



Carlo Westbrook



Windows Admin Center (WAC)

Zentrale Verwaltung von Client- und Servercomputern

- > Einführung und Überblick
- > Bereitstellung, Konfiguration, Anpassung und Erweiterung
- > Zentrale Verwaltung von Client- und Servercomputern
- > Verwaltung von Failoverclustern und Hyper-V-Servern
- > Wartung, Protokollierung und Problembehandlung

Behandelt auch
**Windows
Server 2019**

Carlo Westbrook

Windows Admin Center (WAC)

Zentrale Verwaltung von
Clients und Serversystemen im Netzwerk

CertPro[®] PRESS

an Imprint of CertPro[®] Limited

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Hard- und Softwarebezeichnungen und weitere Stichworte und sonstige Angaben, die in diesem Buch verwendet werden, sind als eingetragene Marken geschützt. Da es nicht möglich ist, in allen Fällen zeitnah zu ermitteln, ob ein Markenschutz besteht, wird das ®-Symbol in diesem Buch nicht verwendet.

Kommentare und Fragen können Sie gerne an uns richten unter E-Mail:
info@certpro-press.de

Print-Ausgabe ISBN 978-3-9447-4937-2
ebook-Ausgabe: ISBN 978-3-9447-4938-9

Copyright © 2019 by CertPro® Press-Verlag,
ein Imprint der CertPro® Limited, Elbinger Str. 23, D-55543 Bad Kreuznach/Germany.
Alle Rechte vorbehalten.

Autor: Carlo Westbrook

Einbandgestaltung: CertPro® Limited
Bilder und Grafiken: CertPro® Limited
Herstellung: CertPro® Limited
Druck und Verarbeitung: BoD [Books on Demand GmbH](#), 22848 Hamburg
Printed in Germany

Auf einen Blick

Kapitel 1 - Einführung und Überblick

Kapitel 2 - Bereitstellung des Windows Admin Center (WAC)

Kapitel 3 - Konfiguration, Anpassung und Erweiterung des WAC

Kapitel 4 - Verwalten von Client- und Servercomputern mit dem WAC

Kapitel 5 - Wartung, Protokollierung und Problembehandlung

Website zum Buch



Liebe Leserin, lieber Leser,

zu diesem Fachbuch bieten wir Ihnen zusätzliche Materialien, wie z. B. Zusatzdokumentation, sowie auch eine Übersicht der darin enthaltenen Weblinks, die Sie bei Bedarf gerne direkt aus unserer Verlagswebsite im Internet herunterladen können unter:

<https://www.CertPro-Press.de/9372.html>

Wichtiger Hinweis!

Die in diesem Fachbuch dargestellten Informationen beziehen sich auf das während der Entwicklung des Buches verfügbare Versionen des Windows Admin Center (WAC). Es ist nicht auszuschließend, dass Microsoft, wie man dies von Office 365 oft kennt, die Gestaltung der grafischen Benutzeroberfläche des Windows Admin Center (WAC) ohne vorherige Ankündigung ändert. Details hierzu findet man auf der Produktwebseite des Windows Admin Center (WAC) im Internet.

Inhalt

| | |
|-----------------------------------------------------------------------------|-----------|
| Auf einen Blick | 5 |
| Typografische Konventionen | 12 |
| Der Autor | 13 |
| Vorwort | 14 |
| KAPITEL 1 - Einführung und Überblick | 15 |
| 1.1 WAC und die „kompatiblen Webbrowser“ | 16 |
| 1.2 Vorteile des Windows Admin Center..... | 17 |
| 1.3 Einsatzmöglichkeiten | 18 |
| 1.3.1 Enthaltene Funktionen für die Server- und Clientverwaltung | 20 |
| 1.3.2 Zugriffsrollen beim Einsatz als Gateway..... | 22 |
| 1.3.3 Optionen für die Authentifizierung von Gateway-Benutzern | 23 |
| 1.3.4 Smartcard-Authentifizierung | 24 |
| 1.3.5 Bedingter Zugriff und die mehrstufige Authentifizierung | 24 |
| 1.3.6 Einmaliges Anmelden (SSO) konfigurieren | 25 |
| 1.4 Rollenbasierte Zugriffssteuerung | 25 |
| 1.4.1 Verfügbare Rollen..... | 27 |
| 1.4.2 Vorbereiten der rollenbasierten Zugriffssteuerung | 28 |
| 1.5 Optionen für die Azure-Integration | 29 |
| 1.5.1 Microsoft Azure Active Directory (Azure AD)..... | 30 |
| 1.5.2 Verwaltung von Azure-VMs..... | 30 |
| 1.5.3 Schützen der Hyper-V-Computer mit Azure Site Recovery | 31 |
| 1.5.4 Zentrale Verwaltung von Updates mit Azure-Updateverwaltung..... | 31 |
| 1.5.5 Microsoft Azure-Netzwerkadapter | 32 |
| KAPITEL 2 - Bereitstellen des Windows Admin Center (WAC) | 33 |
| 2.1 Unterstützte Modi | 33 |
| 2.2 Unterstützte Betriebssysteme | 35 |
| 2.2.1 Unterstützte Betriebssysteme für die Installation des WAC..... | 35 |
| 2.2.2 Unterstützte Betriebssysteme für die Verwaltung mithilfe des WAC..... | 35 |

| | |
|-----------------------------------------------------------------------------------------------------------|-----------|
| 2.3 Voraussetzungen für die Verwendung des WAC | 37 |
| 2.4 Bereitstellungsoptionen für das WAC..... | 38 |
| 2.4.1 Bereitstellen des WAC mit hoher Verfügbarkeit (HA)..... | 39 |
| 2.5 Installation des Windows Admin Center (WAC) | 40 |
| 2.5.1 Installation von WAC unter Windows 10 | 41 |
| 2.5.2 Installation von WAC auf Serversystemen unter Windows Server 2019 oder Windows Server 2016 | 43 |
| 2.5.3 Installation des WAC auf einem Core-Server | 57 |
| 2.6 Verbindung mit dem Windows Admin Center (WAC)..... | 60 |
| 2.6.1 Schritte zum Verbinden mit dem Windows Admin Center (WAC)..... | 62 |
| 2.7 Vorbereitung der Netzwerkinfrastruktur | 63 |
| 2.7.1 Vorbereitung von Windows Server 2008 R2 | 64 |
| 2.7.2 Vorbereitung von Microsoft Hyper-V Server 2012 R2..... | 67 |
| 2.7.3 Vorbereitung von Microsoft Hyper-V Server 2019 und Hyper-V-Server 2016..... | 68 |
| 2.7.4 Vorbereitung von Microsoft Windows 10-Clientcomputern..... | 69 |
| 2.8 Bereitstellen des WAC mit hoher Verfügbarkeit (HA) | 71 |
| 2.8.1 Voraussetzungen für die Bereitstellung im Failovercluster | 71 |
| 2.8.2 Installation des WAC auf einem Failovercluster..... | 72 |
| 2.8.3 Aktualisierung einer vorhandenen HA-Installation..... | 74 |
| 2.8.4 Deinstallation von WAC in einem Failovercluster | 75 |
| KAPITEL 3 - Konfiguration und Anpassung des Windows Admin Center ... | 77 |
| 3.1 Einstellungen im Windows Admin Center (WAC) | 77 |
| 3.1.1 Benutzereinstellungen | 78 |
| 3.1.2 Gateway-Einstellungen | 79 |
| 3.2 Konfiguration des Benutzerzugriffs und der Berechtigungen | 80 |
| 3.2.1 Standardmäßige Zugriffsrollen | 80 |
| 3.2.2 Authentifizierung von Gateway-Benutzern..... | 81 |
| 3.2.3 Smartcard-Authentifizierung..... | 82 |
| 3.2.4 Bedingter Zugriff und die mehrstufige Authentifizierung | 83 |
| 3.2.5 Einmaliges Anmelden (SSO) konfigurieren..... | 83 |

| | |
|-------------------------------------------------------------------------------------------------------------------|------------|
| 3.2.6 Konfiguration der rollenbasierten Zugriffssteuerung (RBAC) | 85 |
| 3.3 Erweiterungen des WAC | 93 |
| 3.3.1 Installieren einer Erweiterung..... | 93 |
| 3.3.2 Installieren von Erweiterungen auf einem Computer ohne Internetzugang... | 95 |
| 3.3.3 Deinstallieren einer Erweiterung | 97 |
| 3.3.4 Verwaltung der Erweiterung des WAC mit der Windows PowerShell | 98 |
| 3.4 Konfigurieren der Microsoft Azure-Integration..... | 99 |
| 3.4.1 Registrierung des Windows Admin Center (WAC) in Azure..... | 100 |
| KAPITEL 4 - Verwaltung von Serversystemen und Clientcomputern mit dem Windows Admin Center (WAC) | 109 |
| 4.1 Hinzufügen von Computersystemen zur Verwaltung..... | 110 |
| 4.1.1 Anzeige der Liste vertrauenswürdiger Computer | 110 |
| 4.1.2 Schritte zum Hinzufügen von Computersystemen zur Liste vertrauenswürdiger Computer..... | 111 |
| 4.1.3 Vereinfachte Verwendung der Liste vertrauenswürdiger Computer durch „Wildcard“-Zeichen (*) | 111 |
| 4.1.4 Löschen der Liste vertrauenswürdiger Computer | 112 |
| 4.2 Authentifizierung gegenüber den verwalteten Computersystemen..... | 113 |
| 4.3 Notwendige Rechte zum Verwalten von Computersystemen mit dem WAC..... | 113 |
| 4.3.1 Rollenbasierte Zugriffssteuerung..... | 114 |
| 4.3.2 Option „Verwalten als“ | 115 |
| 4.4 Verwendung von Tags zum Organisieren von Verbindungen im WAC.... | 115 |
| 4.4.1 Erstellen von Tags | 116 |
| 4.4.2 Zuordnen eines bereits bestehenden Tags..... | 117 |
| 4.4.3 Filtern von Verbindungen im WAC mithilfe von Tags | 118 |
| 4.5 Anzeigen der im WAC enthaltenen Windows PowerShell-Skripts..... | 119 |
| 4.6 Hinzufügen von Computersystemen zum WAC..... | 121 |
| 4.6 Entfernen von Computersystemen aus dem WAC..... | 122 |
| 4.7 Werkzeuge des Windows Admin Center (WAC) | 124 |
| 4.7.1 Werkzeuge für die Verwaltung von Servercomputern mit dem Windows Admin Center (WAC)..... | 125 |

| | |
|-------------------------------------------------------------------------------------------------|------------|
| 4.7.2 Werkzeuge für die Verwaltung von Clientcomputern mit dem Windows Admin Center (WAC) | 130 |
| 4.8 Verwalten von Windows 10-Clientcomputern und Windows-Serversystemen | 135 |
| 4.8.1 Aktivieren der Windows Remote-Verwaltung (WinRM) | 136 |
| 4.8.2 Hinzufügen von Windows 10-Clientcomputern und Windows-Serversystemen zum WAC | 138 |
| 4.8.3 (Massen-)Import von „Verbindungen“ mithilfe der Windows PowerShell | 141 |
| 4.8.4 Beispiele für die Verwaltung von Windows-Servercomputern..... | 145 |
| 4.8.5 Beispiele für die Verwaltung von Windows 10-Clientcomputer | 155 |
| 4.9 Verwalten von Hyper-V-Servern und virtuellen Maschinen..... | 159 |
| 4.9.1 Hinzufügen von Hyper-V-Hostcomputern zum Windows Admin Center (WAC)..... | 159 |
| 4.9.2 Ausführbare Verwaltungsaufgaben rund um Hyper-V im Windows Admin Center | 160 |
| 4.10 Verwalten von Failoverclustern | 167 |
| 4.10.1 Hinzufügen eines Failover-Cluster zum Windows Admin Center (WAC) | 167 |
| 4.10.2 Tools im Failovercluster-Manager des WAC..... | 169 |
| 4.11 Verwalten von Azure-VMs mit dem WAC..... | 170 |
| 4.11.1 Verwalten von Azure-VMs mit öffentlicher IP-Adresse..... | 171 |
| 4.11.2 Verwalten von Azure-VMs ohne öffentliche IP-Adressen..... | 175 |
| KAPITEL 5 - Wartung, Protokollierung und Problembehandlung..... | 177 |
| 5.1 Aktualisierung von Serversystemen mit der Azure-Updateverwaltung | 178 |
| 5.1.1 Konfiguration der Azure-Updateverwaltung mit dem Windows Admin Center (WAC) | 180 |
| 5.2 Verwendung von Azure-Backup mit dem WAC..... | 191 |
| 5.2.1 Konfigurationsschritte zum Einrichten von Azure-Backup im WAC | 192 |
| 5.3 Austausch des automatisch generierten SSL-Zertifikats | 196 |
| 5.4 Problembehandlung für WAC..... | 200 |
| 5.4.1 Standardtools-Auswahl zur Problemerkennung | 200 |
| 5.4.2 Bekannte Probleme im Zusammenhang mit dem WAC | 201 |
| 5.4.3 Unbekannte Probleme im Zusammenhang mit dem WAC | 202 |

| | |
|--------------------------------------------------------|------------|
| 5.5 Protokollierung im Windows Admin Center (WAC)..... | 203 |
| Stichwortverzeichnis..... | 206 |

Typografische Konventionen

Um bestimmten Textpassagen dieses Buches etwas hervorzuheben, wurden die folgenden typografischen Konventionen verwendet:

| Konvention | Bedeutung |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| Befehl | Stellt die Befehlssyntax oder auch Befehlsausführung von Kommandozeilen- oder Windows PowerShell-Befehlen dar. |
| Weiter | Kennzeichnet die Ausführung einer bestimmten Programmfunktion, beispielsweise den Mausklick auf eine Schaltfläche. |
| HINWEIS! | Weist auf einen allgemeinen Hinweis zu bestimmten Themenbereichen hin. |
| WICHTIG! | Gibt einen Hinweis auf wichtige Funktionen oder auch Situationen, die unbedingt beachtet werden sollten. |
| VORSICHT! | Kennzeichnet Informationen oder auch Situationen, die ein Risiko oder eine Bedrohung darstellen können. |
| PRAXISTIPP! | Kennzeichnet Tipps für die praktische Anwendung bzw. Umsetzung. |
| INTERNET! | Weist auf weitere Informationsquellen zu bestimmten Themenbereichen im Internet hin. |

Der Autor

Carlo Westbrook ist seit weit über 30 Jahren u. a. als IT-Trainer, Systemingenieur, Senior Enterprise Consultant, Infrastrukturarchitekt sowie als Learning Consultant und Kursdesigner für technische Kurse & Workshops tätig.



Als Fachautor publizierte er neben einer Vielzahl an Fachbüchern, sowie mittlerweile weit über 120 verschiedenen, technischen Kurs- und Workshop-Unterlagen für Teilnehmer und Trainer bereits auch vielzählige Fachbeiträge bei verschiedenen Verlagen, wie beispielsweise Addison-Wesley, CertPro-PRESS oder auch dem WEKA-Verlag.

Zu seinen Schwerpunkten zählen u. a. die Windows-Betriebssysteme, Active Directory, Windows PowerShell, Microsoft Exchange Server, Microsoft SharePoint Server, Microsoft Zertifikatdienste (PKI), die Microsoft System Center-, sowie Cloud- und Virtualisierungstechnologien und IT-Sicherheit. Neben dem Studium der Informatik hat er zwischenzeitlich auch eine Vielzahl an Herstellerzertifizierungen u.a. zum MCSA-Security, MCSE-Security, MCLC, MCTS, MCITP, zum Microsoft Certified Specialist sowie zum Microsoft Certified Solutions Expert (MCSE) erworben. Sein hohes Fachwissen setzt er im Rahmen unterschiedlichster, oft länderübergreifender IT-Projekte, wie zum Beispiel im Active Directory-Infrastruktur-(Re-)Design, verschiedenster Betriebssystem-Rollout-Projekte mit dem Microsoft System Center Configuration Manager (SCCM), Planung und Aufbau von Zertifikatdienstinfrastrukturen (PKI), sowie beispielsweise - als ein von Mile 2 Security/USA zertifizierter Penetration Testing Specialist (CPTS) - auch zur Absicherung und Härtung vorhandener IT-Infrastrukturen für Unternehmen, Institutionen und Behörden kompetent ein.

Seit nunmehr über 21 Jahren als durchgehend zugelassener Microsoft Certified Trainer (MCT) vermittelt er die Inhalte der originalen, technischen und auch planungstechnischen Kurse des Microsoft Official Curriculum (MOC). Er bereitete dabei bereits viele Hunderte seiner Teilnehmer auf die Teilnahme an den vielzähligen, weltweit anerkannten Herstellerprüfungen von Microsoft, Mile2 und beispielsweise auch CompTIA vor.

Vorwort

Zwischenzeitlich stehen den verantwortlichen IT-Administratoren moderner Computernetzwerke gleich vielzählige Werkzeuge in Form von Managementkonsolen, webbasierten Grafikkonsolen, der Windows PowerShell und der dafür verfügbarer Module, sowie auch fast unzähligen Kommandozeilentools zur Hand, um die täglichen Verwaltungsaufgaben rund um die vorhandenen Computersysteme zu bewältigen.

Mit dem Windows Admin Center (WAC) geht Microsoft nunmehr einen klaren Weg, die für die Verwaltung von den in modernen Computernetzwerken eingesetzten Clientcomputer und Serversysteme gemeinsam und von einer zentralen Stelle aus verwalten zu können. Dieses neue Windows Admin Center (WAC), welches Microsoft zuvor noch während der vorangegangenen Entwicklungsphase als Projekt „Honolulu“ bezeichnete, setzt auf einer webbasierten Grafikkonsole auf, bei der im Hintergrund Windows Management Instrumentation (WMI) und die Windows PowerShell zum Einsatz kommen. Die Besonderheit des WAC besteht aktuell in der Möglichkeit, dass man parallel zu Windows-Serversystemen auch Windows 10-Clientcomputer oder auch Failover-Cluster in der gleichen, grafischen Konsole verwalten kann.

Auch wenn das Windows Admin Center (WAC) in seiner aktuell veröffentlichten Version sicher noch lange nicht alle die in der täglichen Praxis notwendigen Verwaltungsmöglichkeiten bietet, so sollte man sich trotzdem bereits mit diesem neuen Werkzeug vertraut machen.

Dieses Fachbuch soll Ihnen die Bereitstellung, sowie auch den Einstieg in die Verwaltung mit dem Windows Admin Center (WAC) vereinfachen - wozu ich Ihnen meinerseits viel Erfolg wünsche.

Ihr

Carlo Westbrook



KAPITEL 1

Einführung und Überblick

Die Verwaltung von Server- und auch Clientsystemen findet in der täglichen Praxis mit verschiedensten Tools und auch Konsolen statt. Bei der Verwaltung von lokal eingesetzten Windows-Serversystemen verwendet man dabei oft den grafischen Server-Manager oder eine der Vielzahlen Verwaltungskonsolen. Die Verwaltung der in der Microsoft Azure-Cloud vorhandenen Computersysteme erfolgt hingegen oftmals über die web-basierten Portalfenster mithilfe des Webbrowsers direkt in der Microsoft Cloud. Microsoft hat mit dem Projekt „*Honolulu*“ die Entwicklung einer einheitlich verwendbaren, webbasierten Konsole vorangetrieben, die in dem „*Windows Admin Center*“ (WAC) abgeschlossen wurde.

Projekt
„Honolulu“ -
endlich ab-
geschlossen

Mit dieser webbasierten, aus einem der damit kompatiblen Webbrowser heraus verwendbaren, grafischen Verwaltungskonsole ist es nicht nur möglich, Windows-basierte Serversysteme, sondern im Bedarfsfall auch Windows 10-Clientcomputer zu verwalten. Zusätzlich lässt sich diese Konsole neben der rein lokalen Verwaltung - ein gültiges, sowie in der Regel kostenpflichtiges Microsoft Azure-Abonnement vorausgesetzt - auch für die Verwaltung der in der Microsoft Azure-Cloud bereitgestellten Computersysteme verwenden.

1.1 WAC und die „kompatiblen Webbrowser“

Internet Explorer ist mit dem WAC nicht kompatibel

Der Internet Explorer von Microsoft zählt hier explizit nicht zu den mit der neuen Verwaltungskonsole „kompatiblen“ Browsern. Alternativ sollte man auf den Microsoft Edge- oder besser gar auf den Google Chrome-Browser zurückgreifen, um sich mit dem *Windows Admin Center* (WAC) verbinden und dieses für die Verwaltung von Computersystemen verwenden zu können. Die Anbindung an die Microsoft Azure-Cloud ist für die Verwaltung von Serversystemen mithilfe des *Windows Admin Center* (WAC) jedoch keine Voraussetzung, grundsätzlich im Rahmen der möglichen, hybriden Verwaltung von Computersystemen aber möglich.

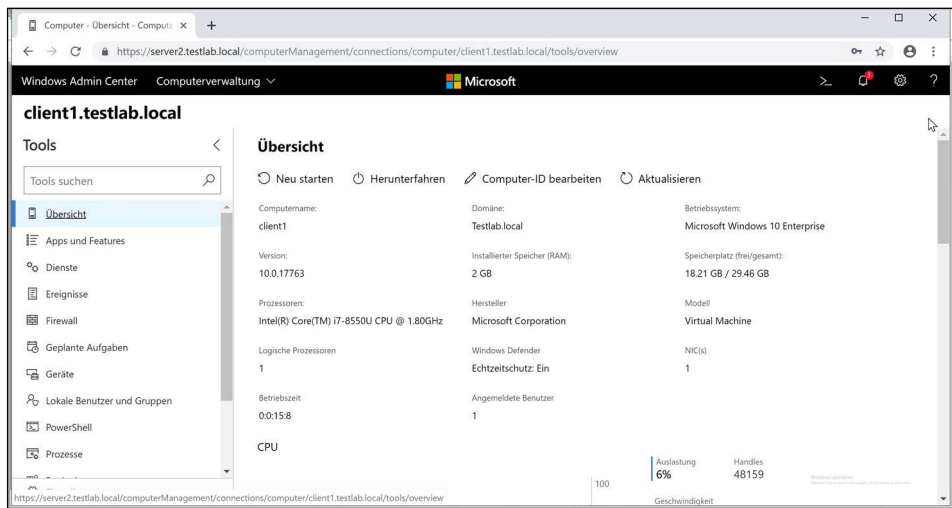


Abb. 1.1: Verwaltung eines Clientcomputers unter Windows 10 im Windows Admin Center (WAC)

PRAXISTIPP! Server- und Clientcomputersysteme lassen sich mit dem Windows Admin Center (WAC) im Bedarfsfall - völlig ohne die Verbindung zur Microsoft Azure-Cloud-Umgebung im Internet - auch nur „lokal“ verwalten. Hierzu kann man das Windows Admin Center (WAC) entweder im sogenannten „Desktop“-Modus auf einem Windows 10 Client lokal, oder aber im „Gateway“-Modus zur Remoteverwaltung auf einem Serversystem mit dem Serverbetriebssystem unter Windows Server 2019 oder Windows Server 2016 installieren.

Microsoft „kämpft“ offensichtlich auch in der aktuellen Version der Verwaltungskonsolle noch immer mit Kompatibilitätsproblemen zwischen dem eigenen Microsoft Edge-Browser und dem Windows Admin Center (WAC), was sich durch häufige Fehlermeldungen bei der Ausführung leider deutlich zeigt. Als einzig weitgehend fehlerfreie Alternative lässt sich aktuell der Google-Chrome-Browser für die Computerverwaltung mit dem Windows Admin Center (WAC) verwenden.

Empfohlen:
Google
Chrome-
Browser

INTERNET! Hinweise auf die vorhandenen Kompatibilitätsprobleme mit dem Edge-Browser von Microsoft im Zusammenhang mit dem Windows Admin Center (WAC) findet man im Internet unter anderem auf der folgenden Webseite:

<https://windowsserver.uservoice.com/forums/295071-management-tools/suggestions/33929671--bug-msft-sme-certificate-manager-failed-to-load>

1.2 Vorteile des Windows Admin Center

Das Windows Admin Center (WAC) besitzt viele Vorteile, die sich die IT-Administratoren in den modernen Computernetzwerken zu Nutze machen können. Zu den Vorteilen des Windows Admin Center (WAC) zählen unter anderem:

- **Einfache Installation und Verwendung** - Die Installation des Windows Admin Center (WAC) lässt sich innerhalb weniger Minuten auf einem Computersystem mit Windows 10, oder auch als Windows Admin Center-Gateway auf einem Serversystem unter Windows Server 2016 oder Windows Server 2019 realisieren.
- **Vertraute Funktionen** - Das Windows Admin Center (WAC) gibt sich als Weiterentwicklung der bereits bekannten Microsoft Management-Konsolen (engl. *Microsoft Management Console, MMC*), mit denen die Windows-Server- und Clientbetriebssysteme bereits seit den frühen Zeiten von Windows NT verwaltet werden konnten. In Windows Admin Center sind viele Funktionen der oft vertrauten Verwaltungstools einbearbeitet.

- **Verwaltung von überall möglich** - Das Windows Admin Center (WAC) kann für den Zugriff aus dem lokalen Netzwerk, oder im Bedarfsfall sogar für den Zugriff aus dem Internet bereitgestellt werden, um auf sichere Weise den Zugriff auf die zu verwaltenden Server- und Clientcomputer zu ermöglichen. Das WAC bietet für den Verwaltungszugriff mit dem Webbrowser die SSL-Verschlüsselung mithilfe eines digitalen Zertifikats.
- **Azure-Integration** - Das Windows Admin Center (WAC) ermöglicht die einfache Integration von Azure-Diensten, wie zum Beispiel Azure Backup, Azure Site Recovery, oder auch Azure Active Directory.
- **Ergänzung vorhandener Lösungen** - Das Windows Admin Center (WAC) ergänzt die bereits vorhandenen Verwaltungstools und -lösungen, wie zum Beispiel die Remoteserver-Verwaltungstools (RSAT), die Microsoft System Center-Produkte, Microsoft Intune oder auch Azure Stack. Das WAC ist dabei nicht als „Ersatz“ für vorhandene Verwaltungslösungen, sondern von Microsoft als reine „Ergänzung“ gedacht.
- **Erweiterbarkeit** - Das Windows Admin Center lässt sich mithilfe des von Microsoft veröffentlichten SDK (Software Development Kit) problemlos auf die Lösungen von Drittanbietern erweitern. Dazu hat Microsoft bereits viele Hilfen und Details in den Webseiten rund um das Windows Admin Center (WAC) veröffentlicht. Es existieren bereits unzählige Erweiterungen von Drittanbietern, die man oft kostenfrei direkt aus dem Internet herunterladen kann.

1.3 Einsatzmöglichkeiten

Kosten-
freier
Download
- und
auch
völlig
kostenfrei
einsetzbar

Das grafische, webbasierte Windows Admin Center (WAC) wird in einem (damit kompatiblen) Webbrowser aufgerufen, und dient unter anderem der Möglichkeit der zentralen Verwaltung von Serversystemen unter Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, sowie auch Windows 10-Clientcomputern. Daneben lassen sich mit dem WAC auch vorhandene Failovercluster und -knoten, sowie auch verteilte Cluster (sog. *hyperkonvergente Cluster*) verwalten.

Windows Admin Center (WAC) - Zentrale Verwaltung von Client- und Servercomputern

Die Installation des Windows Admin Center (WAC) findet hierbei entweder lokal auf einem vorhandenen Computersystem unter Windows 10 (im Desktop-Modus) oder unter Windows Server 2019 bzw. Windows Server 2016 (als Windows Admin Center Gateway) statt. Zum Einsatz im Rahmen der Verwaltungstätigkeiten kommen hierbei die Windows PowerShell sowie auch WMI (Windows Management Instrumentation) über WinRM (Windows Remote Management).



Abb. 1.2: Windows Admin Center (WAC) - Erweiterung vorhandener Verwaltungslösungen (Quelle: Microsoft Corporation)

Wenn man das auf einem Serversystem bereitgestellte Windows Admin Center Gateway (beispielsweise mithilfe der DNS-Namensauflösung) über die Unternehmensfirewall veröffentlicht, ermöglicht dies die Verbindung und auch die Verwaltung von Computersystemen mithilfe des Microsoft Edge- oder alternativ mithilfe des Google-Chrome-Browsers quasi von einem beliebigen Ort aus über das Internet.

Zugriff von überall aus auf das Windows Admin Center

1.3.1 Enthaltene Funktionen für die Server- und Clientverwaltung

Das Windows Admin Center (WAC) sieht sich als Ergänzung zu den bereits vorhandenen Verwaltungswerkzeugen, wie beispielsweise die Microsoft Management-Konsolen (engl. *Microsoft Management Console, MMC*).

HINWEIS! Die Verwaltung spezieller Serverrollen, wie zum Beispiel die Active Directory-Domänendienste (engl. *Active Directory Domain Services, AD DS*), DNS-, DHCP-Dienste oder auch die Webserverrolle (IIS) ist mit dem Windows Admin Center (WAC) aktuell noch nicht möglich.

Die im Windows Admin Center (WAC) enthaltenen, wichtigsten Funktionen für die Verwaltung umfassen dabei u. a.:

- **Verwalten von Geräten (Client- und Servercomputer)**
- **Aktivieren/Deaktivieren von Serverrollen und Funktionen**
- **Anzeigen von Ressourcen und der Ressourcenverwendung**
- **Verwaltung von Zertifikaten**
- **Datei-Explorer**
- **Ereignisanzeige**
- **Verwalten installierter Apps**
- **Konfiguration lokaler Benutzer und Gruppen**
- **Netzwerkeinstellungen**
- **Firewall-Verwaltung**
- **Anzeigen und Beenden von Prozessen**
- **Bearbeiten der Windows-Registry-Einstellungen**
- **Verwalten von geplanten Aufgaben**
- **Verwaltung von Windows-Diensten**
- **Verwalten von Hyper-V-VMs und virtuellen Switches**

- **Verwalten von Speicher, sowie auch Dateifreigaben**
- **Verwalten von Speicherreplikaten**
- **Verwaltung von Windows-Updates**
- **Windows PowerShell-Konsole**
- **Remotedesktop-Verbindung**

Darüber hinaus bietet das Windows Admin Center (WAC) auch noch die folgenden Verwaltungsmöglichkeiten:

- **Computerverwaltung** - zum Verwalten von Windows 10-Clientcomputern
- **Serververwaltung** - zum Verwalten von Windows-Servercomputern unter Windows Server 2019, Windows Server 2016, Windows Server 2012 (R2) und Windows Server 2012
- **Failovercluster-Manager** - für die Verwaltung von Failovercluster, Cluster-Knoten und Cluster-Ressourcen
- **Hyperkonvergente Cluster-Manager** - bietet Verwaltungs- und Überwachungsmöglichkeit für beispielsweise Direkte Speicherplätze (engl. *Direct StorageSpaces*) und Hyper-V.

Microsoft arbeitet daran, das Windows Admin Center (WAC) stets um weitere Verwaltungsmöglichkeiten zu bereichern. Diese werden dann in den zukünftigen Versionen des Windows Admin Center (WAC) enthalten sein.

Stetige
Weiterent-
wicklung

HINWEIS! Microsoft kennzeichnet manche der im Windows Admin Center (WAC) enthaltenen Funktionen mit dem Begriff „Vorschau!“. Dies ist darauf zurückzuführen, dass sich einige der bereits im WAC enthaltenen Funktionen offensichtlich noch in der Entwicklungs- bzw. Erprobungsphase befinden. Microsoft sammelt hierzu noch Erkenntnisse in der Verwendung und wohl auch der Zuverlässigkeit der jeweiligen Funktionen. Die daraus gewonnenen Erkenntnisse fließen dann in die weitere Entwicklung mit ein.

1.3.2 Zugriffsrollen beim Einsatz als Gateway

Wenn das Windows Admin Center (WAC) in der Rolle als *Gateway* auf einem Serversystem unter Windows Server 2016 oder Windows Server 2019 bereitgestellt wird, so kann man den Zugriff auf die WAC-Verwaltungskonsolle mithilfe bestimmter, im WAC vordefinierter Gateway-Zugriffsrollen steuern.

Es existieren die folgenden Gateway-Rollen für die Steuerung des Zugriffs auf das Windows Admin Center Gateway:

- **Gateway-Administratoren** - diese Rolle wird verwendet, um den Zugriff, sowie auch die Authentifizierungsoptionen für Gateway-Benutzer festzulegen. Lokale Administratoren auf dem Gateway-Computer gehören automatisch auch zur Gruppe der Gateway-Administratoren.
- **Gateway-Benutzer** - diese Rolle bietet die Möglichkeit, sich mit dem Windows Admin Center Gateway für die Verwaltung von Computersystemen zu verbinden. Gateway-Benutzer können die Einstellungen für die Zugriffsberechtigung, sowie auch die durch die Gateway-Administratoren festgelegte Authentifizierungsmethode jedoch nicht verändern.

HINWEIS! Beachten Sie, dass durch die Zuweisung von Benutzern zur Gruppe der Gateway-Benutzer zwar der Zugriff auf das betreffende Windows Admin Center Gateway, nicht jedoch auch der Zugriff auf die zu verwaltenden Zielservers delegiert wird. Für die Verwaltung von Server- und Clientcomputern muss der betreffende Benutzer zusätzlich auch über die notwendigen Verwaltungsrechte auf dem zu verwaltenden System verfügen.

Die Details zur Zuordnung von Benutzern in die vorhandenen Zugriffsrollen sind im [Kapitel 3](#) dieses Fachbuches enthalten.

1.3.3 Optionen für die Authentifizierung von Gateway-Benutzern

Die Gateway-Administratoren können beim Festlegen der Authentifizierungsmethoden für die Gateway-Benutzer wählen zwischen:

- **Active Directory- oder lokale Gruppen** - werden standardmäßig zum Steuern des Zugriffs auf das WAC-Gateway verwendet. Im WAC kann man auf der Registerkarte „Benutzer“ festlegen, wer darauf als Gateway-Benutzer den Zugriff erhält.

WICHTIG! Wenn man in dieser Registerkarte „Benutzer“ im WAC keine Benutzergruppe angibt, erhalten standardmäßig alle Benutzer darauf Zugriff, welche die Gateway-URL aufrufen können. Dies wird erst mit dem Festlegen von einer oder mehrerer Sicherheitsgruppen beschränkt.

- **Azure Active Directory (Azure AD)** - kann für die Authentifizierung der Gateway-Benutzer verwendet werden, was jedoch ein - in der Regel kostenpflichtiges - Microsoft Azure-AD-Abonnement klar voraussetzt. Die Verwendung der Authentifizierung mittels Azure AD ermöglicht zusätzlich auch die Verwendung der darin enthaltenen Multifaktor-Authentifizierung oder auch des sogenannten „bedingten Zugriffs“ (engl. *Conditional Access*).

HINWEIS! Auch bei der Verwendung von Azure-AD für die Authentifizierung müssen die betreffenden Benutzer ebenso auch Mitglieder der lokalen Verwaltungsgruppen auf den zu verwaltenden Computersystemen sein.

Die detaillierten Schritte zur Konfiguration der Authentifizierungsoptionen für Gateway-Benutzer werden im [Kapitel 3](#) dieses Fachbuches noch vorgestellt.