Sammlung unterstützt nur einen Port, und alle Ziele müssen zu demselben Port eine Verbindung herstellen.

Das <Weiterleitungs>-Element gibt an, wie ETW-Ereignisse, die von den Ziel Computern empfangen werden, weitergeleitet werden. Es gibt nur eine Weiterleitungsart, die in ETL-Dateien schreibt. Die Parameter geben das Dateinamensmuster, die maximale Größe für jede Datei im Ring und die Größe des Rings für jeden Computer an. Die Einstellung "dexml" gibt an, dass die ETW-Ereignisse in der Binär Form geschrieben werden, während Sie empfangen wurden, ohne in XML zu konvertieren. Weitere Informationen zur Entscheidung, ob die Ereignisse XML-Daten in XML konvertiert werden sollen, finden Sie im Abschnitt XML-Ereignis Konvertierung. Das Dateinamenmuster enthält diese Platzhalter: {Computer} für den Namen des Computers und {#3} für den Index der Datei im Ring.

In dieser Beispieldatei werden zwei Zielcomputer mit dem <Target>-Element definiert. Jede Definition gibt die IP-Adresse mit <IPv4> an, Sie können jedoch auch die Mac-Adresse (z. b.

<mac value=11:22:33:44:55:66/> oder

<mac value=11-22-33-44-55-66/>) oder die SMBIOS-GUID (z. b.

<guid value={269076F9-4B77-46E1-B03B-CA5003775B88}/>) verwenden, um den Zielcomputer zu identifizieren.

Beachten Sie außerdem den Verschlüsselungsschlüssel (identisch mit Bcdedit auf dem Zielcomputer) und den Namen des Computers.

4. Geben Sie die Details für jeden Bereitstellungs Zielcomputer als separates <Ziel> Element in der Konfigurationsdatei ein, und speichern Sie dann newconfig.XML, und schließen Sie den Editor.

5. Wenden Sie die neue Konfiguration mit

```
$result = (Get-Content .\newconfig.xml | Set-SbecActiveConfig); $result
```

 an. Die Ausgabe sollte mit dem Erfolgs Feld true zurückgegeben werden. Wenn Sie ein anderes Ergebnis erzielen, lesen Sie den Abschnitt Problembehandlung in diesem Thema.

Sie können die derzeit aktive Konfiguration mit `(Get-SbecActiveConfig).text` überprüfen.

Sie können eine Überprüfung der Gültigkeit für die Konfigurationsdatei mit

```
$result = (Get-Content .\newconfig.xml | Check-SbecConfig); $result
```

 ausführen.

Obwohl Windows PowerShell-Befehl, um eine neue Konfiguration automatisch angewendet werden soll die Dienstupdates Festnetztelefon, sodass Sie ihn neu starten, können Sie immer den Dienst selbst mit einem der folgenden Befehle neu starten:

- Mit Windows PowerShell: `Restart-Service BootEventCollector`
- In einer normalen Eingabeaufforderung: `sc BootEventCollector beenden; sc BootEventCollector starten`

Konfigurieren von Nano Servern als Zielcomputer

Die minimale Schnittstelle von Nano Server kann manchmal Problemen schwer erkennen. Sie können Nano Server automatisch für Ereignissammlung für Setup und Start konfigurieren, und Diagnosedaten an einen Sammelcomputer ohne weitere Benutzereingriffe von Ihnen senden. Gehen Sie hierzu folgendermaßen vor:

So konfigurieren Sie Nano Server als Zielcomputer

1. Erstellen des grundlegenden Nano Server-Bilds. Einzelheiten finden Sie unter [Erste Schritte mit Nano Server](#).

2. Richten Sie einen Collector-Computer wie im Abschnitt Konfigurieren des Collector-Computers in diesem Thema ein.
3. Fügen Sie AutoLogger-Registrierungsschlüssel zum Senden von Diagnosenachrichten hinzu. Binden Sie die Nano Server virtuelle Festplatte, die in Schritt 1 erstellt wurde, laden Sie die Registrierungsstruktur und fügen Sie bestimmte Registrierungsschlüssel hinzu. In diesem Beispiel befindet sich das Nano Server-Bild unter C:\NanoServer. Der Pfad kann möglicherweise unterschiedlich sein, also passen Sie die Schritte entsprechend an.
 - a. Kopieren Sie auf dem Sammelcomputer den Ordner ..\Windows\System32\WindowsPowerShell\v1.0\Modules\BootEventCollector und fügen Sie ihn in das Verzeichnis ..\Windows\System32\WindowsPowerShell\v1.0\Modules auf dem Computer ein, das Sie verwenden, um die virtuelle Festplatte des Nano-Servers zu ändern.
 - b. Starten Sie eine Windows PowerShell-Konsole mit erhöhten Berechtigungen, und führen Sie Import-Module BootEventCollector aus.
 - c. Aktualisieren Sie die Nano Server VHD-Registrierung, um AutoLoggers zu aktivieren. Führen Sie hierzu Enable-SbecAutoLogger -Path C:\NanoServer\Workloads\IncludingWorkloads.vhd aus. Dadurch wird eine einfache Liste der am häufigsten verwendeten Setup- und Start-Ereignisse hinzugefügt; Sie können andere Benutzer unter [Controlling Event Tracing Sessions](#) recherchieren.
4. Aktualisieren Sie die BCD-Einstellungen im Nano Server-Bild zum Aktivieren der Kennzeichen für Ereignisse und Festlegen des Sammelcomputers, um sicherzustellen, dass die Ereignisse an den richtigen Server gesendet werden. Beachten Sie die IPv4-Adresse, TCP-Port und Verschlüsselungsschlüssel des Sammelcomputers, die Sie in der Active.XML-Datei (an anderer Stelle in diesem Thema beschrieben) der Sammlung konfiguriert haben. Verwenden Sie diesen Befehl in einer Windows PowerShell-Konsole mit erhöhten Berechtigungen:

```
Enable-SbecBcd -Path C:\NanoServer\Workloads\IncludingWorkloads.vhd -CollectorIp 192.168.100.1 -CollectorPort 50000 -Key a.b.c.d
```
5. Aktualisieren Sie den Collector-Computer auf das empfangene Ereignis, das vom Nano Server-Computer gesendet wird, indem Sie entweder den IPv4-Adressbereich, die angegebene IPv4-Adresse oder die Mac-Adresse von Nano Server zur Active. XML-Datei auf dem Collector-Computer hinzufügen (Weitere Informationen finden Sie im Abschnitt Konfigurieren des Collector-Computers in diesem Thema)

Starten Sie den Ereignissammlungsdienst

Nachdem eine gültigen Konfigurationsdatei auf dem Sammelcomputer gespeichert ist, und ein Zielcomputer konfiguriert ist und der Zielcomputer gestartet wird, wird die Verbindung mit der Sammlung erstellt und Ereignisse werden erfasst.

Das Protokoll für den Collector-Dienst selbst (die sich von Setup und Start des vom Dienst erfassten Daten unterscheidet) finden Sie unter Microsoft-Windows-BootEvent-Collector/Admin. Verwenden Sie die Ereignisanzeige für eine grafische Benutzeroberfläche der Ereignisse. Erstellen Sie eine neue Ansicht: Erweitern Sie Anwendungs- und Dienstprotokolle, dann Microsoft und klicken Sie dann auf Windows. Finden Sie BootEvent Collector, erweitern Sie ihn und suchen Sie nach Admin.

- Mit Windows PowerShell: `Get-WinEvent -LogName Microsoft-Windows-BootEvent-Collector/Admin`
- In einer normalen Eingabeaufforderung: `wvtutil qc Microsoft-Windows-BootEvent-Collector/Admin`

Problembehandlung

Problembehandlung bei der Installation des Features

	ERROR	BESCHREIBUNG DES FEHLERS	SYMPTOM	MÖGLICHE PROBLEME
Dism.exe	87	Die Featurenamenoption wird in diesem Kontext nicht erkannt.		<ul style="list-style-type: none"> - Dies kann vorkommen, wenn Sie den Featurenamen falsch schreiben. Stellen Sie sicher, dass die richtige Schreibweise verwenden und versuchen Sie es erneut. - Vergewissern Sie sich, dass dieses Feature mit der Version des Betriebssystems verfügbar ist, die Sie verwenden. Führen Sie in Windows PowerShell das Skript <code>/Online /Get-Features? { \$_-Match-Start}</code>. Wenn keine Übereinstimmung zurückgegeben wird, wird wahrscheinlich eine Version ausgeführt, die dieses Feature nicht unterstützt.
Dism.exe	0x800f080c	Der Name > der Funktions <ist unbekannt.		Wie oben

Problembehandlung bei der Sammlung

Schlags

Die Sammlung protokolliert die eigenen Ereignisse als ETW-Anbieter für die Microsoft-Windows-BootEvent-Sammlung. Zuerst sollten Sie zum Beheben von Problemen in der Sammlung suchen. Sie befinden sich in der Ereignisanzeige unter Anwendungs- und Dienstprotokolle > Microsoft > Windows > BootEvent Collector > Admin, oder Sie können sie in einem Befehlsfenster mit einem der folgenden Befehle aufrufen:

In einer normalen Eingabeaufforderung: **wevtutil qc Microsoft-Windows-BootEvent-Collector/Admin**

In einer Windows PowerShell-Eingabeaufforderung:

```
Get-WinEvent -LogName Microsoft-Windows-BootEvent-Collector/Admin (Sie können -Oldest anfügen, um zuerst die Liste in der zeitlichen Reihenfolge mit den ältesten Ereignissen zurückzugeben)
```

Sie können den Detailgrad in den Protokollen von "Fehler", "Warnung", "Info" (Standard), "Verbose" und "Debug" anpassen. Ausführlichere Ebenen als Informationen sind nützlich für die Diagnose von Problemen mit Ziel Computern, die keine Verbindung herstellen. Sie können jedoch eine große Datenmenge generieren. verwenden Sie Sie daher mit Bedacht.

Sie legen den mindestprotokolliergrad im <Collector> Element der Konfigurationsdatei fest. Beispiel: <Collector configversionmajor = 1 minlog=Verbose>.

Die Ebene "ausführlich" protokolliert einen Eintrag für jedes Paket, das sie verarbeitet. Die Debugebene fügt

ausführliche Verarbeitungsdetails hinzu und sichert den Inhalt aller empfangenen ETW-Pakete.

Auf der Debugebene kann es hilfreich sein, eine Datei zu protokollieren, anstatt sie im üblichen Protokollierungssystem anzuzeigen. Fügen Sie zu diesem Zweck im <Collector> Element der Konfigurationsdatei ein zusätzliches Element hinzu:

```
< Collector configversionmajor = 1 minlog =  
Debugprotokoll=c:\programdata\microsoft\booteventcollector\logs\log.txt >
```

Eine empfohlene Vorgehensweise bei der Problembehandlung für den Collector:

1. Zunächst stellen Sie sicher, dass die Sammlung die Verbindung vom Zielcomputer empfängt (es wird die Datei nur dann erstellt, wenn der Zielcomputer die Nachrichten sendet) mit

```
Get-SbecForwarding
```

Wenn er zurückgibt, dass eine Verbindung von diesem Ziel besteht, liegt das Problem möglicherweise in den Einstellungen des Autologgers. Wenn nichts zurückgegeben wird, ist das Problem die KDNET-Verbindung. Versuchen Sie zur Diagnose von Problemen mit KDNET die Verbindung an beiden Enden zu überprüfen (d. h., von der Sammlung und dem Ziel).

2. Um die erweiterte Diagnose aus dem Collector anzuzeigen, fügen Sie diese dem <Collector> Element der Konfigurationsdatei hinzu:

```
<Collector... minlog = Verbose >
```

Dadurch werden Nachrichten über jedes empfangene Paket aktiviert.

3. Überprüfen Sie, ob alle Pakete empfangen werden. Sie können optional das Protokoll im ausführlichen Modus über ETW statt direkt in eine Datei schreiben. Fügen Sie hierzu dem <Collector> Element der Konfigurationsdatei hinzu:

```
<Collector... minlog = Verbose Log = c:\programdata\microsoft\booteventcollector\logs\log.txt >
```

4. Überprüfen Sie die Ereignisprotokolle für Nachrichten über die empfangenen Pakete. Überprüfen Sie, ob alle Pakete empfangen werden. Wenn die Pakete empfangen, aber falsch sind, überprüfen Sie Ereignisnachrichten für Details.

5. Von der Zielseite gibt KDNET Diagnoseinformationen an die Registrierung. Suchen in **HKLM\SYSTEM\CurrentControlSet\Services\kdnet** nach Nachrichten.
KdInitStatus (DWORD) gibt = 0 bei Erfolg und einen Fehlercode bei Fehlern zurück.
KdInitErrorString = Beschreibung des Fehlers (enthält informative Nachrichten, wenn kein Fehler)

6. Führen Sie Ipconfig.exe auf dem Ziel aus und überprüfen Sie den Gerätenamen. Wenn KDNet ordnungsgemäß geladen wurde, sollte der Gerätename in etwa wie folgt lauten: kdnic anstelle des Namens des ursprünglichen Herstellers.

7. Überprüfen Sie, ob DHCP für das Ziel konfiguriert ist. DHCP ist für KDNET absolut erforderlich.

8. Vergewissern Sie sich, dass die Sammlung im gleichen Netzwerk wie das Ziel ist. Wenn nicht, überprüfen Sie, ob das routing ordnungsgemäß funktioniert, insbesondere ob die Einstellung für DHCP-Standardgateways konfiguriert ist.

Verbindungsstatus

Sie können die aktuelle Liste der vorhandenen Verbindungen sowie Informationen überprüfen, von wo die Daten weitergeleitet werden mit **Get-SbecForwarding**.

Sie können auch den aktuellen Status Änderungsverlauf abrufen, Verbindungen mit **Get-SbecHistory**.

Problembehandlung, wenn eine neue Konfiguration festgelegt wird

Wenn Sie die Konfiguration mit den Windows PowerShell-Befehl angewendet haben

```
$result = (Get-Content .\newconfig.xml | Set-SbecActiveConfig); $result , enthält die Variable $result
```

Informationen über die Bereitstellung. Sie können diese Variable nach verschiedenen Informationen abfragen:

Abrufen von Informationen zu Fehlern mit `$result.ErrorString`. Wenn Fehler gemeldet werden, wird die neue Konfiguration nicht angewendet, und die alte Konfiguration wird nicht geändert.

Abrufen von Warnungen mit `$result.WarningString`.

Abrufen von Informationen zu den Details der Konfiguration mit `$result.InfoString`.

Sie können das vollständige Ergebnis mit `$result | fl *` abrufen.

Wenn Sie das Ergebnis nicht in einer Variablen speichern möchten, können Sie

```
Get-Content .\newconfig.xml | Set-SbecActiveConfig | fl *
```

Problembehandlung von Zielcomputern

ERROR	BESCHREIBUNG DES FEHLERS	SYMPTOM	MÖGLICHE PROBLEME

ERROR	BESCHREIBUNG DES FEHLERS	SYMPTOM	MÖGLICHE PROBLEME
Bereitstellungszielcomputer	Ziel kann nicht mit der Sammlung verbunden werden		<ul style="list-style-type: none"> - Der Zielcomputer wurde nicht neu gestartet, nachdem er konfiguriert wurde. Starten Sie den Zielcomputer neu. - Der Zielcomputer verfügt über falsche BCD-Einstellungen. Überprüfen Sie die Einstellungen im Abschnitt Zielcomputer Einstellungen überprüfen. Korrigieren Sie nach Bedarf, und starten Sie dann den Zielcomputer neu. - Der KDNET/EVENT-NET-Treiber konnte nicht an einen Netzwerkadapter verbunden werden oder wurde mit dem falschen Netzwerkadapter verbunden. Führen Sie in Windows PowerShell <pre>gwmi Win32_NetworkAdapter</pre> aus, und überprüfen Sie die Ausgabe für eine mit dem ServiceName Kdnic. Wenn der falsche Netzwerkadapter ausgewählt ist, führen Sie die Schritte in erneut aus, um einen Netzwerkadapter anzugeben. Wenn der Netzwerkadapter überhaupt nicht angezeigt wird, ist es möglich, dass der Treiber den Netzwerkadapter nicht unterstützt. Siehe auch Eine empfohlene Vorgehensweise für die Problembehandlung des obigen Sammlers, insbesondere die Schritte 5 bis 8.

	ERROR	BESCHREIBUNG DES FEHLERS	SYMPTOM	MÖGLICHE PROBLEME
Sammlung		Ich kann keine Ereignisse sehen, nach der Migration des VMs, auf dem meine Sammlung gehostet wird.		Stellen Sie sicher, dass die IP-Adresse des Sammelcomputers nicht geändert wurde. Wenn dies der Fall ist, überprüfen Sie, um das Senden von ETW-Ereignissen über den Transport Remote zu ermöglichen
Sammlung		ETL-Dateien werden nicht erstellt.	Get-SpecForwarding zeigt an, dass das Ziel ohne Fehler verbunden ist, die ETL-Dateien aber nicht erstellt werden.	Der Zielcomputer hat wahrscheinlich nicht noch keine Daten gesendet werden. ETL-Dateien werden nur erstellt, wenn Daten empfangen werden.

ERROR	BESCHREIBUNG DES FEHLERS	SYMPTOM	MÖGLICHE PROBLEME
Sammlung	Ein Ereignis wird nicht in der ETL-Datei angezeigt.	Der Zielcomputer hat das Ereignis gesendet, aber beim Lesen der ETL-Datei mit der Ereignisanzeige des Message Analyzer ist das Ereignis nicht vorhanden.	<ul style="list-style-type: none"> - Das Ereignis ist möglicherweise noch im Puffer. Ereignisse werden nicht in die ETL-Datei geschrieben, bis ein vollständiger 64 KB Puffer erfasst wird oder ein Timeout von etwa 10-15 Sekunden ohne neuen Ereignisse auftritt. Warten Sie, bis das Timeout abläuft oder leeren Sie den Puffer mit <code>Save-SpecInstance</code>. - Das Manifest-Ereignis ist nicht auf dem Sammelcomputer oder dem Computer verfügbar, auf dem die Ereignisanzeige oder der Message Analyzer ausgeführt wird. In diesem Fall kann die Sammlung möglicherweise das Ereignis nicht verarbeiten (überprüfen Sie das Sammlungsprotokoll) oder der Viewer kann es möglicherweise nicht anzeigen. Es ist ratsam, alle Manifeste auf dem Sammelcomputer installiert zu haben, und Updates auf dem Sammelcomputer vor deren Installation auf den Zielcomputern zu installieren.

Beginnen Sie mit der Protokollierung des Software Bestands

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

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Bei der Protokollierung des Software Bestands werden Microsoft-Software Inventur Daten pro Server erfasst. Bevor Sie die Protokollierung des Software Bestands mit Windows Server 2012 R2 verwenden, stellen Sie sicher, dass Windows Update KB 3000850 und KB 3060681 auf jedem System installiert sind, das inventarisiert wird. Für Windows Server 2016 ist keine Windows Update erforderlich. Wenn Sie die Funktion von SIL zum Weiterleiten von Daten an einen Aggregations Server verwenden möchten, stellen Sie sicher, dass Sie über SSL-Zertifikate für Ihr Netzwerk verfügen.

Featurebeschreibung

Die Protokollierung des Softwarebestands in Windows Server ist ein Feature mit einer Reihe einfacher PowerShell-Cmdlets, über die Serveradministratoren eine Liste der auf Servern installierten Microsoft-Software abrufen können. Darüber hinaus bietet sie die Möglichkeit, diese Daten für die Aggregation in regelmäßigen Abständen mithilfe des HTTPS-Protokolls über das Netzwerk zu sammeln und an einen Zielwebserver weiterzuleiten. Zum Verwalten des Features – in erster Linie zum stündlichen Sammeln und Weiterleiten – werden ebenfalls PowerShell-Befehle verwendet.

NOTE

Ein Aggregationsserver, auf dem ein Webdienst ausgeführt wird, kann separat konfiguriert werden. Weitere Informationen zum [Aggregator der Protokollierung des Softwarebestands](#).

IMPORTANT

Keine der von der Software Inventur Protokollierung gesammelten Daten werden im Rahmen der Funktionalität des Features an Microsoft gesendet.

Praktische Anwendungen

Durch die Protokollierung des Softwarebestands sollen die Betriebskosten für das Abrufen genauer Informationen zu den lokal auf einem Server bereitgestellten Microsoft-Software reduziert werden, vor allem aber für das Abrufen dieser Informationen von mehreren Servern in einer IT-Umgebung (sofern sie in der gesamten IT-Umgebung bereitgestellt und aktiviert wird). Da die Daten an einen Aggregationsserver weitergeleitet werden können (wenn dieser separat von einem IT-Administrator eingerichtet wurde), können sie zentral, einheitlich und automatisch gesammelt werden. Die Schnittstellen können hierzu zwar direkt abgefragt werden, jedoch können mit der Protokollierung des Softwarebestands durch die Nutzung einer auf jedem Server initiierten Weiterleitungsarchitektur (über das Netzwerk) die in vielen Softwareinventur- und Ressourcenverwaltungsszenarios typischen Herausforderungen bei der Computererkennung bewältigt werden. SSL dient zum Sichern von Daten, die über HTTPS an den Aggregationsserver eines Administrators weitergeleitet werden. Da sich die Daten an einer zentralen Stelle (auf einem einzigen Server) befinden, können sie leichter analysiert und bearbeitet werden sowie Berichte erstellt werden. Beachten Sie, dass im Rahmen der Funktionalität

des Features keine Daten an Microsoft gesendet werden. Daten und Funktionen der Protokollierung des Software Bestands sind nur für die Verwendung durch den lizenzierten Besitzer und die Administratoren der Server Software vorgesehen.

Die Softwareinventurprotokollierung kann Serveradministratoren beim Ausführen folgender Aufgaben unterstützen:

- Abrufen von Inventurinformationen für Software und Server von Windows-Servern (remote und bedarfsgesteuert)
- Aggregierte Software-und Server Inventur Informationen für eine Vielzahl von Software Asset Management-Szenarien durch Aktivieren der Protokollierungsfunktion des Software Bestands für jedes Server und Auswählen eines Ziel-URIs für den Webserver und des Zertifikat Fingerabdrucks für die Authentifizierung.

Weitere Informationen

[Aggregator der Protokollierung des Softwarebestands](#)

[Verwaltung der Protokollierung des Softwarebestands](#)

[Cmdlets für die Protokollierung des Software Bestands in Windows PowerShell](#)

[Microsoft Assessment and Planning Toolkit Tool für die Volumen Aktivierungs Verwaltung](#)

Verwaltung der Protokollierung des Softwarebestands

09.04.2020 • 24 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

In diesem Dokument wird beschrieben, wie Sie die Protokollierung des Software Bestands verwalten, ein Feature, mit dem Daten Center Administratoren Microsoft-softwareasset-Verwaltungsdaten problemlos für Ihre bereit Stellungen protokollieren können. In diesem Dokument wird beschrieben, wie Sie die Protokollierung des Softwarebestands verwalten. Bevor Sie die Protokollierung des Software Bestands mit Windows Server 2012 R2 verwenden, stellen Sie sicher, dass auf jedem System, das inventarisiert werden muss, Windows Update [KB 3000850](#) und [KB 3060681](#) installiert sind. Für Windows Server 2016 sind keine windows-Updates erforderlich. Diese Funktion wird auf jedem Server lokal ausgeführt, dessen Bestand protokolliert werden soll. Es werden keine Daten von Remoteservern gesammelt.

Die Protokollierung des Software Bestands kann auch zu zwei Versionen von Windows Server vor Windows Server 2012 R2 hinzugefügt werden. Sie können die folgenden Updates installieren, um die Protokollierungs Funktionalität für den Software bestand zu Windows Server 2012 und Windows Server 2008 R2 SP1 hinzuzufügen:

- **Windows Server 2012 (Standard oder Datacenter Edition)**

NOTE

Vergewissern Sie sich, dass [WMF 4,0](#) installiert ist, bevor Sie das Update Paket unten anwenden.

- WMF 4.0-Updatepaket für Windows Server 2012: [KB 3119938](#)
- **Windows Server 2008 R2 SP1**

NOTE

Vergewissern Sie sich, dass [WMF 4,0](#) installiert ist, bevor Sie das Update Paket unten anwenden.

- Erfordert [.NET Framework 4.5](#)
- WMF 4.0-Updatepaket für Windows Server 2008 R2: [KB 3109118](#)

Es gibt bei der Nutzung dieser Funktion zwei primäre Methoden für die Inventur:

1. Starten der SIL-Protokollfunktion zum Sammeln aus SIL-Datenquellen und ständiges Weiterleiten der Nutzlast über das Netzwerk an ein angegebenes Ziel (URI).
2. Manuelles Abfragen der SIL-Daten in beliebigen Abständen mithilfe von PowerShell oder WMI.

Das Starten der SIL-Protokollierung erfordert einige Planung und Vorausschau, hat jedoch erhebliche Vorteile gegenüber dem manuellen Abfragen der Daten. Die SIL-Protokollierung bietet folgende drei Hauptvorteile für Administratoren im Rechenzentrum:

- Eine Verlauf (Protokoll) kann im Lauf der Zeit erfasst werden und ermöglicht flexible und umfassende Berichte aus einer einzigen Quelle.

- Herausforderungen bei der Ermittlung von Computern, die für viele Inventurwerkzeuge typisch sind, lassen sich überwinden.
- Herausforderungen in Bezug auf Vertrauengrenzen und Anforderungen für erhöhte Benutzerrechte, die für viele Inventurwerkzeuge typisch sind, lassen sich trotz Erhalt des Sicherheitsniveaus überwinden, da die Daten per SSL über HTTPS verschlüsselt werden.

Die Protokollierung des Softwarebestands wird standardmäßig installiert, aber die Protokollierung nicht standardmäßig gestartet. Die gesamte Konfiguration der Protokollierung des Softwarebestands erfolgt mit PowerShell-Cmdlets. Für die Protokollierung des Softwarebestands sind nur wenige Konfigurationsoptionen verfügbar. Dieses Dokument beschreibt diese Optionen und deren Verwendungszweck, sowie die zum Sammeln von Daten verwendeten Cmdlets (bei Verwendung der zweiten oben genannten Methode).

In diesem Dokument

In diesem Dokument werden folgende Konfigurationsoptionen behandelt:

- [Starten und Beenden der Protokollierung des Software Bestands](#)
- [Protokollierung des Software Bestands im Zeitverlauf](#)
- [Anzeigen der Protokollierungs Daten des Software Bestands](#)
- [Löschen der von der Software Inventur Protokollierung protokollierten Daten](#)
- [Sichern und Wiederherstellen von Daten, die von der Protokollierung des Software Bestands protokolliert werden] [Manage-Software-Inventory-Logging. MD # BKMK_Step5](#)
- [Lesen und Veröffentlichen von Daten, die von der Protokollierung des Software Bestands](#)
- [Sicherheit der Software Inventur Protokollierung](#)
- [Arbeiten mit Datums-und Uhrzeit Einstellungen in der Windows Server-Software Inventur Protokollierung](#)
- [Aktivieren und Konfigurieren der Protokollierung des Software Bestands auf einer bereitgestellten virtuellen Festplatte](#)
- [Übersicht über die Verwendung der Protokollierung des Software Bestands in Windows Server 2012 R2 ohne KB 3000850](#)
- [Verwenden der Protokollierung des Software Bestands in einer Windows Server 2012 R2 Hyper-V-Umgebung ohne KB 3000850](#)

NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

Starten und Beenden der Protokollierung des Software Bestands

Die tägliche Erfassung der Software Inventur Protokollierung und die Weiterleitung über das Netzwerk müssen auf einem Computer mit Windows Server 2012 R2 aktiviert sein, um die Software Inventur protokollieren

NOTE

Sie können das PowerShell-Cmdlet [Get-SILogging](#) verwenden, um Informationen zum Dienst für die Protokollierung des Softwarebestands abzurufen, z. B. ob er ausgeführt wird oder beendet wurde.

So starten Sie die Protokollierung des Softwarebestands

1. Melden Sie sich mit einem Konto mit lokalen Administratorrechten am Server an.
2. Öffnen Sie PowerShell als Administrator.
3. Geben Sie an der PowerShell-Eingabeaufforderung [Start SiLogging](#)

NOTE

Es ist möglich, das Ziel festzulegen, ohne einen Fingerabdruck des Zertifikats einzurichten. Ein solches Vorgehen führt jedoch dazu, dass Weiterleitungen fehlschlagen und Daten lokal bis zu 30 Tage lang vorgehalten werden. (Nach Ablauf dieser Zeit werden sie gelöscht.) Sobald ein gültiges Zertifikat-Hash für das Ziel festgelegt (und das entsprechende gültige Zertifikat im LocalMachine/Personal Speicher installiert) wurde, werden lokal gespeicherte Daten an das Ziel weitergeleitet, sofern das Ziel so konfiguriert wurde, dass diese Daten mit diesem Zertifikat akzeptiert werden (weitere Informationen finden Sie unter [Software Inventory Logging Aggregator](#)).

So beenden Sie die Protokollierung des Softwarebestands

1. Melden Sie sich mit einem Konto mit lokalen Administratorrechten am Server an.
2. Öffnen Sie PowerShell als Administrator.
3. Geben Sie an der PowerShell-Eingabeaufforderung [Stop- SiLogging](#)

Konfigurieren der Protokollierung des Softwarebestands

Sie führen drei Schritte aus, um die Protokollierung des Softwarebestands so zu konfigurieren, dass Daten nach und nach an einen Aggregationsserver weitergeleitet werden:

1. Verwenden Sie **Set-sillogging – targetUri**, um die Webadresse Ihres Aggregations Servers anzugeben (muss mit "https://" beginnen).
2. Verwenden Sie **Set-SiLogging –CertificateThumbprint**, um den Fingerabdruckhash Ihres gültigen SSL-Zertifikats anzugeben, der zum Authentifizieren der Datenübertragungen an den Aggregationsserver verwendet werden soll (der Aggregationsserver muss so konfiguriert werden, dass ein Hash akzeptiert wird).
3. Installieren Sie ein gültiges SSL-Zertifikat (für Ihr Netzwerk) im **LocalMachine/Personal-Speicher** (bzw. **/LocalMachine/MY**) des lokalen Servers, von dem aus die Daten weitergeleitet werden sollen.

Es empfiehlt sich, die Schritte vor der Verwendung von **Start-SiLogging** auszuführen. Wenn Sie die Schritte nach der Verwendung von **Start-SiLogging** ausführen möchten, müssen Sie SIL nur beenden und erneut starten. Sie können auch mit dem Cmdlet **Publish-SiData** sicherstellen, dass der Aggregationsserver über eine vollständige Ergänzung der Daten für diesen Server verfügt.

Eine umfassende Anleitung zum Einrichten des SIL-Frameworks als Ganzes finden Sie unter [Software Inventory Logging Aggregator](#). Insbesondere sollten Sie den Abschnitt über die Problembehandlung zurate ziehen, wenn bei **Publish-SiData** ein Fehler auftritt oder wenn die SIL-Protokollierung auf andere Weise fehlschlägt.

Protokollierung des Software Bestands im Zeitverlauf

Wenn die Protokollierung des Softwarebestands von einem Administrator gestartet wurde, beginnt die stündliche Sammlung und Weiterleitung der Daten an den Aggregationsserver (Ziel-URI). Die erste Weiterleitung besteht aus einem vollständigen Datensatz, den [Get-SiData](#) abruft und zu einem bestimmten Zeitpunkt auf der Konsole anzeigt. Danach prüft SIL bei jedem Intervall die Daten und leitet nur eine kleine ID-Bestätigung an den Aggregationsserver weiter, sofern seit der letzten Sammlung keine Änderung aufgetreten ist. Wenn ein Wert geändert wurde, sendet SIL erneut einen vollständigen Datensatz.

IMPORTANT

Wenn in jedem Intervall der Ziel-URI nicht erreichbar ist, oder die Datenübertragung über das Netzwerk aus irgendeinem Grund nicht erfolgreich ist, werden gesammelte Daten lokal bis zu einem Standardwert von 30 Tagen gespeichert. (Nach Ablauf dieser Zeit werden sie gelöscht.) Bei der nächsten erfolgreichen Weiterleitung von Daten auf den Zielserver für die Aggregation werden alle lokal gespeicherten Daten weitergeleitet und lokal zwischengespeicherte Daten werden gelöscht.

Anzeigen der Protokollierungs Daten des Software Bestands

Neben den im vorherigen Abschnitt beschriebenen PowerShell-Cmdlets stehen Ihnen in sechs weitere Cmdlets zum Sammeln von Daten der Protokollierung des Softwarebestands zur Verfügung:

- [**Get-silcomputer**](#) : zeigt die Zeit Punktwerte für bestimmte Server-und betriebssystembezogene Daten sowie den voll qualifizierten Namen oder den Hostnamen des physischen Hosts an, falls verfügbar.
- [**Get-silcomputeridentity \(KB 3000850\)**](#) : zeigt die von SIL verwendeten Bezeichner für einzelne Server an.
- [**Get-sildata**](#) : zeigt eine Zeit Punkt Sammlung aller Protokollierungs Daten des Software Bestands an.
- [**Get-silsoftware**](#) : zeigt die Identität des Zeitpunkts für die gesamte auf dem Computer installierte Software an.
- [**Get-silualaccess**](#) : zeigt die Gesamtanzahl der eindeutigen Client Geräteanforderungen und Client Benutzer Anforderungen des Servers ab zwei Tagen an.
- [**Get-silwindowsupdate**](#) : zeigt den Zeit Punkt der Liste aller auf dem Computer installierten Windows-Updates an.

Ein typischer Anwendungsfall für Cmdlets zur Protokollierung des Softwarebestands wäre das Abfragen der Protokollierung des Softwarebestands für einen bestimmten Zeitpunkt der gesamten Protokollierung durch einen Administrator mithilfe von [**Get-SilSoftware**](#).

Ausgabe Beispiel

```

PS C:\> Get-SilData

ID          : 961FF8A1-8549-4BEC-8DF6-3B3E32C26FFA
UUID        : B49ACB4C-7D9C-4806-9917-AE750BB3DA84
VMGUID      : E84CCCB0-0D0F-486B-A424-9780C7CF92E4
Name        : Server01Guest.Test.Contoso.com
HypervisorHostName : Server01.Test.Contoso.com

ID          : {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}
Name        : Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
InstallDate : 12/5/2013
Publisher   : Microsoft Corporation
Version     : 10.0.40219

ID          : {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}
Name        : Microsoft Silverlight
InstallDate : 3/20/2014
Publisher   : Microsoft Corporation
Version     : 5.1.30214.0

ChassisSerialNumber : 4452-0564-0284-2290-0113-6804-05
CollectedDateTime  : 10/27/2014 4:01:33 PM
Model           : Virtual Machine
Name            : Server01Guest.Test.Contoso.com
NumberOfCores   : 1
NumberOfLogicalProcessors : 1
NumberOfProcessors : 1
OSName          : Microsoft Windows Server 2012 R2 Datacenter
OSSku           : 8
OSSuite         : 400
OSSuiteMask    : 400
OSVersion       : 6.3.9600
ProcessorFamily : 179
ProcessorManufacturer : GenuineIntel
ProcessorName    : Intel(R) Xeon(R) CPU E5440 @ 2.83GHz
SystemManufacturer : Microsoft Corporation

```

NOTE

Die Ausgabe dieses Cmdlets ist identisch mit der kombinierten Ausgabe aller anderen **Get-Sil**-Cmdlets, wobei sich durch die asynchrone Ausgabe auf der Konsole möglicherweise eine unterschiedliche Reihenfolge der Objekte ergibt.

Die Protokollierung des Softwarebestands muss nicht gestartet sein, um die **Get-Sil**-Cmdlets verwenden zu können.

Löschen der von der Software Inventur Protokollierung protokollierten Daten

Die Protokollierung des Softwarebestands wurde nicht als unternehmenskritische Komponente beabsichtigt. Sie ist so konzipiert, dass ihre Auswirkungen auf lokale Systemvorgänge so gering wie möglich sind und gleichzeitig eine hohe Zuverlässigkeit gewahrt wird. Dadurch kann der Administrator die Software Inventur Protokollierungs Datenbank und die unterstützenden Dateien (jede Datei im Verzeichnis "\windows\system32\logfiles\sil") auch manuell löschen, um betriebliche Anforderungen zu erfüllen.

So löschen Sie mit der Protokollierung des Softwarebestands protokolierte Daten

1. Beenden Sie in PowerShell die Protokollierung des Softwarebestands mit dem Befehl **Stop-SilLogging**.
2. Öffnen Sie Windows-Explorer.
3. Wechseln Sie zu \windows\system32\logfiles\sil\

4. Löschen Sie alle Dateien im Ordner.

Sichern und Wiederherstellen von mit der Protokollierung des Software Bestands protokollierten Daten

Die Protokollierung des Softwarebestands speichert vorübergehend eine stündliche Datenerfassung, wenn die Weiterleitung über das Netzwerk fehlschlägt. Die Protokolldateien werden im Verzeichnis „\Windows\System32\LogFiles\SIL“ gespeichert. Mit der regelmäßigen Server-Sicherung können auch diese Daten der Protokollierung des Softwarebestands gesichert werden.

IMPORTANT

Wenn aus irgendeinem Grund eine Reparaturinstallation oder ein Upgrade des Betriebssystems erforderlich ist, gehen alle lokal gespeicherten Protokolldateien verloren. Wenn diese Daten für Vorgänge wichtig sind, sollten Sie vor der Installation eines neuen Betriebssystems gesichert werden. Führen Sie nach der Reparatur oder Aktualisierung einfach die Wiederherstellung am gleichen Speicherort durch.

NOTE

Wenn aus irgendeinem Grund die Verwaltung der Beibehaltungs Dauer von Daten, die von SIL lokal protokolliert werden, wichtig ist, kann dies durch Ändern des folgenden Registrierungs Werts konfiguriert werden: \HKEY_LOCAL_MACHINE\software\microsoft\windows\softwareinventorylogging. Der Standardwert ist "30" für 30 Tage.

Lesen und Veröffentlichen von Daten, die von der Protokollierung des Software Bestands

Daten, die von SIL protokolliert, aber lokal gespeichert werden (wenn der Forward zum Ziel-URI fehlschlägt), oder Daten, die erfolgreich an den Ziel Aggregations Server weitergeleitet werden, werden in einer Binärdatei gespeichert (für die Daten der einzelnen Tage). Um diese Daten in PowerShell anzuzeigen, verwenden Sie das Cmdlet [Import-BinaryMiLog](#).

Sicherheit der Software Inventur Protokollierung

Auf dem lokalen Server sind Administratorrechte erforderlich, um erfolgreich Daten aus dem WMI der Protokollierung des Softwarebestands über PowerShell-APIs abzurufen.

Um alle Funktionen der Protokollierung des Softwarebestands zum stündlichen Weiterleiten von Verlaufsdaten an einen Aggregationspunkt nutzen zu können, muss der Administrator mithilfe von Clientzertifikaten sichere SSL-Sessions für das Weiterleiten von Daten über HTTPS gewährleisten. Eine grundlegende Übersicht über HTTPS-Authentifizierung finden Sie hier: [HTTPS-Authentifizierung](#).

Auf alle Daten, die lokal auf einem Windows-Server gespeichert sind (tritt nur auf, wenn die Funktion gestartet wurde, aber das Ziel nicht erreichbar ist), kann nur mit Administratorrechten auf dem lokalen Server zugegriffen werden.

Arbeiten mit Datums-und Uhrzeit Einstellungen in der Windows Server 2012 R2-Protokollierung des Software Bestands

- Bei Verwendung von „[Set-SilLogging](#) - TimeOfDay“ zum Festlegen des Ausführungszeitpunkts für die SIL-Protokollierung müssen Sie ein Datum und eine Uhrzeit angeben. Das Kalenderdatum wird festgelegt, und die Protokollierung erfolgt erst, wenn das Datum in der lokalen Systemzeit erreicht ist.

- Bei Verwendung von [Get-silsoftware](#) oder [Get-silwindowsupdate](#) zeigt "InstallDate" immer den bedeutungslosen Wert "12:00:00AM" an.
- Bei Verwendung von [Get-silualaccess](#) zeigt "Sample Date" immer den bedeutungslosen Wert "11:59:00PM" an. Date sind die relevanten Daten für diese Cmdlet-Abfragen.

Aktivieren und Konfigurieren der Protokollierung des Software Bestands auf einer bereitgestellten virtuellen Festplatte

Die Protokollierung des Softwarebestands unterstützt auch das Konfigurieren und Aktivieren auf offline geschalteten virtuellen Computern. Die praktische Verwendung hierfür ist das Einrichten der "Gold Image"-Einrichtung für die weite Bereitstellung in Rechenzentren sowie das Konfigurieren von Endbenutzer Images, die von einem lokalen Standort zu einer cloudbereitstellung ausgehen.

Um diese Einsatzbereiche zu unterstützen, sind der Protokollierung des Softwarebestands Registrierungseinträge für jede konfigurierbare Option zugeordnet. Diese Registrierungs Werte finden Sie unter \ HKEY_LOCAL_MACHINE\software\microsoft\windows\softwareinventorylogging.

Funktion	Wertname	Daten	Entsprechendes Cmdlet (nur im laufenden Betriebssystem verfügbar)
Start/Stopp-Feature	CollectionState	1 oder 0	Start-SilLogging , Stop-SilLogging
Legt den Aggregationszielpunkt im Netzwerk fest	TargetUri	string	Set-SilLogging -TargetURI
Legt den Zertifikatfingerabdruck oder Hash des Zertifikats für die SSL-Authentifizierung für den Ziel-Webserver fest	CertificateThumbprint	string	Set-SilLogging -CertificateThumbprint
Legt das Datum und die Uhrzeit für den Startzeitpunkt der Funktion fest (sofern der angegebene Wert in der lokalen Systemzeit in der Zukunft liegt)	CollectionTime	Standard: 2000-01-01T03:00:00	Set-SilLogging -TimeOfDay

Um diese Werte auf einer offline geschalteten virtuellen Festplatte (VM-Betriebssystem wird nicht ausgeführt) zu ändern, muss die VHD zunächst bereitgestellt werden, und dann können die folgenden Befehle verwendet werden, um Änderungen vorzunehmen.

- [Reg load](#)
- [Reg delete](#)
- [Reg add](#)
- [Reg unload](#)

Die Protokollierung des Softwarebestands überprüft diese Werte beim Start des Betriebssystems und verfährt

entsprechend.

Übersicht über die Verwendung der Protokollierung des Software Bestands in Windows Server 2012 R2 ohne KB 3000850

Die folgenden Änderungen am Umfang der Protokollierung des Softwarebestands und an den Standardeinstellungen wurden mit [KB 3000850](#) vorgenommen:

- Das Standardintervall für die Sammlung und Weiterleitung über das Netzwerk beim Starten der SIL-Protokollierung wurde von täglich auf stündlich geändert (nach dem Zufallsprinzip innerhalb jeder Stunde).
- Die Standard-Datennutzlast wurde reduziert und enthält nur Objekte aus Get-SilComputer, Get-SilComputerIdentity und Get-SilSoftware.
- Die Gast-zu-Host-Kanalkommunikation in Hyper-V-Umgebungen wurde entfernt.

Verwenden der Protokollierung des Software Bestands in einer Windows Server 2012 R2 Hyper-V-Umgebung ohne KB 3000850

NOTE

Diese Funktion wird bei Installation des [KB 3000850](#) -Updates entfernt.

Wenn Sie die Protokollierung des Software Bestands auf einem Hyper-V-Host unter Windows Server 2012 R2 verwenden, ist es möglich, SIL-Daten von Windows Server 2012 R2-Gast Computern abzurufen, die lokal ausgeführt werden, wenn die SIL-Protokollierung in den Gastbetriebssystemen gestartet wurde. Dies ist jedoch nur bei Verwendung der PowerShell-Cmdlets Get-sildata und Publish-sildata möglich und nur mit Windows Server 2012 R2 sowohl auf dem Host als auch auf dem Gast möglich. Der Zweck dieser Funktion besteht darin, Administratoren von Rechenzentren, die Gast-VMs für Mandanten oder andere Entitäten eines großen Unternehmens bereitzustellen, das Erfassen von Software Inventur Daten auf dem Hypervisor-Host und das anschließende Weiterleiten dieser Daten an einen Aggregator (oder Ziel-URI) zuzulassen.

Im folgenden finden Sie zwei Beispiele dafür, wie die Ausgabe in der PowerShell-Konsole auf einem Windows Server 2012 R2 Hyper-V-Host, auf dem eine Windows Server 2012 R2-Gast-VM ausgeführt wird, mit der SIL-Protokollierung gestartet wird. Sie werden feststellen, dass im ersten Beispiel, in dem "Get-sildata" allein verwendet wird, alle Daten von dem Host wie erwartet ausgegeben werden. Ebenfalls enthalten sind alle SIL-Daten des Gasts, jedoch in einem reduzierten Format. Um diese Daten vom Gast zu erweitern und anzuzeigen, schneiden Sie einfach den im zweiten Beispiel verwendeten Ausschnitt aus, und fügen Sie ihn ein. SIL-Datenobjekte vom Gast verfügen immer über die VM-GUID, die dem Objekt zugeordnet ist.

NOTE

Da SIL-Daten auf der Konsole ausgegeben werden, werden bei Verwendung des Get-SilData-Cmdlets mit Datenströmen die Objekte nicht immer in vorhersehbarer Reihenfolge ausgegeben. In den beiden folgenden Beispielen wurde der Text farblich (blau für physische Hostdaten und grün für virtuelle Gastdaten) als Illustrations Tool für dieses Dokument codiert.

Ausgabe Beispiel 1

```
PS C:\Windows\system32> Get-SilData
```

```
ID      : {1D8EG291-B0D5-35EC-8441-6616F567A0F7}
Name    : Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219
InstallDate : 12/5/2013
Publisher : Microsoft Corporation
```

Version : 10.0.40219

ID : [89F4137D-6C26-4A84-BDB8-2E5A4BB71E00]

Name : Microsoft Silverlight

InstallDate : 3/11/2014

Publisher : Microsoft Corporation

Version : 5.1.30214.0

Item : MsftSil_Software (ID = "{1D8E6291-B0D5-35EC-8441-6616F567A0F7}")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : MsftSil_Software (ID = "{89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : __PARAMETERS

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : MsftSil_WindowsUpdate (ID = "KB2925418")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : MsftSil_WindowsUpdate (ID = "KB2930275")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : MsftSil_Computer (Name = "BFBLUEGUEST.redmond.corp.microsoft.com")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : MsftSil_UalAccess (RoleGuid = "10a9226f-50ee-49d8-a393-9a501d47ce04")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Item : MsftSil_UalAccess (RoleGuid = "7fb09bd3-7fe6-435e-8348-7d8aefb6cea3")

VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

PSComputerName :

ChassisSerialNumber : 7ZX7TJ1

CollectedDateTime : 3/20/2014 10:35:40 AM

Model : Precision WorkStation T7400

Name : Server01.Test.Contoso.com

NumberOfCores : 4

NumberOfLogicalProcessors : 4

NumberOfProcessors : 1

OSName : Microsoft Windows Server 2012 R2 Datacenter

OSSku : 8

OSSuite : 400

OSSuiteMask : 400

OSVersion : 6.3.9600

ProcessorFamily : 179

ProcessorManufacturer : GenuineIntel

ProcessorName : Intel(R) Xeon(R) CPU E5440 @ 2.83GHz

SystemManufacturer : Dell Inc.

VmGuid :

ID : KB2925418

InstallDate : 3/20/2014

ID : KB2930275

InstallDate : 3/20/2014

ProductName : Windows Server 2012 R2 Datacenter

RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04

RoleName : Datacenter

```

ROLEName      : File Server
SampleDate    : 3/18/2014
UniqueDeviceAccessCount :92
UniqueUserAccessCount :168

ProductName   : Windows Server 2012 R2 Datacenter
RoleGuid      : 7fb09bd3-7fe6-435e-8348-7d8aefb6cea3
RoleName      : Print and Document Services
SampleDate    : 3/18/2014
UniqueDeviceAccessCount :0
UniqueUserAccessCount :0

```

PS C:\Windows\system32>

Ausgabe Beispiel 2 (w/Expand-SilData-Funktion)

```

PS C:\Windows\system32> function Expand-SilData
>> {
>>     [CmdletBinding()]
>>     param (
>>         [Parameter(ValueFromPipeline=$true)]
>>         $Data
>>     )
>>
>>     process {
>>         $Data | ForEach-Object {
>>             # Expand MsftSil_GuestData object.
>>             if ($_.CimClass.CimSystemProperties.Namespace -eq 'root/inventorylogging') -and
($_.CimClass.CimSystemProperties.ClassName -eq 'MsftSil_GuestData') {
>>                 $guestDataObject = $_
>>                 $guestDataObjectPropertyTable = @{}
>>                 $guestDataObject.Item.CimInstanceProperties | ForEach-Object {
>>                     $guestDataObjectPropertyTable."$_.Name" = $_.Value
>>                 }
>>                 $guestPSObject = New-Object PSObject -Property $guestDataObjectPropertyTable
>>                 $guestPSObject | Add-Member NoteProperty VMIId $guestDataObject.VMGuid -
Force -PassThru
>>             } else {
>>                 $_
>>             }
>>         } | Where-Object {
>>             # Filter out EMPTY __PARAMETERS object.
>>             -not ($_.CimClass.CimSystemProperties.Namespace -eq 'root/inventorylogging') -and
($_.CimClass.CimSystemProperties.ClassName -eq '__PARAMETERS')
>>         }
>>     }
>> }
>>
PS C:\Windows\system32> Get-SilData | Expand-SilData

```

```

ID      : {1D8E6291-B0D5-35EC-8441-6616F567A0F7}
Name    : Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219
InstallDate : 12/5/2013
Publisher : Microsoft Corporation
Version  : 10.0.40219

```

```

ID      : {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}
Name    : Microsoft Silverlight

```

InstallDate : 3/11/2014
Publisher : Microsoft Corporation
Version : 5.1.30214.0

Publisher : Microsoft Corporation
Name : Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219
ID : {1D8E6291-B0D5-35EC-8441-6616F567A0F7}
InstallDate : 3/13/2014 12:00:00 AM
Version : 10.0.40219
VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

Publisher : Microsoft Corporation
Name : Microsoft Silverlight
ID : {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}
InstallDate : 3/12/2014 12:00:00 AM
Version : 5.1.30214.0
VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

ID : KB2925418
InstallDate : 3/20/2014 12:00:00 AM
VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

ID : KB2930275
InstallDate : 3/20/2014 12:00:00 AM
VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

OSVersion : 6.3.9693
ProcessorManufacturer : GenuineIntel
OSSku : 8
NumberOfLogicalProcessors : 1
Name : Server02.Test.Contoso.com
VmGuid : B5640CCC-14B5-4A24-98A3-ECB705EF9C01
Model : Virtual Machine
CollectedDateTime : 3/20/2014 3:00:00 AM
SystemManufacturer : Microsoft Corporation
NumberOfCores : 1
OSSuiteMask : 400
NumberOfProcessors : 1
ProcessorName : Intel(R) Xeon(R) CPU E5440 @ 2.83GHz
ChassisSerialNumber : 2534-2168-3964-4094-3050-2760-66
OSSuite : 400
OSName : Microsoft Windows Server 2012 R2 Datacenter
ProcessorFamily : 179
VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

UniqueUserAccessCount : 2
RoleName : File Server
SampleDate : 3/18/2014 11:59:59 PM
UniqueDeviceAccessCount : 1
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
ProductName : Windows Server 2012 R2 Datacenter
VMIId : B5640CCC-14B5-4A24-98A3-ECB705EF9C01

UniqueUserAccessCount : 0
RoleName : Print and Document Services

```
SampleDate      : 3/18/2014 11:59:59 PM
UniqueDeviceAccessCount : 0
RoleGuid       : 7fb09bd3-7fe6-435e-8348-7d8aefb6cea3
ProductName     : Windows Server 2012 R2 Datacenter
VMIID         : B5640CCC-14B5-4A24-98A3-ECB705EF9C01
```

```
ID      : KB2925418
InstallDate : 3/20/2014
```

```
ID      : KB2930275
InstallDate : 3/20/2014
```

```
ChassisSerialNumber   : 7ZX7TJ1
CollectedDateTime    : 3/20/2014 10:36:28 AM
Model                : Precision WorkStation T7400
Name                 : Server01.Test.Contoso.com
NumberOfCores        : 4
NumberOfLogicalProcessors : 4
NumberOfProcessors   : 1
OSName               : Microsoft Windows Server 2012 R2 Datacenter
OSSku                :
OSSuite              : 400
OSSuiteMask          : 400
OSVersion            : 6.3.9600
ProcessorFamily       : 179
ProcessorManufacturer : GenuineIntel
ProcessorName         : Intel(R) Xeon(R) CPU E5440 @ 2.83GHz
SystemManufacturer   : Dell Inc.
VmGuid               :
```

```
ProductName      : Windows Server 2012 R2 Datacenter
RoleGuid        : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName        : File Server
SampleDate      : 3/18/2014
UniqueDeviceAccessCount : 18
UniqueUserAccessCount : 24
```

```
ProductName      : Windows Server 2012 R2 Datacenter
RoleGuid        : 7fb09bd3-7fe6-435e-8348-7d8aefb6cea3
RoleName        : Print and Document Services
SampleDate      : 3/18/2014
UniqueDeviceAccessCount : 2
UniqueUserAccessCount : 6
```

```
PS C:\Windows\system32>
```

Weitere Informationen

Beginnen Sie mit der Protokollierung des Software Bestands

Aggregator der Protokollierung des Softwarebestands

Cmdlets für die Protokollierung des Software Bestands in Windows PowerShell

Import-binarymilog

Export-binarymilog

Aggregator der Protokollierung des Softwarebestands

09.04.2020 • 66 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2012 R2

Was ist der Aggregator der Protokollierung des Software Bestands?

Der Aggregator der Protokollierung des Softwarebestands (SILA) empfängt, aggregiert und erzeugt grundlegende Berichte über die Anzahl und Typen installierter Microsoft Enterprise Software auf Windows-Servern in einem Rechenzentrum.

SILA ist Software, die Sie unter Windows Server installieren, aber sie ist nicht in der Windows Server-Installation enthalten. Um die Software zu installieren, laden Sie sie zunächst kostenlos aus dem Windows Download Center herunter: [Aggregator der Protokollierung des Softwarebestands 1.0 für Windows Server](#)

Das Framework der Protokollierung des Softwarebestands soll die Betriebskosten der Inventarisierung von Microsoft-Software senken, die auf mehreren Servern in einer IT-Umgebung bereitgestellt ist. Dieses Framework besteht aus zwei Komponenten, diesem SIL-Aggregator und der Windows Server-Funktion, die in Windows Server 2012 R2 (Software Inventory Logging, SIL) eingeführt wurde. Dieser Aggregator der Protokollierung des Softwarebestands 1.0 wird auf einem Server installiert und empfängt dann Inventardaten von allen Windows-Servern, die so konfiguriert sind, dass sie Daten an ihn über SIL weiterleiten. Das Design ermöglicht es Administratoren von Rechenzentren, SIL in Windows Server-Masterimages zu aktivieren, die für die breite Verteilung in der jeweiligen Umgebung gedacht sind. Dieses Softwarepaket ist der Zielpunkt und soll von den Kunden in ihren Standorten installiert werden, um eine einfache Protokollierung von Inventardaten im zeitlichen Verlauf zu ermöglichen. Mit dieser Software können Sie außerdem regelmäßig grundlegende Inventarberichte in Microsoft Excel erstellen. Aggregator der Protokollierung des Softwarebestands 1.0-Berichte enthalten die Anzahl der Installationen von Windows Server, System Center und SQL Server.

IMPORTANT

Bei Verwendung dieser Software werden keine Daten an Microsoft gesendet.

Von SIL im zeitlichen Verlauf erfasste Daten

Nachdem er ordnungsgemäß bereitgestellt wurde, können die folgenden Daten im SIL-Aggregator angezeigt werden:

- Eindeutige Windows Server-Installationen in Ihrem Rechenzentrum
- FQDN
- Identifikations-GUIDs
- Anzahl der physischen Prozessoren und Kerne
- Anzahl der virtuellen Prozessoren (bei virtuellen Computern)
- Modell und Typ der physischen Prozessoren
- Ob Hyperthreading auf physischen Prozessoren aktiviert ist oder nicht
- Seriennummer des Gehäuses

- Wert der oberen Grenze für die und Identität der gleichzeitig ausgeführten virtuellen Windows Server-Computer (wenn auf einem Host einen Hypervisor ausgeführt wird) auf jedem Host im zeitlichen Verlauf
- Obere Grenze und Hostname des gleichzeitig laufenden verwalteten (System Center-Agents) Windows Server-VMS auf den einzelnen Hosts im Laufe der Zeit
- Name der System Center-Agents, die auf virtuellen Computern installiert sind, die in verwalteten High-Wasserzeichen
- Anzahl und Speicherort der SQL Server Installationen im Zeitverlauf (nur SKUs und Editionen, die eine Lizenz erfordern)
- Listen der in „Software“ installierten Programme

Wer soll SIL verwenden?

- **IT-Experten oder Administratoren von Rechenzentren**, die eine kostengünstige Methode suchen, wertvolle Softwareinventardaten automatisch und im zeitlichen Verlauf zu sammeln.
- **CIOs und Finanz Controller**, die die Nutzung von Microsoft Enterprise Software in den IT-bereit Stellungen ihrer Organisationen melden müssen.

Erste Schritte

Voraussetzungen

Aggregator der Protokollierung des Softwarebestands (SIL Aggregator) auf mindestens einem Server für Aggregation und Berichte, entweder auf einem virtuellen Computer oder auf physischer Hardware):

- **Windows Server 2012 R2** (Standard oder Datacenter Edition)
- Die IIS-Serverrolle ist zusammen mit .NET Framework 4.5, den WCF-Diensten und der HTTP-Aktivierung in derselben Auswahlstruktur im **Assistenten zum Hinzufügen von Rollen und Features** verfügbar.
- **SQLServer 2012 SP2 Standard Edition oder SQL Server 2014 Standard Edition**
- **64-Bit-Microsoft Excel 2013** (optional für die Installation, aber erforderlich zum Erstellen von Berichten)
- Optional: **VMware PowerCLI 5.5.0.5836** (erforderlich in VMware-Umgebungen)

NOTE

Bei Verwendung von Windows Management Framework gibt es ein bekanntes Kompatibilitätsproblem mit WMF Release 5,1 auf dem SIL-Aggregator. Es ist nicht erforderlich, WMF Version 4,0 auf Servern mit installiertem SIL-Aggregator zu überschreiten.

Protokollierung des Softwarebestands (SIL) ist in Windows Server-Versionen vorhanden, bei denen die folgenden Updates installiert sind:

- **Windows Server 2016** oder höher
- **Windows Server 2012 R2** (Standard oder Datacenter Edition)
 - Windows Server 2012 R2 Update **KB3000850** (November 2014)
 - Windows Server 2012 R2-Update **KB3060681** (Juni 2015)(wird ggf. auf Windows Update als optionales Update angezeigt)

Sicherheit und Kontotypen

Zertifikat Anforderung

SIL und SIL-Aggregator verwenden für authentifizierte Kommunikation SSL-Zertifikate. Die gängige Implementierung hiervon besteht in der Installation des SIL-Aggregators mit einem Zertifikat (übereinstimmender Server- und Zertifikatname), um den Webdienst zu hosten, der Inventardaten empfängt. Anschließend verwenden die Windows-Server, die mithilfe der SIL-Funktion inventarisiert werden sollen, ein anderes Clientzertifikat, um Daten per Push an den SIL-Aggregator zu übertragen. Ein PowerShell-Cmdlet ("Set-silaggregator", weitere Details unten) muss verwendet werden, um Zertifikat Fingerabdrücke der Liste der genehmigten Zertifikate des SIL-Aggregators hinzuzufügen, von denen der Aggregator zugeordnete Daten akzeptiert. Der SIL-Aggregator fährt mit der Verarbeitung und dem Einfügen in die Datenbank fort, nachdem die jeweilige Nutzlast von Daten mit einem Zertifikat authentifiziert wurde. Ausführlichere Informationen zur Funktionsweise finden Sie im Abschnitt **Details zu SIL-Aggregator-Cmdlets**.

Einrichten des Abrufkontos

Wenn Sie dem SIL-Aggregator Anmeldeinformationen hinzufügen, um Abrufvorgänge zu ermöglichen, sollten Sie einen Ansatz mit einem möglichst gering berechtigten Konto verfolgen. Als bewährte Sicherheitsmaßnahme sollten Sie außerdem nicht die gleichen Anmelde Informationen für alle oder viele Hosts in einem Rechenzentrum oder einer anderen IT-Bereitstellung verwenden.

Führen Sie auf einem Windows Server-Host, den Sie für den Abruf durch den SIL-Aggregator einrichten möchten, und um die Verwendung eines Benutzers aus der Administratorengruppe zu vermeiden, diese Schritte aus, um einem Benutzerkonto nur die notwendigen Mindestzugriffsberechtigungen zu erteilen:

So richten Sie ein Abrufkonto ein

1. Erstellen Sie auf dem Windows Server-Hyper-V-Host, von dem Ihr SIL-Aggregator abrufen soll, ein lokales Benutzerkonto, indem Sie die **Computerverwaltung** in Windows verwenden (achten Sie darauf, dass das Kontrollkästchen deaktiviert ist, das eine Kennwortänderung bei der ersten Anmeldung erzwingt).
2. Fügen Sie diesen Benutzer der Gruppe **Remoteverwaltungsbewerber** hinzu.
3. Fügen Sie diesen Benutzer der Gruppe **Hyper-V-Administratoren** hinzu.
4. Öffnen Sie **WMIMgmt.msc** mithilfe von **Start->Ausführen**.
5. Klicken Sie im Abschnitt **Aktionen** auf **Weitere Aktionen**, und wählen Sie **Eigenschaften** aus.
6. Klicken Sie auf **Security**.
7. Wählen Sie in der Strukturansicht **Namespace** den Eintrag **cimv2 namespace** aus.
8. Klicken Sie auf die Schaltfläche **Sicherheit**.
9. Fügen Sie die Gruppe **Remoteverwaltungsbewerber** im Format **Computername\Gruppenname** hinzu.
10. Klicken Sie auf **OK**.
11. Wenn Sie in das Fenster „Sicherheit“ für **root\cimv2** zurückgekehrt sind, wählen Sie die Gruppe **Remoteverwaltungsbewerber** aus.
12. Vergewissern Sie sich, dass im Abschnitt "Berechtigungen" am unteren Rand die Option **Remote Aktivierung** aktiviert ist.
13. Klicken Sie auf **Übernehmen**, und klicken Sie anschließend auf **OK**.
14. Klicken Sie im Fenster **Eigenschaften** auf **OK**.

Installieren des SIL-Aggregators

Es gibt einige Dinge, die Sie vor der Installation des SIL-Aggregators auf einem Windows-Server überprüfen müssen:

- Sie verfügen über ein gültiges SSL-Zertifikat, das Sie zum Hosten des Webdiensts dieser Software

verwenden möchten.

- Das Zertifikat sollte im PFX -Format sein.
- Der Name des Windows-Servers und der Zertifikatname müssen übereinstimmen.
- **SQL Server Standard Edition ist installiert**, oder sie ist auf einem Remoteserver installiert, der mit dieser Software verwendet werden soll.
 - SIL-Aggregator funktioniert sowohl mit SQL Server 2012 SP2 als auch mit SQL Server 2014. Es ist nichts Ungewöhnliches erforderlich, wenn Sie während der Installation von SQL Server Optionen auswählen.
 - Das für die Installation des SIL-Aggregators verwendete Konto muss die sysadmin-Rolle in SQL besitzen, damit es die Datenbank während der Installation erstellen kann.
 - Das für die Installation des SIL-Aggregators verwendete Konto sollte in den SQL Analysis Services als Administrator hinzugefügt werden, bevor der SIL-Aggregator installiert wird.
 - Sobald der SQL Server-Agent installiert ist, sollte er für die automatische Ausführung konfiguriert werden.
- **Die IIS-Serverrolle wird zusammen mit .NET Framework 4.5, den WCF-Diensten und der HTTP-Aktivierung, alle in derselben Auswahlstruktur im Assistenten zum Hinzufügen von Rollen und Features, hinzugefügt.**
- Sie sind bei **dem Server mit einem Konto angemeldet, das auf dem Server über Administratorberechtigungen verfügt**.
- Sie sind bei **dem Server mit einem Konto angemeldet, das auf dem SQL Server über sysadmin-Berechtigungen verfügt**, wenn Windows-Authentifizierung gewünscht ist.

OR

Wenn SQL-Authentifizierung gewünscht ist, **haben Sie das Kennwort für ein Konto mit SQL-Administratorrechten**.

So installieren Sie den Aggregator der Protokollierung des Softwarebestands

1. Doppelklicken Sie auf **Setup.exe**, um die Installation zu starten.
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wenn Sie den Endbenutzer-Lizenzvertrag akzeptieren, aktivieren Sie das Kontrollkästchen, mit dem die Vereinbarung akzeptiert wird, und klicken Sie dann auf **Weiter**.
4. Wählen Sie in **Funktionen auswählen** die Option **Aggregator der Protokollierung des Softwarebestands und Berichtmodul installieren**, und klicken Sie dann auf **Weiter**.

Weitere Informationen zur Installation des Berichtmoduls finden Sie unter [Publish-SilReport](#) im Abschnitt **Details zu SIL-Aggregator-Cmdlets**.

5. Nachdem alle erforderlichen Komponenten überprüft wurden, klicken Sie auf **Weiter**.
6. Wählen Sie in **Kontotyp auswählen**, entweder **Lokaler Benutzer** oder **gMSA** aus, ganz nach Ihren Vorlieben.

Wenn Sie die Option für das lokale Benutzerkonto auswählen, wird ein lokaler Benutzer mit einem automatisch generierten, sicheren Kennwort erstellt. Dieses Konto wird für alle SIL-Aggregatordienste und -aufgabenvorgänge auf dem lokalen Server verwendet. Die Verwendung von gruppenverwalteten Dienstkonten (gMSA) wird empfohlen, wenn der Aggregator Teil der Active Directory-Domäne ist (Windows Server 2012 und höher). Weitere Informationen zu gruppenverwalteten Dienstkonten (gMSA)

finden Sie unter [Gruppenverwaltete Dienstkonten: Übersicht](#).

- Die gMSA-Kontooption muss verwendet werden, wenn Sie die Ausführung der SQL Server-Datenbank auf einem vom SIL-Aggregator getrennten Server planen.
- Vergessen Sie nicht, den Server neu zu starten, nachdem Sie das Computer Konto der GMSA-fähigen Sicherheitsgruppe in Active Directory hinzugefügt haben.

7. Geben Sie in **SQL Server auswählenden** SQL-Server ein, auf dem Ihre SQL-Instanz installiert ist, oder **localhost**, wenn sie auf dem lokalen Server installiert ist.

Es wird nur ein SIL-Aggregator pro SQL Server-Instanz unterstützt.

8. Wählen Sie den Authentifizierungstyp aus, und klicken Sie auf **SQL überprüfen**.

9. Klicken Sie auf **Weiter**, und wählen Sie dann in **Internet Information Services-Serverdetails** eine Portnummer aus, oder übernehmen Sie den Standardwert.

10. Wechseln Sie im Dateisystem zum Speicherort der Datei **PFX**-Datei, und klicken Sie dann auf **Weiter**.

11. Im letzten Bildschirm wird der Installationsstatus angezeigt. Nach erfolgreichem Abschluss klicken Sie auf **Fertig stellen**.

Deinstallieren des SIL-Aggregators

So deinstallieren Sie den Aggregator der Protokollierung des Softwarebestands

1. Öffnen Sie die **PowerShell** als Administrator, und geben Sie `Stop-SilAggregator` ein. Wenn die Eingabeaufforderung wieder angezeigt wird, wurde der SIL-Aggregator beendet.

Standardmäßig verarbeitet der SIL-Aggregator Dateien nach 20 Minuten bzw. nachdem 100 Dateien empfangen wurden. In großen Umgebungen wird dieses Szenario nie eintreten, aber in kleineren Umgebungen können noch zu verarbeitende Dateien zurückbleiben, bevor der Aggregator beendet werden kann. Verwenden Sie den Parameter `-Force`, wenn diese Dateien und Daten nicht aufbewahrt werden müssen.

2. Wechseln Sie zur **Systemsteuerung**, klicken Sie auf **Programme und Funktionen**, klicken Sie auf **Programme deinstallieren**, klicken Sie auf **Aggregator der Protokollierung des Softwarebestands**, und klicken Sie dann auf **Deinstallieren**.

Der Aggregator der Protokollierung des Softwarebestands öffnet ein Fenster, in dem Sie aufgefordert werden, zwischen dem Löschen aller Daten in der Datenbank und dem Behalten aller Daten in der Datenbank auszuwählen. Die Standardauswahl ist die Beibehaltung (falls eine Neuinstallation gewünscht ist, können Sie an die vorhandene Datenbank anfügen, um an der Stelle fortzufahren, wo der Aggregator aufgehört hatte).

3. Wählen Sie entweder **Behalten** oder **Löschen** aus, und klicken Sie dann auf **Weiter**.

4. Sobald der Statusbalken vollständig ist, klicken Sie auf **Fertig stellen**.

Mit der Verwendung von SIL und dem SIL-Aggregator beginnen

Einführung in die PowerShell-Cmdlets des SIL-Aggregators

Die folgenden Befehle können als Administrator in der Windows PowerShell-Konsole ausgeführt werden:

WINDOWS POWERSHELL-CMDLET	FUNKTION
<code>Start-SilAggregator</code>	Startet alle Dienste und Aufgaben des Aggregators der Protokollierung des Softwarebestands. Dies ist erforderlich, damit der Aggregator Daten über HTTPS von Servern mit gestarteter SIL-Protokollierung empfangen kann.

WINDOWS POWERSHELL-CMDLET	FUNKTION
Stop-SilAggregator	Beendet alle Dienste und Aufgaben des Aggregators der Protokollierung des Softwarebestands. Wenn sich Aufgaben oder Dienste in der Ausführung befinden, kann es zu einer Verzögerung beim Abschluss dieses Befehls kommen.
Set-SilAggregator	Ermöglicht dem Administrator die Vornahme von Konfigurationsänderungen am Aggregator der Protokollierung des Softwarebestands.
Add-SilVmHost	Wird verwendet, um bestimmte Hostnamen oder ein Array von Hostnamen hinzuzufügen, die in regelmäßigen Abständen abgerufen werden (der Standardwert ist ein Stunden Intervall).
Remove-SilVmHost	Wird verwendet, um bestimmte Hostnamen oder ein Array von Hostnamen zu entfernen, die bzw. das in regelmäßigen Abständen abgerufen werden soll.
Get-SilVMHost	Wird verwendet, um die Liste der physischen Hosts abzurufen, für die der Aggregator der Protokollierung des Softwarebestands zum Abrufen der laufenden Daten der virtuellen Computerzustände konfiguriert ist.
Get-SILAggregatorData	Wird verwendet, um Daten aus der Datenbank in die PowerShell-Konsole abzurufen.
Publish-SilReport	Wird verwendet, um Berichte aus der Datenbank der Protokollierungsdaten des Softwarebestands zu erstellen. Hinweis: Die Cubeverarbeitung auf dem Aggregator erfolgt einmal täglich. Somit werden vom Aggregator erfasste Daten erst am folgenden Tag in Berichten angezeigt.

Empfohlene Reihenfolge für den Start

Nachdem Sie den Aggregator der Protokollierung des Softwarebestands auf Ihrem Server installiert haben, öffnen Sie die PowerShell als Administrator.

- Auf Ihrem SIL-Aggregator:

- Führen Sie `Start-SilAggregator` aus.

Dies ist erforderlich, damit der Aggregator Daten aktiv empfängt, die von Ihren Servern, die Sie für die Inventarisierung eingerichtet haben (oder einrichten werden), über HTTPS an ihn weitergeleitet werden. Beachten Sie, dass selbst wenn Sie auf Ihren Servern aktiviert haben, dass sie zuerst an diesen Aggregator weiterleiten, dies in Ordnung ist, da sie ihre Datennutzlasten für bis zu 30 Tage lokal zwischenspeichern. Sobald der Aggregator, seine "targetUri", ausgeführt wird, werden alle zwischengespeicherten Daten gleichzeitig an den Aggregator weitergeleitet, und alle Daten werden verarbeitet.

- Führen Sie `Add-SilVMHost` aus.

Beispiel: `add-silvmhost -vmhostname contoso1 -hostcredential get-credential`

- In diesem Beispiel ist **contoso1** der Netzwerkname (oder IP-Adresse) des physischen Hostservers, von dem Ihr Aggregator regelmäßige Aktualisierungen dahingehend abrufen soll, welche virtuellen Computer darauf ausgeführt werden, um diese Daten im zeitlichen Verlauf nachzuverfolgen. „Get-Credential“ fordert den angemeldeten Benutzer auf, ein Konto

einzugeben, das zum Abrufen dieses Hosts von diesem Zeitpunkt an verwendet werden soll. Wenn Sie denselben Befehl auf demselben Host noch mal ausführen, können Sie jederzeit das verwendete Konto aktualisieren. Passen Sie auf Kontokennwortänderungen und -abläufe im Laufe der Zeit auf. Wenn sich Anmeldeinformationen ändern oder diese ablaufen, schlägt das Abrufen auf dem Host fehl.

- Standardmäßig beginnt das Abrufen stündlich, wobei es eine Stunde nach der Ausführung von `Start-SilAggregator` beginnt bzw. eine Stunde nachdem ein Host der Abrufliste neu hinzugefügt wurde. Das Abrufintervall kann mithilfe des `Set-SilAggregator cmdlet`s geändert werden.
- Dieses Cmdlet erkennt automatisch aus einer vordefinierten Liste mit Optionen (siehe Abschnitt **Details zu SIL-Aggregator-Cmdlets**), welcher HostType und HyperVisorType für den Host korrekt ist, den Sie hinzufügen. Wenn es diese nicht erkennen kann, oder wenn die angegebenen Anmeldeinformationen falsch sind, wird eine Eingabeaufforderung angezeigt. Wenn Sie mit der Eingabe von J akzeptieren, wird der Host hinzugefügt und als **Unbekannt** aufgeführt, wird aber nicht abgerufen.
- Führen Sie `Set-SilAggregator -AddCertificateThumbprint` "Fingerabdruck Ihres Client Zertifikats" aus.

Dies ist erforderlich, damit Daten über HTTPS von Windows-Servern mit aktivierter SIL-Protokollierung empfangen werden können. Der Fingerabdruck wird der Liste der Fingerabdrücke hinzugefügt, von denen der Aggregator SIL-Daten akzeptiert. Der SIL-Aggregator ist darauf ausgelegt, gültige Enterprise-Clientauthentifizierungszertifikate zu akzeptieren. Das verwendete Zertifikat muss auf dem Server, auf dem die Daten weitergeleitet werden, im Speicher `\LocalMachine\MY (lokaler Computer > persönlich)` installiert werden.

- Öffnen Sie auf Ihren zu inventarisierenden Windows-Servern die PowerShell als Administrator, und führen Sie diese Befehle aus:

- Führen Sie

```
Set-SilLogging -TargetUri "https://contososilaggregator" -CertificateThumbprint "your client certificate's thumbprint"
```

aus.
- Dies teilt SIL in Windows Server mit, wohin die Inventardaten zu senden sind und welches Zertifikat für die Authentifizierung verwendet werden soll.

IMPORTANT

Stellen Sie sicher, dass sich "https://" im targetUri-Wert befindet.

- Das Enterprise-Clientzertifikat mit diesem Fingerabdruck muss in `\localmachine\MY` installiert werden, oder Sie müssen `certmgr.msc` verwenden, um das Zertifikat im Speicher **Lokaler Computer -> Persönlich** zu installieren.

IMPORTANT

Wenn diese Werte nicht richtig sind oder das Zertifikat nicht im richtigen Speicher installiert (oder ungültig) ist, schlagen Weiterleitungen an das Ziel fehl, wenn die SIL-Protokollierung gestartet wird. Daten werden für bis zu 30 Tage lang lokal zwischengespeichert.

- Führen Sie `Start-SilLogging` aus.

Dies startet die SIL-Protokollierung. Jede Stunde, in zufälligen Intervallen innerhalb dieser Stunde,

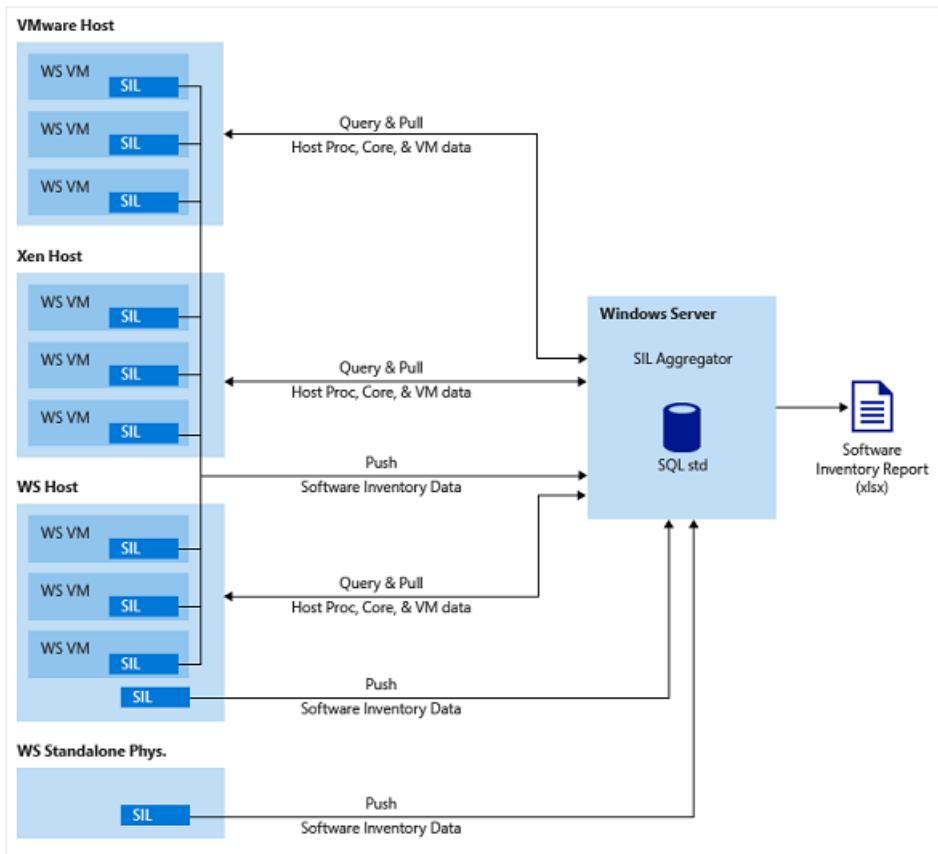
leitet SIL seine Inventardaten an den mithilfe des Parameters `-targeturi` angegebenen Aggregator weiter. Die erste Weiterleitung umfasst einen vollständigen Satz von Daten. Jede nachfolgende weiterleiten ist eher ein "Takt", bei dem nur Daten identifiziert werden, die sich nicht geändert haben. Gibt es eine Änderung an dem Dataset, wird ein weiterer vollständiger Satz von Daten weitergeleitet.

- Führen Sie `Publish-SilData` aus.
 - Bei der ersten Aktivierung von SIL für die Protokollierung ist dieser Schritt optional.
 - Hierbei handelt es sich um eine manuelle, einmalige Weiterleitung eines vollständigen Satzes von Daten.
 - Wenn die SIL Protokollierung schon seit einiger Zeit gestartet ist und ein neuer SIL-Aggregator mithilfe von `Set-SilLogging` festgelegt wird, ist es erforderlich, dieses Cmdlet einmalig auszuführen, um einen vollständigen Satz von Daten an den neuen Aggregator zu senden.

Nachdem Sie diese Schritte ausgeführt haben, um physische Hosts hinzuzufügen, auf denen virtuelle Windows Server-Computer ausgeführt werden UND nachdem Sie die Protokollierung des Softwarebestands (bzw. SIL-Protokollierung) in diesen Windows-Servern aktiviert haben, können Sie jederzeit `Publish-SilReport -OpenReport` auf dem SIL-Aggregator ausführen (erfordert Excel 2013). Beachten Sie jedoch, dass der SQL Server Analysis Services-Cube einmal täglich eine Verarbeitung durchführt, sodass Daten nicht am selben Tag in Berichten verfügbar sind.

Übersicht über die Architektur

SIL arbeitet sowohl im Push- als auch im Pull-Modus und besteht aus zwei Komponenten, die parallel arbeiten: die Funktion „Protokollierung des Softwarebestands (SIL)“ in Windows Server und die herunterladbare MSI-Datei des Aggregators der Protokollierung des Softwarebestands. Die zu inventarisierenden Server senden mithilfe von SIL Inventardaten über HTTPS an den SIL-Aggregator (Push; jede Stunde zu zufälligen Zeitpunkten innerhalb jeder Stunde). Der Aggregator wiederum ruft oder fragt die physischen Hypervisor-Hosts ab (Pull), um stündlich Hardwareinventardaten abzurufen. Beide Funktionen, sowohl Push als auch Pull, müssen ordnungsgemäß konfiguriert sein, um die vollständige Funktionalität von SIL zu ermöglichen. Sie können in beliebiger Reihenfolge konfiguriert werden. Allerdings erfolgt die Cubeverarbeitung auf dem Aggregator einmal täglich, sodass vom Aggregator per Push oder Pull erfasste Daten erst am folgenden Tag in Berichten angezeigt werden.



IMPORTANT

Bei Verwendung dieser Software werden keine Daten an Microsoft gesendet.

Aktivieren von SIL auf mehrerer Servern

Es gibt mehrere Möglichkeiten, um SIL in einer verteilten Serverinfrastruktur, beispielsweise in einer privaten Cloud aus virtuellen Computern, zu aktivieren. Im Folgenden finden Sie ein Beispiel für eine Möglichkeit zum Einrichten von Windows Server-Images, damit diese automatisch Inventardaten an einen SIL-Aggregator senden, wenn sie im Netzwerk zum ersten Mal gestartet werden.

Führen Sie auf jeder ausgeführten virtuellen Maschine bzw. physischem Computer/Gerät mit installiertem Windows Server (siehe Abschnitt **Voraussetzungen**) folgende Cmdlets in der PowerShell-Konsole als Administrator aus:

Sie benötigen ein gültiges SSL-Clientzertifikat im PFX-Format, um diese Schritte auszuführen. Der Fingerabdruck dieses Zertifikats muss mithilfe des Cmdlets `Set-SILAggregator -AddCertificateThumbprint` Ihrem SIL-Aggregator hinzugefügt werden. Dieses Clientzertifikat muss nicht mit dem Namen Ihres SIL-Aggregators übereinstimmen.

- `$secpasswd = ConvertTo-SecureString " " -AsPlainText -Force`
- `$mycreds = New-Object System.Management.Automation.PSCredential (" ", $secpasswd)`
- `$driveLetters = ([int][char]'C')..([int][char]'Z') | % {[char]$_}`
- `$occupiedDriveLetters = Get-Volume | % DriveLetter`
- `$availableDriveLetters = $driveLetters | ? {$occupiedDriveLetters -notcontains $_}`
- `$firstAvailableDriveLetter = $availableDriveLetters[0]`
- `New-PSDrive -Name $firstAvailableDriveLetter -PSProvider filesystem -root <\server\path für die`

Freigabe, die Ihre PFX-Zertifikat Datei > enthält `-credential $mycreds`

- `Copy-Item ${firstAvailableDriveLetter}:\ < certificename.pfx-Datei im Verzeichnis des neuen Laufwerks > c:< Speicherort Ihrer Wahl >`
- `Remove-PSDrive -Name $firstAvailableDriveLetter`
- `$mypwd = ConvertTo-SecureString -String " " -Force -AsPlainText`
- `Import-PfxCertificate -FilePath c:\ < Speicherort\certifiupename.pfx-> cert:\localMachine\my -Password $mypwd`
- `Set-sillogging -targeturi "https://<certificatethumbprint>"`

NOTE

Verwenden Sie den Zertifikat Fingerabdruck aus der PFX-Client Datei, und fügen Sie dem SIL-Aggregator mithilfe des Cmdlets `Set-silaggregator -addcertifikatethrebprint`" hinzu.

- `Start-sillogging`

Wann immer ein SIL-Aggregator nicht erreicht werden kann, werden SIL-Inventardaten SIL lokal für bis zu 30 Tage auf Windows-Servern zwischengespeichert. Nachdem ein erfolgreicher Push an den Aggregator erfolgt ist, werden alle zwischengespeicherten Daten weitergeleitet.

Fügen Sie der oben angeführten Liste `Publish-SilData` hinzu, wenn SIL-Daten nach erfolgreichen Pushvorgängen an den alten Aggregator an einen neuen SIL-Aggregator per Push übertragen werden (hierdurch wird ein vollständiger Ergänzungssatz von SIL-Daten gesendet, die der neue Aggregator für diesen Computer benötigt).

Berichte des Aggregators der Protokollierung des Softwarebestands

Calendar Month	Host Name	Host Type	Hypervisor Type	Processor Manufacturer	Processor Model	VM Name	Simultaneously Running Windows Servers by Host	Physical Processor Count	Physical Core
CY2015-May	Citrixhost-034						11	6	22
	i686 XenServer release 6.2.0-70446c (xenenterprise)	Citrix	XenServer	Intel	Intel(R) Core(TM)2 CPU 6800 @ 2.40GHz	WIN-UK3ATPQ33RP.testdomain.corp.contoso.com	1	2	2
	win-0ue53qb4lq.corp.contoso.com					Microsoft Windows Server 2012 R2 Standard	1	1	4
	x86 VMware ESX Server	VMWare	Esxi	Intel	Intel(R) Xeon(R) CPU W3520 @ 2.67GHz	ServerManager Test	2	1	4
						Unknown OS	1	1	4
						WIN2008R2Enterprise	1	1	4
						Unknown OS	1	1	4
						WIN-EAM4I4PRK.testdomain.corp.contoso.com	1	1	4
						Microsoft Windows Server 2012 R2 Standard	1	1	4
						WIN-TMRUSL5HEZ.testdomain.corp.contoso.com	1	1	4
						Microsoft Windows Server 2012 R2 Standard	1	1	4
	linux-openSUSE-xen						1	0	4
	x86_64 openSUSE Linux Enterprise Server 12	OpenSuSe	Xen	Intel	Intel(R) Xeon(R) CPU W3520 @ 2.67GHz	WIN-NAS54D1KL0.testdomain.corp.contoso.com	1	0	4
						Microsoft Windows Server 2012 R2 Standard	1	0	4
	OpenSuse901.testdomain.corp.contoso.com						1	1	4
	x86_64 openSUSE 13.2 (Hansquin)\x86_64	OpenSuSe	KVM	Intel	Intel(R) Core(TM)2 CPU 6800 @ 2.40GHz	WIN-FOH1U1AO23H.testdomain.corp.contoso.com	1	1	4
	bfrbluehost14.company.corp.contoso.com					Microsoft Windows Server 2012 R2 Standard	1	1	4
	64-bit Microsoft Windows Server 2012 R2 Standard	Windows	HyperV	GenuineIntel	Intel(R) Xeon(R) CPU E5440 @ 2.83GHz	bfr-aggregate7.company.corp.contoso.com	5	1	4
						Microsoft Windows Server 2012 R2 Datacenter	5	1	4
						bfr-blurtn2	5	1	4
						Unknown OS	5	1	4
						bfr-blurtn1.corp.contoso.com	5	1	4
						Microsoft Windows Server 2012 R2 Datacenter	5	1	4
						bfr-blurtn3.corp.contoso.com	5	1	4
						Microsoft Windows Server 2012 R2 Datacenter	5	1	4
						bfr-agregate2.company.corp.contoso.com	5	1	4
						Microsoft Windows Server 2012 R2 Datacenter	5	1	4
						bfr-agregate1.company.corp.contoso.com	5	1	4
						Microsoft Windows Server 2012 R2 Datacenter	5	1	4
						bfr-TPtest1.company.corp.contoso.com	5	1	4
						Microsoft Windows Server Technical Preview 2	5	1	4
	bfrbluehost3.company.corp.contoso.com						1	1	4
	Microsoft Windows Server 2012 R2 Datacenter	Windows	HyperV	GenuineIntel	Intel(R) Xeon(R) CPU E5440 @ 2.83GHz				

Cubeverarbeitung

Auf einem Aggregator der Protokollierung des Softwarebestands wird der SQL Server Analysis Services-Cube einmal täglich um 3:00:00 Uhr lokale Systemzeit verarbeitet. Berichte enthalten alle bis zu diesem Zeitpunkt erfassten Daten, aber keine Daten, die nach diesem Zeitraum am selben Tag liegen.

Obere Grenze

Ein grundlegender Aspekt der Berichte des Aggregators der Protokollierung des Software Bestands ist die Erfassung, was häufig als "obere Grenze" von gleichzeitig auszulaufenden Windows-Servern bezeichnet wird. Dies gilt für die Anzahl von Windows Server und System Center in diesen Berichten. Bei Windows Server hat jeder einzelne physische Host einen Zeitpunkt (unabhängig vom BS-Typ auf dem Host) im Verlauf eines Monats, wenn die meisten virtuellen Windows Server-Computer gleichzeitig ausgeführt werden. Dies ist die obere Grenze

für den Monat. Zusätzlich gibt es für System Center einen Zeitpunkt im Monat, wenn die meisten verwalteten Windows-Server pro physischem Host gleichzeitig ausgeführt werden (ein verwalteter Server wird dadurch gekennzeichnet, dass mindestens ein System Center-Agent vorhanden ist) gleichzeitig ausgeführt werden. Nur die jüngste obere Grenze für jeden physischen Host wird im Bericht angezeigt. Es werden keine Daten angezeigt, die nach der oberen Grenze liegen. Und es ist davon auszugehen, dass die Anzahl virtueller Windows Server-Computer (WS-Registerkarten) oder verwalteter virtueller Windows Server-Computer (SC Registerkarten) nach diesem Punkt unter die obere Grenze gefallen ist. Diese Art der Nachverfolgung und Darstellung der Verwendung soll bei der Kapazitätsplanung sowie bei der Ausrichtung an den Lizenzmodellen für diese Produkte helfen.

Auf SQL-bezogenen Registerkarten im Bericht werden SQL Server Installationen kumulativ gezählt. nicht nach hig-Wasserzeichen. Summen sind eine laufende Zählung der SQL Server-Installationen.

NOTE

Die Verwendung der Protokollierung des Softwarebestands ersetzt nicht die Verpflichtung, die Verwendung von Microsoft-Software gemäß den geltenden Lizenzbedingungen genau zu melden.

Datum/Uhrzeit des Abrufs

Bei Verwendung des Aggregators der Protokollierung des Softwarebestands ist es wichtig zu verstehen, dass die Aggregation für die Zählungen der oberen Grenze abrufgesteuert ist. Mit anderen Worten heißt dies, dass eine obere Grenze nur durch einen Abruf des zugrunde liegenden physischen Hosts erfasst werden kann. Daher sind die Anzahl der oberen Grenzwerte direkt mit einem entsprechenden "Abrufdatum/-Zeit" verknüpft. Zwar kann das Abrufintervall angepasst werden, doch die Zuverlässigkeit der erfassten oberen Grenzen wird beeinträchtigt, wenn ein höherer Intervallwert verwendet wird. Je höher das Intervall, desto weniger repräsentativ sind die Daten für die tatsächliche Verwendung.

Berichte sind „monatlich“ aufgebaut

Alle Berichte, sogar Jahresberichte, werden als monatliche Berichte dargestellt. Obere Grenzen, Summen und Computerdaten werden alle am Anfang jedes Kalendermonats zurückgesetzt.

Berichtsdaten, die u. a. vom Wechsel zu einem neuen Monat betroffen sind:

- Alle oberen Grenzen für alle Hosts werden zu Beginn eines neuen Monats zurückgesetzt.
- Wenn der Aggregator mindestens eine vollständige Nutzlast von einem virtuellen Computer (über HTTPS) empfängt, jedoch keine Takte mehr empfängt, setzen alle Abrufe des zugrunde liegenden Hosts innerhalb dieses Monats die Zuordnung zwischen Host, virtuellem Computer und Daten des virtuellen Computers voraus, weil dieser virtuelle Computer im Verlauf des Monats ausgeführt oder beendet wird. Am Anfang des neuen Monats wird diese Zuordnung gelöscht, bis entweder eine vollständige Nutzlast oder ein Takt von diesem virtuellen Computer empfangen wird.

Zusätzliche Hinweise zum Verhalten von Berichten

- Zusammenfassungsregisterkarten sollen Kurzübersichtslisten des Inventars sein. Hosts und ihre virtuellen Computer werden in derselben Spalte aufgeführt.
- Ignoriert alle Werte, die grau oder Dim sind. Dabei handelt es sich um Artefakte der Berichterstellung aus dem SSAS-Cube.
- Wenn ein virtueller Computer mit "Unbekanntes Betriebssystem" aufgelistet ist, bedeutet dies, dass der Aggregator keine vollständige Daten Nutzlast von diesem virtuellen Computer über SIL über HTTPS erhalten hat.
- Virtuelle Computer, die unter "Unbekannter Host" aufgeführt sind, sind virtuelle Windows Server-Computer, die erfolgreich Inventur Daten über HTTPS an den Aggregator weiterleiten, der Aggregator aber

den zugrunde liegenden Host für diesen virtuellen Computer nicht aktiv oder erfolgreich abfragt
Zählungen sind immer null für diese Einträge, da der zugrunde liegenden Host unbekannt ist. Verwenden Sie das Cmdlet `Add-SILVMHost` mit den richtigen Anmeldeinformationen, um den Host (oder alle Hosts) dem SIL-Aggregator für das Abrufen hinzuzufügen. Nach erfolgreichem Abruf werden die Daten der virtuellen Computer und die Hostdaten im weiteren Verlauf in Berichten zugeordnet.

- Alle Datums- und Zeitangaben sind lokale Systemzeiten und beziehen sich auf das lokale Gebietsschema des SIL-Aggregator. Dies schließt von SIL-aktivierten Systemen über HTTPS empfangene Inventardaten ein. Wenn diese Dateien verarbeitet werden (nicht später als 20 Minuten nach dem Empfang), werden die Daten mit der lokalen Systemzeit in die Datenbank eingefügt.
- "SIL-Aggregator" wird auf jedem Server Computer angegeben, auf dem der Aggregator der Protokollierung des Software Bestands installiert ist.
- Wenn sich bei einem physischen Host die Anzahl der Prozessoren oder die Menge des physischen Arbeitsspeichers ändert, wird im Bericht eine neue Zeile zusammen mit der alten Zeile angezeigt. Für die alte Zeile werden keine Aktualisierungen mehr abgerufen, dafür wird aber mit dem Abrufen von Aktualisierungen für die neue Zeile begonnen, als ob es sich um einen neu hinzugefügten Host handelte.
- Auf den Registerkarten **Zusammenfassung** und **Detail** geben die Summen, die in den Spalten für „Gleichzeitig ausgeführte Windows-Server“ und „Verwaltete Windows-Server“ aufgeführt werden, eine Summe aller oberen Grenzen für alle unten aufgeführten Hosts an. Hierzu gehören Windows-Server, die keine Hypervisor-Hosts sind und auf denen keine virtuellen Computer ausgeführt werden, sowie Server, auf denen virtuelle Computer ausgeführt werden, die aber "unbekannt" sind, da keine Daten aus dem virtuellen Computer von SIL über HTTPS empfangen werden. Diese werden aus Gründen der Bequemlichkeit summiert.
- Im Abschnitt **SQL Server** der Registerkarte **Dashboard** ist die Summe der SQL Server-Installationen eine Zusammenfassung aller Editionssummen im Dashboard. Dies kann zu einer Diskrepanz mit der auf der Registerkarte **SQL-Detail** angezeigten Summe führen, wenn mehrere Editionen von SQL auf einem einzelnen Server installiert sind. Im Dashboard würden diese auf jedem Server getrennt gezählt, was auf der Registerkarte **Detail** nicht der Fall wäre. Mehrere SQL-Editionen, die auf einem Windows-Server installiert sind, werden gemäß den Lizenzbestimmungen immer als eine gezählt.
- Im Abschnitt **Windows Server** der Registerkarte **Dashboard** umfassen die Zeilen für **Weitere Hypervisor-Hosts** und **Hypervisor-Hosts gesamt** physische Windows Server-Hosts, auf denen Hyper-V eventuell ausgeführt oder auch NICHT wird.

Spaltenbeschreibungen

Im Folgenden finden Sie Beschreibungen der einzelnen Spalten auf der Registerkarte **Windows Server-Detail** des Excel-basierten Berichts, der vom SIL-Aggregator erstellt wird. Weitere Datenregisterkarten sind entweder mit diesen Spalten identisch oder eine Teilmenge davon. Die einzige Ausnahme wäre die "Installations Anzahl" auf den SQL Server Registerkarten (siehe obere **Grenze**).

SPALTENÜBERSCHRIFT	BESCHREIBUNG
Calendar Month (Kalendermonat)	Daten in Berichten werden nach Monat gruppiert, der jüngste zuerst. Daten innerhalb des Monats werden in keiner bestimmten Reihenfolge aufgeführt.

SPALTENÜBERSCHRIFT	BESCHREIBUNG
Hostname	<p>Netzwerkname oder FQDN des physischen Hosts, der vom SIL-Aggregator erfolgreich abgerufen wird.</p> <p>Verwenden Sie das Cmdlet „Get-SilVMHost“, um Hosts zu suchen, die hinzugefügt wurden, aber nicht oder nicht mehr erfolgreich abgerufen werden. Der letzte erfolgreiche Abruf wird angezeigt.</p>
Hosttyp	Betriebssystemhersteller auf dem physischen Host.
Hypervisor Type (Hypervisor-Typ)	Hypervisor-Hersteller auf dem physischen Host.
Processor Manufacturer (Prozessorhersteller)	Hersteller der Prozessoren auf dem physischen Host.
Processor Model (Prozessormodell)	Modell der Prozessoren auf dem physischen Host.
Is Hyper Threading Enabled? (Ist Hyperthreading aktiviert?)	Wird entweder als „True“ oder „False“ angezeigt, abhängig davon, ob Hyperthreading auf den Prozessoren des physischen Hosts aktiviert ist.
VM-Name	Der Netzwerkname oder FQDN des virtuellen Windows Server-Computers. Wenn der Aggregator keine Daten von diesem Computer über HTTPS erhalten hat, wird der Anzeigename des virtuellen Computers im Hypervisor aufgeführt.
Simultaneously Running Windows Server VMs by host (Gleichzeitig ausgeführte virtuelle Windows Server-Computer nach Host)	<p>Anzahl der gleichzeitig ausgeführten virtuellen Windows Server-Computer auf dem Host. Die höchste Zahl im Monat für diesen Host ist die obere Grenze, die zu diesem Zeitpunkt erfasst und aufgeführt wird.</p> <p>Siehe im Abschnitt Obere Grenze in dieser Dokumentation.</p> <p>Physische Hosts mit installiertem Windows Server oder mit installiertem Windows Server und ohne bekannte, ausgeführte virtuelle Windows Server-Computer werden immer als eins gezählt. Wenn mindestens ein bekannter, virtueller Windows Server-Computer auf dem Host und Windows Server auf dem Host selbst ausgeführt wird, ist das Hostbetriebssystem in der Zählung nicht enthalten.</p>
Physical Processor Count (Anzahl physische Prozessoren)	Die Anzahl der physischen Prozessoren, die auf dem physischen Host installiert sind.
Physical Core Count (Anzahl physische Kerne)	Die Anzahl der physischen Prozessorkerne, die auf dem physischen Host installiert sind.
Virtual Processor Count (Anzahl virtuelle Prozessoren)	Die Anzahl virtueller Prozessoren, die Windows innerhalb des virtuellen Computers erkennt. Dieser Wert stammt nur aus Daten, die über HTTPS mithilfe von SIL in einem Windows Server weitergeleitet wurden.

SPALTENÜBERSCHRIFT	BESCHREIBUNG
Datum/Uhrzeit des Abrufs	<p>Datum und Uhrzeit des letzten oberen Grenzwertpunkts der virtuellen Windows Server-Computer, die gleichzeitig auf diesem physischen Host ausgeführt werden.</p> <p>Siehe im Abschnitt Datum/Uhrzeit des Abrufs in dieser Dokumentation.</p>
VM Last Seen Date Time (Datum/Uhrzeit der letzten Anzeige des virtuellen Computers)	<p>Datum und Uhrzeit, zu dem der Aggregator zuletzt Inventardaten über HTTPS von diesem virtuellen Windows Server-Computer erhalten hat.</p>
Host Last Seen Date Time (Datum/Uhrzeit der letzten Anzeige des Hosts)	<p>Datum und Uhrzeit, zu dem der Aggregator zuletzt Inventardaten über HTTPS von diesem physischen Windows Server-Host erhalten hat.</p> <p>Hierbei wird das Vorhandensein physischer Hosts, auf denen Windows Server und Hyper-V ausgeführt wird, unterstützt, um SIL zu aktivieren und Inventardaten über HTTPS an einen SIL-Aggregator weiterzuleiten.</p>

Details zu SIL-Aggregator-Cmdlets

Im Folgenden finden Sie Detailinformationen zu den Cmdlets des SIL-Aggregators. Die vollständigen Cmdlet-Dokumentation finden Sie unter: [PowerShell-Cmdlets des SIL-Aggregators](#)

Publish-SilReport

- Mit diesem Cmdlet, das unverändert verwendet wird, wird ein Bericht zur Protokollierung des Software Bestands erstellt und im Verzeichnis "Dokumente" des angemeldeten Benutzers abgelegt (auf dem Computer, auf dem das Cmdlet ausgeführt wird, ist Excel 2013 erforderlich).
- Bei Verwendung mit dem `-OpenReport` -Parameter erstellt es den Bericht und öffnet ihn zur Anzeige in Excel.
- Beachten Sie bei der Installation des SIL-Aggregators, dass es eine Option gibt, um nur das Berichtmodul zu installieren. Es ist möglich, das Berichtmodul auf einem Windows-Clientbetriebssystem wie Windows 8.1 oder Windows 10 zu installieren. Dies ermöglicht einem Thin Client, z. B. einem Laptop oder Tablet, das Herstellen einer Verbindung mit einem SIL-Aggregator-Datenbankserver, um SIL-Berichte direkt zu veröffentlichen.
 - Im folgenden Beispiel wird zur Eingabe der zu verwendenden Anmeldeinformationen aufgefordert, eine Verbindung mit einem SIL-Aggregator-Datenbankserver namens „SILContoso“ hergestellt und ein SIL-Bericht auf dem lokalen Computer erstellt und geöffnet.

```
Publish-SilReport -DBServerName "SILContoso" -DBServerCredential Get-Credential -OpenReport
```

- Vor dem ersten Herstellen einer Verbindung müssen Sie in den meisten Fällen einen Port in der Firewall auf dem SIL-Aggregator-Datenbankserver öffnen, um Verbindungen zuzulassen. IT-Experten können dies im Voraus einrichten, um Ihren Finanz-Controllern oder anderen Inventar-Managern den Zugriff zu gewähren, damit sie eigene Berichte erstellen können. Die hierfür notwendigen Schritte finden Sie unter dem unten stehenden Link. Ein typischer Standardport für SQL Server Analysis Services ist 2383.

Add-SilVMHost

Die folgenden Hosttypen und Hypervisor-Versionen werden unterstützt, wenn das `Add-SilVMHost` -Cmdlet

verwendet wird. Beachten Sie, dass es nicht erforderlich ist, diese anzugeben. Das `Add-SilVMHost` -Cmdlet erkennt eine unterstützte Kombination automatisch. Wenn es eine solche nicht erkennen kann, oder wenn die angegebenen Anmeldeinformationen falsch sind, wird eine Eingabeaufforderung angezeigt. Wenn der Benutzer mit einem "Y"-Eintrag akzeptiert, wird der Host hinzugefügt, aber nicht abgerufen. Er wird als "unbekannt" hinzugefügt.

HYPERVERISOR-VERSION	SIL-AGGREGATOR HOSTTYPE-WERT	SIL-AGGREGATOR HYPERVISORTYPE-WERT
Windows Server 2012 R2	Windows	Hyper-v
VMware 5.5	VMware	Esxi
Xen 4.x	Ubuntu, OpenSuse oder CentOS	Xen
XenServer 6.2	Citrix	XenServer
KVM	Ubuntu, OpenSuse oder CentOS	KVM

Andere Versionen und Typen dieser Hypervisor-Plattformen können möglicherweise ebenfalls funktionieren. Im Lieferumfang des SIL-Aggregators ist die unten aufgeführte sshnet-Version enthalten. Diese wird für die Kommunikation mit Linux-basierten Virtualisierungsplattformen verwendet.

```
sshnet 2014.4.6-beta1
https://sshnet.codeplex.com/releases/view/120504
Copyright (c) 2010, RENCI
```

Get-SilAggregator

`Get-SilAggregator` stellt Konfigurationsinformationen für Ihre Aggregatoranwendung der Protokollierung des Softwarebestands bereit. Die folgende Beispieldausgabe zeigt an:

- Anwendung wird ausgeführt.
- Abrufintervall ist stündlich (kann in Stundeninkrementen geändert werden).
- Startzeit des Abrufs
- Ziel-URI, den andere Computer für das Weiterleiten von Daten an diesen Aggregator festlegen sollten.
- Zertifikatfingerabdrücke, von denen dieser Aggregator SIL-Daten akzeptiert.
- Bei der Installation angegebener Kontotyp

```
PS C:\Windows\system32> Get-SilAggregator
```

```
``
```

```
State : Running HostPollIntervalInHours : Every 1 Hour(s)
```

```
PollStartTime : 8/24/2015 5:07:33 AM
```

```
TargetURI : https://SilContoso
```

```
CertificateThumbprint : 3efc6b8ce7d5eefba5107ede9d1caca550417452,
2dc4ea8fb64b1246a8c1ffa1b701cd1042a3412
```

```
UserProfile : Local
```

Set-SilAggregator

Mit dem `Set-SilAggregator` Cmdlet können Sie Folgendes:

- Ändern des stündlichen Intervalls, in dem der Abruf erfolgt.
- Ändern von Startdatum und Startzeit für den Beginn des Abrufs zum angegebenen Intervall.
- Hinzufügen oder Entfernen von Zertifikatfingerabdrücken, von denen der SIL-Aggregator Daten akzeptiert bzw. denen er Daten zuordnet.

Get-AggregatorData

- Bei Verwendung ohne Parameter zeigt dieses Cmdlet den Inhalt der Registerkarte „Windows Server-Detail“ eines SIL-Aggregator-Excel-Berichts an.
- Wenn dieses Cmdlet mit Parametern verwendet wird, ruft es Daten direkt aus der Datenbank ab, die der Unterstützung bei benutzerdefinierten Verwendungen der SIL-Gesamtlösung dienen sollen.
- Beachten Sie, dass die Parameter `-StartTime` und `-Endtime` Berichtsdaten aus dem ersten des Monats des Startdatums und dem letzten des Monats des Enddatums anzeigen.

```
PS C:\Windows\system32> get-silaggregatordata -computername silatest02.redmond.corp.microsoft.com

ID : f0e29c1c-f660-4731-aad3-3f66b2e52f77
UUID : 8e53d731-4e5f-4ad2-9fd8-e632a2b07467
VMID : 9279dc5-cede-420d-b299-ef5e646c0585
Model : Virtual Machine
VMHostName : bfbluehost4
VMHostOS : Windows
VMName : SILATEST02
VMOS : Microsoft Windows Server 2012 R2 Datacenter
Software : Configuration Manager Client, HelpDesk, Microsoft .NET Framework 4 Multi-Targeting Pack, Microsoft Access MUI (English) 2013, Microsoft Access Setup Metadata MUI (English) 2013, Microsoft Application Error Reporting, Microsoft DCF MUI (English) 2013, Microsoft Endpoint Protection Management Components, Microsoft Excel MUI (English) 2013, Microsoft Forefront Endpoint Protection 2010 Server Management, Microsoft Groove MUI (English) 2013, Microsoft Help Viewer 1.1, Microsoft InfoPath MUI (English) 2013, Microsoft Lync MUI (English) 2013, Microsoft ODBC Driver 11 for SQL Server, Microsoft Office 64-bit Components 2013, Microsoft Office Live Meeting 2007, Microsoft Office OSM MUI (English) 2013, Microsoft Office Proofing (English) 2013, Microsoft Office Proofing Tools 2013 - English, Microsoft Office Proofing Tools 2013 - Español, Microsoft Office Shared 64-bit MUI (English) 2013, Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2013, Microsoft Office Shared MUI (English) 2013, Microsoft Office Shared Setup Metadata MUI (English) 2013, Microsoft OneNote MUI (English) 2013, Microsoft Outlook MUI (English) 2013, Microsoft Policy Platform, Microsoft Power Query for Excel, Microsoft PowerPoint MUI (English) 2013, Microsoft Publisher MUI (English) 2013, Microsoft Report Viewer 2014 Runtime, Microsoft Security Client, Microsoft Silverlight, Microsoft SQL Server 2008 R2 Management Objects, Microsoft SQL Server 2008 Setup Support Files, Microsoft SQL Server 2012 Native Client, Microsoft SQL Server 2014 Policies, Microsoft SQL Server 2014 Transact-SQL Driver, Microsoft SQL Server 2014 Setup (English), Microsoft SQL Server 2014 Transact-SQL Compiler Service, Microsoft SQL Server 2014 Transact-SQL ScriptDom, Microsoft SQL Server System CLR Types, Microsoft System CLR Types for SQL Server 2014, Microsoft Visual C++ 2005 Redistributable (x64), Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148, Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148, Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161, Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219, Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219, Microsoft Visual C++ 2010 x86 Runtime 10.0.40219, Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005, Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005, Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005, Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005, Microsoft Visual Studio 2010 Shell (Isolated) - ENU, Microsoft Visual Studio 2010 Tools for Office Runtime (x64), Microsoft Visual Studio Tools for Applications x64 Runtime 3.0, Microsoft Visual Studio Tools for Applications x86 Runtime 3.0, Microsoft VSS Writer for SQL Server 2014, Microsoft Word MUI (English) 2013, Outils de vérification linguistique 2013 de Microsoft Office-Français, Software Inventory Logging Aggregator, SQL Server 2014 Analysis Services, SQL Server 2014 Client Tools, SQL Server 2014 Common Files, SQL Server 2014 Data quality client, SQL Server 2014 Data quality service, SQL Server 2014 Database Engine Services, SQL Server 2014 Database Engine Shared, SQL Server 2014 Distributed Replay, SQL Server 2014 Documentation Components, SQL Server 2014 Enterprise Edition: Core-based Licensing, SQL Server 2014 Full text search, SQL Server 2014 Integration Services, SQL Server 2014 Management Studio, SQL Server 2014 Master Data Services, SQL Server 2014 Reporting Services, SQL Server 2014 RS_SharePoint_SharedService, SQL Server 2014 SQL Data Quality Common, SQL Server Browser for SQL Server 2014, Sql Server Customer Experience Improvement Program, Visual Studio 2010 Prerequisites - English, VMware Remote Console Plug-in 5.1, VMware VIX, VMware vSphere PowerCLI, Windows Firewall Configuration Provider
ProcessorFamily : 179
ProcessorManufacturer : GenuineIntel
ProcessorName : Intel(R) Xeon(R) CPU E5440 @ 2.83GHz
SystemManufacturer : Microsoft Corporation
ChassisSerialNumber : 1623-2031-5100-3L22-1247-0766-27
NumberOfProcessors : 1
NumberOfCores : 1
LastSeenDateTime : 9/10/2015 4:06:56 AM
```

Get-SilVMHost

- Dieses Cmdlet gibt die Liste der physischen Hosts aus, für deren Abruf der SIL-Aggregator konfiguriert ist, Datum und Uhrzeit des jüngsten erfolgreichen Abrufs sowie den „`HostType`“ (oder BS-Hersteller) und den „`HypervisorType`“ (Hypervisor-Hersteller). Weitere Informationen zu „`HostType`“ und „`HypervisorType`“ finden Sie in den Details zu „`Add-SilVMHost`“.

Wenn ein Host weder Abfragedatum noch -uhrzeit, aber einen unterstützten „`HostType`“ und „`HypervisorType`“ besitzt, bedeutet dies, dass der Abruf noch nicht begonnen hat oder noch nicht erfolgreich war.

- Dieses Cmdlet listet außerdem alle Hostnamen auf, die mittels der Daten, die von virtuellen Computern

selbst stammen (falls sie von dem virtuellen Computer verfügbar waren), hinzugefügt wurden. Diese werden zwar in der Liste angezeigt, besitzen aber weder „HostType“ noch „HypervisorType“. Diese Daten können bei der Zuordnung von virtuellen Computern und Hosts helfen, die möglicherweise nicht für den Abruf eingerichtet sind.

- Mithilfe der Parameter `-StartTime` und `-EndTime` können Ihnen dabei helfen zu verstehen, wann Hosts zum ersten Mal hinzugefügt oder zuletzt abgerufen wurden.

Remove-SilVMHost

- Dieses Cmdlet entfernt jeden Host aus der Liste der abzufragenden Hosts. Wenn ein Host entfernt wird, ist es möglich, dass ein virtueller Computer auf dem Host den Host der Liste erneut hinzufügt, wobei der Host aber nicht mit den richtigen Anmeldeinformationen abgerufen wird, die mithilfe des `Add-SilVMHost` - Cmdlets angegeben werden.
- Wenn ein Host entfernt wird, wird er nicht mehr abgefragt, aber nicht aus Berichten entfernt. Da das Abrufen eingestellt wird, ist der Host in Berichten der folgenden Monate nicht mehr vorhanden.
- Verwenden Sie die Parameter `-StartTime` und `-EndTime` einzeln, um beim Entfernen von Gruppen von Hosts zu helfen, die bis zu einem oder ab einem bestimmten Datum erfolgreich abgerufen wurden.

Vermeiden dieser Fehler und Probleme mit SIL und SIL Aggregator (Handbuch zur Problembehandlung)

- Zu überprüfende Dinge, wenn eins der Cmdlets `SilLogging` und `Publish-SilData` fehlschlägt:
 - Stellen Sie sicher, dass der `targetUri` den Wert `https://` im Eintrag enthält.
 - Stellen Sie sicher, dass alle erforderlichen Updates für Windows Server installiert sind (siehe „Voraussetzungen für SIL“). Eine schnelle Möglichkeit zum Überprüfen besteht darin, diese mithilfe des folgenden Cmdlets zu suchen: `Get-SilWindowsUpdate *3060*, *3000*`
 - Stellen Sie sicher, dass das zur Authentifizierung bei dem Aggregator verwendete Zertifikat im richtigen Speicher auf dem lokalen Server installiert ist, der mithilfe von „SilLogging“ inventarisiert werden soll (siehe im Abschnitt „Erste Schritte“).
 - Stellen Sie auf dem SIL-Aggregator sicher, dass der Zertifikatfingerabdruck des für die Authentifizierung bei dem Aggregator verwendeten Zertifikats der Liste mithilfe des Cmdlets `Set-SilAggregator -AddCertificateThumbprint` hinzugefügt wurde (siehe im Abschnitt „Erste Schritte“).
 - Bei Verwendung von Enterprise-Zertifikaten überprüfen Sie, ob der Server mit aktiver SIL der Domäne beigetreten ist, für die das Zertifikat erstellt wurde, bzw. anderweitig bei einer Stammzertifizierungsstelle überprüfbar ist. Wenn ein Zertifikat auf dem lokalen Computer, der versucht, Daten an den Aggregator weiterzuleiten oder per Push zu übertragen, nicht vertrauenswürdig ist, schlägt diese Aktion mit einem Fehler fehl.
 - Wenn alle oben genannten Punkte überprüft wurden, können Sie überprüfen, ob das zur Installation des SIL-Aggregators verwendete Zertifikat fehlerfrei ist und mit dem Namen des SIL-Aggregatorservers selbst übereinstimmt (dieser Schritt ist nicht erforderlich, wenn andere Computer erfolgreich an denselben SIL-Aggregator weiterleiten).
 - Sie können den folgenden Speicherort auf zwischengespeicherte SIL-Dateien auf dem Server überprüfen, der den Forward/Push-Vorgang versucht, `\Windows\System32\Logfiles\SIL`. Wenn `SilLogging` gestartet wurde und schon länger als eine Stunde ausgeführt wird, oder wenn `Publish-SilData` vor Kurzem ausgeführt wurde und keine Dateien in diesem Verzeichnis vorhanden sind, dann war die Protokollierung auf dem Aggregator erfolgreich.

- Vergewissern Sie sich, dass der angemeldete Benutzer über Zugriff auf die SQL-Datenbank und die Analysis Services verfügt.
 - Dies ist erforderlich für die Installation des SIL-Aggregators.
 - Dies ist erforderlich, wenn Sie PowerShell Remote zum Verwalten des SIL-Aggregators verwenden.
- Beim Veröffentlichen von SIL-Aggregatorberichten von einem Clientdesktop-Betriebssystem aus:
 - Verwenden Sie die Option, mit der nur das Berichtmodul installiert wird, auf Ihrem Windows-Client (8.1/10).
 - Wenn bei dem Versuch, einen Bericht mithilfe von PowerShell remote zu erstellen, Probleme auftreten, müssen Sie wahrscheinlich einen Firewallport auf dem SIL-Aggregator öffnen lassen, mit dem Sie eine Verbindung herstellen möchten (siehe im Abschnitt „Details zu SIL-Aggregator-Cmdlets“ unter dem Cmdlet `Publish-SilReport`).
- Bei Verwendung der gMSA-Option:
 - Vergessen Sie nicht, den Server neu zu starten, nachdem Sie ihn mit der GMSA-fähigen Computergruppe in Active Directory hinzufügen.
 - Verwenden Sie bei der Installation bei der Eingabe von Domäne \ Benutzer nicht die voll qualifizierte Domäne. Verwenden Sie z. b. `meineDomäne \ gmsaaccount`. Geben Sie `mydomain nicht ein. com\gmsaaccount`.
- Bei Verwendung von Windows Management Framework in Ihrer Umgebung:
 - Stellen Sie sicher, dass auf den Servern, auf denen Sila installiert ist, WMF 5,1 nicht installiert ist. Es ist möglich, einen Fehler im Ereignisprotokoll bezüglich der DLL "mpunits. dll" zu finden. Dadurch wird der ordnungsgemäße Betrieb verhindert. Sila erfordert nur WMF 4,0.

Verwalten von SIL im zeitlichen Verlauf

Deinstallieren/Neuinstallieren des SIL-Aggregators

Falls es erforderlich werden sollte, den SIL-Aggregator zu deinstallieren und neu zu installieren, können Sie dies durchführen, ohne dabei vorhandene oder historische Inventardaten zu verlieren. Führen Sie einfach eine Deinstallation durch (befolgen Sie die Schritte in dieser Dokumentation), und aktivieren Sie die Option zum Beibehalten der Datenbank der Protokollierung des Softwarebestands. Installieren Sie dann den SIL-Aggregator neu (befolgen Sie die Schritte in dieser Dokumentation), und aktivieren Sie die Option zum Anfügen an eine vorhandene Datenbank.

Nach dem Ausführen dieses Vorgangs ist es notwendig, die Anmeldeinformationen mithilfe des Cmdlets `Add-SilVMHost` auf allen Hosts zu aktualisieren, die zuvor vom SIL-Aggregator abgerufen wurden (vorausgesetzt, dass es gewünscht ist, das Sammeln von Daten von diesen Hosts fortzusetzen). Darüber hinaus ist es zur Vermeidung doppelter Einträge für denselben Host in Berichten notwendig, Hosts für den Abruf unter Verwendung derselben Netzwerkadresse, mit der sie ursprünglich hinzugefügt wurden, erneut hinzuzufügen. Im Folgenden finden Sie die drei unterstützten „vmhostname“-Typen, die zum Hinzufügen eines Hosts mithilfe des Cmdlets `Add-SilVMHost` verwendet werden können:

- IP-Adresse
- Vollqualifizierter Domänenname (FQDN)
- NetBIOS-Name

Ändern des SIL-Aggregators

Wenn Sie die Inventarisierung von Servern in Ihrer Umgebung mit einem anderen SIL-Aggregator starten

möchten, verwenden Sie einfach das SIL-Cmdlet auf diesen Servern, um den „targeturi“ (und ggf. den Zertifikatfingerabdruck) zu ändern, `Set-SilLogging -TargetUri`. Beachten Sie, dass es nach der Durchführung dieses Vorgangs notwendig ist, das Cmdlet `Publish-SilData` mindestens einmal zu verwenden, um ein vollständiges Inventar an den neu angegebenen SIL-Aggregator weiterzuleiten.

Ändern oder Aktualisieren von Zertifikaten

WICHTIGE SCHRITTE ZUR VERMEIDUNG VON DATENVERLUSTEN: Wenn es erforderlich ist, das Zertifikat zu ändern, das Server zum Weiterleiten von Daten an einen SIL-Aggregator verwenden, der Zielaggregator bleibt aber derselbe, gehen Sie folgendermaßen vor, um während des Übergangs zu dem Aggregator potenzielle Datenverluste zu vermeiden:

- Verwenden Sie auf dem SIL-Aggregator das Cmdlet `Set-SilAggregator -AddCertificateThumbprint`, um dem SIL-Aggregator die neuen Fingerabdrücke hinzuzufügen.
- Installieren Sie auf ALLEN Servern, die Daten weiterleiten, das neue, zu verwendende Zertifikat mit Ihrer bevorzugten Methode in `\LOCALMACHINE\MY`.
- Verwenden Sie auf allen Servern, die Daten weiterleiten, das Cmdlet
`Set-SilLogging -CertificateThumbprint`, um auf den Fingerabdruck des neuen Zertifikats zu aktualisieren.
- **KRITISCH: Erst nachdem alle Server, die Daten weiterleiten, aktualisiert wurden, entfernen Sie den alten Fingerabdruck** von dem SIL-Aggregator mithilfe des Cmdlets
`Set-SilAggregator -RemoveCertificateThumbprint`. Wenn ein Server, der Daten weiterleitet, die Weiterleitung unter Verwendung eines alten Zertifikats fortsetzt, das vom SIL-Aggregator entfernt wurde, gehen Daten verloren und werden nicht in die Datenbank auf dem Aggregator eingefügt. Dies wirkt sich nur auf Szenarien aus, in denen ein Server zuvor Daten erfolgreich an einen SIL-Aggregator weitergeleitet hat und das Zertifikat dann aus der Liste der Fingerabdrücke des SIL-Aggregators entfernt wird, um Daten von zu akzeptieren.

Anmerkungen zu dieser Version

- Es gibt das bekannte Problem, dass der SIL-Aggregator bei Vorhandensein von Installationen der SQL Server Standard Edition keine Verarbeitungen durchführt oder Berichte erstellt. Dieser Fehler lässt sich mit folgenden Schritten beheben:
 1. Öffnen Sie SQL Server Management Studio auf Ihrem SIL-Aggregator.
 2. Stellen Sie eine Verbindung mit dem Datenbankmodul her.
 3. Erweitern Sie in der Auswahlstruktur die Datenbank „SoftwareInventoryLogging“ und dann „Tabellen“.
 4. Rechts klicken Sie auf `dbo. Sqlserveredition`, und wählen Sie dann "Top 200 Rows bearbeiten" aus.
 5. Ändern Sie den PropertyNumValue-Wert neben "Standard Edition" in **2760240536** (von- 1534726760).
 6. Schließen Sie die Abfrage, um die Änderung zu speichern.
 7. Für Server mit SIL, die bereits Daten in diesem Aggregator protokolliert haben, muss möglicherweise das Cmdlet `Publish-SilData` einmal ausgeführt werden, damit der Aggregator das Vorhandensein der SQL Server Standard Edition ordnungsgemäß verarbeitet.
- In SIL-generierten Berichten umfasst jede Prozessorkernanzahl die Anzahl der Threads, wenn Hyperthreading auf dem physischen Server aktiviert ist. Um die tatsächliche Anzahl der physischen Kerne auf Servern mit aktiviertem Hyperthreading zu erhalten, ist es notwendig, diese Zähler um die Hälfte zu

verringern.

- Gesamtwerte in den Zeilen (auf der Registerkarte **Dashboard**) und Spalten (auf der Registerkarte **Zusammenfassung und Detail**) mit der Bezeichnung "gleichzeitig ausgeführt..." für Windows Server und System Center Stimmen zwischen den beiden Standorten nicht genau überein. Auf der Registerkarte **Dashboard** ist es erforderlich, den Wert "**Windows Server-Geräte (ohne bekannte VMS)**" dem Wert "gleichzeitig ausgeführt..." hinzuzufügen. Wert, der dieser Zahl auf den Registerkarten **Zusammenfassung und Detail** entspricht.
- Siehe **WICHTIGE SCHRITTE ZUR VERMEIDUNG VON DATENVERLUSTEN** , wenn Sie Zertifikate unter dem Abschnitt **Verwalten von SIL im zeitlichen Verlauf** dieser Dokumentation ändern oder aktualisieren.
- Es ist zwar möglich, Windows Server 2008 R2- und Windows Server 2012-Hosts der Liste der abzurufenden Hosts hinzuzufügen, doch diese Version (1.0) von SIL-Aggregator unterstützt nur den Abruf von Windows Server 2012 R2-Hosts für Windows-/Hyper-V-basierte Hosts, damit alle Features und Funktionen erfolgreich ausgeführt werden. Insbesondere ist bekannt, dass virtuelle Computer und Hosts beim Abrufen von Windows Server 2008 R2-Hosts in den Berichten des SIL-Aggregators möglicherweise nicht zugeordnet werden können.

Weitere Informationen

[Aggregator der Protokollierung des Software Bestands 1,0 für Windows Server](#)

[PowerShell-Cmdlets des SIL-Aggregators](#)

[SIL-PowerShell-Cmdlets](#)

[Eine Übersicht über SIL](#)

[Verwalten von SIL](#)

Einstieg in die Benutzer Zugriffs Protokollierung

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

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Die Benutzer Zugriffs Protokollierung (User Access Logging, UAL) ist eine Funktion in Windows Server, die Client Verwendungs Daten nach Rolle und Produkten auf einem lokalen Server aggregiert. Dadurch können Windows Server-Administratoren Anforderungen von Client Computern nach Rollen und Diensten auf einem lokalen Server quantifizieren.

Die Benutzer Zugriffs Protokollierung ist standardmäßig installiert und aktiviert und erfasst Daten nahezu in Echtzeit. Es ist keine Konfiguration durch den Administrator erforderlich, wenngleich die Benutzerzugriffsprotokollierung deaktiviert oder aktiviert werden kann. Weitere Informationen finden Sie unter [Verwalten der Benutzerzugriffsprotokollierung](#). Der Dienst für die Benutzer Zugriffs Protokollierung aggregiert Client Verwendungs Daten nach Rollen und Produkten in lokalen Datenbankdateien. IT-Administratoren können später Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) oder Windows PowerShell-Cmdlets verwenden, um Mengen und Instanzen nach Serverrolle (oder Softwareprodukt), Benutzer, Gerät, lokalem Server und Datum abzurufen.

NOTE

Die UAL unterstützt das [Microsoft Assessment and Planning Toolkit](#).

Praktische Anwendungen

Die Benutzer Zugriffs Protokollierung aggregiert eindeutige Client Geräte-und Benutzer Anforderungs Ereignisse, die in einer lokalen Datenbank protokolliert werden. Diese Datensätze werden dann (über die Abfrage eines Serveradministrators) zur Verfügung gestellt, um Mengen und Instanzen nach Serverrolle, Benutzer, Gerät, lokalem Server und Datum abzurufen. Außerdem wurde die Benutzer Zugriffs Protokollierung erweitert, damit nicht-Microsoft-Softwareentwickler ihre UAL-Ereignisse so instrumentieren, dass Sie von Windows Server aggregiert werden.

Die Benutzer Zugriffs Protokollierung kann die folgenden Aufgaben ausführen:

- Berechnen der Clientbenutzeranforderungen für lokale physische oder virtuelle Server.
- Berechnen der Clientbenutzeranforderungen für installierte Softwareprodukte auf einem lokalen physischen oder virtuellen Server.
- Abrufen von Daten auf einem lokalen Server, auf dem Hyper-V ausgeführt wird, um Phasen mit hoher und niedriger Nachfrage auf dem Hyper-V-Computer zu ermitteln.
- Abrufen von Daten der Benutzerzugriffsprotokollierung von mehreren Remoteservern.

Außerdem können Softwareentwickler Ereignisse der Benutzer Zugriffs Protokollierung instrumentieren, die dann mithilfe von WMI-und Windows PowerShell-Schnittstellen aggregiert und abgerufen werden können.

Die folgenden Serverrollen und Dienste können von der Benutzerzugriffsprotokollierung unterstützt werden:

- Active Directory-Zertifikatdienste (AD CS)

- Active Directory-Rechteverwaltungsdienste (AD RMS)
- BranchCache
- Domain Name System (DNS)

NOTE

Die UAL sammelt DNS-Daten alle 24 Stunden, und es gibt ein separates UAL-Cmdlet für dieses Szenario.

- Dynamic Host Configuration-Protokoll (DHCP)
- Faxserver
- Dateidienste
- File Transfer Protocol-Server (FTP)
- Hyper-V

NOTE

Die UAL sammelt Hyper-V-Daten alle 24 Stunden, und es gibt ein separates UAL-Cmdlet für dieses Szenario.

- Web Server (IIS)

WARNING

Um die UAL mit IIS zu verwenden, müssen Sie "iisual.exe" verwenden. Weitere Informationen finden Sie unter [Analysieren von Clientverwendungsdaten mit der IIS-Benutzerzugriffsprotokollierung](#).

- Microsoft Message Queuing-Dienste (MSMQ)
- Netzwerkrichtlinie und Access Services
- Druck- und Dokumentdienste
- Routing- und RAS-Dienst (RRAS)
- Windows-Bereitstellungsdienste (Windows Deployment Services, WDS)
- Windows Server Update Services (WSUS)

IMPORTANT

Für direkt mit dem Internet verbundene Server (z. B. Webserver in einem Adressraum, der über das Internet zugänglich ist) oder Szenarien, in denen eine extrem hohe Leistung die primäre Funktion des Servers ist (z. B. in Umgebungen mit High Performance Computing-Auslastung), wird die Verwendung der Benutzerzugriffsprotokollierung nicht empfohlen. Die Benutzer Zugriffs Protokollierung ist in erster Linie für Intranetszenarios in kleinen, mittelgroßen und großen Unternehmen gedacht, bei denen ein hohes Volumen erwartet wird, aber nicht so hoch wie bereit Stellungen, die regelmäßig Internet Datenverkehr verarbeiten.

Wichtige Funktionen

In der folgenden Tabelle werden die Hauptfunktionen der Benutzerzugriffsprotokollierung und ihre mögliche Bedeutung beschrieben.

FUNKTIONALITÄT	WERT
Sammeln und Aggregieren von Client-Anforderungsereignisdaten nahezu in Echtzeit.	Es können bis zu drei Jahre an Daten gespeichert werden. Wichtig: Administratoren müssen die Konformität der gesammelten Daten und der Beibehaltungs Dauer der Daten mit den Datenschutzbestimmungen der Organisation und den lokalen Vorschriften erzwingen.
Zum Abrufen von Client-Anforderungsdaten auf einem lokalen Server oder Remoteserver wird UAL über WMI- oder Windows PowerShell-Schnittstellen abgefragt.	UAL ermöglicht eine einzige Ansicht der fortlaufenden Nutzungsdaten. Server- und Unternehmensadministratoren können diese Daten abrufen und zusammen mit Business Administratoren auswerten, um die Nutzung von Volumenlizenzen für Software zu optimieren.
Standardmäßig aktiviert.	Serveradministratoren müssen diese Funktion nicht konfigurieren oder anderweitig festlegen, damit alle wichtigen Funktionen verfügbar und funktionsfähig sind.

Von der Benutzerzugriffsprotokollierung protokollierte Daten

Die folgenden benutzerspezifischen Daten werden von der Benutzerzugriffsprotokollierung protokolliert.

DATEN	BESCHREIBUNG
UserName	Benutzername des Clients, der die Einträge der Benutzerzugriffsprotokollierung aus installierten Rollen und Produkten ggf. begleitet.
Activitycount	Die Anzahl der Zugriffe auf eine Rolle oder einen Dienst durch einen bestimmten Benutzer.
Firstseen	Datum und Uhrzeit des ersten Zugriffs auf eine Rolle oder einen Dienst durch einen Benutzer.
Lastseen	Datum und Uhrzeit des letzten Zugriffs auf eine Rolle oder einen Dienst durch einen Benutzer.
ProductName	Name des Softwareprodukts (z. B. Windows), das Daten für die Benutzerzugriffsprotokollierung bereitstellt.
Roleguid	Die von der Benutzerzugriffsprotokollierung zugewiesene oder registrierte GUID, die die Serverrolle bzw. das installierte Produkt darstellt.
RoleName	Name der Rolle, der Komponente oder des untergeordneten Produkts, die bzw. das die Daten für die Benutzerzugriffsprotokollierung bereitstellt. Hier besteht außerdem eine Verknüpfung mit %quot;ProductName%quot; und %quot;RoleGUID%quot;.
Tenantidentifier	Eindeutige GUID für den Mandantenclient einer installierten Rolle oder ggf. für ein Produkt, das die Daten der Benutzerzugriffsprotokollierung begleitet.

Die folgenden gerätespezifischen Daten werden von der Benutzerzugriffsprotokollierung protokolliert.

DATEN	BESCHREIBUNG
IPAddress	IP-Adresse eines Clientgeräts, das für den Zugriff auf eine Rolle oder einen Dienst verwendet wird.
Activitycount	Die Anzahl der Zugriffe auf eine Rolle oder einen Dienst durch ein bestimmtes Gerät.
Firstseen	Datum und Uhrzeit der ersten Verwendung einer IP-Adresse für den Zugriff auf eine Rolle oder einen Dienst.
Lastseen	Datum und Uhrzeit der letzten Verwendung einer IP-Adresse für den Zugriff auf eine Rolle oder einen Dienst.
ProductName	Name des Softwareprodukts (z. B. Windows), das Daten für die Benutzerzugriffsprotokollierung bereitstellt.
Roleguid	Die von der Benutzerzugriffsprotokollierung zugewiesene oder registrierte GUID, die die Serverrolle bzw. das installierte Produkt darstellt.
RoleName	Name der Rolle, der Komponente oder des untergeordneten Produkts, die bzw. das die Daten für die Benutzerzugriffsprotokollierung bereitstellt. Hier besteht außerdem eine Verknüpfung mit %quot;ProductName%quot; und %quot;RoleGUID%quot;.
Tenantidentifier	Eindeutige GUID für den Mandantclient einer installierten Rolle oder ggf. für ein Produkt, das die Daten der Benutzerzugriffsprotokollierung begleitet.

Software Anforderungen

Die Benutzer Zugriffs Protokollierung kann auf jedem Computer verwendet werden, auf dem Windows Server-Versionen nach Windows Server 2012 ausgeführt werden.

Siehe auch

[Benutzerzugriffsprotokollierung in MSDN.](#)

[Verwalten der Benutzerzugriffsprotokollierung](#)

Verwalten der Benutzerzugriffsprotokollierung

09.04.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In diesem Dokument wird beschrieben, wie Sie die Benutzerzugriffsprotokollierung verwalten.

Die Benutzerzugriffsprotokollierung ist ein Feature, mit dessen Hilfe Serveradministratoren die Anzahl eindeutiger Clientanforderungen von Rollen und Diensten auf einem lokalen Server messen können.

Die Benutzerzugriffsprotokollierung wird standardmäßig installiert und aktiviert und erfasst Daten nahezu in Echtzeit. Für die Benutzerzugriffsprotokollierung sind nur wenige Konfigurationsoptionen verfügbar. Diese Optionen und ihr Verwendungszweck werden in diesem Dokument beschrieben.

Weitere Informationen zu den Vorteilen der [Benutzer Zugriffs Protokollierung](#) finden Sie unter [Einstieg in die Benutzer Zugriffs Protokollierung](#).

In diesem Dokument

In diesem Dokument werden folgende Konfigurationsoptionen behandelt:

- Deaktivieren und Aktivieren des Diensts für die Benutzerzugriffsprotokollierung
- Sammeln und Entfernen von Daten
- Löschen der von der Benutzerzugriffsprotokollierung protokollierten Daten
- Verwalten der Benutzerzugriffsprotokollierung in Umgebungen mit hohem Aufkommen an Clientanforderungen
- Wiederherstellen nach einer Beschädigung
- Aktivieren der Nachverfolgung der Arbeitsordner-Nutzungslizenz

Deaktivieren und Aktivieren des Dienstes für die Benutzer Zugriffs Protokollierung

Die Benutzer Zugriffs Protokollierung ist standardmäßig aktiviert und wird ausgeführt, wenn ein Computer unter Windows Server 2012 oder höher installiert und zum ersten Mal gestartet wird. Mitunter müssen Administratoren die Benutzerzugriffsprotokollierung deaktivieren, um Datenschutzanforderungen oder andere betriebliche Anforderungen zu erfüllen. Sie können die Benutzer Zugriffs Protokollierung mithilfe der Dienste-Konsole, über die Befehlszeile oder mithilfe von PowerShell-Cmdlets deaktivieren. Um sicherzustellen, dass die Benutzer Zugriffs Protokollierung beim nächsten Start des Computers nicht wieder ausgeführt wird, müssen Sie auch den Dienst deaktivieren. Die folgenden Prozeduren beschreiben, wie Sie die Benutzer Zugriffs Protokollierung deaktivieren und deaktivieren.

NOTE

Sie können das PowerShell-Cmdlet `Get-Service UALSV` verwenden, um Informationen zum Dienst für die Benutzerzugriffsprotokollierung abzurufen, z. B. ob er ausgeführt wird oder beendet wurde und ob er aktiviert oder deaktiviert ist.

So beenden und deaktivieren Sie den Dienst für die Benutzerzugriffsprotokollierung mithilfe der Konsole
%%amp;quot;Dienste%%amp;quot;

1. Melden Sie sich mit einem Konto mit lokalen Administratorrechten am Server an.
2. Zeigen Sie in Server-Manager auf **Tools**, und klicken Sie anschließend auf **Dienste**.
3. Führen Sie einen Bildlauf nach unten durch, und wählen Sie **Dienst für die Benutzerzugriffsprotokollierung** aus. Klicken Sie auf **Dienst beenden**.
4. Klicken Sie mit der rechten-auf den Dienstnamen und dann auf **Eigenschaften**. Ändern Sie auf der Registerkarte **Allgemein** die Einstellung von **Starttyp** in **Deaktiviert**, und klicken Sie dann auf **OK**.

So beenden und deaktivieren Sie die Benutzerzugriffsprotokollierung über die Befehlszeile

1. Melden Sie sich mit einem Konto mit lokalen Administratorrechten am Server an.
2. Drücken Sie die WINDOWS-TASTE+R, und geben Sie dann **cmd** ein, um ein Eingabeaufforderungsfenster zu öffnen.

IMPORTANT

Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.

3. Geben Sie **net stop ualsvc** ein, und drücken Sie dann die EINGABETASTE.
4. Geben Sie **netsh ualsvc set opmode mode=disable** ein, und drücken Sie dann die EINGABETASTE.

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

Sie können die Benutzerzugriffsprotokollierung auch mit den Windows PowerShell-Befehlen %%amp;quot;Stop-service%%amp;quot; und %%amp;quot;Disable-Ual%%amp;quot; beenden und deaktivieren.

```
Stop-service ualsvc
```

```
Disable-ual
```

Wenn Sie zu einem späteren Zeitpunkt einen Neustart durchführen und die Benutzer Zugriffs Protokollierung erneut aktivieren möchten, können Sie dies mit den folgenden Verfahren tun.

So starten und aktivieren Sie den Dienst für die Benutzerzugriffsprotokollierung mithilfe der Konsole
%%amp;quot;Dienste%%amp;quot;

1. Melden Sie sich mit einem Konto mit lokalen Administratorrechten am Server an.
2. Zeigen Sie in Server-Manager auf **Tools**, und klicken Sie anschließend auf **Dienste**.
3. Führen Sie einen Bildlauf nach unten durch, und wählen Sie **Dienst für die Benutzerzugriffsprotokollierung** aus. Klicken Sie auf **Dienst starten**.
4. Klicken Sie mit der rechten Maustaste auf den Namen des Diensts, und wählen Sie **Eigenschaften** aus. Ändern Sie auf der Registerkarte **Allgemein** die Einstellung von **Starttyp** in **Automatisch**, und klicken Sie dann auf **OK**.

So starten und aktivieren Sie die Benutzerzugriffsprotokollierung über die Befehlszeile

1. Melden Sie sich mit den Anmeldeinformationen eines lokalen Administrators am Server an.
2. Drücken Sie die WINDOWS-TASTE+R, und geben Sie dann **cmd** ein, um ein Eingabeaufforderungsfenster

zu öffnen.

IMPORTANT

Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.

3. Geben Sie **net start ualsvc** ein, und drücken Sie dann die EINGABETASTE.

4. Geben Sie **netsh ualsvc set opmode mode=enable** ein, und drücken Sie dann die EINGABETASTE.

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

Sie können die Benutzerzugriffsprotokollierung auch mit den Windows PowerShell-Befehlen `%amp;quot;Start-service%amp;quot;` und `%amp;quot;Enable-Ual%amp;quot;` starten und aktivieren.

```
Enable-ual
```

```
Start-service ualsvc
```

Sammeln von UAL-Daten

Zusätzlich zu den im vorherigen Abschnitt beschriebenen PowerShell-Cmdlets können 12 weitere Cmdlets verwendet werden, um die Daten der Benutzer Zugriffs Protokollierung zu erfassen:

- **Get-UalOverview:** Stellt Details im Zusammenhang mit der Benutzerzugriffsprotokollierung und einen Verlauf der installierten Produkte und Rollen bereit.
- **Get-UalServerUser:** Stellt Daten zu Clientbenutzerzugriffen für den lokalen Server oder Zielserver bereit.
- **Get-UalServerDevice:** Stellt Daten zu Clientgerätezugriffen für den lokalen Server oder Zielserver bereit.
- **Get-UalUserAccess:** Stellt Daten zu Clientbenutzerzugriffen für alle Rollen oder Produkte bereit, die auf dem lokalen Server oder Zielserver installiert sind.
- **Get-UalDeviceAccess:** Stellt Daten zu Clientgerätezugriffen für alle Rollen oder Produkte bereit, die auf dem lokalen Server oder Zielserver installiert sind.
- **Get-UalDailyUserAccess:** Stellt Daten zu Clientbenutzerzugriffen für jeden Tag des Jahrs bereit.
- **Get-UalDailyDeviceAccess:** Stellt Daten zu Clientgerätezugriffen für jeden Tag des Jahrs bereit.
- **Get-UalDailyAccess:** Stellt Daten zu Clientgerätezugriffen und Clientbenutzerzugriffen für jeden Tag des Jahrs bereit.
- **Get-UalHyperV:** Stellt für den lokalen Server oder Zielserver relevante Daten zu virtuellen Computern bereit.
- **Get-UalDns:** Stellt spezifische Daten zum DNS-Client des lokalen DNS-Servers oder DNS-Zielserver bereit.
- **Get-UalSystemId:** Stellt systemspezifische Daten zur eindeutigen Identifizierung des lokalen Servers oder Zielserver bereit.

`Get-UalSystemId` stellt ein eindeutiges Profil eines Servers bereit, mit dem alle anderen Daten dieses Servers

korreliert werden. Wenn ein Server eine Änderung in einer der Parameter von `Get-UalSystemId`, wird ein neues Profil erstellt. `Get-UalOverview` stellt eine Liste der auf dem Server installierten und verwendeten Rollen für den Administrator bereit.

NOTE

Grundlegende Funktionen von Druck- und Dokumentdienste und Datei Diensten werden standardmäßig installiert. Administratoren können daher davon ausgehen, dass für diese Dienste immer Informationen für eine vollständige Installation der Rollen angezeigt werden. Aufgrund der eindeutigen Daten, die die Benutzer Zugriffs Protokollierung für diese Server Rollen sammelt, sind separate UAL-Cmdlets für Hyper-V und DNS enthalten.

Ein typisches Verwendungsszenario der Cmdlets für die Benutzerzugriffsprotokollierung ist das Abfragen der eindeutigen Clientzugriffe in einem bestimmten Datumsbereich. Dies kann auf unterschiedlichste Weise erfolgen. Die folgende Methode wird empfohlen, um eindeutige Geräte Zugriffe über einen Datumsbereich abzufragen.

```
PS C:\Windows\system32>Gwmi -Namespace "root\AccessLogging" -query "SELECT * FROM MsftUal_DeviceAccess WHERE LastSeen >='1/01/2013' and LastSeen <='3/31/2013'"
```

Dieser Befehl gibt eine ausführliche Liste mit den IP-Adressen aller eindeutigen Clientgeräte zurück, die im jeweiligen Datumsbereich Anforderungen an den Server gesendet haben.

"Activitycount" für jeden eindeutigen Client ist auf 65.535 pro Tag beschränkt. Außerdem ist das Aufrufen von WMI über PowerShell nur erforderlich, wenn Sie nach Datum Abfragen. Alle anderen Cmdlet-Parameter für die Benutzer Zugriffs Protokollierung können wie erwartet innerhalb von PS-Abfragen verwendet werden, wie im folgenden Beispiel gezeigt:

```
PS C:\Windows\system32> Get-UalDeviceAccess -IPAddress "10.36.206.112"

ActivityCount      : 1
FirstSeen          : 6/23/2012 5:06:50 AM
IPAddress         : 10.36.206.112
LastSeen           : 6/23/2012 5:06:50 AM
ProductName        : Windows Server 2012 Datacenter
RoleGuid           : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName           : File Server
TenantIdentifier   : 00000000-0000-0000-0000-000000000000
PSComputerName     :
```

Die Benutzer Zugriffs Protokollierung bewahrt den Verlauf von bis zu zwei Jahren auf. Um den Abruf von Daten der Benutzer Zugriffs Protokollierung durch einen Administrator zu ermöglichen, wenn der Dienst ausgeführt wird, erstellt die Benutzer Zugriffs Protokollierung alle 24 Stunden eine Kopie der aktiven Datenbankdatei (*Current.mdb*) für die Verwendung durch den WMI-Anbieter.

Am ersten Tag des Jahres erstellt die Benutzerzugriffsprotokollierung eine neue Datei *GUID.mdb*. Die alte *GUID.mdb* wird als Archiv für die Verwendung durch den Anbieter aufbewahrt. Nach zwei Jahren wird die ursprüngliche Datei *GUID.mdb* überschrieben.

IMPORTANT

Die folgenden Verfahren sollten nur von einem erfahrenen Benutzer ausgeführt werden. Sie werden üblicherweise von Entwicklern verwendet, um ihre eigene Instrumentation der Anwendungsprogrammierschnittstellen für die Benutzerzugriffsprotokollierung zu testen.

So passen Sie das Standardintervall von 24 Stunden an, um Daten für den WMI-Anbieter sichtbar zu machen

1. Melden Sie sich mit einem Konto mit lokalen Administratorrechten am Server an.
2. Drücken Sie die WINDOWS-TASTE+R, und geben Sie dann cmd ein, um ein Eingabeaufforderungsfenster zu öffnen.
3. Fügen Sie den folgenden Registrierungswert hinzu:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WMI\AutoLogger\Sum\PollingInterval (REG_DWORD).

WARNING

Eine fehlerhafte Bearbeitung der Registrierung kann Ihr System schwer beschädigen. Bevor Änderungen an der Registrierung vorgenommen werden, sollten Sie eine Sicherungskopie aller wichtigen Daten auf dem Computer erstellen.

Im folgenden Beispiel wird gezeigt, wie Sie ein Intervall von zwei Minuten hinzufügen (nicht empfohlen als Zustand mit langer Laufzeit): **reg Add**

hkLM\SYSTEM\CurrentControlSet\Control\WMI\Autologger\Sum/v PollingInterval/t reg_DWORD/d 120000/F

Die Zeitwerte werden in Millisekunden angegeben. Der Mindestwert ist 60 Sekunden, der Höchstwert ist sieben Tage, und der Standardwert ist 24 Stunden.

4. Verwenden Sie die Konsole "%quot;Dienste%quot;", um den Dienst für die Benutzerzugriffsprotokollierung zu beenden und neu zu starten.

Löschen der von der Benutzerzugriffsprotokollierung protokollierten Daten

Die Benutzerzugriffsprotokollierung ist keine unternehmenskritische Komponente. Sie ist so konzipiert, dass ihre Auswirkungen auf lokale Systemvorgänge so gering wie möglich sind und gleichzeitig eine hohe Zuverlässigkeit gewahrt wird. Dadurch kann der Administrator die DatenbankDatenbank und die unterstützenden Dateien (jede Datei im Verzeichnis "windows\system32\logfilesum") auch manuell löschen, um betriebliche Anforderungen zu erfüllen.

So löschen Sie von der Benutzerzugriffsprotokollierung protokolierte Daten

1. Beenden Sie den Dienst für die Benutzerzugriffsprotokollierung.
2. Öffnen Sie Windows-Explorer.
3. Wechseln Sie zu \windows\system32\logfiles\sum\ .
4. Löschen Sie alle Dateien im Ordner.

Verwalten der Benutzerzugriffsprotokollierung in Umgebungen mit hohem Aufkommen an Clientanforderungen

In diesem Abschnitt werden die Besonderheiten erläutert, die bei der Verwendung der Benutzerzugriffsprotokollierung auf einem Server mit vielen Clients zu berücksichtigen sind:

Die Benutzerzugriffsprotokollierung kann maximal 65.535 Zugriffe pro Tag aufzeichnen. Die Benutzer Zugriffs Protokollierung wird nicht für Server empfohlen, die direkt mit dem Internet verbunden sind, z. B. Webserver, die direkt mit dem Internet verbunden sind, oder in Szenarios, in denen eine extrem hohe Leistung die primäre Funktion des Servers ist (z. B. in HPC-Arbeits Auslastungs Umgebungen). Die Benutzer Zugriffs Protokollierung ist in erster Linie für Intranetszenarios in kleinen, mittelgroßen und großen Unternehmen gedacht, bei denen ein

hohes Volumen erwartet wird, aber nicht so hoch wie viele bereit Stellungen, die regelmäßig Internet Datenverkehr verarbeiten.

Benutzer Zugriffs Protokollierung im Arbeitsspeicher: da die Benutzer Zugriffs Protokollierung die Extensible Storage Engine (ESE) verwendet, erhöhen sich die Arbeitsspeicher Anforderungen der Benutzer Zugriffs Protokollierung im Laufe der Zeit (oder nach Anzahl von Client Anforderungen) Der Arbeitsspeicher wird jedoch freigegeben, wenn er vom System benötigt wird, um die Auswirkungen auf die Systemleistung zu minimieren.

Benutzer Zugriffs Protokollierung auf Datenträger: die Festplatten Anforderungen der Benutzer Zugriffs Protokollierung lauten ungefähr wie unten dargestellt:

- 0 eindeutige Clientdatensätze: 22 MB
- 50.000 eindeutige Clientdatensätze: 80 MB
- 500.000 eindeutige Clientdatensätze: 384 MB
- 1.000.000 eindeutige Clientdatensätze: 729 MB

Wiederherstellen nach einer Beschädigung

In diesem Abschnitt wird erläutert, wie die Extensible Storage Engine (ESE) auf hoher Ebene verwendet wird und was ein Administrator tun kann, wenn Daten der Benutzer Zugriffs Protokollierung beschädigt oder nicht wiederherstellbar sind.

Die Benutzerzugriffsprotokollierung verwendet die ESE, um die Verwendung von Systemressourcen und ihre Beständigkeit gegenüber Beschädigungen zu optimieren. Weitere Informationen zu den Vorteilen der ESE finden Sie unter [Extensible Storage Engine](#) auf MSDN.

Bei jedem Start des Diensts für die Benutzerzugriffsprotokollierung führt die ESE eine Wiederherstellung aus. Weitere Informationen finden Sie unter [Extensible Storage Engine-Dateien](#) auf MSDN.

Falls bei der Wiederherstellung ein Problem auftritt, führt die ESE eine Wiederherstellung nach Systemabsturz aus. Weitere Informationen finden Sie unter [JetInit-Funktion](#) auf MSDN.

Kann die Benutzerzugriffsprotokollierung danach noch immer nicht mit den vorhandenen ESE-Dateien gestartet werden, werden alle Dateien im Verzeichnis %quot;\Windows\System32\LogFiles\SUM%quot; gelöscht. Nachdem diese Dateien gelöscht wurden, wird der Dienst für die Benutzerzugriffsprotokollierung neu gestartet, und es werden neue Dateien erstellt. Der Dienst für die Benutzerzugriffsprotokollierung wird dann wie auf einem neu installierten Computer fortgesetzt.

IMPORTANT

Die Dateien im Datenbankverzeichnis der Benutzerzugriffsprotokollierung sollten niemals verschoben oder geändert werden. Andernfalls werden die Wiederherstellungsschritte initiiert (einschließlich der in diesem Abschnitt beschriebenen Bereinigungsroutine). Falls Sicherungen des Verzeichnisses \Windows\System32\LogFiles\SUM\ benötigt werden, müssen alle Dateien im Verzeichnis zusammen gesichert werden, damit die Wiederherstellung wie erwartet funktioniert.

Aktivieren der Nachverfolgung der Arbeitsordner-Nutzungslizenz

Arbeitsordnerserver können die Benutzerzugriffsprotokollierung für Clientnutzungsberichte verwenden. Im Gegensatz zur Benutzerzugriffsprotokollierung ist die Arbeitsordnerprotokollierung nicht standardmäßig aktiviert. Sie können sie mit der folgenden Registrierungsschlüsseländerung aktivieren:

```
Reg add HKLM\Software\Microsoft\Windows\CurrentVersion\SyncShareSrv /v EnableWorkFoldersUAL /t REG_DWORD /d 1
```

Nach dem Hinzufügen des Registrierungsschlüssels müssen Sie den SyncShareSvc-Dienst auf dem Server neu starten, um die Protokollierung zu aktivieren.

Nachdem die Protokollierung aktiviert ist, werden immer dann, wenn sich ein Client mit dem Server verbindet, zwei Informationsereignisse auf dem Kanal "Windowsprotokolle\Anwendung" protokolliert. Für Arbeitsordner kann jeder Benutzer ein oder mehrere Clientgeräte verwenden, die sich alle 10 Minuten mit dem Server verbinden und prüfen, ob Updates vorhanden sind. Wenn sich 1.000 Benutzer mit jeweils zwei Geräten mit dem Server verbinden, werden die Anwendungsprotokolle alle 70 Minuten überschrieben, was die Problembehandlung bei nicht zusammenhängenden Problemen erschwert. Um dies zu vermeiden, können Sie den Dienst für die Benutzer Zugriffs Protokollierung temporär deaktivieren oder die Größe des Windows-logs\anwendungskanals des Servers erhöhen.

Siehe auch

- [Einstieg in die Benutzer Zugriffs Protokollierung](#)

Richtlinien zur Optimierung der Leistung für Windows Server 2016

24.04.2020 • 3 minutes to read • [Edit Online](#)

Wenn Sie ein Serversystem in Ihrer Organisation ausführen, werden die geschäftlichen Anforderungen mit Standardservereinstellungen möglicherweise nicht erfüllt. Beispielsweise benötigen Sie vielleicht den niedrigstmöglichen Energieverbrauch, die niedrigstmögliche Latenz oder den maximal möglichen Durchsatz auf Ihrem Server. Dieses Handbuch enthält eine Reihe von Richtlinien, mit denen Sie die Servereinstellungen in Windows Server 2016 optimieren und Leistungs- oder Energieeffizienzsteigerungen erzielen können, insbesondere wenn sich die Art der Auslastung im Laufe der Zeit nur wenig ändert.

Es ist wichtig, dass Sie bei Ihren Optimierungsänderungen die Hardware, die Arbeitsauslastung, den Energiehaushalt und die Leistungsziele Ihres Servers berücksichtigen. In diesem Handbuch werden jede Einstellung und ihre möglichen Auswirkungen beschrieben, damit sie eine fundierte Entscheidung bezüglich ihrer Relevanz für Ihr System, Ihre Arbeitsauslastung, Leistung und Energienutzungsziele treffen können.

WARNING

Registrierungseinstellungen und Optimierungsparameter haben sich von Version zu Version von Windows Server erheblich geändert. Achten Sie darauf, aktuelle Optimierungsrichtlinien zu verwenden, um unerwartete Ergebnisse zu vermeiden.

Inhalt dieser Anleitung

Die Leitfäden zu Leistung und Optimierung für Windows Server 2016 sind in diesem Handbuch in drei Optimierungskategorien gegliedert:

SERVERHARDWARE	SERVERROLLE	SERVERSUBSYSTEM
Überlegungen zur Hardwareleistung	Active Directory-Server	Cache- und Arbeitsspeicherverwaltung
Überlegungen zum Hardwareenergiebedarf	Dateiserver	Netzwerksubsystem
	Hyper-V-Server	Direkte Speicherplätze
	Remotedesktopdienste	Software-Defined Networking (SDN)
	Webserver	
	Windows Server-Container	

Änderungen in dieser Version

Hinzugefügte Abschnitte

- Überlegungen zur Konfiguration des Nano Server-Installationstyps
- Software Defined Networking, einschließlich HNV und SLB-Gateway-Konfigurationsleitfaden
- Direkte Speicherplätze

- [HTTP1.1 und HTTP2](#)
- [Windows Server-Container](#)

Geänderte Abschnitte

- Updates des Abschnitts [Active Directory-Leitfaden](#)
- Updates des Abschnitts [Dateiserverleitfaden](#)
- Updates des Abschnitts [Webserverleitfaden](#)
- Updates des Abschnitts [Hardwareenergiebedarf-Leitfaden](#)
- Updates des Abschnitts [PowerShell-Optimierungsleitfaden](#)
- Wichtige Updates des Abschnitts [Hyper-V-Leitfaden](#)
- *Leistungsoptimierung für Auslastungen wurde entfernt*, Zeiger zu relevanten Ressourcen wurden dem [Artikel über zusätzliche Optimierungsressourcen](#) hinzugefügt
- *Entfernen dedizierter Speicherabschnitte* zugunsten des neuen Abschnitts [Direkte Speicherplätze](#) und von kanonischem TechNet-Inhalt
- *Entfernen des dedizierten Netzwerkabschnitts* zugunsten von kanonischem TechNet-Inhalt

Microsoft Server Performance Advisor

02.12.2019 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Laden Sie Microsoft Server Performance Advisor (Spa) herunter, um bei der Bereitstellung von Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 Leistungsprobleme zu diagnostizieren. Spa generiert umfassende Diagnose Berichte und-Diagramme und bietet Empfehlungen, mit deren Hilfe Sie Probleme schnell analysieren und Korrekturmaßnahmen entwickeln können.

- [Übersicht über den Server Performance Advisor](#)
- [Herunterladen von Server Performance Advisor](#)
- [Server Performance Advisor-Benutzerhandbuch](#)
- [Server Performance Advisor Pack-Entwicklungsleitfaden](#)

Übersicht über den Server Performance Advisor

Der Server Performance Advisor besteht aus zwei Teilen: dem Spa-Framework und den Spa Advisor-Paketen.

Das Server Performance Advisor-Framework

Die Engine, die für das Erfassen von Daten verantwortlich ist, die von den Advisor-Paketen festgelegt werden, das Schreiben der gesammelten Daten in eine Microsoft SQL Server Datenbank, das Erstellen einer IT-freundlichen Umgebung zum Ausführen von Skripts für die Spa Advisor-Pakete und das Anzeigen der abschließenden Berichte. Sie müssen das Spa-Framework nur in der Spa-Konsole installieren. Die Spa-Konsole kann entweder auf einem eigenständigen Computer installiert werden, um Remote auf die zu testenden Server zuzugreifen oder auf einem getesteten Server installiert zu werden.

Server Performance Advisor Packs

Spa Advisor Packs stellen den Mittelpunkt aller Optimierungs Regeln dar, die aus einer Reihe von Metadaten und SQL-Skriptdateien bestehen. Spa umfasst die folgenden Advisor-Pakete:

- Das Core-Betriebssystem Advisor-Paket analysiert die Leistung allgemeiner Betriebssystemfunktionen unabhängig von spezialisierten Server Rollen.
- Das Internet Information Server (IIS) Advisor Pack verfolgt die Leistung von IIS.
- Mit dem Hyper-v Advisor Pack wird die allgemeine Leistung der Hyper-v-Server Rolle analysiert.

Hinweis Das Hyper-V Advisor Pack analysiert keine Gast Betriebssysteme.

- Das Active Directory Advisor Pack analysiert die allgemeine Leistung der Active Directory-Rolle.

Spa bietet auch ein erweiterbares Modell für Entwickler, die nicht von Microsoft unterstützt werden, um Advisor Packs entsprechend Ihren Anforderungen zu schreiben.

Hinweis Spa kann nicht alle Hardware-und Benutzer szenariokontexte verstehen. Verwenden Sie die Empfehlungen, die vom Tool bereitgestellt werden, um Entscheidungen zu treffen und die Konsequenzen von möglichen Änderungen zu verstehen, die an den Servern vorgenommen werden.

Herunterladen von Server Performance Advisor

Verwenden Sie die folgenden Links zum Herunterladen von Server Performance Advisor für Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008:

- [Microsoft Server Performance Advisor 3,1 \(32 Bit\)](#)
- [Microsoft Server Performance Advisor 3,1 \(64 Bit\)](#)

Sie können die Dateien in der CAB-Datei mit den folgenden Befehlen extrahieren:

- für die x86-Version: `extrac32.exe /e /a /l d:\SPA d:\SPA\SPAPlus_x86.cab`
- für x64-Version: `extrac32.exe /e /a /l d:\SPA d:\SPA\SPAPlus_amd64.cab`

Vorsicht Wenn Sie die CAB-Datei extrahieren, muss Spa die hierarchische Verzeichnisstruktur beibehalten, damit Sie ordnungsgemäß funktioniert. Abhängig von den CAB-Tools, die auf dem Server installiert sind, kann die Extraktion zu einer nicht operativen Verzeichnisstruktur führen. Um die hierarchische Verzeichnisstruktur beizubehalten, können Sie ein Tool zum Extrahieren von Hilfsprogramm verwenden, das eine Datei Verzeichnisstruktur extrahiert.

Wenn das CAB-Extraktions Tool die Dateien ordnungsgemäß extrahiert hat, werden die Unterordner automatisch im Extraktions Zielordner angezeigt.

Voraussetzungen für Spa

Die Spa-Konsole erfordert, dass die folgende Software installiert ist:

- Microsoft .NET Framework 4
- SQL Server 2008 R2 Express SP1 oder Microsoft SQL Server 2008 R2 SP1

Neuere Versionen sind möglicherweise kompatibel. Alle bekannten Produkt Inkompatibilitäten mit der Spa-Konsole werden vermerkt.

Server Performance Advisor-Benutzerhandbuch

19.02.2020 • 116 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 10, Windows 8

Dieses Benutzerhandbuch für Microsoft Server Performance Advisor (Spa) enthält Richtlinien für die Verwendung von Spa, um Leistungsengpässe in Systemen zu identifizieren, die in verschiedenen Server Rollen bereitgestellt werden.

Spa kann Ihnen Folgendes helfen:

- Verwalten Sie die Serverleistung, und beheben Sie Probleme mit der Serverleistung.
- Stellen Sie Daten Berichte und Empfehlungen zu häufigen Konfigurations- und Leistungsproblemen bereit.
- Geben Sie Empfehlungen zu bewährten Methoden auf Grundlage der gesammelten Daten an.

NOTE

Die Spa-Konsole nimmt keine Änderungen an den Servern vor.

Weitere Informationen zum Entwickeln von Spa Advisor-Paketen finden Sie im [Entwicklungs Handbuch zum Server Performance Advisor Pack](#).

Übersicht über den Server Performance Advisor

In diesem Abschnitt wird der Verlauf der Spa erläutert, die Zielgruppe und die Zielgruppe beschrieben und eine architektonische Übersicht über das Tool vorgestellt.

Verlauf der Spa

Die ursprüngliche Version von Microsoft Server Performance Advisor (Spa) wurde in 2005-2006 veröffentlicht. Dabei handelt es sich hauptsächlich um Windows Server 2003, einschließlich der wichtigsten Betriebssystem- und Server Rollen wie Internetinformationsdienste (IIS) und Active Directory. Das Tool soll Ihnen helfen, die Serverleistung zu bewerten und Probleme mit der Serverleistung zu beheben.

Spa bietet Daten Berichte und Empfehlungen für Systemadministratoren zu häufigen Konfigurations- und Leistungsproblemen. Spa sammelt leistungsbezogene Daten aus verschiedenen Quellen auf Servern, z. B. Leistungsindikatoren, Registrierungs Schlüsseln, WMI-Abfragen, Konfigurationsdateien und Ereignis Ablauf Verfolgung für Windows (ETW). Basierend auf den erfassten Server Leistungsdaten bietet Spa eine ausführliche Betrachtung der aktuellen Serverleistung und gibt Empfehlungen dazu, was verbessert werden kann.

Das Original-Spa-Tool hat mehr als 1 Million Downloads und unterstützt viele Systemadministratoren dabei, die Leistung Ihrer Server zu verwalten. Es handelt sich um ein sehr erfolgreiches Tool zur Problembehandlung bei der Leistung.

Seit der Veröffentlichung der ursprünglichen Spa gibt es einige wesentliche Änderungen in der Server Leistungs Welt. Insbesondere das Release von Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 und Windows Server 2008 mit neuen Versionen der entsprechenden Server Rollen wie Internetinformationsdienste (IIS) 8,5. Neuere Versionen von Server Performance Advisor erweitern die Funktionalität der ursprünglichen Spa auf die neuesten Server Betriebssysteme und Server Rollen.

Obwohl Spa 3,1 die gleichen Entwurfs Ziele und Leistungsanalyse Paradigma wie das ursprüngliche Tool nutzt, wurde es mit der neuesten Technologie umgeschrieben. Außerdem bietet es die folgenden wichtigen Verbesserungen:

- Kann Analysen für Server ausführen, auf denen Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 und Windows Server 2008 ausgeführt wird.
- Unterstützt die Remote Analysefunktion, die es Spa 3,1 ermöglicht, Daten aus einer zentralen Konsole zu erfassen und zu analysieren, ohne dass Code auf den zu analysierenden Servern installiert werden muss.
- Verwendet einen Microsoft SQL Server für die Datenanalyse und den Speicher, der die Verarbeitung und Speicherung großer Datenmengen ermöglicht.
- Trennt das Tool von den Advisor-Paketen. Die Leistungsanalyse Logik für jede Server Rolle wird in Form eines Advisor-Pakets freigegeben, das getrennt vom Tool veröffentlicht oder aktualisiert werden kann.
- Stellt Advisor-Pakete bereit, die in SQL-Skripts mit einer offenen Architektur entwickelt wurden. Parteien, die nicht von Microsoft sind, können Advisor Packs entwickeln oder die vorhandenen Advisor Packs von Microsoft erweitern, um besondere Anforderungen zu erfüllen.
- Unterstützt neue Features wie parallele Vergleichsberichte und Trend-und Vergangenheits Diagramme, die Ihnen bei der Suche nach Anomalien helfen.
- Bietet Features wie z. b. die Schwellenwerte zum ändern, importieren und exportieren, mit denen Sie die Berichte und Benachrichtigungen optimieren und diese für andere Spa-Benutzer freigeben können.
- Unterstützt mehrere-Projekte, die zum Gruppieren von Ziel Servern verwendet werden können.
- Ermöglicht die wiederholte Erfassung von Daten in der Spa-Konsole.
- Aktiviert benutzerdefinierte Abfragen und die Generierung von Berichten mithilfe von Microsoft SQL Server (für fortgeschrittene Benutzer).
- Angepasste Windows PowerShell-Cmdlets sind für die Verwendung mit Spa verfügbar.
- Abwärts kompatibel zum Importieren und Anzeigen von Berichten aus einer Spa 3,0-Datenbank

Zielgruppe

Das Spa-Tool ist hauptsächlich für Systemadministratoren konzipiert, die weniger als 100 Server in verschiedenen Server Rollen verwalten. Es kann auch von Support Technikern verwendet werden, um Leistungsdaten zu erfassen und Leistungsprobleme für Kunden zu beheben.

Spa bietet Empfehlungen, mit denen Sie Leistungsprobleme beheben können. Es basiert jedoch auf Annahmen, die möglicherweise nicht auf Ihre bestimmte Serverumgebung anwendbar sind. Die Empfehlungen, die über Spa angeboten werden, sollten als Vorschläge angesehen werden. Wir gehen davon aus, dass Spa-Benutzer ein gutes Verständnis der Systemkonfiguration, der Anwendungsfälle und der Auswirkungen der Systemoptimierung auf das gesamte Systemverhalten haben. System Administratoren sollten entscheiden, ob die Spa-Empfehlungen auf Ihre Umgebung angewendet werden sollen.

Welche Neuerungen gibt es in Spa 3,1?

Die folgenden Features und Verbesserungen wurden in Spa 3,1 hinzugefügt:

- Das Active Directory Advisor Pack hilft bei der Analyse der allgemeinen Leistung der Server Rolle "Active Directory-Domänen Dienste" des Servers.
- Unterstützung für Entwickler zum Hinzufügen verlorener ETW-Ereignis Benachrichtigungs Warnungen in den Advisor Packs und zum Anzeigen der Warnung, wenn ein Bericht generiert wurde und Ereignisse aufgrund der Häufigkeit der Protokollierung auf einem langsamen oder stark in Konflikt befindlichen Datenträger verloren gegangen sind

Ziel Szenarien

Im folgenden sind die Ziel Szenarien für Spa aufgeführt:

- **Server Umgebung**

Spa ist so konzipiert, dass es problemlos eingerichtet und gewartet werden kann. Dies gilt für Serverumgebungen, die 1 bis 100 Server verwenden. Spa ist nicht gut skalierbar, wenn Sie versuchen, die Leistung für mehr als 100 Server zu verwalten. Für größere oder anspruchsvollere Umgebungen sollten Sie die Verwendung von System Center Operations Manager in Erwägung gezogen.

- **Behandlung von Leistungsproblemen**

Sie können Spa als Tool zur Leistungsproblem Behandlung verwenden. Er bietet die Möglichkeit, Leistungsdaten auf hoher Ebene zu erfassen. er führt eine gründliche Verarbeitung der Daten durch, um Ihnen ein besseres Verständnis für das gesamte Systemverhalten zu bieten, und Kenn gibt jegliche Anomalien. Wenn ein Kunde von einem Leistungsproblem vermutet wird, können Sie die Spa verwenden, um Leistungsdaten vom Server zu erfassen und zu analysieren.

Spa generiert einen Bericht, den Sie anzeigen können. Spa-Berichte bieten eine Benachrichtigungsliste, die mögliche Probleme hervorhebt, und einen Daten Abschnitt, der verschiedene Leistungsindizes, Konfigurationen und Einstellungen für den Server enthält. Mithilfe dieses Berichts können Sie das spezifische Leistungsproblem identifizieren und die Empfehlungen verwenden, um Lösungen für das Problem zu finden. Berichte können mit anderen Berichten verglichen werden, die zu einem anderen Zeitpunkt oder von einem anderen Server generiert wurden. Mit diesem parallelen Vergleich können Sie Unterschiede zwischen der normalen Baseline und dem normalen Verhalten ermitteln.

Hinweis Spa ist nicht als Debuggen oder Messungs Tool konzipiert. Außerdem kann Sie aus der Perspektive der Server als Schreib geschütztes Tool angesehen werden, und die Serverkonfigurationen werden nicht geändert.

- **Leistungsindex Überwachung**

Sie können Spa verwenden, um den Leistungsindex von-Servern zu überwachen. Sie können festlegen, dass Spa regelmäßig auf Servern ausgeführt werden soll, um Leistungsdaten zu erfassen, und dann ein Trend Diagramm oder ein Verlaufs Diagramm ausführen, um die Anomalien zu erkennen. Sie können den Bericht für eine bestimmte Analyse anzeigen, weitere Informationen zum Leistungsproblem anzeigen und dann die Empfehlungen oder andere Berichtsdaten verwenden, um das Problem zu beheben.

Spa-Architektur

Die Spa-Daten Sammlungs Logik basiert auf einem Protokoll in Windows namens Leistungsprotokolle und-Warnungen (PLA). Mithilfe von Pla können Programme Leistungsdaten von lokalen Servern oder Remote Servern erfassen, wie z. b. Leistungsindikatoren, WMI-Abfragen, etw-Ablauf Verfolgungen, Registrierungs Schlüsseln und Konfigurationsdateien. Wenn das Spa eine Leistungsanalyse auf einem Zielserver ausführt, erstellt es einen Pla-Datensammler Satz, der auf dem von Ihnen ausgewählten Spa Advisor-Paket basiert. Das Advisor-Paket enthält die zu sammelnde Datenquelle und die Dateifreigabe, in der die Protokolle gespeichert werden sollen. Bei der Spa-Datensammlung wird nur ein einzelnes Benutzerkonto gespeichert. das gleiche Benutzerkonto, das von Pla verwendet wird, wird auch verwendet, um die Protokolle zu schreiben.

Spa verwendet eine SQL Server Datenbank, um die Leistungs Protokolle zu speichern, die von den Ziel Servern gesammelt werden. Spa importiert alle Leistungs Protokolle aus der Dateifreigabe in die Datenbank und verwendet dann die Datenanalyse Logik innerhalb jedes Advisor-Pakets, um die Daten zu verarbeiten und die Berichte zu generieren. Ein Advisor-Paket analysiert die Leistungsdaten, die von den Ziel Servern gesammelt wurden, und generiert die Spa-Berichte. Weitere Informationen zum Aufbau eines Advisor-Pakets finden Sie im [Entwicklungs Handbuch zum Server Performance Advisor Pack](#).

Die Benutzeroberflächen und Interaktionen der Spa-Konsole werden als Teil der "spaconsole. exe" erstellt. Sie

können die-Konsole verwenden, um eine Datenbank zu erstellen, Advisor-Pakete hinzuzufügen oder zu entfernen, Zielserver zu verwalten, Leistungsanalysen auszuführen und Leistungsberichte anzuzeigen.

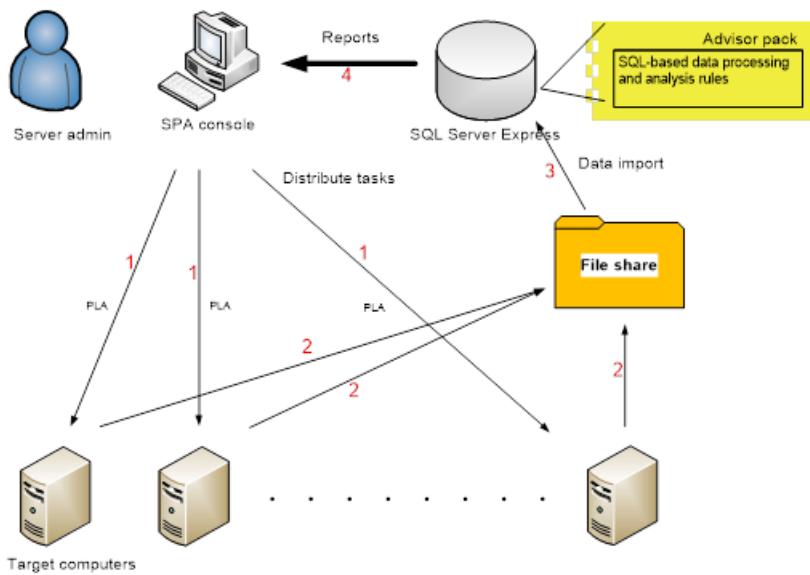
Die Spa-Konsole kann unter den folgenden Betriebssystemen ausgeführt werden:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- WindowsServer 2008

In einer typischen Geschäftsanwendung gibt es drei Ebenen: die Präsentationsschicht, die Geschäftslogik Schicht und die Speicher Ebene. Spa ist als ein zweistufiges Produkt der-Konsole und der-Datenbank konzipiert. Die-Konsole fungiert als Präsentationsschicht mit bestimmter prozessbezogener Logik, und die-Datenbank fungiert als Speicherschicht und Geschäftslogik Schicht. Die-Konsole erfasst Benutzereingaben und steuert die Schritte für die Datensammlung, die Datenverarbeitung und die Bericht Generierung. Spa ist nicht von den Windows-System Diensten abhängig.

Das folgende Diagramm zeigt die allgemeine Architektur des Spa-Systems. Der Prozess lautet wie folgt:

1. In der Spa-Konsole führen Sie die Leistungsanalyse auf den angegebenen Servern aus.
2. Wenn die Leistungsdaten gesammelt werden, werden die Protokolle von Pla auf den Ziel Servern zurück in die Dateifreigabe geschrieben, die durch den Datensammler Satz angegeben wird.
3. Nachdem die Datensammlung auf einem Bereitstellungs Zielcomputer fertiggestellt wurde, importiert die Spa-Konsole die Protokolle in die SQL Server Datenbank.
4. Die-Konsole Ruft die Datenverarbeitungs Logik eines bestimmten Advisor-Pakets auf.
5. Das Advisor Pack verarbeitet die Daten und ruft Spa-APIs auf, um Datensätze in die vom Spa-Framework definierten System Berichts Tabellen einzufügen.
6. Sie können den Bericht-Viewer in der-Konsole verwenden, um die generierten Berichte anzuzeigen. Um Ihnen bei der Behebung von Leistungsproblemen zu helfen, bietet Spa drei Arten von Berichten: einzelne Berichte, parallele Berichte und Trend-oder Vergangenheits Diagramme. Weitere Informationen zu Berichten finden Sie unter [Anzeigen von Berichten](#).



Einstieg in die Spa

Voraussetzungen

Die Spa-Konsole kann auf Windows 8.1, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 und Windows Server 2008 installiert werden. Das Ausführen von Spa unter früheren Versionen des Windows Server-Betriebssystems wird nicht unterstützt. Spa wird auf x86 oder x64 ausgeführt, unterstützt jedoch keine ia64-oder ARM-Architekturen.

Spa basiert auf Windows Presentation Foundation (WPF) 2,0, das Teil von Microsoft .NET Framework 4 ist, sodass .NET Framework 4 erforderlich ist.

Außerdem müssen Sie SQL Server 2008 R2 Express auf demselben Computer installieren, auf dem Spa installiert ist. SQL Server 2008 R2 Express ist eine kostenlose Datenbank-Engine, die von Microsoft veröffentlicht wird. Sie können Microsoft SQL Server 2008 R2 Express aus dem Microsoft Download Center herunterladen. Obwohl wir SQL Server 2008 R2 Express vorschlagen, können neuere Versionen von SQL Server auch mit Spa kompatibel sein.

Hinweis Das Spa umfasst weder SQL Server noch die .NET Framework als Teil des Installationspaketes. Nach der Installation von Microsoft SQL Server 2008 R2 und .NET Framework 4,0 empfiehlt es sich, vor der Installation von Spa Windows Update auszuführen.

Da Benutzerdaten Banken mit Spa erstellen und verwalten können, muss das Benutzerkonto, das zum Ausführen von Spa verwendet wird, über dieselben Administratorrechte wie SQL Server verfügen.

Einrichten von Spa

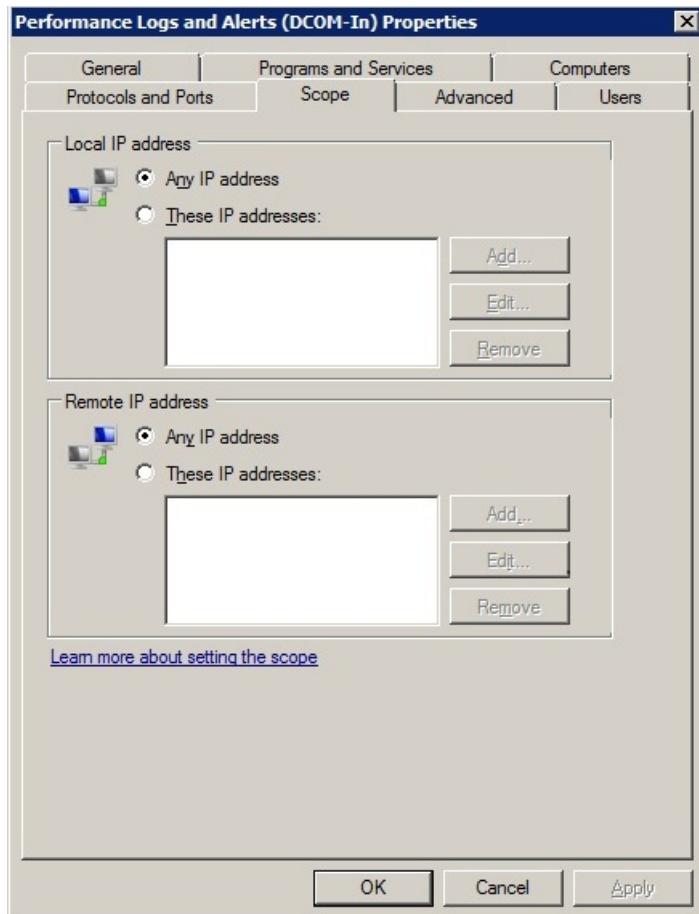
Spa ist als CAB-Datei verpackt, die alle Binärdateien für das Spa-Framework, die Windows PowerShell-Cmdlets, die in erweiterten Szenarien verwendet werden, und die folgenden Advisor-Pakete enthält: Core OS, Hyper-V, Active Directory und IIS. Nachdem Sie die CAB-Datei in einen Ordner extrahiert haben, ist keine weitere Installation erforderlich. Zum Ausführen von Spa müssen Sie die Datensammlung auf den Ziel Servern jedoch wie folgt aktivieren:

- Zum Ausführen der Pla-Datensammlung muss das Benutzerkonto, das Sie zum Ausführen der Spa-Konsole verwenden, der Sicherheitsgruppe "Administratoren" auf dem Zielserver angehören. Wenn sich der Zielserver und die-Konsole in derselben Domäne befinden, muss das Domänen Benutzerkonto Teil der Sicherheitsgruppe Administratoren auf dem Zielserver sein. Wenn sich der Zielserver und die-Konsole nicht in derselben Domäne befinden, erstellen Sie ein Administrator Konto auf dem Zielserver mit demselben Benutzernamen und Kennwort wie das Benutzerkonto, das Sie zum Ausführen der Spa-Konsole verwenden.
- Erstellen Sie einen freigegebenen Ordner für die Ergebnisse auf dem Server.

- Stellen Sie sicher, dass das Benutzerkonto, das Sie zum Ausführen der Spa-Konsole verwenden, über Lese- und Schreibberechtigungen für den freigegebenen Ordner verfügt. Mit diesem Konto werden von Pla Protokolle in den Ordner geschrieben. Die Spa-Konsole verwendet dasselbe Konto, um Protokolle zu lesen und in die-Datenbank zu importieren.

Hinweis Etw implementiert einen Zirkel Puffer zum Speichern der Ablauf Verfolgung und verschiebt Sie nach Möglichkeit in den freigegebenen Ordner. Wenn der Server ausgelastet ist oder der Schreibvorgang langsam ist, löscht etw die Ablauf Verfolgungen, wenn der Puffer voll ist. Es ist wichtig, dass sich der freigegebene Ordner auf einem Server befindet, der überschnellen e/a-Zugriff verfügt. Es wird empfohlen, dass jeder Zielserver über einen freigegebenen Ordner verfügt, um Datenverluste zu minimieren, die durch langsame Datei-e/a

- Legen Sie für die Windows-Firewall für den Zugriff auf Zielserver mit der Windows-Firewall den Zugriff auf Remote Leistungsprotokolle und-Warnungen auf Ziel Servern fest. Die Pla verwendet den TCP-Port 139.
- Stellen Sie sicher, dass die **Leistungs Protokolle & Warnungs Dienst** ausgeführt werden.
- Wenn sich die Konsole und der Zielserver in unterschiedlichen Subnetzen befinden, müssen Sie auch das Feld Remote-IP-Adresse in den Regeln für die eingehende Firewall in den **Bereichs Einstellungen** auf der Seite **Leistungsprotokolle und-Warnungen** festlegen, wie hier gezeigt.



- Aktivieren Sie die Netzwerk Ermittlung in der-Konsole und auf jedem der Zielserver.
- Wenn der Zielserver keiner Domäne hinzugefügt wird, aktivieren Sie die folgende Registrierungs Einstellung:
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\localaccountdekenfilterpolicy.

Hinweis Standardmäßig schreibt Spa Diagnoseprotokolle in den Ordner, in dem sich "spaconsole.exe" befindet. Wenn die Spa im Ordner "Programme" installiert ist, kann die Spa nur das Protokoll schreiben, wenn "spaconsole.exe" als Administrator ausgeführt wird.

Wenn Sie die Datenanalyse auf dem Computer mit der-Konsole ausführen möchten, müssen Sie Spa als Administrator ausführen. Die Pla durchläuft einen anderen Codepfad, wenn Sie auf einem lokalen Computer ausgeführt wird, für den Administratorrechte erforderlich sind.

Wenn Sie das IIS Spa Advisor Pack für Ihre Server ausführen möchten, müssen Sie die WMI-Abfrage und die ETW-Ablauf Verfolgung für den IIS-Server aktivieren. Hierzu können Sie die Ablauf Verfolgung unter dem Integritäts - und Diagnose Rollen Dienst und die IIS-Verwaltungs Skripts und-Tools unter Verwaltungs Tools der Server Rolle " Webserver (IIS) " aktivieren.

Erstellen Ihres ersten Projekts

Nachdem alles eingerichtet wurde, können Sie Ihr erstes Spa-Projekt erstellen. Wie im vorherigen Abschnitt beschrieben, speichert Spa alle Elemente, die sich auf die Analyse von Leistungsdaten in einer Datenbank beziehen. Jedes Spa-Projekt entspricht einer einzelnen Datenbank. Der **Assistent zum ersten Mal** führt Sie durch die folgenden Schritte:

So erstellen Sie ein Spa-Projekt

1. Starten Sie "spaconsole.exe". Die Konsole wechselt in einen getrennten Modus, in dem die Spa nicht mit einer Datenbank verbunden ist und das Hauptfenster leer ist.
2. Um ein neues Projekt zu erstellen, klicken Sie auf **Datei** und dann auf **Neues Projekt**. Hiermit wird der Assistent zum ersten Mal verwendet. Auf der ersten Seite werden die Schritte angezeigt, die Sie bei der Verwendung des Assistenten befolgen:
 - Erstellen einer Datenbank
 - Advisor-Pakete bereitstellen
 - Hinzufügen von Servern zur Zielserver Liste
3. Klicken Sie auf **Weiter**. Auf der Seite **Projektdatenbank erstellen** werden Sie aufgefordert, den Namen der Microsoft SQL Server Instanz anzugeben, in der Sie die Datenbank erstellen möchten. Wenn Sie sich z. b. auf dem gleichen Computer wie die-Konsole befindet, können Sie **localhost\<den SQL Server-Namen>** verwenden.

Hinweis Der Standardinstanzname für eine SQL Server 2008 R2 Express-Installation lautet SQLExpress. Für eine Instanz von SQL Server 2008 R2 Express, die auf dem lokalen Computer installiert ist, wird die Datenbank in der Regel standardmäßig **localhost\SQLExpress**. Es wurde jedoch möglicherweise während SQL Server Installation geändert, daher müssen Sie sicherstellen, dass Sie den richtigen SQL Server Instanznamen verwenden.

4. Geben Sie den Datenbanknamen an. Nur Buchstaben, Ziffern und Unterstriche (_) sind als gültige Zeichen für einen Datenbanknamen zulässig. Ein angemessener Vorschlag für den Namen der Spa-Datenbank wäre "Spa". Wenn Sie einen ungültigen Namen eingeben, wird ein rotes Fehler Symbol angezeigt. Die zugehörige QuickInfo gibt den Grund für den Überprüfungs Fehler aus.

Hinweis Es ist wichtig, den Datenbanknamen und den Serverinstanznamen zu merken, da dies die einzigen Bezeichner für Ihr Projekt sind. Sie müssen diese Informationen angeben, wenn Sie zu dieser Datenbank wechseln möchten.

5. Nachdem Sie den Serverinstanznamen und den Datenbanknamen bereitgestellt haben, generiert der Assistent zum ersten Mal den Speicherort für die Datenbankdatei.
6. Klicken Sie auf der Seite "**Projektdatenbank erstellen**" auf "**weiter**". Beim ersten Mal erstellt der Assistent eine Datenbank und generiert alle Spa-bezogenen Datenbankschemas, Funktionen und gespeicherten Prozeduren in der Datenbank. Dieser Schritt kann je nach Hardware-und Netzwerkgeschwindigkeit einige Sekunden in Anspruch nehmen.

Hinweis wenn dieser Schritt fehlschlägt, wird eine Fehlermeldung angezeigt. Einige häufige Probleme sind: die-Konsole kann keine Verbindung mit der SQL Server-Instanz herstellen, unzureichende Berechtigungen zum Erstellen einer Datenbank, oder der Datenbankname ist bereits vorhanden.

7. Wenn der vorherige Schritt erfolgreich ausgeführt wurde, wird die Seite " **Advisor-Paket bereit stellen**" angezeigt. Sie listet alle Advisor-Pakete auf, die auf Ihrem Computer verfügbar sind. Spa scannt den Ordner mit dem Namen **APS** automatisch unter dem Spa-Stammverzeichnis. Sie listet den vollständigen Namen, die Version und den Autor für jedes Advisor Pack auf.

Hinweis Weitere Informationen zur Verwendung des vollständigen Namens und der Version in der Spa finden Sie unter [Verwalten von Advisor Packs](#) .

8. Wählen Sie aus, welche Ratgeber Pakete Sie in der Projektdatenbank bereitstellen möchten, und klicken Sie dann auf **weiter**. Sie können auch auf über **springen** klicken, um zum nächsten Schritt zu wechseln, ohne Advisor-Pakete bereitzustellen.

Hinweis Sie können Ratgeber Pakete jederzeit bereitstellen, wenn Sie das Tool verwenden. Weitere Informationen finden Sie unter [Verwalten von Advisor Packs](#).

9. Auf der Seite **Server hinzufügen** müssen für jeden Server, der der Liste Zielserver hinzugefügt werden soll, zwei Pflichtfelder ausgefüllt werden: **Name des Servers und der Dateifreigabe**.

Hinweis Es gibt auch ein Feld für die **Anmerkung**, das hauptsächlich zum Klassifizieren oder Suchen des Servers verwendet wird. In Fällen, in denen Sie viele Server haben, können Sie eine Datei mit Komma getrennten Werten (CSV-Datei) importieren, die den Servernamen, den Ergebnis Ordner und das optionale Feld für die Anmerkung enthält. Das Feld " **Anmerkung** " wird verwendet, um den Server zu beschreiben, und der Begriff kann zum Filtern von Servern für die Datensammlung verwendet werden. Wenn Sie die Server über die CSV-Datei initialisieren, werden die Server durch einen Fehler beim fehl geschachtelungs Fehler in der Datei nicht geladen.

10. Es müssen mehrere Konfigurationen festgelegt werden, um die Pla-Datensammlung zu aktivieren, wie unter [Einrichten von Spabeschrieben](#). Die Seite **Server hinzufügen** bietet eine Test Konfigurationsfunktion, mit der Sie Konfigurationsprobleme beheben können. Aktivieren Sie das Kontrollkästchen, das dem Computer zugeordnet ist, und klicken Sie dann auf **Verbindung testen**. Spa versucht, einen Datensammler Satz auf Ziel Servern zu generieren, und versucht, die Ergebnisse zurück in die Datenbank zu importieren. Wenn alles richtig ist, zeigt der **Status " Pass** an. Wenn ein Fehler auftritt, wird eine QuickInfo angezeigt, die den Grund für den Fehler beschreibt.
11. Jeder Server wird der Datenbank automatisch hinzugefügt, auch wenn er den Konfigurations Test nicht bestanden hat. Wenn Sie Server aus der Liste entfernen möchten, wählen Sie den Servernamen aus, und klicken Sie auf **Entfernen**.
12. Wenn alles abgeschlossen ist, klicken Sie auf **Fertig** stellen, um den Assistenten zum ersten Mal zu schließen. Wenn Sie den Assistenten zum ersten Mal verwenden, bevor Sie ihn abschließen, werden alle vorherigen Schritte beibehalten, und für keinen wird automatisch ein Rollback ausgeführt. Sie müssen zukünftige Änderungen manuell vornehmen.

Analyse wird ausgeführt

Nachdem Sie die Datenbank eingerichtet haben, können Sie die Leistungsanalyse auf den Servern ausführen.

Jedes Mal, wenn die Spa-Konsole gestartet wird, wird das letzte Projekt, das vom aktuellen Benutzer verwendet wurde, automatisch geöffnet. Das Hauptfenster enthält eine Liste von Servern. Jeder Server verfügt über vier Eigenschaften: Server Name, Analyseergebnis, aktueller Status und Hinweis.

- **Server Name** Der Name des Servers, der der Bezeichner für den Server ist. Doppelte Namen sind nicht zulässig.

- **Analyseergebnis** Standardmäßig wird das Ergebnis der aktuellen Leistungsanalyse angezeigt, die auf dem Server ausgeführt wird. Wenn keine Leistungsanalyse auf dem Server ausgeführt wurde, wird **kein Bericht** angezeigt. Wenn vom Bericht eine Warnung ausgelöst wird, wird eine **Warnung** und der Zeitstempel angezeigt, wenn der aktuelle Bericht generiert wurde. Wenn während der letzten Analyse auf dem Server kein Problem gefunden wurde, wird die Meldung "OK" und der Zeitstempel angezeigt.

Hinweis Wenn Sie vor kurzem eine Systemeinstellung geändert haben, empfiehlt es sich, die Analyse erneut auszuführen, um die allgemeinen Auswirkungen der Änderung zu evaluieren und einen aktualisierten Bericht zum Systemstatus zu erhalten. Spa verfolgt keine Konfigurationsänderungen am getesteten System nach.

- **Aktueller Status** Zeigt den Status von Leistungsanalyse Tasks an, die zurzeit auf dem Server ausgeführt werden. Sie können eine laufende Aufgabe abbrechen, indem Sie auf das Symbol "Abbrechen" klicken, das durch ein rotes X gekennzeichnet ist.
- **Anmerkung** Beschreibt den aktuellen Zielserver. Beispielsweise können Sie den Server mithilfe der Server Rolle (z. B. SQL Server) oder eines Speicher Orts (z. B. Kent) beschreiben. Spa verwendet den **Servernamen** und die- **Anmerkung**, um die Suche nach dem richtigen Server zu unterstützen. Sie können in das Textfeld Suchen eingeben. Wenn die Spalten **Servername** oder **Anmerkung** die genaue Zeichenfolge enthält, die Sie im Suchfeld eingegeben haben, wird der Server in der Liste Server angezeigt.

Die folgenden Steuerelemente sind auch in der-Konsole verfügbar:

- **Wiederholen** Ein Kontrollkästchen, das die Möglichkeit beschreibt, eine Auflistung basierend auf einem Zeitintervall regelmäßig zu wiederholen. Bei den meisten Serverinstallationen sollten Sie eine Spa-Sammlung ständig wiederholen, um für die Analyse ausreichend Verlauf zu haben. Wenn Sie die Sammlung nur einmal ausführen möchten, sollten Sie das Kontrollkästchen **wiederholen** nicht aktivieren.
- **Wiederholung entfernen** Eine Schaltfläche, die es Ihnen ermöglicht, einen laufenden Wiederholungs Sammlungs Auftrag abzubrechen. Die Wiederholungs Auflistung wird abgebrochen, aber nicht die aktuelle Auflistung (sofern vorhanden). Mit dieser Option können Sie ein neues Wiederholungs Sammlungs Intervall zurücksetzen oder die Auflistung manuell ausführen.

Bevor Sie mit der Leistungsanalyse beginnen, wählen Sie die Dauer der Datensammlung aus. Obwohl durch das Erfassen von mehr Daten eine genauere Darstellung der Server leistungssituation erzielt werden kann, wird auch eine größere Anzahl von Protokollen generiert, und es kann eine größere Auswirkung auf den Server haben. Wählen Sie die richtige Daten Sammlungs Dauer basierend auf Ihrem speziellen Bedarf aus. Jedes Advisor-Paket definiert eine minimale gültige Dauer. Die von Ihnen gewählte Dauer für die Datensammlung muss länger sein als die minimale Dauer der ausgewählten Advisor Packs.

Wenn Sie die Leistungsanalyse auf Ziel Servern ausführen möchten, wählen Sie die Server aus, für die Sie die Leistungsanalyse ausführen möchten, und klicken Sie auf **Analyse ausführen**. Daraufhin werden Sie aufgefordert, die Advisor Packs auszuwählen, die auf den Servern ausgeführt werden sollen. Die ausgewählten Advisor Packs werden gleichzeitig ausgeführt. Die generierten Berichte basieren auf den Leistungsdaten, die während des gleichen Zeitraums gesammelt werden.

Hinweis Wenn Sie einen Server auswählen, auf dem eine wiederkehrende Leistungsanalyse ausgeführt wird, können Sie mit der Schaltfläche **Wiederholung entfernen** die wiederkehrende Datensammlung abbrechen. Die Spa lässt nicht mehrere Daten Sammlungs Sitzungen gleichzeitig auf demselben Computer zu.

Anzeigen von Berichten

In Spa gibt es drei Typen von Leistungsanalyse Berichten: einzelner Bericht, paralleler Bericht und Trend-und Verlaufs Diagramme.

Nach dem Ausführen der Leistungsanalyse wird für jedes Advisor-Paket, das auf dem Bereitstellungs Zielcomputer

ausgeführt wird, ein Bericht generiert. Aus der Serverliste im Hauptfenster können Sie das **Analyseergebnis** erweitern, um alle Advisor-Pakete anzuzeigen, die auf dem jeweiligen Server ausgeführt wurden. Sie können auf einen Berichts Namen klicken, um einen einzelnen Bericht anzuzeigen.

Neben dem Namen des Advisor-Pakets sind drei Symbole vorhanden, die den Status der letzten Analyse anzeigen, die auf dem Server ausgeführt wird:

- Das **neueste** Symbol zeigt den Bericht, der von der aktuellen Leistungsanalyse auf diesem Server für das Advisor Pack generiert wurde.
- Das Symbol **Suchen** zeigt die Liste der Leistungsanalyse Berichte an, mit deren Hilfe Sie den richtigen Bericht auswählen können. Die Felder **Advisor Pack** und **Zielserver** sind mit dem aktuellen Advisor Pack und den Zielserver Informationen vorab gefüllt. Der Standardzeit Bereich ist auf eine Woche festgelegt, und das Enddatum wird auf heute festgelegt. Wenn Sie in der oberen rechten Ecke auf die Schaltfläche **Suchen** klicken, können Sie eine Liste aller Leistungsanalyse Berichte für den ausgewählten Server und das Advisor-Paket im Zeitbereich erhalten.
- Das Symbol **Diagramme anzeigen** öffnet die Diagramm Ansicht Trend und Vergangenheits Diagramm.

In der folgenden Abbildung werden die Symbole für das **neueste**, das **Suchen** und **Anzeigen von Diagrammen** nach den einzelnen Advisor-Paketen angezeigt:

Server Name	Analysis Result	Current Status	Remark
26-145LJ08702		2/8/2012 10:19:36 AM	HP SQL
		Microsoft CoreOS Advisor Pack	
		Microsoft Hyper-V Advisor Pack	
		Microsoft IIS Advisor Pack	
26-145LJ08703		2/13/2012 4:46:48 PM	HP SQL
26-145LJ08704		2/13/2012 4:46:48 PM	HP IIS
26-145LJ08705		2/13/2012 4:47:05 PM	HP IIS
26-145LJ08706		2/13/2012 4:47:05 PM	DELL SQL
26-145LJ08707		2/13/2012 4:47:21 PM	DELL SQL
26-145LJ08708		2/13/2012 4:46:30 PM	DELL IIS

Suchen nach und innerhalb von Berichten

Die Suche nach Berichten erfolgt über den **Berichts-Explorer**. Dies ermöglicht es Ihnen, nach dem Datumsbereich, dem Servernamen und dem Advisor-Paket nach Berichten zu suchen. Dies ist die empfohlene Vorgehensweise, um einen anderen Bericht als den letzten Bericht zu finden. Der letzte Testlauf ist über **Bericht anzeigen** für diesen Server verfügbar.

Wenn Sie einen bestimmten Bericht anzeigen, können Sie ganz einfach zum nächsten und vorherigen Bericht navigieren, oder Sie können sich einen verknüpften Bericht ansehen, z. B. eine andere, gleichzeitig laufende Zugriffspunkt-app. Diese Optionen sind unter **Aktionen** verfügbar.

Es ist auch möglich, in einem Bericht zu suchen. Für eine Reihe von Berichten ist das Suchfeld **Such Zeichenfolge** für die schnelle Text Zeichenfolgen-Suche im Bericht verfügbar. Um das Textfeld zu entfernen, können Sie es verwerfen. Wenn Sie ein Suchfeld (in Fenstern mit Text Suche) aktivieren möchten, können Sie die Verknüpfung Steuerelement + F verwenden. Das **Feld Suchen** ermöglicht dem Benutzer die Angabe der Groß-/Kleinschreibung bei der Suche nach Bedarf mit der Option Groß-/Kleinschreibung .

In der folgenden Abbildung wird das Suchfeld suchen mit der Zeichenfolge Power auf der Registerkarte Bericht angezeigt.

The screenshot shows a 'Report Viewer' interface with a search bar at the top containing the text 'Power'. A red circle highlights the search bar, and a red arrow points to the word 'Power' in the list of results. The results table has two columns: 'Name' and 'Value'. The 'Power Profile' row is highlighted with a blue background, and a red arrow points to it. Other rows include Operating System (Microsoft Windows Server 2008 R2 Enterprise), OS Version (6.1.7600), OS Architecture (64-bit), OS Location (C:\), Number of Cores (1), Number of Logical Processors (1), Physical Memory Size (GB) (2.00), Number of Physical Disks (1), Number of Logical Disks (2), Pagefile Location (C:\), and Number of Physical Network Adapters (2). The 'Power Profile' row shows 'High performance'.

Name	Value
Operating System	Microsoft Windows Server 2008 R2 Enterprise
OS Version	6.1.7600
OS Architecture	64-bit
OS Location	C:\
Number of Cores	1
Number of Logical Processors	1
Physical Memory Size (GB)	2.00
Number of Physical Disks	1
Number of Logical Disks	2
Pagefile Location	C:\
Number of Physical Network Adapters	2
Power Profile	High performance
Is Domain Joined	False
Is Hyper-V Role Enabled	False
Is Running In VM	False
BIOS Version	PTLTD - 6040000
BIOS Serial Number	USE546N2V9
BIOS Manufacturer	HP
BIOS Caption	Phoenix ServerBIOS 3 Release 6.1

Installed Updates of Windows

Einzelner Bericht

Ein einzelner Bericht zeigt die Ergebnisse der Leistungsanalyse aus einer einzelnen Ausführung eines Advisor-Pakets auf einem einzelnen Computer an. Der Bericht zeigt den Namen des Advisor-Pakets, den Namen des Zielservers, den Zeitpunkt, zu dem der Bericht generiert wurde, und die Dauer für die Datensammlung an.

Ein einzelner Bericht enthält einen Benachrichtigungs Abschnitt und die Datenabschnitte.

Benachrichtigungs Abschnitt

Der Benachrichtigungs Abschnitt besteht aus einer Reihe von Leistungsanalyse Regeln. Jede Benachrichtigung enthält einige Datenquellen, einige Schwellenwerte und einige Geschäftslogik. Wenn Sie die Leistungsanalyse ausführen, wertet die Geschäftslogik die Datenquellen anhand der Schwellenwerte aus, um zu bestimmen, ob die Regel weitergeleitet wird. Wenn dies nicht der Fall ist, wird eine Warnung angezeigt, um Sie über ein mögliches Leistungsproblem zu informieren. Außerdem finden Sie hier Empfehlungen, die Ihnen helfen, das Problem zu beheben. Der Benachrichtigungs Abschnitt ist immer die erste Registerkarte in der einzelnen Berichtsansicht.

Der Benachrichtigungs Abschnitt ist in zwei Teile unterteilt: **Warnung** und **andere Benachrichtigungen**.

Wenn die Datenquelle für eine Regel bestimmte Bedingungen basierend auf den Logik- und Schwellenwert Einstellungen erfüllt, wird im **Warnungs** Bereich eine Warnung angezeigt. Eine Warnung umfasst die folgenden Teile:

- Ein Warnsymbol gibt das vorhanden sein eines potenziellen Problems an.
- Der Name der Regel. Beispielsweise ist das **Netzwerk Empfangs Paket Drop** ein Link, der auf die Regel Detailseite zeigt, wie unter [Verwalten von Advisor Packs](#) beschrieben.
- Eine einfache Beschreibung des potenziellen Problems.
- Eine Empfehlung für eine mögliche Lösung für das potenzielle Leistungsproblem.

Unterschiedliche Server können die Konfiguration und die Verwendungs Muster erheblich unterscheiden, und es

ist nicht möglich, die Schwellenwerte und Regeln festzulegen, die für alle Server unter allen Bedingungen gelten. Spa bietet die Möglichkeit, die Schwellenwerte zu ändern. Sie können eine Regel auch deaktivieren, wenn die Regel nicht für Ihr Szenario gilt. Standardmäßig sind alle Regeln aktiviert. Eine deaktivierte Regel wird nicht im Benachrichtigungsbereich angezeigt. Weitere Informationen finden Sie unter [Managing Advisor Packs](#).

Der **andere Benachrichtigungs** Bereich enthält alle anderen Regeln, bei denen keine Warnung ausgelöst oder die Regel nicht anwendbar ist. Sie enthält ähnliche Teile wie im **Warnungs** Bereich. Der größte Unterschied besteht darin, dass, wenn keine Warnung ausgelöst wird oder die Regel nicht anwendbar ist, normalerweise keine Empfehlung bereitgestellt wird.

Datenabschnitte

Datenabschnitte enthalten die Leistungsdaten, die vom Advisor-Paket basierend auf den von den Ziel Servern gesammelten Rohdaten generiert werden. Datenabschnitte enthalten eine Reihe von Abschnitten der obersten Ebene und mehrere Ebenen von Unterabschnitten. Die Abschnitte der obersten Ebene werden als Registerkarten dargestellt. Alle Unterabschnitte in den Abschnitten der obersten Ebene werden in erweiterbaren Bereichen angezeigt. Sie können die einzelnen Abschnitte reduzieren oder erweitern, um den Fokus auf den Interessenbereich zu setzen, wie in der folgenden Abbildung dargestellt.

The screenshot shows a Windows application window titled "Report Viewer". The title bar includes standard buttons for minimize, maximize, and close, along with a "Find:" search bar and navigation buttons for "Previous" and "Next". Below the title bar is a toolbar with icons for "Actions >>" and other report-related functions.

The main content area displays two sections:

- CPU Consumption Details:** A table showing CPU usage statistics. The columns are: Name, CPU ID, Average, Min, Max, and 90%. The rows include various processor and DPC time metrics.

Name	CPU ID	Average	Min	Max	90%
% Processor Time	_Total	8.94	0.00	15.63	14.29
% Processor Time	0_Total	8.94	0.00	15.63	14.29
% Processor Time	0_0	8.94	0.00	15.63	14.29
% Privileged Time	_Total	2.25	0.00	6.35	6.25
% Privileged Time	0_Total	2.25	0.00	6.35	6.25
% Privileged Time	0_0	2.25	0.00	6.35	6.25
% DPC Time	_Total	0.09	0.00	1.59	0.00
% DPC Time	0_Total	0.09	0.00	1.59	0.00
% DPC Time	0_0	0.09	0.00	1.59	0.00
DPC Rate	_Total	1.00	0.00	7.00	2.00
DPC Rate	0_Total	1.00	0.00	7.00	2.00
DPC Rate	0_0	1.00	0.00	7.00	2.00
DPC Queued/sec	_Total	88.00	22.25	139.00	132.00
DPC Queued/sec	0_Total	88.00	22.25	139.00	132.00
DPC Queued/sec	0_0	88.00	22.25	139.00	132.00
Interrupts/sec	_Total	236.05	108.00	342.99	313.60
Interrupts/sec	0_Total	236.05	108.00	342.99	313.60
Interrupts/sec	0_0	236.05	108.00	342.99	313.60

- Top Activities:** A table showing the top 10 processes in terms of average CPU usage (%). The columns are: Process, Process ID, Average, Min, Max, and 90%. The rows list various system processes like plasmav.exe, svchost.exe, lsass.exe, System, and services.exe.

Process	Process ID	Average	Min	Max	90%	Details
plasmav.exe	2,160	7.78	0.00	14.29	14.06	<NULL>
svchost.exe	760	0.51	0.00	1.56	1.56	CertPropSvc, gpssvc, IKEEXT, iplhpsvc, LanmanServer, ProfSvc, Schedule, SENS, SessionEnv, ShellHWDetection, Winmgmt
lsass.exe	452	0.26	0.00	1.56	1.56	SamS
System	4	0.17	0.00	1.56	0.00	<NULL>
services.exe	444	0.00	0.00	0.00	0.00	<NULL>

Das Core OS Spa Advisor Pack und das IIS Spa Advisor Pack enthalten einen Abschnitt **System Übersicht**. Dieser Abschnitt enthält die Informationen der obersten Ebene zur Ressourcenverwendung und-Konfiguration. Andere Abschnitte der obersten Ebene stellen Bereiche von Leistungsdaten dar. Spa zeigt Berichtsdaten auf folgende Weise an:

- Einzelner Wert** Ein Schlüssel-Wert-Paar. Der Schlüssel ist eine Zeichenfolge, die die Bedeutung des Werts darstellt. Der Wert kann eine Zeichenfolge, ein numerischer Wert oder ein boolescher Wert sein. Dies wird häufig verwendet, um statische Informationen wie z. B. die CPU-Architektur, die Gesamtgröße des Arbeitsspeichers und die BIOS-Version anzuzeigen, die sich im Laufe der Zeit nicht ändern.
- Listen Wert** Manchmal handelt es sich um ein Schlüssel-Wert-Paar, aber der Listen Wert kann mehrere Felder enthalten. Beispielsweise kann das-Attribut der CPU in einer Tabelle mit mehreren Spalten und mehreren Zeilen angezeigt werden. Jede Zeile stellt eine CPU dar, und jede Spalte stellt ein Attribut der CPU dar.
- Statistik** Kann als spezieller Typ eines einzelnen Werts angesehen werden. Er darf nur numerische Daten enthalten. Während der Datensammlung schwanken viele der numerischen Datenpunkte und bleiben nicht

konstant. Beispielsweise ändert sich die CPU-Auslastung bei jeder Erfassung des Leistungs Zählers durch das Pla. Die Anzeige nur eines einzelnen Werts kann die leistungssituation nicht exakt widerspiegeln. Anstatt nur einen Wert, den Mittelwert, den Höchstwert, den Minimalwert und den Wert von 90% für solche dynamischen numerischen Datenpunkte anzuzeigen. Der Wert 90% stellt eine Aktivität bei oder oberhalb des 90. Perzentils für alle Ereignisse dieses Zählers in diesem angegebenen Sammlungs Intervall dar.

- **Obere Liste** Enthält normalerweise die häufigsten Consumer einer bestimmten Ressource oder die obersten Entitäten, für die bestimmte Ereignisse auftreten. Die **10 wichtigsten Prozesse in Bezug auf die durchschnittliche CPU-Auslastung** umfassen beispielsweise die zehn wichtigsten Prozesse mit der höchsten durchschnittlichen CPU-Auslastung während der Datensammlung. Da die CPU-Auslastung auch ein dynamischer numerischer Datenpunkt ist, sind andere Statistiken wie Maximum, minimal und 90% ebenfalls in der Liste enthalten, um dem Benutzer ein ausführlichere Bild der CPU-Auslastung zu verschaffen.

Wie in den vorherigen Abschnitten erwähnt, baut Spa auf der Erstellung der etw-Ablauf Verfolgung, WMI-Abfragen, Leistungsindikatoren, Registrierungsschlüssel und Konfigurationsdateien auf, um den Bericht zu generieren. Es ist wichtig, dass Sie die Datenquelle hinter den einzelnen Datenpunkten im Bericht verstehen. Spa stellt Informationen über Quick Infos bereit. Sie können mit dem Mauszeiger auf die Schlüssel Spalten oder Zeilen zeigen, um die QuickInfo für die Datenquelle anzuzeigen. **WMI: Win32_disdrive: Caption** bedeutet beispielsweise, dass die Datenquelle aus einer WMI-Abfrage, der WMI-Klassenname Win32_diskdrive und die-Eigenschaft **Beschriftung**ist.

Paralleler Bericht

Einzelne Berichte stellen Benachrichtigungen und einen Daten Abschnitt bereit, um den Benutzer bei der Suche nach potenziellen Leistungsproblemen zu unterstützen. es ist jedoch oft schwierig, ein mögliches Leistungsproblem zu erkennen, indem Sie einen einzelnen Bericht direkt betrachten. Ein einzelner Bericht kann zu viele Datenpunkte enthalten, wodurch es schwierig wird, potenzielle Probleme zu finden.

Um dieses Problem zu beheben, bietet Spa die Möglichkeit, zwei Berichte zu vergleichen. Sie können einen Bericht mit einem potenziellen Problem mit einem Basisbericht vergleichen, um die Unterschiede zu ermitteln.

Parallele Berichte können von einem Einzel Bericht-Viewer aus gestartet werden. Benutzer können auf **Aktionen**klicken und dann auf **Berichte vergleichen** klicken, um die Berichte auszuwählen. Es ist nur sinnvoll, Berichte desselben Advisor-Pakets zu vergleichen. Sie können den Bericht mit einem vorherigen Bericht in der Zeit, dem nächsten Bericht in der Zeit oder einem beliebigen Bericht vergleichen, der über Suchfunktionen ausgewählt wird. Um z. b. nicht normales Verhalten zu isolieren, können Sie einen Baseline-Server Bericht mit einem Bericht vergleichen, der auf demselben Computer zu einem anderen Zeitpunkt generiert wurde, oder auf einem Bericht, der auf einem anderen Computer mit einer ähnlichen Server Rolle und Last generiert wurde.

Ein paralleler Bericht sieht in etwa wie der einzige Bericht aus. Sie enthält einen Benachrichtigungs Abschnitt und Datenabschnitte. Sie enthält die gleiche Anzahl von Benachrichtigungen und Daten Abschnitten wie die einzelne Bericht Anzeige. Der einzige Unterschied besteht darin, dass die Berichte nebeneinander angezeigt werden. Jeder Abschnitt enthält die Daten aus dem Quell Bericht (Bericht 1) und dem Ziel Bericht (Bericht 2). Der parallele Bericht zeigt den Namen des Advisor-Pakets, den Namen des Zielservers (auf der linken Seite und den Bericht 2 auf der rechten Seite), den Zeitpunkt, zu dem der Bericht generiert wurde, und die Dauer der Datensammlung für die einzelnen Berichte an.

Wenn Sie das Dialogfeld **Suchen** schließen, können Sie es reaktivieren, indem Sie Steuerelement + F eingeben. In diesem Dialogfeld werden Text Zeichenfolgen im aktuellen Abschnitt gefunden und hervorgehoben.

Wenn im Abschnitt Benachrichtigung eine der Ergebnisse aus den zwei verglichenen Berichten eine Warnung ist, wird Sie im **Warnungs** Bereich aufgelistet. Andernfalls werden die Ergebnisse im Bereich **andere Benachrichtigungen** aufgeführt. Da der Schlüssel für einen parallelen Bericht darin besteht, Unterschiede Zwischenberichten zu identifizieren, werden keine detaillierten Informationen zu einer Regel angezeigt. Benutzer können auf den Regel Namen klicken, um das Regel Detail Formular für weitere Informationen zur Regel

anzuzeigen.

In den Daten Abschnitten werden die Daten nebeneinander und Daten aus Bericht 1 auf der linken Seite und Daten aus Bericht 2 auf der rechten Seite angezeigt. Spalten zeigen einzelne Werte in derselben Tabelle an. statt jedoch den Spalten Wert zu bezeichnen, werden Sie als "Report 1" bzw. "Report 2" bezeichnet. Der parallele Bericht zeigt alle anderen Formen von Daten in parallelen Tabellen an.

Die Seite-an-Seite-Bericht Anzeige bietet auch Quick Infos zur Datenquelle.

Vergangenheits-und Trenddiagramme

Es ist nur sinnvoll, Trend- und Vergangenheits Diagramme für einen bestimmten Server und ein bestimmtes Advisor-Pack anzuzeigen. Sie müssen den Zeitbereich auswählen (der Standardwert für die letzte Woche ist), und dann auf OK klicken, um den Trend und den Verlaufs Diagramm-Viewer anzuzeigen.

Der Trend- und Verlaufs Diagramm-Viewer enthält drei Registerkarten: das Verlaufs Diagramm, das 24-Stunden-Trend Diagramm und das 7-tägige Trend Diagramm.

Verlaufs Diagramm

Das Verlaufs Diagramm zeigt eine Reihe von Werten für einen numerischen Datenpunkt über den angegebenen Zeitrahmen an. Beispielsweise die **durchschnittliche Anforderungs Wartezeit** für IIS auf einem einzelnen Server während der letzten 15 Tage. Jeder Datenpunkt in einem Verlaufs Diagramm stellt den Wert einer bestimmten Datenquelle dar, die in einer Leistungsanalyse Sitzung erstellt wurde.

Es gibt mehrere Möglichkeiten, ein Verlaufs Diagramm zu verwenden:

1. Die **durchschnittliche Anforderungs Latenz** von IIS springt von ungefähr 200 ms auf 500 ms, um zu einem bestimmten Zeitpunkt bei einem Daten 2:00 Punkt nach Anomalien zu suchen.
2. Zum Korrelieren mehrerer Datenpunkte. Beispielsweise werden die **durchschnittliche Anforderungs Latenz** und die **durchschnittliche Anforderungs Anzahl** in den letzten 15 Tagen angezeigt. Der Bericht zeigt möglicherweise an, dass die Anforderungs Latenz und die Anzahl der Anforderungen zum gleichen Zeitpunkt zunehmen, was darauf hindeuten kann, dass die Erhöhung der Anforderungs Latenz durch eine Erhöhung der Anforderungs Anzahl verursacht wird.

In einem Verlaufs Diagramm können Benutzer folgende Aktionen ausführen:

- Zeigen Sie mehrere Datenreihen in der Diagrammbereich an. Jede Datenreihe wird als Liniendiagramm im Berichts-Viewer angezeigt. Jedes Liniendiagramm wird automatisch so skaliert, dass es in den Berichts-Viewer passt.
- Fügen Sie der Datenreihen Liste unten im Verlaufs Diagramm-Viewer eine Datenreihe hinzu, oder entfernen Sie Sie.
- Ein- oder Ausblenden von Datenreihen in der Datenreihen Liste. Benutzer können auf eine bestimmte Datenreihe in der Liste klicken, um das entsprechende Liniendiagramm im Diagrammbereich hervorzuheben.
- Vergrößern Sie einen bestimmten Zeitraum, indem Sie den Zeitraum in der Diagramm Fläche auswählen. Zum Verkleinern klicken Sie auf die Schaltfläche, die sich in der unteren linken Ecke des Diagramms befindet.
- Untersuchen Sie einen einzelnen Bericht, indem Sie auf einen bestimmten Datenpunkt doppelklicken.
- Kopieren Sie die Daten, und stellen Sie sie für andere Programme (z. B. Microsoft Excel) zur Verfügung. Dies ermöglicht es Ihnen, bei Bedarf Microsoft Excel-Diagramm Funktionen zu nutzen.

Trend Diagramme

Viele wiederkehrende Leistungsprobleme werden dadurch verursacht, dass regelmäßige Tasks auf oder auf Ziel

Servern ausgeführt werden. Beispielsweise kann eine Unterhaltungs orientierte Website während des Wochenendes mehr Treffer erhalten, oder ein Task "Datenträger Sicherung planen" kann die Leistung eines Servers täglich um 2:00 Uhr senken.

Ein Trend Diagramm ist so konzipiert, dass Sie derartige Leistungsprobleme finden. Leistungsprobleme können wiederholt in verschiedenen Mustern auftreten. Bei den gängigsten Mustern handelt es sich um tägliche Muster und wöchentliche Muster, bei denen Leistungsprobleme während der gleichen Stunde eines Tages oder desselben Tags auftreten. Daher bietet Spa ein 24-Stunden-Trend Diagramm und ein 7-Tage-Trend Diagramm.

Das Trendanalyse Diagramm bietet einen tieferen Grad an Untersuchung zu einem Satz von Daten und sucht nach Trends basierend auf der Tageszeit. Die X-Achse wird auf einen 24-Stunden-Zeitraum festgelegt, beginnend um 0:00 Uhr (Mitternacht) und endet bei 23:59. Spa zeigt nicht gleichzeitig Trends für mehrere Datenreihen an. Sie können auf **Datenreihe auswählen** klicken, um eine Datenreihe zum anzeigen auszuwählen.

Um die Daten zu verarbeiten, sucht Spa nach allen Momentaufnahmen, die für jede Stunde zwischen 0:00 und 0:59 erstellt wurden. Spa bestimmt die minimalen, maximalen, durchschnittlichen und Sigma-Werte für den Satz von Momentaufnahmen, die während dieser Stunde erstellt wurden, und zeigt Diagramme als Kerzen Diagramme an. Spa wiederholt den Prozess für Momentaufnahmen, die zwischen 1:00 und 1:59, dann 2:00 bis 2:59 usw. erstellt wurden. Wenn für die angegebene Stunde keine Momentaufnahmen vorhanden sind, bleibt diese Stunde im Diagramm leer und fährt mit der nächsten Stunde fort.

Ein 7-Tage-Trend Diagramm ähnelt dem 24-Stunden-Trend Diagramm. Der einzige Unterschied besteht darin, dass eine Datenreihe auf der Grundlage des Wochentags und nicht der Stunde des Tages gruppiert wird.

Die Datenreihen, die Sie in Trend-und Vergangenheits Diagrammen auswählen, werden als Benutzereinstellung gespeichert. Wenn der Trend-und Verlaufs Diagramm-Viewer das nächste Mal für das gleiche Advisor-Pack geöffnet wird, wird derselbe Satz von Datenreihen als Standard aufgeführt.

Verwalten von Berichten

Löschen der Berichte

Berichte können entfernt werden, um die Anzahl von Berichten zu minimieren, die von Spa verwaltet werden müssen. Abhängig von der Häufigkeit der Berichte und der Anzahl der Server wird empfohlen, unnötige Berichte zu löschen. Obwohl die Spa nicht über eine Beschränkung für Berichte verfügt, die Sie verwalten kann, kann die zugrunde liegende Datenbank eine Größenbeschränkung aufweisen.

Hinweis gelöschte Berichte können nicht wieder hergestellt werden.

Exportieren und Importieren von Berichten

Berichte können in eine XML-Datei exportiert werden, um Sie in eine andere Spa-Konsole zu transportieren oder an einen anderen Benutzer zu senden. Wenn Sie den Bericht exportieren, wird der Bericht nicht gelöscht. Klicken Sie zum Exportieren des aktuell angezeigten Berichts in der **BerichtsAnzeige** auf **Aktionen**, und klicken Sie dann auf **exportieren**. Wenn Sie mehrere Berichte exportieren möchten, klicken Sie im **Berichts-Explorerauf Mehrfachauswahl aktivieren**, wählen Sie im Auswahlfeld mehrere Berichte aus, und klicken Sie dann auf **exportieren**. Dadurch werden die Berichte im XML-Format in das ausgewählte Zielverzeichnis exportiert.

Ein exportierter Bericht kann in Spa angezeigt werden. importierte Berichte werden der Spa-Datenbank nicht hinzugefügt. Sie sind in erster Linie als XML-Viewer-Anwendung für den exportierten Bericht zu fungieren. Auf dem Server für den importierten Bericht müssen nicht dieselben Advisor-Pakete installiert sein wie die Original-Konsole des exportierten Berichts.

Verwalten von Advisor-Paketen

Spa umfasst Advisor-Pakete für das Haupt Betriebssystem, Hyper-V, Active Directory und IIS. Spa bietet eine offene Architektur zum Entwickeln von Advisor-Paketen mithilfe von SQL. Daher ist es auch für Entwickler von

Drittanbietern möglich, Versionen von Advisor Packs zu erstellen. Es gibt vier Optionen zum Verwalten eines Advisor-Pakets: bereitstellen, anpassen, zurücksetzen oder entfernen.

Neue Ratgeber Pakete bereitstellen

Neue Ratgeber Pakete können von Microsoft oder von Entwicklern, die nicht von Microsoft sind, veröffentlicht werden. Ein Advisor-Pack enthält eine Datei "provisionmetadata.xml" und einen Satz von SQL-Skripts, die die Logik beschreiben.

So stellen Sie ein neues Advisor Pack bereit

1. Kopieren Sie den gesamten Inhalt des Advisor-Pakets unter dem Verzeichnis %sparoot%\APS.
2. Klicken Sie im Hauptfenster auf **Konfiguration**, und klicken Sie dann auf **Advisor Packs konfigurieren**. Das Dialogfeld **Advisor-Pakete konfigurieren** wird geöffnet.

Hinweis Dieses Dialogfeld ähnelt der Seite des Assistenten zum Bereitstellen von **Advisor-Paketen**. Es wird eine Liste von Advisor-Paketen angezeigt, die zur Verwaltung verfügbar sind. Jedes Advisor-Paket in der Liste verfügt über Eigenschaften wie Name, installierte Version, Version und Autor. Name ist der vollständige Name des Advisor-Pakets, und die installierte Version ist die Version dieses Advisor-Pakets, das bereits im Projekt bereitgestellt wurde. Wenn das Advisor-Pack nicht in der aktuellen Datenbank bereitgestellt wird, wird im Textfeld installierte Version **nicht installiert** angezeigt. Das Feld Version gibt die Version dieses Advisor-Pakets an, das unter dem Advisor Packs-Ordner abgelegt wird.

3. Wählen Sie das Advisor-Pack aus der Liste aus. Wenn das Advisor-Paket nicht bereitgestellt wurde oder eine neuere Version im Advisor Packs-Ordner als der in der Datenbank vorhanden ist, wird die Schaltfläche **bereit stellen** aktiviert. Klicken Sie auf "**bereit stellen**".
4. Wenn die Bereitstellung vollständig ist, enthält das Feld **installierte Version** des ausgewählten Advisor-Pakets die neuen Versionsinformationen.

Anpassen von Advisor-Paketen

Spa definiert eine offene Architektur, mit der Benutzer die Advisor-Pakete ändern können. Benutzer können die Advisor Pack-Dateien ändern, indem Sie Schwellenwerte ändern, Schwellenwerte freigeben und Regeln aktivieren bzw. deaktivieren.

Weitere Informationen zum Ändern und Erstellen von Advisor-Paketen finden Sie im [Entwicklungs Handbuch zum Server Performance Advisor Pack](#).

Ändern von Schwellenwerten

In Spa werden Schwellenwerte verwendet, um zu bestimmen, ob die Auslöserbedingung einer Regel erfüllt ist. Die tatsächlichen Schwellenwerte für echte Kunden Szenarien können aufgrund der Arbeitsauslastung, der Hardware Umgebung und der geschäftlichen Anforderungen erheblich variieren. Die Standard Schwellenwerte sind für den aktuellen Benutzer Fall möglicherweise nicht richtig, sodass Spa die Möglichkeit bietet, den vorhandenen Schwellenwert zu ändern.

Sie können Schwellenwerte ändern, indem Sie auf den Regel Namen in einem einzelnen oder einem parallelen Bericht klicken. Oder um alle Regeln eines bestimmten Advisor-Pakets zu verwalten, können Sie die Schwellenwerte im **Konfigurations** Menü ändern.

So ändern Sie einen Schwellenwert

1. Klicken Sie im Menü **Konfiguration** auf **Advisor Packs konfigurieren**, klicken Sie auf den Namen des Advisor-Pakets, das geändert werden soll, und klicken Sie dann auf **Konfigurieren**.

Hinweis Ihnen wird eine Liste aller Regeln angezeigt, die im Advisor-Paket enthalten sind. Das Kontrollkästchen links neben dem Advisor-Paketnamen gibt an, ob die Regel aktiviert ist. Wenn eine Regel deaktiviert ist, wird Sie in allen Berichten ausgeblendet.

2. Klicken Sie auf die jeweilige Regel, die Sie ändern möchten. Das Formular " **Regel Details** " für die ausgewählte Regel wird geöffnet.

Das Formular "Regel Details" enthält ausführliche Informationen zu einer bestimmten Regel. Sie enthält den Namen, die Beschreibung, den Status, mögliche Ergebnisse und Schwellenwerte. Spa unterstützt zwei Arten von Regel Ergebnissen: **Warnung** und **OK**. Für jeden Typ gibt es Empfehlungs Text und eine Empfehlung.

Für einige Regeln sind keine Schwellenwerte definiert. Beispielsweise prüft die **HTTP Keep-Alive** -Regel, ob eine boolesche Einstellung für IIS festgelegt ist. Daher ist die Liste der Schwellenwerte möglicherweise leer. Andernfalls werden alle Schwellenwerte aufgelistet, die von der aktuellen Regel verwendet werden. Eine ausführliche Beschreibung, wie ein Schwellenwert in der Regel verwendet wird, ist als Teil der Beschreibung enthalten.

Wenn das Formular " **Regel Details** " im **Konfigurations** Menü gestartet wird, enthält die Schwellenwert Liste drei Spalten: Name, ursprüngliche Einstellung und Änderungs Einstellung. Wenn Sie über einen einzelnen oder einen parallelen Bericht gestartet wird, werden die Schwellenwerte, die vom Bericht verwendet werden, ebenfalls eingeschlossen. Benutzer können die aktuellen Schwellenwerte ändern, indem Sie den Wert in der Spalte **Änderungs Einstellung** ändern und dann auf **Speichern** klicken, um die Änderungen in der Datenbank zu speichern.

Alle Änderungen, die an Schwellenwerten vorgenommen werden, werden nur auf Berichte angewendet, die nach den Änderungen generiert werden. Vorhandene Berichte sind von diesen Änderungen nicht betroffen.

Freigabe Schwellenwerte

Wenn Sie Ihre Server in ähnlichen Situationen verwalten, können Sie auch denselben Satz von Schwellenwerten verwenden. Mithilfe des **Konfigurations** Menüs können Sie Schwellenwerte für ein bestimmtes Advisor Pack exportieren und importieren. Sie können das jeweilige Advisor-Paket auswählen und dann auf **Konfigurierenklicken**. Die exportierte Schwellenwert Datei hat ein XML-Format.

Beim Importieren eines Schwellenwerts überprüft Spa das XML-Dateiformat und überprüft, ob die Datei mit dem ausgewählten Advisor Pack übereinstimmt. Wenn dies erfolgreich ist, importiert Spa alle Werte aus der Schwellenwert Datei in die aktuelle Projektdatenbank. Ähnlich wie beim vorherigen Szenario mit veränderlichen Schwellenwerten werden alle Schwellenwert Änderungen nur für Berichte wirksam, die in Zukunft generiert werden. Vorhandene Berichte sind nicht betroffen.

Aktivieren oder Deaktivieren von Regeln

Eine Regel kann im Formular " **Regel Details** " aktiviert oder deaktiviert werden. Sie müssen auf **Speichern** klicken, um die vorgenommenen Änderungen beizubehalten. Wenn eine Regel deaktiviert ist, kann Sie nicht in einem der Berichte angezeigt werden. Die zugrunde liegende Geschäftslogik wird jedoch beim Erstellen des Berichts ausgelöst. Wenn Sie also die Regel erneut aktivieren, wird Sie erneut in Berichten angezeigt.

Zurücksetzen von Advisor Packs in den ursprünglichen Zustand

Sie können ein bereitgestelltes Advisor-Paket in der-Datenbank ändern. Mit Ausnahme der Änderung der Schwellenwerte können Sie auch die SQL-Skripts ändern. Spa unterstützt das Ändern von Berichts Metadaten oder das Hinzufügen oder Entfernen von Regeln für ein bereitgestelltes Advisor Pack nicht. Das manuelle Ändern dieser Bereiche kann zu unerwartetem Verhalten führen.

Weitere Informationen zum Ändern eines bereitgestellten Advisor-Pakets finden Sie im [Entwicklungs Handbuch zum Server Performance Advisor Pack](#).

Wenn Sie Änderungen zurücksetzen möchten, die an einem bereitgestellten Advisor-Paket vorgenommen wurden, können Sie das Advisor-Paket zurücksetzen. Dies überschreibt alle SQL-Skripts, die mit dem Advisor-Paket verknüpft sind, und setzt alle Standard Schwellenwerte zurück. Dadurch werden alle vorhandenen Berichte beibehalten.

zum Zurücksetzen des Advisor-Pakets können Sie das Formular **Advisor Packs konfigurieren** verwenden. Sie müssen das Advisor-Paket auswählen, das zurückgesetzt werden soll, und dann auf **Zurücksetzenklicken**.

Advisor-Pakete entfernen

Wenn ein Advisor-Pack nicht mehr benötigt wird, können Benutzer es aus der Datenbank entfernen. Wenn Sie das Advisor-Paket entfernen, werden alle Informationen über das Advisor-Pack aus der Datenbank entfernt, einschließlich der Regeln und Schwellenwerte, aller SQL-Skripts und sämtlicher Berichte. Für keine der Aktionen kann ein Rollback ausgeführt werden.

zum Entfernen des Advisor-Pakets können Sie das Formular **Advisor Packs konfigurieren** verwenden. Wählen Sie das zu entfernende Advisor-Paket aus, und klicken Sie dann auf Aufhebung der Bereitstellung.

Aktualisieren vorhandener Advisor-Pakete

Das Aktualisieren vorhandener Advisor Packs ähnelt dem Zurücksetzen des Advisor-Pakets auf seinen ursprünglichen Zustand. Wenn Sie das Advisor Pack auf eine neuere Version aktualisieren möchten, kopieren Sie das neue Advisor-Paket in den Advisor Pack-Ordner. Ein Advisor-Pack gilt nur dann als Update für ein vorhandenes Advisor Pack, wenn keine Änderung der Berichts Metadaten vorliegt. Der Bericht und die Regel-IDs müssen identisch sein. Andernfalls sollten Sie als zwei verschiedene Advisor-Packs behandelt werden.

Wenn nur Änderungen an der Geschäftslogik und keine Änderungen an der Berichts Metadaten für ein Advisor-Paket vorgenommen werden, sollte eine neue Versionsnummer angegeben werden, z. b. von 1,0 bis 2,0. Wenn sich die Änderung der Berichts Metadaten ändert, sollte dem Advisor-Paket ein anderer vollständiger Name zugewiesen werden. Beispielsweise könnte Microsoft.serverperformanceadvisor.IIS.v1 in Microsoft.serverperformanceadvisor.IIS.v2 geändert werden.

Wenn eine neuere Version des Advisor-Pakets vorhanden ist, füllt die Liste im Formular **Advisor-Pakete konfigurieren** automatisch die **Versions** Spalte mit der neuesten Version des Advisor-Pakets aus. Sie können das Advisor-Paket auswählen und dann auf Zurücksetzen klicken. Das Advisor Pack wird mit der neuen Geschäftslogik und den Schwellenwerten aktualisiert. Alle Berichte für dieses Advisor Pack werden beibehalten.

Verwalten von Servern

Spa stellt grundlegende Funktionen für die Verwaltung von Ziel Servern bereit. Sie können auswählen, ob Sie der Liste der Zielserver neue Server hinzufügen, Server aus der Liste entfernen oder die Hinweise für Server ändern möchten.

So können Sie Server hinzufügen oder entfernen oder Server Informationen ändern

1. Klicken Sie auf das Menü **Konfiguration**, und klicken Sie auf **Server konfigurieren**.
2. In der Liste der Server, die zurzeit in der Projektdatenbank vorhanden sind, ist die letzte Zeile leer. Klicken Sie auf die Zeile, und füllen Sie die Felder aus. Die Felder **Servername** und **Dateifreigabe Speicherort** Ordner sind obligatorisch, und der Servername muss eindeutig sein.
3. Geben Sie für jeden Server in der Spalte "Anmerkung" weitere Server Informationen ein.

Hinweis In diesem Feld wird ein kostenloses Textformat verwendet, sodass Sie es als Beschreibungsfeld verwenden können. Oder verwenden Sie dieses Feld, um die Server zu markieren, damit Sie im Hauptfenster problemlos gefunden werden können, oder zum Gruppieren von Servern, z. b. nach Standort oder Server Rolle.

4. Wenn Sie Spa mit einer großen Anzahl von Servern verwenden möchten, unterstützt Spa ein durch Kommas getrenntes Format (.CSV) für den Import. Die Datei muss mindestens zwei Felder enthalten: **Server**- und **Dateifreigabe Speicherort**. Das dritte Feld, "Anmerkung", ist optional, aber es wird empfohlen, die Server zu organisieren. Sie können die Serverliste auch in eine CSV-Datei exportieren, um das entsprechende Format zu ermitteln oder die Serverkonfiguration zu sichern.

Suchen und Filtern

Wenn Sie mehr als ein paar Server verwalten, bietet Spa grundlegende Unterstützung für die schnelle Suche der

Server im Hauptfenster. Sie können auf die Spaltenüberschrift klicken, um Sie basierend auf dem Servernamen, den Analyseergebnissen, dem aktuellen Task Status oder den Anmerkungen zu sortieren. Sie können auch die Suchfunktion verwenden. In der oberen rechten Ecke des Hauptfenster können Sie eine Zeichenfolge eingeben, nach der gesucht werden soll. Die Liste der Zielservers im Hauptfenster verwendet die Zeichenfolge zum Filtern der Server und zum Anzeigen von Servern mit den Feldern "Name" und "Anmerkung", die die Such Zeichenfolge enthalten.

In der folgenden Abbildung wird gezeigt, wie die Zeichenfolge Dell Server mit der Zeichenfolge Dell oder Servern mit dem Feld "Anmerkung" vergleicht, das Dell enthält.

Server Name	Analysis Result	Current Status	Remark
26-1451J08706	Warning	3/7/2012 6:44:04 PM	Completed at 3/7/2012 6:44:05 PM. DELL SQL
26-1451J08707	Warning	3/7/2012 6:44:36 PM	Completed at 3/7/2012 6:44:36 PM. DELL IIS
26-1451J08708	Warning	3/7/2012 6:44:22 PM	Completed at 3/7/2012 6:44:23 PM. DELL IIS
	<small>Microsoft CoreOS Advisor Pack</small>		
	<small>Microsoft IIS Advisor Pack</small>		
	<small>Microsoft Hyper-V Advisor Pack</small>		

Erweiterte Funktionalität

Arbeiten mit Windows PowerShell-Cmdlets für Spa

Die Spa-Konsole unterstützt die Benutzeroberfläche für die wiederholte Datensammlung. Wenn diese Funktionalität für Ihre Umgebung nicht ausreicht, gibt es Windows PowerShell-Cmdlets, mit denen ein erweiterter Administrator die Datensammlung anpassen kann. Diese Windows PowerShell-Cmdlets ermöglichen Systemadministratoren das automatische Ausführen von Leistungsanalysen auf Ziel Servern und die Verwendung von Spa für den Remote Kundensupport. Systemadministratoren können z. B. Skripts zum Aufrufen von Spa-Cmdlets in bestimmten Zeitintervallen schreiben, um die Leistung der Zielserver in regelmäßigen Abständen zu testen.

Es wird empfohlen, die Anwendung spaconsole.exe zu schließen, bevor Sie diese Cmdlets verwenden.

Bevor Sie Windows PowerShell-Cmdlets ausführen, müssen Sie die Cmdlets auf dem Konsolen Computer registrieren.

So registrieren Sie die Windows PowerShell-Cmdlets

1. Geben Sie an einer Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten den Befehl `registerpsacmdlets.cmd` ein. Die Meldung zum Registrieren von Spa-Cmdlets wird angezeigt.
2. Führen Sie `Spa-PowerShell.cmd` aus. Wenn Sie den Pfad an eine Windows PowerShell-Skriptdatei übergeben, führen Sie die Skripts automatisch aus. Andernfalls wird eine Windows PowerShell-Eingabeaufforderung geöffnet, die zum Ausführen von Windows PowerShell-Cmdlets für das Spa bereit ist.

In der folgenden Tabelle werden die Windows PowerShell-Cmdlets für Spa beschrieben:

CMDLET-NAME	PARAMETER	BESCHREIBUNG
Start-spaanalysis	<p>-Servername Der Name des Zielservers.</p> <p>-Advisorpakcname Vollständiger Name des Advisor-Pakets, das auf dem Server in die Warteschlange gestellt werden soll. Wenn mehrere Pakete zur gleichen Zeit ausgeführt werden sollen, muss der Wert des -Parameters als AP1name, AP2name formatiert werden.</p> <p>-Dauer Dauer für die Datensammlung.</p> <p>-Credential Benutzer Anmelde Informationen für das Konto, mit dem die Datensammlung auf dem Zielserver ausgeführt wird.</p> <p>-SqlInstanceName Der Name der SQL Server Instanz.</p> <p>-SQLDatabaseName Der Name der Spa-Projektdatenbank.</p>	Startet eine Spa-Daten Sammlungs Sitzung auf dem angegebenen Server.
"Ende-spaanalysis"	<p>-SqlInstanceName Der Name der SQL Server Instanz.</p> <p>-SQLDatabaseName Der Name der Spa-Projektdatenbank.</p> <p>-Servername Der Name des Zielservers.</p>	Versucht, eine laufende Spa-Sitzung zu verhindern. Wenn eine Sitzung bereits beendet ist, wird Sie zurückgegeben, ohne etwas zu tun.
Get-spaserver	<p>-SqlInstanceName Der Name der SQL Server Instanz.</p> <p>-SQLDatabaseName Der Name der Spa-Projektdatenbank.</p>	Ruft die Serverliste in der Datenbank ab. Sie gibt eine Liste von Objekten zurück, einschließlich der folgenden Eigenschaften: Name, Status, Dateifreigabe und Anmerkung.
Get-spaadvisorpacks	<p>-SqlInstanceName Name der SQL Server Instanz</p> <p>-SQLDatabaseName Name der Spa-Projektdatenbank</p>	Ruft die Advisor Pack-Liste in der Datenbank ab. Sie gibt eine Liste von Objekten zurück, einschließlich der folgenden Eigenschaften: Name, DisplayName, Author und Version.

Windows PowerShell bietet die Möglichkeit, Anmelde Informationen über verschlüsselte Dateien zu übergeben, um Automatisierungs Szenarios zu ermöglichen. Weitere Informationen zur Verwendung verschlüsselter Dateien zum Übergeben von Anmelde Informationen an ein Cmdlet finden Sie unter [Erstellen von Windows PowerShell-Skripts, die Anmelde Informationen akzeptieren](#).

Automatisieren der Spa-Bericht Sammlung mithilfe von Windows PowerShell

Die folgenden Prozeduren stellen ein Beispiel für das Automatisieren einer Spa-Bericht Sammlung mithilfe der Windows PowerShell-Cmdlets für Spa dar.

Benutzer Anmelde Informationen können mithilfe von Windows PowerShell verschlüsselt und zwischengespeichert werden. Diese Anmelde Informationen werden verwendet, um sich bei Remote Servern anzumelden. Obwohl es sich nicht um die Spa handelt, wird im folgenden Beispiel dieses Verfahren veranschaulicht:

```

$fileName = 'D:\temp\operator.txt'
$userName = 'domainname\operator'

# save credential to file
$(Get-Credential).Password | convertFrom-SecureString | Set-Content $fileName

# load credential from file
$credential = New-Object System.Management.Automation.PsCredential $userName, $(Get-Content $fileName | convertTo-SecureString)

# run command
.\start-SpaAnalysis ServerName: Server1 Credential: $credential
AdvisorPackName:Microsoft.ServerPerformanceAdvisor.CoreOS.V1 10 Duration:10 SqlInstanceName: .\SQLExpress
SqlDatabaseName:SPA8294

```

Bevor Sie diese Datei ausführen können, müssen Sie **Set-ExecutionPolicy RemoteSigned** ausführen.

Sie können Sie mithilfe des folgenden Befehls aus einer Batchdatei ausführen:

```
PowerShell -command "& '.\RunSpa.ps1' "
```

Verwenden von T-SQL zum Generieren von Berichten

Spa-Berichtsdaten können mithilfe von SQL extrahiert werden, um benutzerdefinierte Berichte zu erstellen, die nicht in der Datei "spaconsole.exe" bereitgestellt werden.

der folgende T-SQL-Befehl stellt z. B. eine Top 10-Liste der Server nach CPU für den Zeitraum bereit, der die letzten drei Tage umfasst:

```

select TOP 10
    MachineName,
    AverageCpu
FROM (
    select
        __MachineName MachineName,
        AVG(AverageValue) AverageCpu
    FROM [SPA].[Microsoft.ServerPerformanceAdvisor.CoreOS.V1].vwCpuPerformance
    WHERE __Creationtime > dateadd(DAY, -3, GETUTCDATE())
        AND Name = N'% Processor time' AND CpuId = N'_Total'
    GROUP BY __MachineName
) t
ORDER BY t.AverageCpu DESC

```

Arbeiten mit mehreren Projekten

In einigen Fällen möchten Sie möglicherweise die von Spa verwendeten SQL Server Datenbanken partitionieren. Dies kann dazu beitragen, die Datengröße der SQL Server Datenbank zu reduzieren oder die Server logisch zu partitionieren. In diesen Fällen werden von der Spa-Konsole mehrere Projekte unterstützt. Sie können eine neue Projektdatenbank erstellen, indem Sie auf **Datei** und dann auf **Neues Projekt** klicken. Der Assistent zum ersten Mal wird zum Erstellen der neuen Projektdatenbank angezeigt.

Nachdem die Projekte erstellt wurden, können Sie auf **Datei** und dann auf **Projekt öffnen** klicken, um zwischen Projekten zu wechseln. Die Spa-Konsole lässt das Wechseln von Datenbanken nicht zu, wenn eine ausstehende Leistungsanalyse innerhalb des aktuell geöffneten Projekts ausgeführt wird. Dies dient zum Schutz der Integrität der Leistungsdaten.

Wenn Sie eine neue Projektdatenbank erstellen oder eine andere Projektdatenbank öffnen, wird das aktuelle Projekt geschlossen. Alle geöffneten Berichte werden geschlossen, wenn das aktuelle Projekt geschlossen wird.

Hinweis SQL Server 2008 R2 Express hat eine Daten Bank Beschränkung von 10 GB. Wenn Sie mehrere Projekte

verwenden, können Sie eine oder mehrere SQL Server Datenbanken verwenden und unter dem Limit von 10 GB SQL Server 2008 R2 Express bleiben.

Protokollierung und Debugging

Spa stellt grundlegende Protokollierungsfunktionen bereit. Es können nur Protokolle in eine Protokolldatei geschrieben werden, die sich im selben Ordner wie "spaconsole.exe" befindet. Das Benutzerkonto, in dem die Spa-Konsole ausgeführt wird, muss über die Berechtigung Schreiben für den Ordner verfügen, in dem Spa installiert wurde, um sicherzustellen, dass die Protokolle in die Protokolldatei geschrieben werden können.

Spa enthält die folgenden gültigen Protokoll Ebenen:

- **Information** Sichert Protokolle für jede Aktion, die von der Spa-Konsole ausgeführt wird, und ist in erster Linie für Debugzwecke konzipiert.
- **Warnung** Protokolliert alle Fehler und Ausnahmen, die innerhalb der Spa-Konsole auftreten. Einige der Fehler sind einfach Validierungs Fehler, die von der Spa-Konsole behandelt werden können.
- **Kritisch** Protokolliert nur Fehler und Ausnahmen, die von der Spa-Konsole nicht behandelt werden können. Diese Fehler verursachen einen Absturz der Spa-Konsole. Die Protokolle stellen die Kontextinformationen zu solchen Fehlern bereit.

Standardmäßig ist die Protokollebene "Warnung", was bedeutet, dass die Spa nur Fehler und Ausnahmen protokolliert, die in Spa auftreten. Die Protokollebene kann geändert werden, indem die Datei " spaconsole.exe.config " im selben Ordner wie "spaconsole.exe" bearbeitet wird. Alle Protokolle werden in die Datei log.txt in demselben Ordner geschrieben.

Spa bietet auch einige grundlegende Funktionen für das Debuggen. Um das Debuggen für Spa zu aktivieren, müssen Benutzer die Spa-Projektdatenbank manuell ändern. Die Einstellung wird in einer Konfigurations Tabelle gespeichert. Der Benutzer muss das folgende SQL-Skript ausführen, um das Spa-Projekt in den Debugmodus zu ändern:

```
UPDATE [Configurations] SET Value = N'true' WHERE Name = N'Debugmode'.
```

Im Debugmodus behält das Spa-Framework alle temporären Daten bei, die während der Leistungsanalyse generiert werden, damit Sie Probleme in den Advisor-Paketen beheben können. Dieses Skript ist hauptsächlich für die Verwendung durch Advisor Pack-Entwickler konzipiert.

Weitere Informationen zu den Debuggingfunktionen in Spa finden Sie im [Entwicklungs Handbuch zum Server Performance Advisor Pack](#).

Verwalten der Datenbank

Sichern und Wiederherstellen der Datenbank

Die Spa-Konsole stellt keine Funktionen zum Sichern und Wiederherstellen der Spa-Datenbank bereit. Zum Sichern und Wiederherstellen von Datenbanken sollten Sie standardmäßige Microsoft SQL Server Tools und Skripts verwenden.

Bereinigen der Datenbank

Die Größe der Spa-Projekt Datenbanken kann zunehmen, wenn eine höhere Leistungsanalyse ausgeführt wird. Standardmäßig speichert Spa alle Berichte. Möglicherweise möchten Sie alte Berichte entfernen, um die Leistung zu verbessern. Berichte können über die Benutzeroberfläche des **Berichts-Explorers** gelöscht werden.

Datenschutz und Sicherheit

Spa unterstützt nur die Datensammlung von Ziel Servern zur Spa-Konsole. Es ist nicht darauf ausgelegt, Informationen an Microsoft-oder nicht-Microsoft-Entwickler zu senden. Weitere Informationen zum Datenschutz in

Spa finden Sie in den Microsoft-Software-Lizenzbedingungen für den Server Performance Advisor.

Alle Daten, die von Spa gesammelt werden, werden in den Projekt Datenbanken gespeichert. Aufgrund der Art einiger etw-Ablauf Verfolgungen kann Spa vertrauliche Informationen erfassen, die eine hohe geschäftliche Wichtigkeit aufweisen können. Sie sollten sich über das potenzielle Risiko im Zusammenhang mit der Freigabe des Zugriffs auf die Spa-Projekt Datenbanken im klaren sein. Temporäre Protokolldateien werden in den freigegebenen Ordner gespeichert, die auf den einzelnen Bereitstellungs Ziel Computern angegeben werden. Obwohl Spa versucht, diese temporären Protokolldateien zu löschen, wenn der Datenimport abgeschlossen ist, gibt es keine Garantie dafür, dass diese Protokolldateien immer gelöscht werden. Stellen Sie sicher, dass sich die freigegebenen Ordner an sicheren Orten befinden.

Spa Advisor Packs enthalten SQL-Skripts zum Analysieren und Analysieren von Leistungs Berichten zum Generieren von Leistungs Berichten. Spa versucht, die Berechtigung einzuschränken, unter der diese Skripts ausgeführt werden. Es besteht jedoch weiterhin die Möglichkeit, dass die Skripts vertrauliche Informationen über die Spa von den Ziel Servern sammeln oder vertrauliche Informationen abrufen oder ändern können, die in derselben Spa-Projektdatenbank gespeichert sind. Sie müssen sicherstellen, dass alle Advisor-Pakete, die in der Spa-Projektdatenbank bereitgestellt werden, aus vertrauenswürdigen Quellen stammen.

Fehler und Problembehandlung

"Spaconsole. exe" startet oder schreibt die Protokolldatei nicht.

Wenn Sie versuchen, "spaconsole. exe" zum ersten Mal auszuführen, wenn die .NET Framework nicht installiert ist, wird die Protokolldatei von der Anwendung nicht gestartet oder geschrieben. Stellen Sie sicher, dass ein compatible.NET-Framework installiert ist und ordnungsgemäß funktioniert, bevor Sie Spa starten.

Suchen von Protokollinformationen

Spa speichert Fehlerinformationen in der Datei log. txt im Ordner Spa. ausführliche Fehlermeldungen und Informationen zur aufrufsstapel werden in diesen Ordner geschrieben. Wenn Fehler auftreten, die weitere Informationen zur Interpretation benötigen, können Sie die Datei "Log. txt" öffnen, um die Fehlerdetails anzuzeigen.

Einschränkungen der Datenbankgröße für SQL Server Express

SQL Server Express hat für eine Benutzerdatenbank eine Größenbeschränkung von 10 GB. Diese Datenbankgröße verfügt über die Kapazität, 20.000 30.000 Berichte zu speichern. Um die Wahrscheinlichkeit zu verringern, dass das Daten Bank Limit erreicht wird, empfiehlt es sich, Berichte regelmäßig zu löschen und/oder eine andere Version von SQL Server zu verwenden, die nicht die 10-GB-Einschränkung der Benutzerdatenbank

SQL Server Express Protokoll Größe und Datenträger Kapazität

Wenn Sie SQL Server Express verwenden, ist die Benutzerdatenbank auf 10 GB beschränkt, aber die zugehörige Protokolldatei kann 70 GB überschreiten. Aus diesen Gründen empfehlen wir 100 GB oder mehr freien Speicherplatz für SQL Server Express. Dieser Speicherplatz muss ausreichen, um ca. 20.000 bis 30.000 Berichte zu speichern. Diese Protokolldatei hat den Namen spadb_Log. ldf und befindet sich unter % Program Files%\Microsoft SQL Server\MSSQL10. SQLExpress\MSSQL-\Daten.

Fehler beim Herstellen einer Verbindung mit dem Zielserver.

Wenn Sie die Leistungsanalyse auf Ziel Servern ausführen, benötigt das Benutzerkonto, unter dem die Spa-Konsole ausgeführt wird, bestimmte Berechtigungen, um den Datensammler auf den Ziel Servern in die Warteschlange des Datensammler Satzes zu setzen. Die Windows-Firewall-Einstellungen müssen auch geändert werden, damit die Pla-Kommunikation durchlaufen werden kann. Ausführliche Konfigurations Anweisungen finden Sie unter [Einrichten von Spa](#).

Fehler beim Erstellen des Pla-Daten Sammlungs Satzes auf dem Zielserver.

Wenn Sie die Meldung zum Erstellen eines Daten Sammlungs Satzes auf dem Zielserver nicht erstellen können, stellen Sie sicher, dass Sie die folgenden Schritte ausführen:

- Stellen Sie sicher, dass die **Leistungs Protokolle & Warnungs Dienst** ausgeführt werden.
- Die Sicherheitseinstellung **Netzwerk Zugriff: keine Speicherung von Kenn Wörtern und Anmelde Informationen für die Netzwerk Authentifizierung zulassen** ist deaktiviert. Die Sicherheitseinstellung muss deaktiviert werden, da Spa die Benutzer Anmelde Informationen verwenden muss, um den Daten Sammlungs Satz auf dem Zielserver zu erstellen.

Ausführen von Spa mit der Konsole

Die Pla durchläuft einen anderen Channel, wenn der Zielserver mit der Spa-Konsole identisch ist. Auch wenn für das Benutzerkonto die Spa-Konsole mit Administratorrechten ausgeführt wird, schlägt die Ausführung von Pla fehl. Wenn die Spa-Konsole auf einem Zielserver installiert ist, müssen die Benutzer die Spa als Administrator starten, um sicherzustellen, dass die Leistungsanalyse Aufgabe in der Konsole ausgeführt werden kann.

Gleichzeitig Ausführen mehrerer Konsolen

Spa unterstützt nicht mehrere Konsolen, die gleichzeitig für dieselbe Spa-Projektdatenbank ausgeführt werden. Spa bietet auch keine Sperr- und Synchronisierungs Mechanismen, um die Ausführung zu verhindern. Wenn zwei Spa-Konsolen gleichzeitig ausgeführt werden, verhält sich die Konsole in Abhängigkeit von der Zeitsequenz, in der diese Spa-Konsolen ausgeführt werden, inkonsistent. Um dies zu verhindern, sollten alle in der Warteschlange befindlichen Leistungsanalyse Sitzungen aus der Liste entfernt werden, bevor Sie von der-Konsole verarbeitet werden, die die Analyse startet.

Spa schützt die Integrität der einzelnen Berichte, die von Spa erfolgreich generiert wurden. Gleichzeitig garantiert Spa nicht, dass alle in der Warteschlange befindlichen Analyseaufgaben abgeschlossen sind. Wenn inkonsistente Statusänderungen für Leistungsanalyse Sitzungen oder Fehler angezeigt werden, die behaupten, dass das System keine Leistungs Protokolle finden kann, die vom Datensammler Satz generiert werden, wird es wahrscheinlich durch mehrere Spa-Konsolen Instanzen verursacht, die für denselben Spa-Projektdatenbank.

Das Ausführen von Windows PowerShell-Cmdlets für Spa kann auch von einer Spa-Konsole beeinflusst werden, die für dieselbe Spa-Datenbank ausgeführt wird. Es wird empfohlen, dass Sie die Spa-Konsole schließen, bevor Sie die Windows PowerShell-Cmdlets für Spa ausführen.

Die wiederkehrende Sammlung "spaconsole.exe" wird unterbrochen.

Wenn Sie "spaconsole.exe" ausführen und eine wiederholte Datensammlung (z. b. eine stündliche Sammlung) verwenden, sollte sich der Server, auf dem die Datei "spaconsole.exe" ausgeführt wird, nicht im Energiesparmodus befinden, sodass er angehalten werden kann. Spa prüft nicht, ob eine Energiespar Richtlinie verwendet wird. Diese angehaltene Aktivität kann die reguläre wiederkehrende Datensammlung stören.

Verlorene ETW-Ereignisse

Um minimale Auswirkungen auf die Leistung auf Ziel Servern zu erzielen, ist die Ausführung von Pla mit niedriger Priorität geplant, während Leistungsinformationen gesammelt werden. Wenn der Zielserver ausgelastet ist, können Sie einige der Daten Sammlungs Tasks löschen, um Sie für Aufgaben mit hoher Priorität, die auf Ziel Servern ausgeführt werden, zu erzielen. Sie sollten das Einrichten des freigegebenen Ordners in Erwägung nehmen, in dem die Ereignisse auf einem Datenträger geschrieben werden, der keinen Konflikt mit der e/a-Auslastung der Arbeitsauslastung oder einem schnelleren Laufwerk (z. b. SSD) hat. Wenn Ereignisse gelöscht werden, werden Sie in der Berichtsansicht angezeigt, da verlorene Ereignisse die Zuverlässigkeit der generierten Leistungsmetriken beeinträchtigen können.

Bestimmte Berechtigungsprobleme können auch bewirken, dass Registrierungs- oder WMI-Abfragen übersprungen werden. Dies ist jedoch weitaus weniger wahrscheinlich als bei einem ETW-Ereignis Verlust. Folglich enthalten die Ergebnisse des Datensammler Satzes manchmal nicht alle angeforderten Werte. Sie müssen sicherstellen, dass die Situation von den T-SQL-Skripts für alle Advisor Packs behandelt wird. Wenn die Daten im Daten Sammlungs Ergebnis nicht vorhanden sind, werden Sie in den Berichten als keine Daten gekennzeichnet.

Da der ETW-Ereignis Verlust bei Pla häufig auftritt, sind Datenpunkte, die basierend auf einer etw-Ablauf Verfolgung generiert werden, möglicherweise nicht konsistent mit Datenpunkten, die basierend auf, z. b.

Leistungsindikatoren, generiert werden. Beispielsweise ist es möglich, zu sehen, dass die CPU-Gesamtauslastung durch IIS 80% beträgt (was aus Leistungsindikatoren stammt) und dass die Top-URLs nur 10% der gesamten CPU-Zeit (ein Datenpunkt, der aus der etw-Ablauf Verfolgung stammt) verwenden. Normalerweise kann die Datenquelle für einen Datenpunkt über die QuickInfo des Daten Punkts angezeigt werden. Sie sollten sich über die Auswirkungen dieses Daten Verlusts im klaren sein.

Um derartige Ereignis Verluste zu vermeiden, sollte der Ergebnis Ordner auf dem Zielserver geschlossen werden.

Wenn die Ergebnisse des Daten Sammlers unvollständige Daten als etw-Ablauf Verfolgungs Verlust enthalten und der Advisor Pack-Entwickler Unterstützung für die Benachrichtigung über etw-Ereignis Verlust hinzugefügt hat, wird eine Informationsleiste oberhalb des einzelnen Berichts angezeigt, um den Benutzer über die potenziell Inkonsistenter Bericht aufgrund eines Daten Verlusts. Ausführliche Informationen zum Datenverlust finden Sie in der Datei "Log.txt".

Glossar

Im folgenden finden Sie einige der in Spa verwendeten Begriffe:

- **Advisor-Pack** Eine Auflistung von Metadaten und T-SQL-Skripts, mit denen die vom Zielserver gesammelten Leistungs Protokolle verarbeitet werden. Das Advisor-Pack generiert dann Berichte aus den Leistungs Protokolldaten. Die Metadaten im Advisor-Pack definieren die Daten, die vom Zielserver für Leistungsmessungen gesammelt werden sollen. Die Metadaten definieren auch den Satz von Regeln, die Schwellenwerte und das Berichtsformat. In den meisten Fällen wird ein Advisor-Pack speziell für eine einzelne Server Rolle geschrieben, z. b. Internetinformationsdienste (IIS).
- **Spa-Konsole** Spaconsole.exe, das zentrale Teil der Spa. Die Spa muss nicht auf dem Zielserver ausgeführt werden, den Sie testen. Die Spa-Konsole enthält alle Benutzeroberflächen für Spa, von der Einrichtung des Projekts bis hin zur Ausführung von Analysen und Anzeigen von Berichten. Das Spa ist eine Anwendung mit zwei Ebenen. Die Spa-Konsole enthält die UI-Schicht und einen Teil der Geschäftslogik Ebene. Die Spa-Konsole plant und verarbeitet Leistungsanalyse Anforderungen.
- **Spa-Framework** Bietet alle Benutzeroberflächen, die Verarbeitung von Leistungs Protokollen, die Konfiguration, die Fehlerbehandlung und Datenbank-APIs sowie Verwaltungs Prozeduren.
- **Spa-Projekt** Eine Datenbank, die alle Informationen zu den Ziel Servern, Advisor Packs und Leistungsanalyse Berichten enthält, die auf den Ziel Servern für die Advisor-Pakete generiert werden. Sie können Verlaufs-und Trenddiagramme innerhalb desselben Spa-Projekts vergleichen und anzeigen. Sie können mehr als ein Projekt erstellen. Die Spa-Projekte sind voneinander unabhängig, und es gibt keine Daten, die von allen Projekten gemeinsam genutzt werden.
- **Zielserver** Der physische oder virtuelle Computer, auf dem Windows Server mit bestimmten Server Rollen (z. b. IIS) ausgeführt wird.
- **Datenanalyse Sitzung** Eine Leistungsanalyse auf einem bestimmten Zielserver. Eine Datenanalyse Sitzung kann mehrere Advisor-Pakete enthalten. Die Datensammler Sätze aus diesen Advisor-Paketen werden zu einem einzelnen Datensammler Satz zusammengeführt. Alle Leistungs Protokolle für eine einzelne Datenanalyse Sitzung werden innerhalb desselben Zeitraums gesammelt. Das Analysieren von Berichten, die von Advisor-Paketen generiert werden, die in derselben Datenanalyse Sitzung ausgeführt werden, kann Benutzern helfen, die Gesamtleistung zu verstehen und die Ursachen für Leistungsprobleme zu identifizieren.
- **Ereignis Ablauf Verfolgung für Windows** Ein leistungsfähiges, skalierbares, skalierbares Ablauf Verfolgungssystem, das in Windows bereitgestellt wird. Es bietet Profil Erstellungs- und Debuggingfunktionen, die zur Problembehandlung für eine Vielzahl von Szenarien verwendet werden können. Spa verwendet ETW-Ereignisse als Datenquelle zum Erstellen von Leistungs Berichten. Allgemeine Informationen zu etw finden Sie unter verbessertes [Debugging und Leistungsoptimierung mit etw](#).

- **Windows-Verwaltungsinstrumentation (WMI)** Die Infrastruktur für Verwaltungsdaten und-Vorgänge in Windows. Sie können WMI-Skripts oder-Anwendungen schreiben, um administrative Aufgaben auf Remote Computern zu automatisieren. WMI stellt auch Verwaltungsdaten für andere Teile des Betriebssystems und für Produkte bereit. Spa verwendet WMI-Klassen Informationen und Datenpunkte als Quellen zum Erstellen von Leistungs Berichten.
- **Leistungsindikatoren** Wird verwendet, um Informationen darüber bereitzustellen, wie gut das Betriebssystem, die Anwendung, der Dienst oder der Treiber ausgeführt wird. Die Leistungsdaten können Ihnen helfen, Engpässe im System zu ermitteln und die System-und Anwendungsleistung zu optimieren. Das Betriebssystem, das Netzwerk und die Geräte bieten Leistungsdaten, die von einer Anwendung genutzt werden können, um Benutzern eine grafische Ansicht der Leistung des Systems zu bieten. Die Spa verwendet Leistungsdaten und Datenpunkte als Quellen zum Generieren von Leistungs Berichten.
- **Leistungsprotokolle und-Warnungen (PLA)** Sammelt Leistungs Protokolle und Ablauf Verfolgungen und löst Leistungs Warnungen aus, wenn bestimmte Trigger erfüllt sind. Mithilfe von Pla können Leistungsindikatoren, Ereignis Ablauf Verfolgung für Windows (ETW), WMI-Abfragen, Registrierungsschlüssel und Konfigurationsdateien erfasst werden. Außerdem unterstützt die Verwendung von Remote Prozedur aufrufen (RPC) die Remote Datensammlung. Der Benutzer definiert einen Datensammler Satz, der Informationen über die zu sammelnden Daten, die Häufigkeit der Datensammlung, die Dauer der Datenerfassung, Filter und einen Speicherort zum Speichern der Ergebnissedateien enthält. Spa sammelt mithilfe von PLA alle Leistungsdaten von den Ziel Servern.
- **Einzelner Bericht** Ein Spa-Bericht, der auf der Grundlage einer Datenanalyse Sitzung für ein Advisor Pack auf einem einzelnen Zielserver generiert wird. Es kann Benachrichtigungen und verschiedene Datenabschnitte enthalten.
- **Paralleler Bericht** Ein Spa-Bericht, in dem zwei einzelne Berichte für dasselbe Advisor Pack verglichen werden. Die beiden Berichte können von verschiedenen Ziel Servern oder von separaten Leistungsanalysen auf demselben Zielserver generiert werden. Der parallele Bericht erstellt die Funktion zum Vergleichen von zwei Berichten, damit Benutzer ungewöhnliche Verhalten oder Einstellungen in einem der Berichte identifizieren können. Ein paralleler Bericht enthält Benachrichtigungen und verschiedene Datenabschnitte. In jedem Abschnitt werden die Daten aus beiden Berichten nebeneinander aufgelistet.
- **Trend Diagramm** Ein Spa-Bericht, der verwendet wird, um wiederkehrende Muster von Leistungsproblemen zu untersuchen. Viele sich wiederholende Leistungsprobleme werden durch geplante Server Lade Änderungen vom Server oder von Client Computern verursacht, die täglich oder wöchentlich auftreten können. Spa bietet ein 24-Stunden-Trend Diagramm und ein 7-Tage-Trend Diagramm, um diese Probleme zu identifizieren.

Der Benutzer kann eine oder mehrere Datenreihen gleichzeitig auswählen, wobei es sich um einen numerischen Wert innerhalb des einzelnen Berichts handelt, z. b. die **durchschnittliche CPU-Gesamtauslastung**. genauer gesagt handelt es sich bei einem numerischen Wert um einen skalaren Wert von einem einzelnen Server, der von einem einzelnen AP-Wert zu einer bestimmten Zeit Instanz generiert wird. Spa gruppiert diese Werte in 24 Gruppen, eine für jede Stunde des Tages (sieben für einen 7-tägigen Bericht, eine für jeden Tag der Woche). Spa berechnet durchschnittliche, minimale, maximale und standardmäßige Abweichungen für jede Gruppe.

- **Verlaufs Diagramm** Ein Spa-Bericht, der verwendet wird, um Änderungen an bestimmten numerischen Werten in einzelnen Berichten für ein bestimmtes Server-und Advisor Pack-Paar im Zeitverlauf anzuzeigen. Der Benutzer kann mehrere Datenreihen auswählen und diese zusammen im Verlaufs Diagramm anzeigen, um die Korrelation zwischen verschiedenen Datenreihen nachzuvollziehen.
- **Datenreihe** Numerische Daten, die über einen bestimmten Zeitraum aus derselben Datenquelle gesammelt werden. Dieselbe Quelle bedeutet, dass die Daten vom gleichen Zielserver stammen müssen, z. b. die durchschnittliche Länge der Anforderungs Warteschlange für IIS auf einem Server.

- **Regeln** Kombinationen aus Logik, Schwellenwerten und Beschreibungen. Sie stellen ein mögliches Leistungsproblem dar. Jedes Advisor-Paket enthält mehrere Regeln. Jede Regel wird durch einen Bericht Generierungsprozess ausgelöst. Eine Regel wendet die Logik und die Schwellenwerte auf die Daten in einem einzelnen Bericht an. Wenn die Kriterien erfüllt sind, wird eine Warnmeldung ausgelöst. Wenn dies nicht der Wert ist, wird die Benachrichtigung auf den Status **OK** festgelegt. Wenn die Regel nicht angewendet wird, wird die Benachrichtigung auf den Status nicht zutreffend (**na**) festgelegt.
- **Benachrichtigungen** Informationen, die von einer Regel für Benutzer angezeigt werden. Sie enthält den Status der Regel (**OK**, **na** oder eine **Warnung**), den Namen der Regel und mögliche Empfehlungen, um die Leistungsprobleme zu beheben.

Server Performance Advisor Pack-Entwicklungsleitfaden

15.01.2020 • 79 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 8, Windows 10

In diesem Entwicklungs Leit Faden für Microsoft Server Performance Advisor (Spa) finden Sie Richtlinien, die Entwicklern und Systemadministratoren bei der Entwicklung von Advisor Packs zur Analyse der Server Leistung helfen.

Dabei wird davon ausgegangen, dass Sie mit Leistungsprotokolle und-Warnungen (PLA), Leistungsindikatoren, Registrierungs Einstellungen, Windows-Verwaltungsinstrumentation (WMI), Ereignis Ablauf Verfolgung für Windows (ETW) und Transact SQL (T-SQL) vertraut sind.

Weitere Informationen zur Verwendung von Spa finden Sie [im Benutzerhandbuch für den Server Performance Advisor](#).

Übersicht über das Spa Advisor Pack

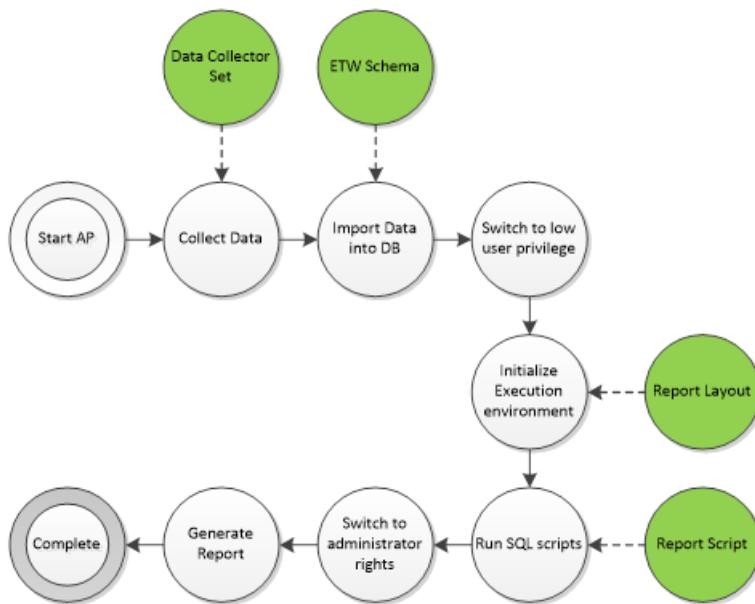
Ein Advisor Pack ist in der Regel für eine bestimmte Server Rolle konzipiert und definiert Folgendes:

- Daten, die über die Pla gesammelt werden sollen, einschließlich Windows-Verwaltungsinstrumentation (WMI), Leistungsindikatoren, Registrierungs Einstellungen, Dateien und Ereignis Ablauf Verfolgung für Windows (ETW)
- Regeln, die Warnungen und Empfehlungen anzeigen
- Daten, die angezeigt werden sollen (gesammelte Rohdaten, aggregierte Daten oder Top 10-Listen)
- Statistik zum Anzeigen eines Werts, der sich im Laufe der Zeit ändert
- Statistik Werte, für die ein Trend durchgeführt werden kann

Ein Advisor-Pack umfasst die folgenden Elemente:

- **XML-Metadaten** ("provisionmetadata.xml")
 - [Leistungsprotokolle und-Warnungen \(PLA\)](#) -Datensammler Satz
 - Berichtslayout
- **SQL-Skripts**
 - Eine gespeicherte Haupt Prozedur
 - SQL-Objekte, z. b. gespeicherte Prozeduren und benutzerdefinierte Funktionen
- **Etw-Schema Datei** (Schema.man) Dies ist optional.

Advisor Pack-Workflow



In diesem Flussdiagramm stellen die grünen Kreise Advisor-Pakete dar. Alle anderen Kreise stellen die Phasen dar, die im Rahmen des Spa-Frameworks ausgeführt werden. Spa verwendet ein Advisor Pack zum Sammeln von Daten, Importieren der Daten in die Datenbank, Initialisieren der Ausführungsumgebung und Ausführen von SQL-Skripts.

Sammeln von Daten

Wenn ein Advisor-Pack mithilfe von Spa für einen bestimmten Server in die Warteschlange eingereiht wird, fragt das Daten Sammlungsmodul den Datensammler Satz-XML-Code aus dem Advisor Pack ab und sammelt Daten vom Zielserver. Die Rohdaten werden in einer benutzerdefinierten Dateifreigabe gespeichert. Die Datensammlung wird erst beendet, wenn die vom Benutzer festgelegte Spa-Ausführungsduer überschritten wurde.

Importieren von Daten in die Datenbank

Nachdem die Datensammlung abgeschlossen ist, wird jeder Datentyp in eine entsprechende Tabelle in der SQL Server-Datenbank importiert. Registrierungs Einstellungen werden z. b. in eine Tabelle namens "#RegistryKeys" importiert.

zum Importieren der etw-Datei ist eine ETW-Schema Datei zum Decodieren der ETL-Datei erforderlich. Die ETW-Schema Datei ist eine XML-Datei. Sie kann mithilfe von tracerpt. exe generiert werden, das in Windows enthalten ist. Die ETW-Schema Datei ist nur erforderlich, wenn das Advisor-Paket etw-Daten importieren muss.

Zu niedrigen Benutzerrechten wechseln

Das Spa-Framework passt die Berechtigungen automatisch an, um die erforderliche Sicherheits Zugriffsebene zu minimieren. Da Advisor Packs von jedem Benutzer entwickelt oder geändert werden können, ist es möglich, dass ein Advisor-Pack manipulierte SQL-Skripts enthält. Um das Sicherheitsrisiko zu verringern, sollte jedes SQL-Skript für ein Advisor-Pack mit niedrigen Benutzerrechten ausgeführt werden. Sie kann nur auf eingeschränkte Datenbankobjekte zugreifen, z.b. temporäre Tabellen und Spa-APIs, die als gespeicherte Prozeduren verfügbar gemacht werden. Die SQL-Skripts in einem Advisor-Pack können diese gespeicherten Prozeduren zum interagieren mit dem Spa-Framework aufruft.

Ausführungsumgebung initialisieren

Advisor Packs können unterschiedliche Arten von Ausgaben generieren, z. b. Benachrichtigungen, Empfehlungen, Fakten Tabellen, Statistiken und Diagramme für Statistiken. Die SQL-Skripts führen bestimmte Berechnungen für die gesammelten Daten aus. Die Ergebnisse der Ergebnisse werden in temporären Tabellen über öffentliche Spa-APIs gespeichert. In der Initialisierungsphase müssen diese temporären Tabellen und anderen Systemressourcen bereitgestellt werden.

SQL-Skripts ausführen

Es gibt eine Haupt gespeicherte Prozedur, die vom Advisor Pack-Entwickler benannt wird. Das Spa-Framework ruft diese gespeicherte Prozedur auf, um die Berechnung zu initiieren. Die gespeicherte Prozedur verwendet die gesammelten Daten und kommuniziert das Endergebnis an das Spa-Framework.

Zu Administratorrechten wechseln

Zum Generieren eines Berichts sind Administrator Rechte erforderlich. Die Bericht Generierung wird vollständig von Spa gesteuert. Es ist weniger wahrscheinlich, manipuliert zu werden.

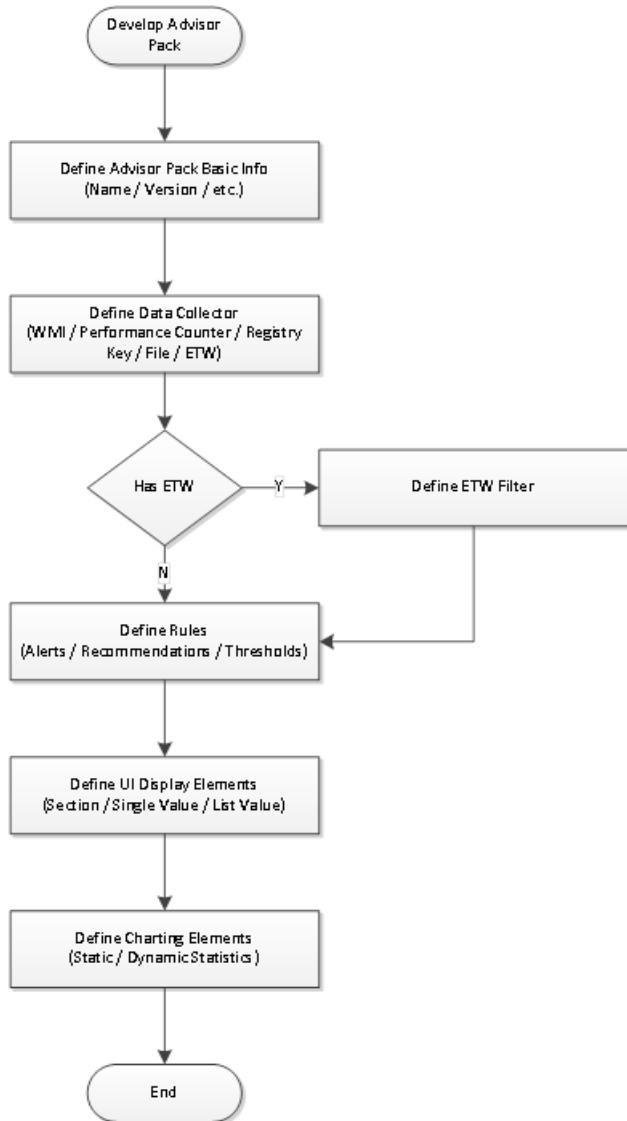
Generieren eines Berichts

Bevor die gespeicherte Haupt Prozedur für ein Advisor Pack abgeschlossen wird, werden alle berechneten Ergebnisse, wie z. b. Benachrichtigungen und Statistiken, nicht beibehalten. In dieser Phase überträgt das Spa-Framework die Endergebnisse aus temporären Tabellen auf Tabellen in einem bestimmten Format. Nachdem diese Phase fertiggestellt wurde, können Sie die Berichte mithilfe der Spa-Konsole anzeigen.

Erstellen eines Advisor-Pakets

Schnelle Richtlinien

Im folgenden Flussdiagramm werden die Schritte beschrieben, mit denen Sie ein voll funktionsfähiges Advisor Pack entwickeln können. Dieser Abschnitt enthält auch schrittweise Anleitungen zur besseren Erläuterung der einzelnen Schritte.



Ein Advisor-Pack ist normalerweise wie folgt strukturiert:

Advisor-Pack

"Provisionmetadata.xml"

Scripts

Main. SQL

Func. SQL

Schema. man

Jedes Advisor-Paket muss über eine Datei namens "provisionmetadata.xml" verfügen. Es definiert grundlegende Advisor-Paketinformationen, die zu sammelnden Daten, Benachrichtigungen und Regeln sowie die Art und Weise, wie der Bericht gespeichert und angezeigt werden muss. Das Spa-Framework verwendet diese Informationen zum Generieren einer temporären Tabelle und zum anschließenden übertragen der Ergebnisse in der temporären Tabelle in eine Tabelle, auf die Benutzer zugreifen können.

Alle Berichts-SQL-Skripts müssen in einem Unterordner namens " Scripts" gespeichert werden. Zu Wartungszwecken empfiehlt es sich, unterschiedliche Datenbankobjekte in verschiedenen SQL Server Dateien zu speichern. Es muss mindestens eine gespeicherte Prozedur als Haupteinstiegspunkt vorhanden sein.

NOTE

Die Datei "Schema. man" ist nur erforderlich, wenn Ihr Advisor-Pack etw-Ablauf Verfolgungen sammelt. Diese Schema Datei wird verwendet, um das Schema der ETW-Ereignisse zu beschreiben und ETW-Ereignisse zu decodieren.

Definieren grundlegender Informationen

In diesem Abschnitt werden einige der grundlegenden Elemente beschrieben, aus denen ein Advisor-Pack besteht, einschließlich "provisionmetadata.xml" und Attribute.

Im folgenden finden Sie eine Beispiel Kopfzeile für die Datei "provisionmetadata.xml":

```
<advisorPack  
xmlns="https://microsoft.com/schemas/ServerPerformanceAdvisor/ap/2010"  
name="Microsoft.ServerPerformanceAdvisor.CoreOS.V2"  
displayName="Microsoft CoreOS Advisor Pack V2"  
description="Microsoft CoreOS Advisor Pack"  
author="Microsoft"  
version="1.0"  
frameworkversion="3.0"  
minOSversion="6.0"  
reportScript="ReportScript">  
</advisorPack>
```

Advisor Pack-Version

Attribut Name: Version

Advisor Pack-Entwickler können die Haupt- und neben Versionen für das Advisor-Pack definieren:

- Eine Hauptversion umfasst in der Regel bedeutende Verbesserungen. Die Ergebnisse, die von einer alten Version generiert werden, sind möglicherweise nicht mit der neuen kompatibel. Es wird dringend empfohlen, dass Sie die Hauptversion in den Advisor Pack-Namen einschließen.
- Spa ermöglicht neben Versions Upgrades, wenn es nur geringfügige Änderungen ohne Daten Inkompatibilitäts Probleme gibt.

Weitere Informationen zur Versionsverwaltung finden Sie unter [Advanced Topics](#).

Skript Einstiegspunkt

Attribut Name: Report Script

Das Spa-Framework sucht im Skript Einstiegspunkt nach dem Namen der gespeicherten Haupt Prozedur und führt ihn auf sichere Weise aus.

Andere Attribute

Im folgenden finden Sie einige weitere Attribute, die zum Identifizieren eines Advisor-Pakets verwendet werden können:

- Anzeige Name: **Display Name**
- Beschreibung: **Beschreibung**
- Autor: **Autor**
- Framework-Version: **Frameworkversion** (standardmäßig 3,0)
- Mindestversion des Betriebssystems: **minosversion** (diese ist für die spätere Erweiterbarkeit reserviert)
- Benachrichtigung über verlorene Ereignisse: **showeventlostwarning**

Definieren des Datensammler Satzes

Ein Datensammler Satz definiert die Leistungsdaten, die das Spa-Framework vom Zielserver sammeln soll. Es unterstützt Registrierungs Einstellungen, WMI, Leistungsindikatoren, Dateien vom Zielserver und etw.

```
<advisorPack>
<dataSourceDefinition xmlns="https://microsoft.com/schemas/ServerPerformanceAdvisor/dc/2010">
    <dataCollectorSet duration="10">
        <registryKeys>
            ?<registryKey>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\\</registryKey>
        </registryKeys>
        <managementpaths>
            ?<path>Root\Cimv2:select * FROM Win32_DiskDrive</path>
        </managementpaths>
        <performanceCounters interval="2">
            ?<performanceCounter>\PhysicalDisk(*)\Avg. Disk sec/Transfer</performanceCounter>
        </performanceCounters>
        <files>
            ?<path>%windir%\System32\inetsrv\config\applicationHost.config</path>
        </files>
        <providers>
            ?<provider session="NT Kernel Logger" guid="{9E814AAD-3204-11D2-9A82-006008A86939}" keywordsany="06010201" keywordsAll="00000000" level="00000000" />
        </providers>
    </dataCollectorSet>
</dataSourceDefinition>
</advisorPack>
```

Mit dem **Duration** -Attribut von **<datacollector Set/>** im vorherigen Beispiel wird die Dauer der Datensammlung definiert (die Zeiteinheit ist Sekunden). **Duration** ist ein erforderliches Attribut. Mit dieser Einstellung wird die von Leistungsindikatoren und etw verwendete Sammlungs Dauer gesteuert.

Sammeln von Registrierungsdaten

Sie können Registrierungsdaten aus den folgenden Registrierungs Strukturen erfassen:

- HKEY-_Klassen_root
- HKEY-_aktuelle_config
- HKEY-_aktueller_Benutzer
- HKEY_lokalen_Computer

- HKEY-_Benutzer

Um eine Registrierungs Einstellung zu erfassen, geben Sie den vollständigen Pfad zum Wertnamen an:
HKEY_lokalen_Computer\MyKey\meinWert

Um alle Einstellungen unter einem Registrierungsschlüssel zu erfassen, geben Sie den vollständigen Pfad zum Registrierungsschlüssel an: HKEY_lokalen_Computers\MyKey\

Wenn Sie alle Werte unter einem Registrierungsschlüssel und seinen untergeordneten Schlüsseln erfassen möchten (die Daten werden von der Datenbank rekursiv gesammelt), verwenden Sie zwei umgekehrte Schrägstriche für das letzte Pfad Trennzeichen: HKEY_local_Machine\MyKey\\

Um Registrierungsinformationen von einem Remote Computer zu erfassen, fügen Sie den Computernamen am Anfang des Registrierungs Pfads ein: HKEY_lokalen_Machine\MyKey\meinWert

Beispielsweise können Sie über einen Registrierungsschlüssel verfügen, der wie folgt aussieht:

```
Windows registry editor version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes]
"activePowerScheme"="db310065-829b-4671-9647-2261c00e86ef"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\db310065-829b-4671-9647-
2261c00e86ef]
"Description"=
FriendlyName = Power Source Optimized

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\db310065-829b-4671-9647-
2261c00e86ef \0012ee47-9041-4b5d-9b77-535fba8b1442\6738e2c4-e8a5-4a42-b16a-e040e769756e
"ACSettingIndex"=dword:000000b4
"DCSettingIndex"=dword:0000001e
```

Beispiel 1: Zurückgeben der aktiven powerschemas und ihrer Werte:

```
<registryKey>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes</registryKey>
```

Beispiel 2: gibt alle Schlüssel-Wert-Paare unter diesem Pfad zurück:

NOTE

Die Ausführung von Pla erfolgt unter Benutzer Anmelde Informationen. Für einige Registrierungsschlüssel sind administrative Anmelde Informationen erforderlich. Die Enumeration wird beendet, wenn der Zugriff auf keine der untergeordneten Schlüssel fehlschlägt.

```
<registryKey>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\\</registryKey>
```

Alle gesammelten Daten werden in eine temporäre Tabelle namens #RegistryKeys importiert, bevor ein SQL-Berichts Skript ausgeführt wird. In der folgenden Tabelle werden die Ergebnisse für Beispiel 2 angezeigt:

KEYNAME	KEYTYPEID	VALUE
HKEY_LOCAL_MACHINE.\powerschemas	1	db310065-829b-4671-9647-2261c00e86ef
\db310065-829b-4671-9647-2261c00e86ef\description	2	

KEYNAME	KEYTYPEID	VALUE
\db310065-829b-4671-9647-2261c00e86ef\friendlyname	2	Stromquelle optimiert
. ..\6738e2c4-e8a5-4a42-b16a-e040e769756e\acsettingindex	4	180
. ..\6738e2c4-e8a5-4a42-b16a-e040e769756e\dcsettingindex	4	30

Das Schema für die #registryKeys Tabelle lautet wie folgt:

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
KeyName	Nvarchar (300) nicht NULL	Vollständiger Pfadname des Registrierungsschlüssels
Keytypeid	Smallint not NULL	Interne Typ-ID
Value	Nvarchar (4000) nicht NULL	Alle Werte

Die keytypeid -Spalte kann einen der folgenden Typen aufweisen:

ID	GEBEN SIE IN DAS SUCHFELD AUF DER TASKLEISTE
1	Zeichenfolge
2	ExpandString
3	Binär
4	DWord
5	DwordbigEndian
6	Link
7	"Multiplestring"
8	ResourceList
9	Fullresourcedescriptor
10	Resourcerequirementslist
11	QWord

WMI-Erfassung

Sie können eine beliebige WMI-Abfrage hinzufügen. Weitere Informationen zum Schreiben von WMI-Abfragen finden Sie unter [WQL \(SQL für WMI\)](#). Im folgenden Beispiel wird eine Auslagerungs Datei abgefragt:

```
<path>Root\cimv2:select * FROM Win32_PageFileUsage</path>
```

Die Abfrage im obigen Beispiel gibt einen Datensatz zurück:

UNTERTITEL FÜR HÖRGESCHÄDIGTE	NAME	PEER USAGE
C:\pagefile.sys	C:\pagefile.sys	215

Da WMI eine Tabelle mit unterschiedlichen Spalten zurückgibt und die gesammelten Daten in eine Datenbank importiert werden, führt Spa eine Daten Normalisierung durch und wird den folgenden Tabellen hinzugefügt:

wmiobjects-Tabelle (#)

SEQUENCEID	NAMESPACE	CLASSNAME	RELATIVEPATH	WMIQUERYID
10	Root\Cimv2	Win32_PageFileUsage	. Name = C:\Pagefile.sys	1

#Tabelle "wmiobjectsproperties"

ID	QUERY
1	Root\cimv2: SELECT * from Win32_PageFileUsage

#wmiqueries-Tabelle

ID	QUERY
1	Root\cimv2: SELECT * from Win32_PageFileUsage

wmiobjects-Tabellen Schema (#)

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
Sequenceld	Int not NULL	Korrelieren der Zeile und ihrer Eigenschaften
Namespace	Nvarchar (200) nicht NULL	WMI-Namespace
ClassName	Nvarchar (200) nicht NULL	WMI-Klassenname
RelativePath	Nvarchar (500) nicht NULL	Relativer WMI-Pfad
Wmiqueryid	Int not NULL	Korrelieren Sie den Schlüssel #WmiQueries

wmiobjectproperties-Tabellen Schema

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
Sequenceld	Int not NULL	Korrelieren der Zeile und ihrer Eigenschaften

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
Name	Nvarchar (1000) nicht NULL	Eigenschaftenname
Value	Nvarchar (4000) NULL	Der Wert der aktuellen Eigenschaft.

#wmqueries-Tabellen Schema

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
ID	Int not NULL	eindeutige Abfrage-ID >
query	Nvarchar (4000) nicht NULL	Ursprüngliche Abfrage Zeichenfolge in den Bereitstellungs Metadaten

Leistungsindikatoren erfassen

Hier finden Sie ein Beispiel für die Erfassung eines Leistungs Zählers:

```
<performanceCounters interval="1">
  <performanceCounter>\PhysicalDisk(*)\Avg. Disk sec/Transfer</performanceCounter>
</performanceCounters>
```

Das **Interval** -Attribut ist eine erforderliche globale Einstellung für alle Leistungsindikatoren. Er definiert das Intervall (die Zeiteinheit ist Sekunden) für die Erfassung von Leistungsdaten.

Im vorherigen Beispiel wird die Leistungsindikator \PhysicalDisk (*)\Mittlere Sek./Übertragung pro Sekunde abgefragt.

Es können zwei Instanzen vorhanden sein: **_Gesamt** und **0 C: D:**, und die Ausgabe könnte wie folgt lauten:

TIMESTAMP	CATEGORYNAME	COUNTERNAME	INSTANZWERT _TOTAL	INSTANZWERT 0 C: D:
13:45:52.630	PhysicalDisk	Mittlere Sek./Übertragung	0.00100008362473995	0.0010000836247395
13:45:53.629	PhysicalDisk	Mittlere Sek./Übertragung	0.00280023414927187	0.00280023414927187
13:45:54.627	PhysicalDisk	Mittlere Sek./Übertragung	0.00385999853230048	0.00385999853230048
13:45:55.626	PhysicalDisk	Mittlere Sek./Übertragung	0.000933297607934224	0.000933297607934224

Um die Daten in die Datenbank zu importieren, werden die Daten in eine Tabelle mit dem Namen **#performanceCountersnormalisiert**.

CATEGORYDISPLAYNAME	INSTANCENAME	COUNTER DISPLAY NAME	VALUE
PhysicalDisk	_Gesamt	Mittlere Sek./Übertragung	0.00100008362473995
PhysicalDisk	0 C: D:	Mittlere Sek./Übertragung	0.00100008362473995

CATEGORYDISPLAYNAME	INSTANCENAME	COUNTER DISPLAY NAME	VALUE
PhysicalDisk	_Gesamt	Mittlere Sek./Übertragung	0.00280023414927187
PhysicalDisk	0 C: D:	Mittlere Sek./Übertragung	0.00280023414927187
PhysicalDisk	_Gesamt	Mittlere Sek./Übertragung	0.00385999853230048
PhysicalDisk	0 C: D:	Mittlere Sek./Übertragung	0.00385999853230048
PhysicalDisk	_Gesamt	Mittlere Sek./Übertragung	0.000933297607934224
PhysicalDisk	0 C: D:	Mittlere Sek./Übertragung	0.000933297607934224

Hinweis Die lokalisierten Namen, wie z. b. `categorydisplayname` und `counterdisplayname`, variieren je nach der auf dem Zielserver verwendeten Anzeige Sprache. Verwenden Sie diese Felder nicht, wenn Sie ein sprach neutrales Advisor Pack erstellen möchten.

#performanceCounters -Tabellen Schema

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
timestamp	datetime2 (3) nicht NULL	Datum/Uhrzeit der Erfassung in UNC
CategoryName	Nvarchar (200) nicht NULL	Kategorienname
Categorydisplayname	Nvarchar (200) nicht NULL	Lokalisierte Kategorienname
InstanceName	Nvarchar (200) NULL	Instanzenname
CounterName	Nvarchar (200) nicht NULL	Name des Leistungsindikators
Counter Display Name	Nvarchar (200) nicht NULL	Lokalisierte namens Name
Value	Float not NULL	Der gesammelte Wert

Dateien sammeln

Die Pfade können absolut oder relativ sein. Der Dateiname kann das Platzhalter Zeichen (*) und das Fragezeichen (?) enthalten. Wenn Sie z. b. alle Dateien im temporären Ordner sammeln möchten, können Sie `c:\Temp*` angeben. Das Platzhalter Zeichen gilt für Dateien im angegebenen Ordner.

Wenn Sie auch Dateien aus den Unterordnern des angegebenen Ordners sammeln möchten, verwenden Sie zwei umgekehrte Schrägstriche für das letzte Ordner Trennzeichen, z. b. `c:\Temp*`.

Hier ist ein Beispiel für die Abfrage der Datei "ApplicationHost.config":

```
<path>%windir%\System32\inetsrv\config\applicationHost.config</path>
```

Die Ergebnisse finden Sie in einer Tabelle namens #Dateien, z. b.:

QUERYPATH	FULLPATH	ELEMENT PFAD	DATEINAME	INHALT
% windir%\applicationhost.config	C:\Windows\...\applicationhost.config	C:\Windows\...\Config	ApplicationHost.	0x3c3f

Tabellen Schema für #Dateien

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
querypath	Nvarchar (300) nicht NULL	Ursprüngliche Abfrage Anweisung
FullPath	Nvarchar (300) nicht NULL	Absoluter Dateipfad und Dateiname
Element Pfad	Nvarchar (300) nicht NULL	Dateipfad
Dateiname	Nvarchar (300) nicht NULL	Dateiname
Inhalt	Varbinary (max) NULL	Dateinhalt in Binärdatei

Definieren von Regeln

Nachdem genügend Daten mithilfe von Pla von einem Zielsystem gesammelt wurden, kann das Advisor Pack diese Daten für die Überprüfung verwenden und eine kurze Zusammenfassung der Systemadministratoren anzeigen.

Mit Regeln wird eine kurze Übersicht über die Leistung des Servers erzielt. Es werden Probleme hervorgehoben und Empfehlungen bereitgestellt. Sie können alle Regeln auflisten, die Sie für ein Advisor-Pack überprüfen möchten. Wenn Sie z. B. ein Kernbetriebssystem Advisor-Paket entwickeln möchten, können Sie folgende Regeln einschließen:

- Ob der CPU-Energiesparmodus Energiesparmodus ist
- Ob sich der Server in einer virtualisierten Umgebung befindet
- Ob Datenträger-e/a-Druck vorhanden ist

Regeln enthalten die folgenden Elemente:

- Abhängiger Schwellenwert (ein konfigurierbarer Teil einer Regel)
- Regel Definition (Warnungen und Empfehlungen)

Hier ist ein Beispiel für eine einfache Regel:

```
<advisorPack>

  <reportDefinition>
    <thresholds>
      <threshold />
    </thresholds>
    <rules>
      <rule />
    </rules>
  </reportDefinition>
</advisorPack>
```

Schwellenwert

Der Schwellenwert ist ein konfigurierbarer Faktor, mit dem Systemadministratoren entscheiden können, wann eine Regel einen guten oder einen ungültigen Status aufweisen soll. Das folgende Beispiel zeigt eine Regel, mit der der freie Speicherplatz auf einem Systemlaufwerk erkannt wird, und eine Warnung, wenn der freie Speicherplatz weniger als 10 GB beträgt.

```
<threshold name="freediskSize" caption="Free Disk Size (GB)" description="Free Disk Size" value="10" />
```

In diesem Fall verfügt der Systemadministrator jedoch über eine kleinere Festplatte. Er meint, dass 5 GB freier Speicherplatz immer noch eine gute Bedingung sind, und er möchte keine Warnung anzeigen. Er kann den Standardwert von 10 auf 5 über die Spa-Konsole aktualisieren, ohne sich mit der Entwicklung eines Advisor-Pakets vertraut machen zu müssen.

Durch die Einführung eines Schwellenwerts können Systemadministratoren den Wert schnell ändern, ohne das Advisor-Paket ändern zu müssen.

Im Beispiel sind alle Attribute außer **Description** erforderlich. Sie können eine beliebige Zahl als **Wert** verwenden.

Ein Schwellenwert kann über die Regeln hinweg gemeinsam genutzt werden.

Warnungen und Empfehlungen

Die Regel Definition umfasst keine Logik Berechnungen. Es definiert, wie die Benutzeroberfläche aussehen könnte und wie das SQL Server Berichts Skript die Ergebnisse an die Benutzeroberfläche übermittelt.

Eine Regel besteht aus drei Teilen:

- Warnung (Regel Beschriftung)
- Empfehlung (Ratschläge)
- Zugeordneter Schwellenwert (optionale Informationen zu Abhängigkeiten)

Im folgenden finden Sie ein Beispiel für eine Regel:

```
<rule name="freediskSize" caption="Free Disk Size on System Drive" description="This rule checks free disk size on system drive">
<advice name="SuccessAdvice" level="Success" message="No issue found.">No Recommendation.</advice>
<advice name="WarningAdvice" level="Warning" message="Not enough free space on system drive.">
Install OS on larger disk.</advice>
<dependencies>
<threshold ref="freediskSize"/>
</dependencies>
</rule>
```

Sie können beliebig viele Ratschläge definieren, und Sie sollten in der Regel Empfehlungen definieren. Der Grad der Empfehlung kann "Erfolg" oder "Warnung" lauten.

Sie können mit beliebig vielen Schwellenwerten verknüpfen. Sie können sogar eine Verknüpfung mit einem Schwellenwert herstellen, der für die aktuelle Regel irrelevant ist. Durch die Verknüpfung können Sie die Schwellenwerte problemlos verwalten.

Der Regelname und die Empfehlungen sind Schlüssel, die in Ihrem Bereich eindeutig sind. Es können nicht zwei Regeln denselben Namen aufweisen, und es können nicht zwei Empfehlungen innerhalb einer Regel denselben Namen haben. Diese Namen sind sehr wichtig, wenn Sie einen SQL-Skript Bericht schreiben. Sie können den [dbo-]abrufen.[setnotification] API, um den Regel Status festzulegen.

Definieren von Benutzeroberflächen-Anzeigeelementen

Nachdem die Regeln definiert wurden, können Systemadministratoren die Berichts Zusammenfassung anzeigen. Allerdings sind Systemadministratoren oft an den aggregierten Daten interessiert und möchten die Datenquellen überprüfen, die in den Leistungs Regeln verwendet wurden.

Wenn Sie mit dem vorherigen Beispiel fortfahren, weiß der Benutzer, ob genügend freier Speicherplatz auf dem Systemlaufwerk vorhanden ist. Benutzer sind möglicherweise auch an der tatsächlichen Größe des freien Speicherplatzes interessiert. Eine einzelne Wert Gruppe wird zum Speichern und anzeigen derartiger Ergebnisse verwendet. Mehrere einzelne Werte können gruppiert und in einer Tabelle in der Spa-Konsole angezeigt werden. Die Tabelle hat nur zwei Spalten, Name und Wert, wie hier gezeigt.

NAME	VALUE
Freie Datenträger Größe auf System Laufwerk (GB)	100
Gesamte installierte Datenträger Größe (GB)	500

Wenn ein Benutzer eine Liste aller Festplatten sehen möchte, die auf dem Server und dessen Datenträger Größe installiert sind, können wir einen Listen Wert, der drei Spalten und mehrere Zeilen enthält, wie hier gezeigt, abrufen.

FESTPLATTE	GRÖSSE DES FREIEN DATENTRÄGERS (GB)	GESAMTGRÖSSE (GB)
0	100	500
1	20	320

In einem Advisor-Pack können viele Tabellen vorhanden sein (Einzelwert Gruppen und Listen Wert Tabellen). Wir können einen Abschnitt verwenden, um diese Tabellen zu organisieren und zu kategorisieren.

Zusammenfassend gibt es drei Typen von Benutzeroberflächen Elementen:

- [Abschnitte](#)
- [Einzelwert Gruppen](#)
- [Auflisten von Wert Tabellen](#)

Hier sehen Sie ein Beispiel, das die Elemente der Benutzeroberfläche anzeigt:

```
<advisorPack>
<dataSourceDefinition/>
<reportDefinition>
  <datatypes>
    <datatype .../>
  </datatypes>
  <thresholds/>
  <rule/>
  <sections>
    <section .../>
  </sections>
  <singleValues>
    <singleValue .../>
  </singleValues>
  <listValues>
    <listValue .../>
  </listValues>
</reportDefinition>
</advisorPack>
```

Strecken

Ein Abschnitt ist ausschließlich für das Layout der Benutzeroberfläche vorgesehen. Er ist nicht an logischen Berechnungen beteiligt. Jeder einzelne Bericht enthält eine Reihe von Abschnitten der obersten Ebene, für die kein übergeordneter Abschnitt vorhanden ist. Die Abschnitte der obersten Ebene werden als Registerkarten im Bericht angezeigt. Abschnitte können Unterabschnitte mit maximal 10 Ebenen aufweisen. Alle Unterabschnitte in den Abschnitten der obersten Ebene werden in erweiterbaren Bereichen angezeigt. Ein Abschnitt kann mehrere Unterabschnitte, Einzelwert Gruppen und Listen Wert Tabellen enthalten. Einzelwert Gruppen und Listen Wert Tabellen werden als Tabellen dargestellt.

Im folgenden finden Sie ein Beispiel für den Abschnitt der obersten Ebene.

```
<section name="CPU" caption="CPU"/>
```

Ein Abschnitts Name muss eindeutig sein. Sie wird als Schlüssel verwendet, der mit anderen Abschnitten, Einzelwert Gruppen und Listen Wert Tabellen verknüpft werden kann.

Das folgende Beispiel verfügt über ein über **geordnetes** Attribut, das auf den Abschnitt CPU zeigt. Cpufacts ist ein untergeordnetes Element des Abschnitts mit dem Namen CPU. das über **geordnete** Element muss auf einen vorherigen Abschnittsnamen verweisen. Andernfalls kann dies zu einer-Schleife führen.

```
<section name="CPUFacts" caption="Facts" parent="CPU"/>
```

Die folgende Einzelwert Gruppe verfügt über ein-Attribut , **undes** kann auf einen beliebigen Abschnitt verweisen, der auf dem Benutzeroberflächen Entwurf basiert.

```
<singleValue name="CPUInformation" section="CPUFacts" caption="Physical CPU Information"> </singleValue>
```

Datentypen

Eine Einzelwert Gruppe und eine Listen Wert Tabelle enthalten unterschiedliche Datentypen, z. b. String, int und float. Da diese Werte in der SQL Server-Datenbank gespeichert werden, können Sie einen SQL-Datentyp für jede Dateneigenschaft definieren. Die Definition eines SQL-Datentyps ist jedoch recht kompliziert. Sie müssen die Länge oder Genauigkeit angeben, die möglicherweise geändert werden kann.

Zum Definieren logischer Datentypen können Sie das erste untergeordnete Element von **<ReportDefinition/>** verwenden. hier können Sie eine Zuordnung des SQL-Datentyps und des logischen Typs definieren.

Im folgenden Beispiel werden zwei Datentypen definiert. Eine ist eine **Zeichenfolge** , und die andere ist " **companycode**" .

```
<datatype name="string" = sqltype="nvarchar(4000)" />
<datatype name="companyCode" sqltype="nvarchar(100)" />
```

Ein Datentyp Name kann eine beliebige gültige Zeichenfolge sein. Im folgenden finden Sie eine Liste der zulässigen SQL-Datentypen:

- BIGINT
- binär
- bit
- char
- date

- datetime
- datetime2
- datetimeoffset
- Dezimalzahl
- float
- int
- Verdienst
- nchar
- numeric
- nvarchar
- Reelle
- smalldatetime
- smallint
- SMALLMONEY
- Zeit
- tinyint
- uniqueidentifier
- varbinary
- varchar

Weitere Informationen zu diesen SQL-Datentypen finden Sie unter [Datentypen \(Transact-SQL\)](#).

Einzelwert Gruppen

In einer Einzelwert Gruppe werden mehrere einzelne Werte in einer Tabelle gruppiert, wie hier gezeigt.

```
<singleValue name="Systemoverview" section="SystemoverviewSection" caption="Facts">
  <value name="OsName" type="string" caption="Operating system" description="WMI:
    Win32_OperatingSystem/Caption"/>
  <value name="Osversion" type="string" caption="OS version" description="WMI:
    Win32_OperatingSystem/version"/>
  <value name="OsLocation" type="string" caption="OS location" description="WMI:
    Win32_OperatingSystem/SystemDrive"/>
</singleValue>
```

Im vorherigen Beispiel haben wir eine Einzelwert Gruppe definiert. Es handelt sich um einen untergeordneten Knoten des Abschnitts **systemoverviewsection**. Diese Gruppe verfügt über einzelne Werte, d... **osname**, **OSVersion**und **oslocation**.

Ein einzelner Wert muss über ein globales Attribut für einen eindeutigen Namen verfügen. In diesem Beispiel ist das Attribut Global Unique Name **systemoverview**. Der eindeutige Name wird verwendet, um eine entsprechende Ansicht für den benutzerdefinierten Bericht zu generieren. Jede Ansicht enthält das Präfix **VW**, z. b. **vwsystemoverview**.

Obwohl Sie mehrere Einzelwert Gruppen definieren können, dürfen keine zwei einzelnen Werte Namen identisch sein, auch wenn Sie sich in unterschiedlichen Gruppen befinden. Der Einzelwert Name wird vom SQL-

Skript Bericht verwendet, um den Wert entsprechend festzulegen.

Sie können einen Datentyp für jeden einzelnen Wert definieren. Die zulässige Eingabe für **Type** ist in **<DataType/>** definiert. Der endgültige Bericht könnte wie folgt aussehen:

Fakten

NAME	VALUE
Betriebssystem	<ein Wert vom Berichts Skript festgelegt wird>
BS-Version	<ein Wert vom Berichts Skript festgelegt wird>
Betriebssystem Standort	<ein Wert vom Berichts Skript festgelegt wird>

Das **Caption** -Attribut **<Werts/>** wird in der ersten Spalte angezeigt. Werte in der Spalte Wert werden in der Zukunft vom Skript Bericht über [dbo]-festgelegt.[setsinglevalue-]. Das **Description** -Attribut von **<Wert/>** wird in einer QuickInfo angezeigt. Normalerweise zeigt die QuickInfo den Benutzern die Quelle der Daten an. Weitere Informationen zu Quick Infos finden Sie unter Quick Infos.

Auflisten von Wert Tabellen

Die Definition eines Listen Werts entspricht dem Definieren einer Tabelle.

```
<listValue name="NetworkAdapterInformation" section="NetworkIOFacts" caption="Physical network adapter information">
<column name="NetworkAdapterId" type="string" caption="ID" description="WMI: Win32_NetworkAdapter/DeviceID"/>
<column name="NetworkAdapterName" type="string" caption="Name" description="WMI: Win32_NetworkAdapter/Name"/>
<column name="type" type="string" caption="type" description="WMI: Win32_NetworkAdapter/Adaptertype"/>
<column name="Speed" type="decimal" caption="Speed (Mbps)" description="WMI: Win32_NetworkAdapter/Speed"/>
<column name="MACAddress" type="string" caption="MAC address" description="WMI: Win32_NetworkAdapter/MACAddress"/>
</listValue>
```

Der Name des Listen Werts muss global eindeutig sein. Dieser Name wird zum Namen einer temporären Tabelle. Im vorherigen Beispiel wird die Tabelle mit dem Namen #networkadapterinformation in der Initialisierungsphase der Ausführungsumgebung erstellt, in der alle beschriebenen Spalten enthalten sind. Ähnlich wie bei einem einzelnen Wertnamen wird auch ein Listen Wert Name als Teil des benutzerdefinierten Ansichts namens verwendet, z.b. vwnetworkadapterinformation.

@type von **<Column/>** wird durch **<DataType/>** definiert.

Die Mock-Benutzeroberfläche des letzten Berichts könnte wie folgt aussehen:

Informationen zum physischen Netzwerkadapter

ID	NAME	GEBEN SIE IN DAS SUCHFELD AUF DER TASKLEISTE	GESCHWINDIGKEIT (MBIT/S)	MAC-ADRESSE

Das **Caption** -Attribut **<Spalte/>** wird als Spaltenname angezeigt, und das **Beschreibungs** Attribut **<Spalte/>** wird als QuickInfo für den entsprechenden Spaltenheader angezeigt. In der Regel wird der Benutzer von der QuickInfo die Quelle der Daten angezeigt. Weitere Informationen finden Sie unter Quick Infos.

In einigen Fällen kann eine Tabelle viele Spalten und nur wenige Zeilen enthalten, sodass das Austauschen der Spalten und Zeilen die Tabelle erheblich besser aussehen würde. Zum Austauschen der Spalten und Zeilen können Sie das folgende Formatvorlagen Attribut hinzufügen:

```
<listValue style="Transpose"
```

Definieren von Diagrammelementen

Sie können einen beliebigen Statistik Schlüssel auswählen und die Werte in einem Verlaufs Diagramm oder einem Trend Diagramm anzeigen. Es gibt zwei Arten von Statistiken:

- **Statische Statistik** Ein einzelner Wert, der zur Entwurfszeit bekannt ist. Der freie Speicherplatz auf einem Systemlaufwerk wäre z. b. eine statische Statistik.
- **Dynamische Statistik** Möglicherweise ist zur Entwurfszeit unbekannt. Beispielsweise ist die durchschnittliche CPU-Auslastung der einzelnen Kerne eine dynamische Statistik, da Sie nicht wissen, wie viele CPU-Kerne zur Entwurfszeit im System stehen können.

Der Statistik Schlüssel weist eine Einschränkung auf, dass die Daten mit dem Double-Datentyp kompatibel sein müssen. Dabei kann es sich um eine ganze Zahl, einen Dezimalwert oder eine Zeichenfolge handeln, die in Double konvertiert werden kann.

Spa verwendet eine Einzelwert Gruppe zur Unterstützung statischer Statistiken und eine Listen Wert Tabelle, um dynamische Statistiken zu unterstützen. In den folgenden Abschnitten wird beschrieben, wie statische Statistik- und dynamische Statistik Schlüssel definiert werden.

Statische Statistik

Wie bereits erwähnt, ist eine statische Statistik ein einzelner Wert. Logisch können alle einzelnen Werte als statische Statistik definiert werden. Es ist jedoch bedeutungslos, einen einzelnen Wert anzuzeigen, der nicht in einen Nummertyp umgewandelt werden kann. Wenn Sie eine statische Statistik definieren möchten, können Sie das Attribut einfach dem entsprechenden Einzelwert Schlüssel hinzufügen, wie unten gezeigt:

```
<value name="freediskSize" type="int" trendable="true"
```

Dynamische Statistik

Dynamische Statistik Schlüssel sind zur Entwurfszeit nicht bekannt, sodass die Anzahl möglicher Werte unbekannt ist. Da Listen Werte jedoch in mehreren Zeilen gespeichert werden, wäre es einfach, eine Listen Wert Tabelle zum Speichern dynamischer Statistiken zu verwenden.

Wenn wir z. b. Diagramme für die durchschnittliche CPU-Auslastung unterschiedlicher Kerne anzeigen müssen, können wir eine Tabelle mit Spalten für **CPUID** und **averagecpuusage** definieren:

```
<listValue name="CpuPerformance">
<column name="CpuId" type="string" caption="CPU ID" columntype="Key"/>
<column name="AverageCpuUsage" type="decimal" caption="Average" columntype="Value"/>
</listValue>
```

Ein anderes Attribut, **ColumnType**, kann **Schlüssel**, **Wert** oder **Information** sein. Der Datentyp der **Schlüssel** Spalte muss "Double" oder "Double" konvertierbar sein. In einer **Schlüssel** Spalte können Sie dieselben Schlüssel nicht in eine Tabelle einfügen. **Werte** oder **Informations** Spalten weisen diese Einschränkung nicht auf.

Die Statistik Werte werden in **Wert** Spalten gespeichert.

Informations Spalten ähneln gewöhnlichen Spalten in normalen Listen Wert Tabellen. **Information** ist der

Standard Spaltentyp, wenn Sie keinen angeben. Solche Spalten wirken sich nicht auf die Anzahl der Statistik Schlüssel aus oder nehmen an Statistik bezogenen Berechnungen Teil.

Wenn ein Server über zwei CPU-Kerne verfügt, könnte das Ergebnis in der Tabelle wie folgt aussehen:

CPUID	AVERAGECPUUSAGE
0	10
1	30

Gleichzeitig werden zwei Statistik Schlüssel durch das Spa-Framework generiert. Eine ist für CPU 0 und die andere für CPU 1.

Das folgende Beispiel zeigt, dass mehrere **Wert** Spalten mit mehreren **Schlüssel** Spalten unterstützt werden.

COUNTERNAME	INSTANCENAME	MITTELMÄSSIG	SUMME
Prozessorzeit (%)	_Gesamt	10	20
Prozessorzeit (%)	CPU0	20	30

In diesem Beispiel verfügen Sie über zwei **Schlüssel** Spalten und zwei **Wert** Spalten. Spa generiert zwei Statistik Schlüssel für die Average-Spalte und weitere zwei Schlüssel für die Sum-Spalte. Die Statistik Schlüssel lauten:

- Counter Name (Prozessorzeit (%))/instanceName (_gesamt)/Durchschnitt
- Counter Name (Prozessorzeit (%))/instanceName (cpu0)/Durchschnitt
- Counter Name (Prozessorzeit (%))/instanceName (_gesamt)/Summe
- Counter Name (Prozessorzeit (%))/instanceName (cpu0)/Sum

Counter Name und instanceName werden als ein Schlüssel kombiniert. Der kombinierte Schlüssel darf keine Duplikierung aufweisen.

Die Spa generiert viele Statistik Schlüssel. Einige davon sind für Sie möglicherweise nicht interessant, und Sie möchten Sie möglicherweise über die Benutzeroberfläche ausblenden. Mithilfe von Spa können Entwickler einen Filter erstellen, um nur hilfreiche Statistik Schlüssel anzuzeigen.

im vorherigen Beispiel sind die Systemadministratoren möglicherweise nur an Schlüsseln interessiert, bei denen "instanceName" _"Total" oder "CPU1" ist. Der Filter kann wie folgt definiert werden:

```
<listValue name="CpuPerformance">
<column name="CounterName" type="string" columntype="Key"/>
<column name="InstanceName" type="string" columntype="Key">
  <trendableKeyValues>
    <value>_Total</value>
    <value>CPU1</value>
  </trendableKeyValues>
</column>
<column name="Average" type="decimal" columntype="Value"/>
<column name="Sum" type="decimal" columntype="Value"/>
</listValue>
```

<trendablekeyvalues/> können unter jeder Schlüssel Spalte definiert werden. Wenn mehr als eine Schlüssel Spalte einen solchen Filter konfiguriert hat, wird Logik angewendet.

Entwickeln von Berichts Skripts

Nachdem die Bereitstellungs Metadaten definiert sind, können Sie mit dem Schreiben des Berichts Skripts beginnen, bei dem es sich um eine gespeicherte T-SQL-Prozedur handelt.

Der Header "Bereitstellen von Metadaten" enthält die Attribute " **Name** " und " **reportscript** ", wie hier gezeigt:

```
<advisorPack name="Microsoft.ServerPerformanceAdvisor.CoreOS.V1" reportScript="ReportScript"
```

Das Hauptberichts Skript wird durch Kombinieren der Attribute " **Name** " und " **reportscript** " benannt. Im folgenden Beispiel wird [Microsoft.serverperformanceadvisor.coreos.v2].[reportscript].

```
create PROCEDURE [Microsoft.ServerPerformanceAdvisor.CoreOS.V2].[ReportScript] AS SET NOCOUNT ON  
- Set alert and notification  
- Prepare data for report view
```

Das **Name** -Attribut wird als Name des Datenbankschemas verwendet, z. b. als Namespace. Diese Regel gilt für alle anderen Datenbankobjekte, die zum aktuellen Advisor-Paket gehören, z. b. Listen Wert und gespeicherte Prozeduren.

Zu den Vorteilen dieses Schema namens vor den Datenbankobjekten gehören:

- Vermeiden von Namenskonflikten für verschiedene Advisor-Pakete
- Höhere Sicherheit

In der SQL Server-Datenbank lautet der Standardschema Name **dbo**. Datenbankbesitzer-Anmelde Informationen sind normalerweise erforderlich, um Datenbankobjekte unter **dbo** auszuführen. Wenn wir kein Schema für jedes Advisor-Paket erstellen, ist es wahrscheinlich, dass zwei Advisor-Pakete einen Listen Wert mit demselben Namen definieren. Dies sollte unerheblich sein, da Sie einen Schema Namen einführen können, um dieses Problem zu beheben. Außerdem ist das Aufheben der Bereitstellung eines Advisor-Pakets viel einfacher. Da das Advisor Pack-Objekt zu einem anderen Schema als **dbo** gehört, ermöglicht es Spa, eine niedrigere Benutzer Berechtigung für den Zugriff auf diese zu verwenden.

Ein normales Berichts Skript führt folgende Schritte aus:

- Greift auf aufgelistete Daten zu
- Führt Berechnungen auf Grundlage der Rohdaten aus.
- Änderungen an Warnungen und Empfehlungen
- Bereitet Daten für die Berichtsansicht vor

Auf Rohdaten der gesammelten Daten zugreifen

Alle gesammelten Daten werden in die folgenden entsprechenden Tabellen importiert. Weitere Informationen zum Tabellen Schema finden Sie unter [Definieren des Datensammler Satzes](#).

- registry
 - RegistryKeys #
- WMI
 - wmiobjects-#
 - wmiobjectproperties-#
 - #wmiqueries

- Leistungsindikator
 - #Performance Counters
- File
 - #Dateien
- ETW
 - Ereignisse #
 - #eventproperties

Festlegen des Regel Status

Der [dbo].[setnotification] API den Regel Status festlegt, wird auf der Benutzeroberfläche ein Symbol für Erfolg oder Warnung angezeigt.

- @ruleName nvarchar (50)
- @adviceName nvarchar (50)

Die Warn-und Empfehlungs Nachrichten werden in der XML-Datei mit den Bereitstellungs Metadaten gespeichert. Dadurch wird das Berichts Skript einfacher zu verwalten.

Anfänglich ist jeder Regel Status N/v. Sie können diese API verwenden, um einen Regel Status festzulegen, indem Sie einen Namen für die Empfehlung angeben. Der Name der Empfehlung wird als Regel Status verwendet.

Denken Sie daran, dass wir die folgende Regel bereits definiert haben:

```
<rule name="freediskSize" caption="Free Disk Size on System Drive" description="This rule checks free disk size on the system drive ">
<advice name="SuccessAdvice" level="Success" message="No issue found.">No recommendation.</advice>
<advice name="WarningAdvice" level="Warning" message="Not enough free space on system drive.">Install the operating system on a larger disk.</advice>
</rule>
```

Wenn der freie Speicherplatz weniger als 2 GB beträgt, muss die Regel auf die Warnstufe festgelegt werden.

Das SQL-Skript sieht wie folgt aus:

```
if (@freediskSizeInGB < 2)
BEGIN
    exec dbo.SetNotification N'freediskSize', N'WarningAdvice'
END
ELSE
BEGIN
    exec dbo.SetNotification N'freediskSize', N'SuccessAdvice'
END
```

Schwellenwert erhalten

Der [dbo].[getthreshold] API die Schwellenwerte abrufen:

- @key nvarchar (50)
- @value float-Ausgabe

NOTE

Die Schwellenwerte sind Name-Wert-Paare, auf die in beliebigen Regeln verwiesen werden kann. Die Systemadministratoren können die-Konsole verwenden, um die Schwellenwerte zu ändern.

Wenn Sie mit dem vorherigen Beispiel fortfahren, lautet die Definition für einen Schwellenwert wie folgt:

```
<thresholds>
  <threshold name="freediskSize" caption="Free Disk Size (GB)" description="Free Disk Size value="10" />
</thresholds>
<rule name="freediskSize" caption="Free Disk Size on System Drive" description="This rule checks free disk size on system drive">
  <advice name="SuccessAdvice" level="Success" message="No issue found.">No recommendation.</advice>
  <advice name="WarningAdvice" level="Warning" message="Not enough free space on the system drive.">
    Install the operating system on a larger disk.</advice>
  <dependencies>
    <threshold ref="freediskSize"/>
  </dependencies>
</rule>
```

Das Berichts Skript kann wie hier gezeigt geändert werden:

```
DECLARE @freediskSize FLOat
exec dbo.GetThreshold N freediskSize , @freediskSize output

if (@freediskSizeInGB < @freediskSize)
```

Festlegen oder Entfernen eines einzelnen Werts

Der [dbo].[setsinglevalue]-API legt den einzelnen Wert fest:

- @key nvarchar (50)
- @value SQL_-Variant

Dieser Wert kann mehrmals für den gleichen Einzelwert Schlüssel ausgeführt werden. Der letzte Wert wird gespeichert.

Das folgende Beispiel zeigt einige definierte Einzelwerte:

```
<singleValue section="Systemoverview" caption="Facts">
  <value name="OsName" type="string" caption="Operating System" description="WMI: Win32_OperatingSystem/Caption"/>
  <value name="Osversion" type="string" caption="OS version" description="WMI: Win32_OperatingSystem/version"/>
  <value name="OsLocation" type="string" caption="OS Location" description="WMI: Win32_OperatingSystem/SystemDrive"/>
</singleValue>
```

Anschließend können Sie den einzelnen Wert festlegen, wie hier gezeigt:

```
exec dbo.SetSingleValue N OsName , Windows 7
exec dbo.SetSingleValue N Osversion , 6.1.7601
exec dbo.SetSingleValue N OsLocation , c:\
```

In seltenen Fällen möchten Sie möglicherweise das zuvor festgelegte Ergebnis mithilfe der [dbo]-entfernen. [removesinglevalue] API.

- @key nvarchar (50)

Sie können das folgende Skript verwenden, um den zuvor festgelegten Wert zu entfernen.

```
exec dbo.removeSingleValue N Osversion
```

Sammeln von Informationen zur Datensammlung

Der [dbo-].[getduration]-API ruft die vom Benutzer festgelegte Dauer in Sekunden für die Datensammlung ab:

- @duration int-Ausgabe

Hier ist ein Beispiel für ein Berichts Skript:

```
DECLARE @duration int
exec dbo.GetDuration @duration output
```

Der [dbo-].[getinternal]-API ruft das Intervall eines Leistungs Zählers ab. Der Wert kann NULL zurückgeben, wenn der aktuelle Bericht keine Leistungsdaten des Leistungs Zählers enthält.

- @interval int-Ausgabe

Hier ist ein Beispiel für ein Berichts Skript:

```
DECLARE @interval int
exec dbo.GetInterval @interval output
```

Festlegen einer Listen Wert Tabelle

Es ist keine API zum Aktualisieren von Listen Wert Tabellen vorhanden. Sie können jedoch direkt auf die Listen Wert Tabellen zugreifen. in der Initialisierungsphase wird eine entsprechende temporäre Tabelle für jeden Listen Wert erstellt.

Das folgende Beispiel zeigt eine Listen Wert Tabelle:

```
<listValue name="NetworkAdapterInformation" section="NetworkIOFacts" caption="Physical Network Adapter Information">
<column name="NetworkAdapterId" type="string" caption="ID" description="WMI: Win32_NetworkAdapter/DeviceID"/>
<column name="NetworkAdapterName" type="string" caption="Name" description="WMI: Win32_NetworkAdapter/Name"/>
<column name="type" type="string" caption="type" description="WMI: Win32_NetworkAdapter/Adaptertype"/>
<column name="Speed" type="decimal" caption="Speed (Mbps)" description="WMI: Win32_NetworkAdapter/Speed"/>
<column name="MACAddress" type="string" caption="MAC address" description="WMI: Win32_NetworkAdapter/MACaddress"/>
</listValue>
```

Anschließend können Sie ein SQL-Skript schreiben, um die Ergebnisse einzufügen, zu aktualisieren oder zu löschen:

```
INSERT INTO #NetworkAdapterInformation (
    NetworkAdapterId,
    NetworkAdapterName,
    type,
    Speed,
    MACAddress
)
VALUES (
)
```

Entwicklung und Debuggen

Schreiben von Protokollen

Wenn weitere Informationen vorhanden sind, die Sie mit den Systemadministratoren kommunizieren möchten, können Sie Protokolle schreiben. Wenn ein Protokoll für einen bestimmten Bericht vorhanden ist, wird ein gelbes Banner in der Berichts Kopfzeile angezeigt. Im folgenden Beispiel wird gezeigt, wie Sie ein Protokoll schreiben können:

```
exec dbo.WriteSystemLog N'Any information you want to show to the system administrators , N Warning
```

Der erste Parameter ist die Meldung, die im Protokoll angezeigt werden soll. Der zweite Parameter ist die Protokollebene. Die gültige Eingabe für den zweiten Parameter kann " **Information**", " **Warning**" oder " **Error**" lauten.

Debugprotokolle

Die Spa-Konsole kann in zwei Modi ausgeführt werden: "Debug" oder "Release". Der Releasemodus ist die Standardeinstellung und bereinigt alle gesammelten Rohdaten, nachdem der Bericht generiert wurde. Im Debugmodus werden alle Rohdaten in der Dateifreigabe und in der Datenbank gespeichert, sodass Sie das Berichts Skript in Zukunft Debuggen können.

So debuggen Sie ein Berichts Skript

1. Installieren Sie Microsoft SQL Server Management Studio (SSMS).
2. Stellen Sie nach dem Starten von SSMS eine Verbindung mit localhost\SQLExpress her. Beachten Sie, dass Sie localhost anstelle von verwenden müssen.. Andernfalls können Sie den Debugger möglicherweise nicht in SQL Server starten.
3. Führen Sie folgendes Skript aus, um den Debugmodus zu aktivieren:

```
USE SPADB
UPDATE dbo.Configurations
SET Value = N'true'
WHERE Name = N'Debugmode'
```

4. Starten Sie die-Konsole, und führen Sie das Advisor-Paket aus, das Sie debuggen möchten.
5. Warten Sie, bis die Aufgabe beendet wurde. Wenn der Bericht erfolgreich generiert wurde, wechseln Sie zurück zu SSMS, und suchen Sie nach der aktuellen Aufgabe.

```
select TOP 1 * FROM dbo.Tasks ORDER BY Id DESC
```

Beispielsweise könnte die Ausgabe wie folgt lauten:

ID	SESSIONID	ADVISORYPACK AGEID	REPORTSTATUS -ID	LASTUPDATETI ME	STAMMOLDVER SIONID
12	17	1	2	2011-05-11 05:35:24.387	1

6. Sie können das folgende Skript so oft ausführen, wie Sie das Berichts Skript für ID 12 ausführen möchten:

```
exec dbo.DebugReportScript 12
```

Hinweis Sie können auch F11 drücken, um die vorherige Anweisung zu durchlaufen und zu debuggen.

Ausführen [dbo].[debugreportscript] gibt mehrere Resultsets zurück, einschließlich:

1. Microsoft SQL Server Meldungen und Advisor Pack-Protokolle
2. Ergebnisse von Regeln
3. Statistik Schlüssel und-Werte
4. Einzelne Werte
5. Alle Listen Wert Tabellen

Bewährte Verfahren

Benennungs Konventionen und Stile

PASCAL-SCHREIBWEISE	CAMEL-CASE-SCHREIBWEISE	GROSSBUCHSTABEN
<ul style="list-style-type: none"> • Namen in "provisionmetadata.xml" • Gespeicherte Prozeduren • Funktionen • Namen anzeigen • Temporäre Tabellennamen 	<ul style="list-style-type: none"> • Parameternamen • Lokale Variablen 	Für alle reservierten SQL-Schlüsselwörter verwenden

Weitere Empfehlungen

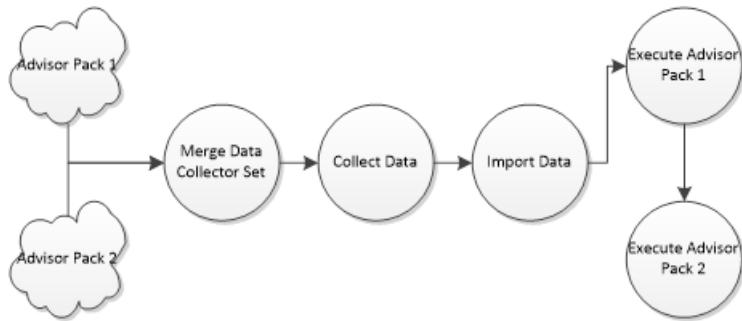
- Verschieben Sie die meisten logischen Teile in andere gespeicherte Prozeduren und benutzerdefinierte Funktionen.
- Machen Sie Ihr Hauptskript zu Wartungszwecken so kurz wie möglich.
- Verwenden Sie den vollständigen Namen des SQL-Objekts.
- Behandeln Sie den SQL-Code als Groß-/Kleinschreibung
- Fügen Sie SET NOCOUNT am Anfang jeder gespeicherten Prozedur hinzu.
- Verwenden Sie temporäre Tabellen für die Übertragung großer Datenmengen.
- Verwenden Sie ggf. Set XACT_Abort on , um den Prozess zu beenden, wenn ein Fehler auftritt.
- Schließen Sie die Hauptversionsnummer immer in den Anzeige Namen des Advisor-Pakets ein.

Erweiterte Themen

Gleichzeitiges Ausführen mehrerer Advisor-Pakete

Spa unterstützt gleichzeitig das Ausführen mehrerer Advisor Packs. Dies ist besonders nützlich, wenn Sie die Leistung von Internetinformationsdienste (IIS) und des Kern Betriebssystems gleichzeitig untersuchen möchten. Viele Datensammler, die vom IIS Advisor Pack verwendet werden, können auch vom Core OS Advisor Pack verwendet werden. Wenn zwei oder mehr Advisor-Pakete auf demselben Zielcomputer ausgeführt werden, sammelt Spa die gleichen Daten nicht zweimal.

Das folgende Beispiel zeigt den Workflow für das Ausführen von zwei Advisor-Paketen.



Der Zusammenführungs Daten-sammlersatz dient nur zum Erfassen von Leistungsdaten Quellen und etw-Datenquellen. Die folgenden Zusammenschluss Regeln gelten:

1. Spa hat die größte Dauer wie die neue Dauer.
2. Bei Mergekonflikten werden folgende Regeln befolgt:
 - a. Nehmen Sie das kleinste Intervall für das neue Intervall an.
 - b. Nehmen Sie die Obermenge der Leistungsindikatoren an. Beispielsweise werden mit dem Prozess (*)\% Prozessorzeit und Prozess (*)*\Prozess (*)\\ * mehr Daten zurückgegeben, sodass Prozess (*)\Prozessorzeit (%) und Prozess (*)\\ * aus dem zusammengeföhrten Datensammler Satz entfernt wird.

Dynamische Daten erfassen

Spa benötigt zur Entwurfszeit einen definierten Datensammler Satz. Es ist nicht immer möglich zu wissen, welche Daten für die Bericht Generierung benötigt werden, da die dynamischen Daten und der Abfrage Pfad erst bekannt sind, wenn die abhängigen Daten verfügbar sind.

Wenn Sie z. b. alle anzeigen Amen von Netzwerkadapters auflisten möchten, müssen Sie zuerst WMI Abfragen, um alle Netzwerkadapter aufzuzählen. Jedes zurückgegebene WMI-Objekt verfügt über einen Registrierungsschlüssel Pfad, in dem der Anzeige Name gespeichert wird. Der Registrierungsschlüssel Pfad ist zur Entwurfszeit nicht bekannt. In diesem Fall benötigen wir dynamische Daten Unterstützung.

Zum Auflisten aller Netzwerkadapter können Sie die folgende WMI-Abfrage mithilfe von Windows PowerShell verwenden:

```
Get-WmiObject -Namespace Root\Cimv2 -query "select PNPDeviceID FROM Win32_NetworkAdapter" | foreach-object { Write-Output $_.PNPDeviceID }
```

Es wird eine Liste der Netzwerkadapter Objekte zurückgegeben. Jedes-Objekt verfügt über eine Eigenschaft mit dem Namen "**pnpdebug Eid**", die einen relativen Registrierungsschlüssel Pfad beibehält. Hier sehen Sie eine Beispieldaten aus der vorherigen Abfrage:

```
ROOT\*ISatAP\0001
PCI\VEN_8086&DEV_4238&SUBSYS_11118086&REV_35\4&372A6B86&0&00E4
ROOT\*IPHTTPS\0000
```

Um den Wert **FriendlyName** zu ermitteln, öffnen Sie den Registrierungs-Editor, und navigieren Sie zu der Registrierungs Einstellung, indem Sie **HKEY_lokalen_Machine\System\CurrentControlSet\Enum-** mit jeder Zeile im vorherigen Beispiel kombinieren. Beispiel:

HKEY_local_Machine\System\CurrentControlSet\Enum\ root*IPHTTPS\0000.

Fügen Sie das Skript im folgenden Codebeispiel hinzu, um die vorherigen Schritte in die Spa-Bereitstellungs Metadaten zu übersetzen:

```
<advisorPack>
<dataSourceDefinition xmlns="https://microsoft.com/schemas/ServerPerformanceAdvisor/dc/2010">
  <dataCollectorSet >
    <registryKeys>
      ?
      <registryKey>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\$({NetworkAdapter.PNPDeviceID})\FriendlyName</re
      gistryKey>
    </registryKeys>
    <managementpaths>
      ?<path name="NetworkAdapter">Root\Cimv2:select PNPDeviceID FROM Win32_NetworkAdapter</path>
    </managementpaths>
```

In diesem Beispiel fügen Sie zunächst eine WMI-Abfrage unter Management Path hinzu und definieren den Schlüsselnamen **NetworkAdapter**. Fügen Sie dann einen Registrierungsschlüssel hinzu, und verweisen Sie mithilfe der Syntax **\$ (NetworkAdapter. pnpdeviceid)** auf **Network Adapter**.

In der folgenden Tabelle wird definiert, ob ein Datensammler in Spa dynamische Daten unterstützt und ob von anderen Datensammern darauf verwiesen werden kann:

DATENTYP	DYNAMISCHE DATEN UNTERSTÜTZEN	KANN REFERENZIERT WERDEN
Registrierungsschlüssel	„Ja“	„Ja“
WMI	„Ja“	„Ja“
File	„Ja“	Nein
Leistungsindikator	Nein	Nein
ETW	Nein	Nein

Bei einem WMI-Datensammler verfügt jedes WMI-Objekt über viele angefügte Attribute. Jeder Typ von WMI-Objekt hat immer drei Attribute: **_Namespace**, **_Klasse** und **_RelPath**.

Um einen Datensammler zu definieren, auf den von anderen Datensammern verwiesen wird, weisen Sie das **Name** -Attribut mit einem eindeutigen Schlüssel in der Datei "provisionmetadata.xml" zu. Dieser Schlüssel wird von abhängigen Datensammern verwendet, um dynamische Daten zu generieren.

Hier ist ein Beispiel für den Registrierungsschlüssel:

```
<registryKey name="registry">HKEY_LOCAL_MACHINE </registryKey>
```

Und ein Beispiel für WMI:

```
<path name="wmi">Root\Cimv2:select PNPDeviceID FROM Win32_NetworkAdapter</path>
```

Zum Definieren eines abhängigen Daten Sammlers wird die folgende Syntax verwendet: **\$ ({Name}). {Attribute}**

).

" {Name} " und " {Attribute} " sind Platzhalter.

Wenn das Spa Daten von einem Zielserver sammelt, ersetzt es dynamisch das Muster \$ (***) durch die tatsächlich gesammelten Daten aus dem zugehörigen Verweis Datensammler (Registrierungsschlüssel/WMI), z. b.:

```
<registryKey>HKEY_LOCAL_MACHINE\$(registry.key)\ </registryKey>
<registryKey name="registry">HKEY_LOCAL_MACHINE\$(wmi.Relativeregistrypath)\ </registryKey>
<path name="wmi"> </path>
<file>$(wmi.FileName)</file>
```

Hinweis Spa unterstützt eine unbegrenzte Tiefe der Referenz, aber beachten Sie den Leistungs Aufwand, wenn Sie zu viele Ebenen haben. Stellen Sie sicher, dass kein Zirkel Verweis oder selbst Verweis vorhanden ist, der nicht unterstützt wird.

Einschränkungen der Versionsverwaltung

Spa unterstützt Updates für zurücksetzen und neben Versionen. Diese Prozesse verwenden denselben Algorithmus. Der Prozess besteht darin, alle Datenbankobjekte und Schwellenwert Einstellungen zu aktualisieren, aber die vorhandenen Daten beizubehalten. Dies kann auf eine höhere Version aktualisiert oder auf eine niedrigere Version herabgestuft werden. Wählen Sie das Advisor-Paket aus, und klicken Sie dann im Dialogfeld **Advisor-Pakete konfigurieren** in Spa auf zurück **setzen**, um die Updates zurückzusetzen oder anzuwenden.

Diese Funktion ist hauptsächlich bei geringfügigen Updates. Die Anzeigeelemente der Benutzeroberfläche können nicht drastisch geändert werden. Wenn Sie bedeutende Änderungen vornehmen möchten, müssen Sie ein anderes Advisor-Pack erstellen. Sie sollten die Hauptversion in den Advisor Pack-Namen einschließen.

Die Einschränkungen von Änderungen an der geringfügigen Version bestehen darin, dass Sie keine der folgenden Aktionen ausführen können :

- Ändern des Schema namens
- Ändern des Datentyps einer einzelnen Wertegruppe oder der Spalten einer Listen Wert Tabelle
- Schwellenwerte hinzufügen oder entfernen
- Regeln hinzufügen oder entfernen
- Hinzufügen oder Entfernen von Empfehlungen
- Einzelne Werte hinzufügen oder entfernen
- Hinzufügen oder Entfernen von Listen Werten
- Hinzufügen oder Entfernen einer Spalte mit Listen Werten

Quick Infos

Fast alle **Beschreibungs** Attribute werden in der Spa-Konsole als QuickInfo angezeigt.

für eine Listen Wert Tabelle kann eine zeilenbasierte QuickInfo durch Hinzufügen des folgenden Attributs erreicht werden:

```
<listValue descriptionColumn="Description">
<column name="Name"/>
<column name="Description"/>
</listValue>
```

Das **descriptioncolumn**-Attribut verweist auf den Namen der Spalte. In diesem Beispiel wird die Beschreibungs Spalte nicht als physische Spalte angezeigt. Es wird jedoch als QuickInfo angezeigt, wenn Sie mit der Maus auf die einzelnen Zeilen der ersten Spalte zeigen.

Es wird empfohlen, dass in der QuickInfo die Datenquelle für den Benutzer angezeigt wird. Im folgenden finden Sie die folgenden Formate für die Anzeige der Datenquellen:

DATENQUELLE	FORMAT	BEISPIEL
WMI	WMI: <WMIClass->/<Feld>	WMI: Win32_OperatingSystem/Caption
Leistungsindikator	PerfCounter: <CategoryName>/<instanceName>	PerfCounter: Prozess\Prozessorzeit (%)
registry	Registrierung: <Register Key>	Registrierung: HKLM\Software\Microsoft \ASP.net\Rootver
Konfigurationsdatei	Configfile: <filePath> [; XPath: <XPath->] Hinweis XPath ist optional und nur gültig, wenn es sich bei der Datei um eine XML-Datei handelt.	Configfile: windir%\System32\inetsrv\config\ApplicationHost.config XPath: Configuration\System. Webserver \httpProtocol@allowKeepAlive
ETW	Etw: <Provider/>(Schlüsselwörter)	Etw: Windows-Kernel-Ablauf Verfolgung (Prozess, net)

Tabellen Sortierung

Wenn ein Advisor-Paket komplizierter wird, können Sie eigene Variablen Tabellen oder temporäre Tabellen erstellen, um Zwischenergebnisse im Berichts Skript zu speichern.

Das Sortieren von Zeichen folgen Spalten kann problematisch sein, da die von Ihnen erstellte Tabellen Sortierung sich von der Tabelle unterscheiden kann, die durch das Spa-Framework erstellt wird. Wenn Sie zwei Zeichen folgen Spalten in verschiedenen Tabellen korrelieren, wird möglicherweise ein Sortierungs Fehler angezeigt. Um dieses Problem zu vermeiden, sollten Sie immer die Zeichenfolge für eine Spalten Sortierung als **SQL_latin1_allgemein_CP1_CI_** definieren, als wenn Sie eine Tabelle definieren.

Hier finden Sie Informationen zum Definieren einer Variablen Tabelle:

```
DECLARE @filesIO TABLE (
    Name nvarchar(500) COLLATE SQL_Latin1_General_CI_AS,
    AverageFileAccessvolume float,
    AverageFileAccessCount float,
    Filepath nvarchar(500) COLLATE SQL_Latin1_General_CI_AS
)
```

Etw erfassen

Hier finden Sie Informationen zum Definieren von etw in einer Datei "provisionmetadata.xml":

```
<dataSourceDefinition>
    <providers>
        <provider session="NT Kernel Logger" guid="{9E814AAD-3204-11D2-9A82-006008A86939}"/>
    </providers>
</dataSourceDefinition>
```

Die folgenden Anbieter Attribute sind für die Erfassung von etw verfügbar:

ATTRIBUT	GEBEN SIE IN DAS SUCHFELD AUF DER TASKLEISTE	BESCHREIBUNG
guid	GUID	Anbieter-GUID
Sitzung	String	Etw-Sitzungsname (optional, nur für Kernel Ereignisse erforderlich)
keywordsany	Hexadezimal	Beliebige Schlüsselwörter (optional, kein 0x-Präfix)
keywordsall	Hexadezimal	Alle Schlüsselwörter (optional)
Eigenschaften	Hexadezimal	Eigenschaften (optional)
level	Hexadezimal	Ebene (optional)
bufferSize	Ganze Zahl	Puffergröße (optional)
flushtime	Ganze Zahl	Leerungs Zeit (optional)
maxBuffer	Ganze Zahl	Maximaler Puffer (optional)
minbuffer	Ganze Zahl	Minimaler Puffer (optional)

Es gibt zwei Ausgabe Tabellen, wie hier gezeigt.

Tabellen Schema für #Ereignisse

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
SequenceID	Int not NULL	Korrelations Sequenz-ID
Eventtypeid	Int not NULL	Ereignistyp-ID (siehe [dbo].[EventTypes])
ProcessId	Bigint not NULL	Prozess-ID
ThreadID	Bigint not NULL	Thread-ID
timestamp	datetime2 nicht NULL	timestamp
Kernelzeit	Bigint not NULL	Kernel Zeit
Usertime	Bigint not NULL	Benutzer Zeit

#eventproperties-Tabellen Schema

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
SequenceID	Int not NULL	Korrelations Sequenz-ID

NAME DER SPALTE	SQL-DATENTYP	BESCHREIBUNG
Name	Nvarchar (100)	Eigenschaftenname
Value	Nvarchar(4000)	Value

Etw-Schema

Ein etw-Schema kann durch Ausführen von "tracerpt. exe" für die ETL-Datei generiert werden. Eine "Schema. man"-Datei wird generiert. Da das Format der ETL-Datei Computer abhängig ist, funktioniert das folgende Skript nur in den folgenden Situationen:

1. Führen Sie das Skript auf dem Computer aus, auf dem die entsprechende ETL-Datei gesammelt wird.
2. Oder führen Sie das Skript auf einem Computer aus, auf dem dasselbe Betriebssystem und dieselben Komponenten installiert sind.

```
tracerpt *.etl -export
```

Glossar

In diesem Dokument werden die folgenden Begriffe verwendet:

Advisor-Pack

Ein Advisor-Paket ist eine Sammlung von Metadaten und SQL-Skripts, die die Leistungs Protokolle verarbeiten, die vom Zielserver gesammelt werden. Das Advisor-Pack generiert dann Berichte aus den Leistungs Protokolldaten. Die Metadaten im Advisor-Pack definieren die Daten, die vom Zielserver für Leistungsmessungen gesammelt werden sollen. Die Metadaten definieren auch den Satz von Regeln, die Schwellenwerte und das Berichtsformat. In den meisten Fällen wird ein Advisor-Pack speziell für eine einzelne Server Rolle geschrieben, z. b. Internetinformationsdienste (IIS).

Spa-Konsole

Die Spa-Konsole bezieht sich auf spaconsole. exe, das der zentrale Bestandteil von Server Performance Advisor ist. Die Spa muss nicht auf dem Zielserver ausgeführt werden, den Sie testen. Die Spa-Konsole enthält alle Benutzeroberflächen für Spa, von der Einrichtung des Projekts bis hin zur Ausführung von Analysen und Anzeigen von Berichten. Das Spa ist eine Anwendung mit zwei Ebenen. Die Spa-Konsole enthält die UI-Schicht und einen Teil der Geschäftslogik Ebene. Die Spa-Konsole plant und verarbeitet Leistungsanalyse Anforderungen.

Spa-Framework

Spa enthält zwei Hauptkomponenten: das Framework und die Advisor-Pakete. Das Spa-Framework bietet alle Benutzeroberflächen, die Verarbeitung von Leistungs Protokollen, die Konfiguration, die Fehlerbehandlung und Datenbank-APIs sowie Verwaltungs Prozeduren.

Spa-Projekt

Ein Spa-Projekt ist eine Datenbank, die alle Informationen zu den Ziel Servern, Advisor Packs und Leistungsanalyse Berichten enthält, die auf den Ziel Servern für die Advisor-Pakete generiert werden. Sie können Verlaufs-und Trenddiagramme innerhalb desselben Spa-Projekts vergleichen und anzeigen. Der Benutzer kann mehr als ein Projekt erstellen. Die Spa-Projekte sind voneinander unabhängig, und es gibt keine Daten, die von allen Projekten gemeinsam genutzt werden.

Zielserver

Der Zielserver ist der physische oder virtuelle Computer, auf dem der Windows-Server mit bestimmten Server Rollen (z. b. IIS) ausgeführt wird.

Datenanalyse Sitzung

Eine Datenanalyse Sitzung ist eine Leistungsanalyse auf einem bestimmten Zielserver. Eine Datenanalyse Sitzung kann mehrere Advisor-Pakete enthalten. Die Datensammler Sätze aus diesen Advisor-Paketen werden zu einem einzelnen Datensammler Satz zusammengeführt. Alle Leistungs Protokolle für eine einzelne Datenanalyse Sitzung werden innerhalb desselben Zeitraums gesammelt. Das Analysieren von Berichten, die von Advisor-Paketen generiert werden, die in derselben Datenanalyse Sitzung ausgeführt werden, kann Benutzern helfen, die Gesamtleistung zu verstehen und die Ursachen für Leistungsprobleme zu identifizieren.

Ereignisablaufverfolgung für Windows

Die Ereignis Ablauf Verfolgung für Windows ([Event Tracing](#) for Windows, etw) ist ein hochleistungsfähiges, skalierbares Ablauf Verfolgungssystem, das in den Windows-Betriebssystemen bereitgestellt wird. Es bietet Profil Erstellungs-und Debuggingfunktionen, die zur Problembehandlung für eine Vielzahl von Szenarien verwendet werden können. Spa verwendet ETW-Ereignisse als Datenquelle zum Erstellen von Leistungs Berichten. Allgemeine Informationen zu etw finden Sie unter verbessertes [Debugging und Leistungsoptimierung mit etw](#).

WMI-Abfrage

Windows-Verwaltungsinstrumentation (WMI) ist die Infrastruktur für Verwaltungsdaten und Vorgänge in Windows-Betriebssystemen. Sie können WMI-Skripts oder-Anwendungen schreiben, um administrative Aufgaben auf Remote Computern zu automatisieren. WMI stellt auch Verwaltungsdaten für andere Teile des Betriebssystems und für Produkte bereit. Spa verwendet WMI-Klassen Informationen und Datenpunkte als Quellen zum Erstellen von Leistungs Berichten.

Leistungsindikatoren

Leistungsindikatoren werden verwendet, um Informationen darüber bereitzustellen, wie gut die Leistung des Betriebssystems oder einer Anwendung, eines Diensts oder Treibers ist. Die Leistungsdaten können Ihnen helfen, Engpässe im System zu ermitteln und die System-und Anwendungsleistung zu optimieren. Das Betriebssystem, das Netzwerk und die Geräte bieten Leistungsdaten, die von einer Anwendung genutzt werden können, um Benutzern eine grafische Ansicht der Leistung des Systems zu bieten. Die Spa verwendet Leistungsdaten und Datenpunkte als Quellen zum Generieren von Leistungs Berichten.

Leistungsprotokolle und -warnungen

Leistungsprotokolle und-Warnungen (PLA) ist ein integrierter Dienst im Windows-Betriebssystem. Es ist für die Erfassung von Leistungs Protokollen und Ablauf Verfolgungen konzipiert und löst auch Leistungs Warnungen aus, wenn bestimmte Trigger erfüllt sind. Mithilfe von Pla können Leistungsindikatoren, Ereignis Ablauf Verfolgung für Windows (ETW), WMI-Abfragen, Registrierungsschlüssel und Konfigurationsdateien erfasst werden. Außerdem unterstützt die Verwendung von Remote Prozedur aufrufen (RPC) die Remote Datensammlung. Der Benutzer definiert einen Datensammler Satz, der Informationen über die zu sammelnden Daten, die Häufigkeit der Datensammlung, die Dauer der Datenerfassung, Filter und einen Speicherort zum Speichern der Ergebnisdateien enthält. Spa sammelt mithilfe von PLA alle Leistungsdaten von den Ziel Servern.

Einzelner Bericht

Ein einzelner Bericht ist der Spa-Bericht, der auf der Grundlage einer Datenanalyse Sitzung für ein Advisor Pack auf einem einzelnen Zielserver generiert wird. Es kann Benachrichtigungen und verschiedene Datenabschnitte enthalten.

Paralleler Bericht

Ein paralleler Bericht ist ein Spa-Bericht, in dem zwei einzelne Berichte für dasselbe Advisor Pack verglichen

werden. Die beiden Berichte können von verschiedenen Ziel Servern oder von separaten Leistungsanalysen auf demselben Zielserver generiert werden. Der parallele Bericht erstellt die Funktion zum Vergleichen von zwei Berichten, damit Benutzer ungewöhnliche Verhalten oder Einstellungen in einem der Berichte identifizieren können. Ein paralleler Bericht enthält Benachrichtigungen und verschiedene Datenabschnitte. In jedem Abschnitt werden die Daten aus beiden Berichten nebeneinander aufgelistet.

Trend Diagramm

Ein Trend Diagramm ist der Spa-Bericht, der verwendet wird, um sich wiederholende Muster von Leistungsproblemen zu untersuchen. Viele sich wiederholende Leistungsprobleme werden durch geplante Server Lade Änderungen vom Server oder von Client Computern verursacht, die täglich oder wöchentlich auftreten können. Spa bietet ein 24-Stunden-Trend Diagramm und ein 7-Tage-Trend Diagramm, um diese Probleme zu identifizieren.

Der Benutzer kann eine oder mehrere Datenreihen gleichzeitig auswählen, wobei es sich um einen numerischen Wert innerhalb des einzelnen Berichts handelt, z. b. die **durchschnittliche CPU-Gesamtauslastung**. genauer gesagt handelt es sich bei einem numerischen Wert um einen skalaren Wert von einem einzelnen Server, der von einem einzelnen AP-Wert zu einer bestimmten Zeit Instanz generiert wird. Spa gruppiert diese Werte in 24 Gruppen, eine für jede Stunde des Tages (sieben für einen 7-tägigen Bericht, eine für jeden Tag der Woche). Spa berechnet durchschnittliche, minimale, maximale und standardmäßige Abweichungen für jede Gruppe.

Verlaufs Diagramm

Ein Verlaufs Diagramm ist der Spa-Bericht, der verwendet wird, um Änderungen an bestimmten numerischen Werten in einzelnen Berichten für ein bestimmtes Server-und Advisor Pack-Paar im Zeitverlauf anzuzeigen. Der Benutzer kann mehrere Datenreihen auswählen und diese zusammen im Verlaufs Diagramm anzeigen, um die Korrelation zwischen verschiedenen Datenreihen nachzuvollziehen.

Datenreihe

Bei einer Datenreihe handelt es sich um numerische Daten, die über einen bestimmten Zeitraum aus derselben Datenquelle gesammelt werden. Dieselbe Quelle bedeutet, dass die Daten vom gleichen Zielserver stammen müssen, z. b. die durchschnittliche Länge der Anforderungs Warteschlange für IIS auf einem Server.

Regeln

Regeln sind Kombinationen aus Logik, Schwellenwerten und Beschreibungen. Sie stellen ein mögliches Leistungsproblem dar. Jedes Advisor-Paket enthält mehrere Regeln. Jede Regel wird durch einen Bericht Generierungsprozess ausgelöst. Eine Regel wendet die Logik und die Schwellenwerte auf die Daten in einem einzelnen Bericht an. Wenn die Kriterien erfüllt sind, wird eine Warnmeldung ausgelöst. Wenn dies nicht der Fall ist, wird die Benachrichtigung auf den Status OK festgelegt. Wenn die Regel nicht angewendet wird, wird die Benachrichtigung auf den Status nicht zutreffend (na) festgelegt.

Benachrichtigungen

Eine Benachrichtigung sind die Informationen, die von einer Regel für Benutzer angezeigt werden. Sie enthält den Status der Regel ("OK", "na" oder "Warnung"), den Namen der Regel und mögliche Empfehlungen, um die Leistungsprobleme zu beheben.

Windows-Befehle

13.06.2020 • 18 minutes to read • [Edit Online](#)

Für alle unterstützten Versionen von Windows (Server und Client) ist eine Reihe von Win32-Konsolen Befehlen integriert.

In diesem Dokumentations Satz werden die Windows-Befehle beschrieben, die Sie zum Automatisieren von Aufgaben mithilfe von Skripts oder Skript Erstellungs Tools verwenden können.

Wenn Sie Informationen zu einem bestimmten Befehl suchen möchten, klicken Sie im folgenden a-Z-Menü auf den Buchstaben, mit dem der Befehl beginnt, und klicken Sie dann auf den Befehlsnamen.

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [F](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [J](#) | [Z](#)

Voraussetzungen

Die in diesem Thema enthaltenen Informationen gelten für:

- Windows Server 2019
- Windows Server (Halbjährlicher Kanal)
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- WindowsServer 2008
- Windows 10
- Windows 8.1

Übersicht über Befehlsshell

Die Befehlsshell war die erste Shell, die in Windows integriert wurde, um Routineaufgaben wie die Verwaltung von Benutzerkonten oder nächtliche Sicherungen mit Batch Dateien (BAT-Dateien) zu automatisieren. Mit Windows Script Host können Sie komplexere Skripts in der Befehlsshell ausführen. Weitere Informationen finden Sie unter [cscript](#) oder [WScript](#). Sie können Vorgänge effizienter mithilfe von Skripts ausführen, als dies mithilfe der Benutzeroberfläche möglich ist. Skripts akzeptieren alle Befehle, die in der Befehlszeile verfügbar sind.

Windows verfügt über zwei Befehls Shells: die Befehlsshell und [PowerShell](#). Bei jeder Shell handelt es sich um ein Softwareprogramm, das eine direkte Kommunikation zwischen Ihnen und dem Betriebssystem oder der Anwendung ermöglicht und eine Umgebung zum Automatisieren des IT-betriebsbereit stellt

PowerShell wurde entwickelt, um die Funktionen der Befehlsshell zum Ausführen von PowerShell-Befehlen zu erweitern, die als Cmdlets bezeichnet werden. Cmdlets ähneln Windows-Befehlen, bieten jedoch eine erweiterbare Skriptsprache. Sie können Windows-Befehle und PowerShell-Cmdlets in PowerShell ausführen, aber in der Befehlsshell können nur Windows-Befehle und keine PowerShell-Cmdlets ausgeführt werden.

Bei der stabilsten aktuellen Windows-Automatisierung empfiehlt es sich, PowerShell anstelle von Windows-Befehlen oder Windows Script Host für Windows Automation zu verwenden.

NOTE

Sie können auch [PowerShell Core](#) herunterladen und installieren, die Open Source-Version von PowerShell.

Caution

Durch eine fehlerhafte Bearbeitung der Registrierung können schwerwiegende Schäden am System verursacht werden. Bevor Sie die folgenden Änderungen an der Registrierung vornehmen, sollten Sie alle wichtigen Daten auf dem Computer sichern.

NOTE

Führen Sie **regedit.exe** aus, und legen Sie den folgenden **reg_DWord Wertfest**, um die Vervollständigung von Datei- und Verzeichnisnamen in der Befehlsshell für eine Computer- oder Benutzer Anmelde Sitzung zu aktivieren bzw

HKEY_LOCAL_MACHINE \software\microsoft\command processor\completionchar\ reg_DWord

Um den **reg_DWord Wert festzulegen**, verwenden Sie den Hexadezimalwert eines Steuer Zeichens für eine bestimmte Funktion (z. b. **0 9** ist Tab und **0 08** ist RÜCKTASTE). Benutzerdefinierte Einstellungen haben Vorrang vor Computereinstellungen, und Befehlszeilenoptionen haben Vorrang vor den Registrierungs Einstellungen.

Befehlszeilen Referenz A-Z

Wenn Sie Informationen zu einem bestimmten Windows-Befehl suchen möchten, klicken Sie im folgenden a-Z-Menü auf den Buchstaben, mit dem der Befehl beginnt, und klicken Sie dann auf den Befehlsnamen.

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [F](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [J](#) | [Z](#)

Ein

- [active](#)
- [add](#)
- [add alias](#)
- [add volume](#)
- [append](#)
- [arp](#)
- [assign](#)
- [assoc](#)
- [at](#)
- [atmadm](#)
- [attach-vdisk](#)
- [attrib](#)
- [attributes](#)
 - [attributes disk](#)
 - [attributes volume](#)
- [auditpol](#)
 - [auditpol backup](#)
 - [auditpol clear](#)
 - [auditpol get](#)
 - [auditpol list](#)
 - [auditpol remove](#)
 - [auditpol resourcesad](#)
 - [auditpol restore](#)
 - [auditpol set](#)
- [autochk](#)
- [autoconv](#)
- [autofmt](#)

- [automount](#)

B

- [bcdboot](#)
- [bcdedit](#)
- [bdehdcfg](#)
 - [bdehdcfg driveinfo](#)
 - [bdehdcfg newdriveletter](#)
 - [bdehdcfg quiet](#)
 - [bdehdcfg restart](#)
 - [bdehdcfg size](#)
 - [bdehdcfg target](#)
- [begin backup](#)
- [begin restore](#)
- [bitsadmin](#)
 - [bitsadmin addfile](#)
 - [bitsadmin addfileset](#)
 - [bitsadmin addfilewithranges](#)
 - [bitsadmin cache](#)
 - [bitsadmin cache and delete](#)
 - [bitsadmin cache and deleteurl](#)
 - [bitsadmin cache and getexpirationtime](#)
 - [bitsadmin cache and getlimit](#)
 - [bitsadmin cache and help](#)
 - [bitsadmin cache and info](#)
 - [bitsadmin cache and list](#)
 - [bitsadmin cache and setexpirationtime](#)
 - [bitsadmin cache and setlimit](#)
 - [bitsadmin cache and clear](#)
 - [bitsadmin cancel](#)
 - [bitsadmin complete](#)
 - [bitsadmin create](#)
 - [bitsadmin examples](#)
 - [bitsadmin getaclflags](#)
 - [bitsadmin getbytestotal](#)
 - [bitsadmin getbytestransferred](#)
 - [bitsadmin getclientcertificate](#)
 - [bitsadmin getcompletiontime](#)
 - [bitsadmin getcreationtime](#)
 - [bitsadmin getcustomheaders](#)
 - [bitsadmin getdescription](#)
 - [bitsadmin getdisplayname](#)
 - [bitsadmin geterror](#)
 - [bitsadmin geterrorcount](#)
 - [bitsadmin getfilestotal](#)
 - [bitsadmin getfilestransferred](#)
 - [bitsadmin gethelptokenflags](#)

- [bitsadmin gethelptokensid](#)
- [bitsadmin gethttpmethod](#)
- [bitsadmin getmaxdownloadtime](#)
- [bitsadmin getminretrydelay](#)
- [bitsadmin getmodificationtime](#)
- [bitsadmin getnoprogresstimeout](#)
- [bitsadmin getnotifycmdline](#)
- [bitsadmin getnotifyflags](#)
- [bitsadmin getnotifyinterface](#)
- [bitsadmin getowner](#)
- [bitsadmin getpeercachingflags](#)
- [bitsadmin getpriority](#)
- [bitsadmin getproxybypasslist](#)
- [bitsadmin getproxylist](#)
- [bitsadmin getproxyusage](#)
- [bitsadmin getreplydata](#)
- [bitsadmin getreplyfilename](#)
- [bitsadmin getreplyprogress](#)
- [bitsadmin getsecurityflags](#)
- [bitsadmin getstate](#)
- [bitsadmin gettemporaryname](#)
- [bitsadmin gettype](#)
- [bitsadmin getvalidationstate](#)
- [bitsadmin help](#)
- [bitsadmin info](#)
- [bitsadmin list](#)
- [bitsadmin listfiles](#)
- [bitsadmin makecustomheaderswriteonly](#)
- [bitsadmin monitor](#)
- [bitsadmin nowrap](#)
- [bitsadmin peercaching](#)
 - [bitsadmin peercaching and getconfigurationflags](#)
 - [bitsadmin peercaching and help](#)
 - [bitsadmin peercaching and setconfigurationflags](#)
- [bitsadmin peers](#)
 - [bitsadmin peers and clear](#)
 - [bitsadmin peers and discover](#)
 - [bitsadmin peers and help](#)
 - [bitsadmin peers and list](#)
- [bitsadmin rawreturn](#)
- [bitsadmin removeclientcertificate](#)
- [bitsadmin removecredentials](#)
- [bitsadmin replaceremoteprefix](#)
- [bitsadmin reset](#)
- [bitsadmin resume](#)
- [bitsadmin setaclflag](#)

- [bitsadmin setclientcertificatebyid](#)
- [bitsadmin setclientcertificatebyname](#)
- [bitsadmin setcredentials](#)
- [bitsadmin setcustomheaders](#)
- [bitsadmin setdescription](#)
- [bitsadmin setdisplayname](#)
- [bitsadmin sethelptoken](#)
- [bitsadmin sethelptokenflags](#)
- [bitsadmin sethttpmethod](#)
- [bitsadmin setmaxdownloadtime](#)
- [bitsadmin setminretrydelay](#)
- [bitsadmin setnoprogresstimeout](#)
- [bitsadmin setnotifycmdline](#)
- [bitsadmin setnotifyflags](#)
- [bitsadmin setpeercachingflags](#)
- [bitsadmin setpriority](#)
- [bitsadmin setproxysettings](#)
- [bitsadmin setreplyfilename](#)
- [bitsadmin setsecurityflags](#)
- [bitsadmin setvalidationstate](#)
- [bitsadmin suspend](#)
- [bitsadmin takeownership](#)
- [bitsadmin transfer](#)
- [bitsadmin util
 - \[bitsadmin util and enableanalyticchannel\]\(#\)
 - \[bitsadmin util and getieproxy\]\(#\)
 - \[bitsadmin util and help\]\(#\)
 - \[bitsadmin util and repairservice\]\(#\)
 - \[bitsadmin util and setieproxy\]\(#\)
 - \[bitsadmin util and version\]\(#\)](#)
- [bitsadmin wrap](#)
- [bootcfg
 - \[bootcfg addsw\]\(#\)
 - \[bootcfg copy\]\(#\)
 - \[bootcfg dbg1394\]\(#\)
 - \[bootcfg debug\]\(#\)
 - \[bootcfg default\]\(#\)
 - \[bootcfg delete\]\(#\)
 - \[bootcfg ems\]\(#\)
 - \[bootcfg query\]\(#\)
 - \[bootcfg raw\]\(#\)
 - \[bootcfg rmsw\]\(#\)
 - \[bootcfg timeout\]\(#\)](#)
- [break](#)
- [C](#)
- [cacls](#)

- [call](#)
- [cd](#)
- [certreq](#)
- [certutil](#)
- [change](#)
 - [change logon](#)
 - [change port](#)
 - [change user](#)
- [chcp](#)
- [chdir](#)
- [chglogon](#)
- [chgport](#)
- [chgusr](#)
- [chkdsk](#)
- [chkntfs](#)
- [choice](#)
- [cipher](#)
- [clean](#)
- [cleanmgr](#)
- [clip](#)
- [cls](#)
- [cmd](#)
- [cmdkey](#)
- [cmstp](#)
- [color](#)
- [comp](#)
- [compact](#)
- [Compact Vdisk](#)
- [convert](#)
 - [convert basic](#)
 - [dynamisch konvertieren](#)
 - [convert gpt](#)
 - [convert mbr](#)
- [copy](#)
- [cprofile](#)
- [erstellen](#)
 - [Erstellen von EFI-Partitionen](#)
 - [\[erweiterte Partition erstellen](#)
 - [logische Partition erstellen](#)
 - [Erstellen einer Partition MSR](#)
 - [create partition primary](#)
 - [volumespiegelung erstellen](#)
 - [Erstellen eines Volume-RAID](#)
 - [einfaches Volume erstellen](#)
 - [volumestripe erstellen](#)
- [cscript](#)

D

- [date](#)
- [dcgpofix](#)
- [defrag](#)
- [del](#)
- [delete](#)
 - [Datenträger löschen](#)
 - [Partition löschen](#)
 - [Schatten löschen](#)
 - [delete volume](#)
- [detach vdisk](#)
- [einzelnen](#)
 - [Detail Festplatte](#)
 - [Detail Partition](#)
 - [Detail-Vdisk](#)
 - [Detail Volume](#)
- [Dfsdiag](#)
 - [Dfsdiag-testdcs](#)
 - [Dfsdiag testdfsconfig](#)
 - [Dfsdiag testdfsintegrity](#)
 - [Dfsdiag testreferral](#)
 - [Dfsdiag Testsites](#)
- [dfsmig](#)
- [diantz](#)
- [dir](#)
- [diskcomp](#)
- [diskcopy](#)
- [diskpart](#)
- [diskperf](#)
- [diskraid](#)
- [diskshadow](#)
- [displdiag](#)
- [dnscmd](#)
- [doskey](#)
- [driverquery](#)

E

- [echo](#)
- [edit](#)
- [endlocal](#)
- [Wiederherstellung beenden](#)
- [erase](#)
- [eventcreate](#)
- [eventquery](#)
- [eventtriggers](#)
- [Evntcmd](#)
- [exec](#)

- [exit](#)
- [expand](#)
- [Erweitern von Vdisk](#)
- [sichtbar](#)
- [extend](#)
- [extract](#)

F

- [fc](#)
- [filesystems](#)
- [find](#)
- [findstr](#)
- [finger](#)
- [flattemp](#)
- [fondu](#)
- [for](#)
- [forfiles](#)
- [format](#)
- [freedisk](#)
- [fsutil](#)
 - [fsutil 8dot3name](#)
 - [fsutil behavior](#)
 - [fsutil dirty](#)
 - [fsutil file](#)
 - [fsutil fsinfo](#)
 - [fsutil hardlink](#)
 - [fsutil objectid](#)
 - [fsutil quota](#)
 - [fsutil repair](#)
 - [fsutil reparsepoint](#)
 - [fsutil resource](#)
 - [fsutil sparse](#)
 - [fsutil tiering](#)
 - [fsutil transaction](#)
 - [fsutil usn](#)
 - [fsutil volume](#)
 - [fsutil wim](#)
- [ftp](#)
 - [ftp append](#)
 - [ftp ascii](#)
 - [ftp bell](#)
 - [ftp binary](#)
 - [ftp bye](#)
 - [ftp cd](#)
 - [ftp close](#)
 - [ftp debug](#)
 - [ftp delete](#)

- [ftp dir](#)
- [ftp disconnect](#)
- [ftp get](#)
- [ftp glob](#)
- [ftp hash](#)
- [ftp lcd](#)
- [ftp literal](#)
- [ftp ls](#)
- [ftp mget](#)
- [ftp mkdir](#)
- [ftp mls](#)
- [ftp mput](#)
- [ftp open](#)
- [ftp prompt](#)
- [ftp put](#)
- [ftp pwd](#)
- [ftp quit](#)
- [ftp quote](#)
- [ftp recv](#)
- [ftp remotehelp](#)
- [ftp rename](#)
- [ftp rmdir](#)
- [ftp send](#)
- [ftp status](#)
- [ftp trace](#)
- [ftp type](#)
- [ftp user](#)
- [ftp verbose](#)
- [ftp mdelete](#)
- [ftp mdir](#)
- [ftype](#)
- [fveupdate](#)

G

- [getmac](#)
- [gettype](#)
- [goto](#)
- [gfixup](#)
- [gpresult](#)
- [gpt](#)
- [gpupdate](#)
- [graftabl](#)

H

- [help](#)
- [helpctr](#)
- [hostname](#)

- [icacls](#)
- [if](#)
- [Importieren \(shadowdisk\)](#)
- [Importieren \(DiskPart\)](#)
- [inactive](#)
- [inuse](#)
- [ipconfig](#)
- [ipxroute](#)
- [irftp](#)

J

- [jetpack](#)

K

- [klist](#)
- [ksetup](#)
 - [ksetup addenctypeattr](#)
 - [ksetup addhosttorealmmap](#)
 - [ksetup addkdc](#)
 - [ksetup addkpasswd](#)
 - [ksetup addrealmflags](#)
 - [ksetup changepassword](#)
 - [ksetup delenctypeattr](#)
 - [ksetup delhosttorealmmap](#)
 - [ksetup delkdc](#)
 - [ksetup delkpasswd](#)
 - [ksetup delrealmflags](#)
 - [ksetup domain](#)
 - [ksetup dumpstate](#)
 - [ksetup getenctypeattr](#)
 - [ksetup listrealmflags](#)
 - [ksetup mapuser](#)
 - [ksetup removerealm](#)
 - [ksetup server](#)
 - [ksetup setcomputerpassword](#)
 - [ksetup setenctypeattr](#)
 - [ksetup setrealm](#)
 - [ksetup setrealmflags](#)
- [ktutil](#)
- [ktpass](#)

L

- [label](#)
- [list](#)
 - [Anbieter auflisten](#)
 - [Schatten auflisten](#)
 - [Writer auflisten](#)

- [Metadaten laden](#)
- [lodctr](#)
- [logman](#)
 - [logman create](#)
 - [Warnung zu logman Create](#)
 - [logman Create-API](#)
 - [logman Create cfg](#)
 - [logman Create Counter](#)
 - [logman Create Trace](#)
 - [logman delete](#)
 - [Importieren und logman-Export von logman](#)
 - [logman query](#)
 - [logman Start und logman beendet](#)
 - [logman update](#)
 - [logman Update-Warnung](#)
 - [logman Update-API](#)
 - [logman update cfg](#)
 - [logman update Counter](#)
 - [logman update Trace](#)
- [logoff](#)
- [lpq](#)
- [lpr](#)

M

- [macfile](#)
- [makecab](#)
- [Verwalten von BDE](#)
 - [Verwalten des BDE-Status](#)
 - [Verwalten von BDE](#)
 - [Verwalten von BDE](#)
 - [Verwalten von BDE Pause](#)
 - [Verwalten von BDE Resume](#)
 - [BDE-Sperre verwalten](#)
 - [Verwalten von BDE Unlock](#)
 - [Verwalten von BDE Entsperrens](#)
 - [BDE-Schutzvorrichtungen verwalten](#)
 - [Verwalten von BDE TPM](#)
 - [Verwalten von BDE-tidentifier](#)
 - [Verwalten von BDE forcerecovery](#)
 - [Verwalten von BDE ChangePassword](#)
 - [Verwalten von BDE changepin](#)
 - [Verwalten von BDE ChangeKey](#)
 - [Verwalten von BDE KeyPackage](#)
 - [Verwalten des BDE-Upgrades](#)
 - [Verwalten von BDE wipeer FreeSpace](#)
- [mapadmin](#)
- [md](#)

- [Vdisk zusammenführen](#)
- [mkdir](#)
- [mklink](#)
- [mmc](#)
- [mode](#)
- [more](#)
- [mount](#)
- [mountvol](#)
- [move](#)
- [mqbkup](#)
- [mqsvc](#)
- [mqtgsvc](#)
- [msdt](#)
- [msg](#)
- [msiexec](#)
- [msinfo32](#)
- [mstsc](#)

N

- [nbtstat](#)
- [netcfg](#)
- [NET Print](#)
- [netsh](#)
- [netstat](#)
- [nfsadmin](#)
- [nfsshare](#)
- [nfsstat](#)
- [nlbmgr](#)
- [nslookup](#)
 - [Befehl „nslookup exit“](#)
 - [Befehl „nslookup finger“](#)
 - [nslookup help](#)
 - [nslookup ls](#)
 - [nslookup lserver](#)
 - [nslookup root](#)
 - [nslookup server](#)
 - [nslookup set](#)
 - [nslookup set all](#)
 - [nslookup set class](#)
 - [nslookup set d2](#)
 - [nslookup set debug](#)
 - [nslookup set domain](#)
 - [nslookup set port](#)
 - [nslookup set querytype](#)
 - [nslookup set recurse](#)
 - [nslookup set retry](#)
 - [nslookup set root](#)

- [nslookup set search](#)
- [nslookup set srchlist](#)
- [nslookup set timeout](#)
- [nslookup set type](#)
- [nslookup set vc](#)
- [nslookup view](#)
- [ntbackup](#)
- [ntcmdprompt](#)
- [ntfrsutil](#)

O

- [aufzü](#)
 - [Offline-Datenträger](#)
 - [Offline-Volume](#)
- [Internet](#)
 - [Online-Datenträger](#)
 - [Online Volume](#)
- [openfiles](#)

P

- [pagefileconfig](#)
- [path](#)
- [pathping](#)
- [pause](#)
- [pbadmin](#)
- [pentnt](#)
- [perfmon](#)
- [ping](#)
- [pnpunattend](#)
- [pnputil](#)
- [popd](#)
- [PowerShell](#)
- [PowerShell ISE](#)
- [print](#)
- [prncnfg](#)
- [prndrvr](#)
- [prnjobs](#)
- [prnmngr](#)
- [prnport](#)
- [prnqctl](#)
- [prompt](#)
- [pubprn](#)
- [pushd](#)
- [pushprinterconnections](#)
- [pwlauncher](#)

Q

- [qappsrv](#)

- [qprocess](#)
- [Frage](#)
 - [query process](#)
 - [Abfrage Sitzung](#)
 - [termserver Abfragen](#)
 - [Benutzer Abfragen](#)
- [quser](#)
- [qwinsta](#)

R

- [rcp](#)
- [rd](#)
- [rdpsign](#)
- [recover](#)
- [Datenträger Gruppe wiederherstellen](#)
- [reg](#)
 - [reg hinzufügen](#)
 - [reg-Vergleich](#)
 - [reg-Kopie](#)
 - [reg löschen](#)
 - [reg-Export](#)
 - [reg-Import](#)
 - [reg laden](#)
 - [reg-Abfrage](#)
 - [reg-Wiederherstellung](#)
 - [REG speichern](#)
 - [reg entladen](#)
- [regini](#)
- [regsvr32](#)
- [relog](#)
- [REM-Batchdatei](#)
- [REM-Skript](#)
- [remove](#)
- [ren](#)
- [rename](#)
- [Reparieren](#)
 - [Reparieren von BDE](#)
- [replace](#)
- [neu einlesen](#)
- [reset](#)
 - [reset session](#)
- [erhalten](#)
- [umzukehren](#)
- [rexec](#)
- [risetup](#)
- [rmdir](#)
- [robocopy](#)

- [Route WS2008](#)
- [rpcinfo](#)
- [rpcping](#)
- [rsh](#)
- [rundll32](#)
- [rundll32 Datei printui](#)
- [rwinsta](#)

E

- [chen](#)
- [SC-Konfiguration](#)
- [SC erstellen](#)
- [SC löschen](#)
- [SC-Abfrage](#)
- [schtasks](#)
- [scwcmd](#)
 - [scwcmd-Analyse](#)
 - [scwcmd konfigurieren](#)
 - [scwcmd-Register](#)
 - [scwcmd-Rollback](#)
 - [scwcmd-Transformation](#)
 - [scwcmd-Ansicht](#)
- [secedit](#)
 - "Secedit" analysieren
 - [secedit konfigurieren](#)
 - [secedit-Export](#)
 - [generaterollback für secedit](#)
 - [secedit-Import](#)
 - [secedit-Überprüfung](#)
- [select](#)
 - [select disk](#)
 - [Partition auswählen](#)
 - [Vdisk auswählen](#)
 - [select volume](#)
- [serverceipoptin](#)
- [ServerManagerCmd](#)
- [serverweroptin](#)
- [Festlegen von Umgebungsvariablen](#)
- [Schatten Kopie festlegen](#)
 - [Kontext festlegen](#)
 - [ID festlegen](#)
 - [setlocal](#)
 - [Metadaten festlegen](#)
 - [Set-Option](#)
 - [ausführlich festlegen](#)
- [setx](#)
- [sfc](#)

- [shadow](#)
- [shift](#)
- [showmount](#)
- [shrink](#)
- [shutdown](#)
- Wiederherstellung simulieren
- [sort](#)
- [start](#)
- Unterbefehls Satz Gerät
- Unterbefehls Satz "drivergroup"
- Unterbefehls Satz "drivergroupfilter"
- Unterbefehls Satz "DriverPackage"
- Bild des untergeordneten Befehlssatzes
- Unterbefehls Satz-ImageGroup
- Unterbefehls Satz Server
- Unterbefehls Satz Transportserver
- Unterbefehls Satz MulticastTransmission
- Namespace des Unterbefehls starten
- Unterbefehl zum Start Server
- Unterbefehl starten von Transportserver
- Unterbefehl zum Abbrechen des Servers
- Unterbefehl zum Abbrechen von Transportserver
- [subst](#)
- [sxstrace](#)
- [sysocmgr](#)
- [systeminfo](#)

T

- [takeown](#)
- [tapiCfg](#)
- [taskkill](#)
- [tasklist](#)
- [tcmsetup](#)
- [telnet](#)
 - Telnet schließen
 - Telnet-Anzeige
 - Telnet geöffnet
 - Telnet-Quit
 - Telnet-Sendevorgang
 - Telnet-Satz
 - Telnet-Status
 - Telnet nicht festgelegt
- [tftp](#)
- [time](#)
- [timeout](#)
- [title](#)
- [tlntadmn](#)

- [tpmtool](#)
- [tpmvscmgr](#)
- [tracerpt](#)
- [tracert](#)
- [tree](#)
- [tscon](#)
- [tsdiscon](#)
- [tsecimp](#)
- [tskill](#)
- [tsprof](#)
- [type](#)
- [typeperf](#)
- [tzutil](#)

U

- [Heben des](#)
- [Uniqueld](#)
- [unlodctr](#)

V

- [ver](#)
- [verifier](#)
- [verify](#)
- [vol](#)
- [vssadmin](#)
 - [vssadmin delete shadows](#)
 - [vssadmin list shadows](#)
 - [vssadmin list writers](#)
 - [vssadmin resize shadowstorage](#)

W

- [waitfor](#)
- [wbadmin](#)
 - [Wbadmin delete-Katalog](#)
 - [Wbadmin delete systemstatebackup](#)
 - [Wbadmin-Sicherung deaktivieren](#)
 - [Wbadmin-Sicherung aktivieren](#)
 - [Wbadmin Get Disks](#)
 - [Wbadmin-Get-Elemente](#)
 - [Wbadmin-Status "Get"](#)
 - [Wbadmin-Get-Versionen](#)
 - [Wbadmin-Wiederherstellungs Katalog](#)
 - [Wbadmin-Sicherung starten](#)
 - [Wbadmin-Wiederherstellung starten](#)
 - [WBADMIN-START SYSRECOVERY](#)
 - [Wbadmin start systemstatebackup](#)
 - [Wbadmin start Systemstatus](#)
 - [Auftrag zum Abbrechen von Wbadmin](#)

- [wdsutil](#)
- [wecutil](#)
- [wevtutil](#)
- [where](#)
- [whoami](#)
- [winnt](#)
- [winnt32](#)
- [winpop](#)
- [winrs](#)
- [WinSAT-Arbeitsspeicher](#)
- [WinSAT-MF-Medien](#)
- [wmic](#)
- [Maschine](#)
- [wscript](#)

X

- [xcopy](#)