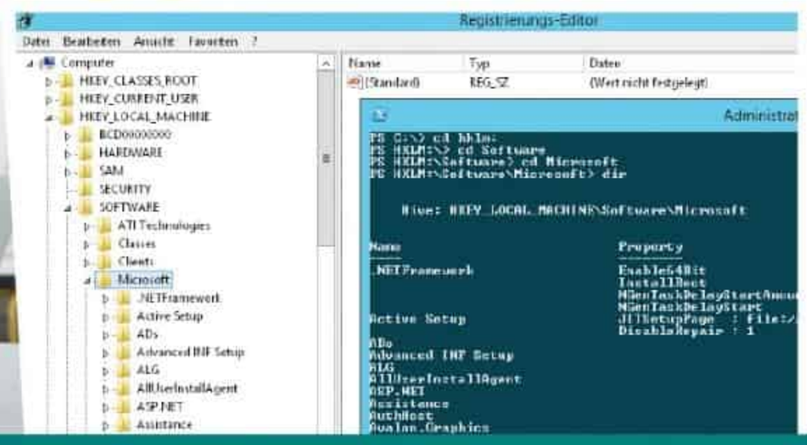
Peter Kloep
Karsten Weigel
Kevin Momber
Raphael Rojas
Annette Frankl







Windows Server 2019

Das umfassende Handbuch

- Infrastruktur, Installation, Konfiguration, Administration
- Alle Serverrollen erklärt: Active Directory, Hyper-V, DHCP- und DNS-Server, Datei-, Druck- und Webserver
- Windows Admin Center, Server Manager, WSUS, PowerShell, Azure Hybrid Cloud

Rheinwerk Computing

Kapitel 2
Rollen und Features

Dieses Kapitel widmet sich den Rollen und Features von Windows Server 2019. Sie verleihen dem Betriebssystem-Gerüst, das den Rahmen vorgibt, erst Herz und Seele. Wir zeigen Ihnen hier, welche Aufgaben der Server übernehmen kann und wie Sie diese installieren.

Wenn Sie Windows Server 2019 installiert haben und es in Betrieb nehmen, tun Sie das, weil dieser Server eine von Ihnen definierte Aufgabe übernehmen soll. Aber erst durch die Installation einer oder mehrerer Rollen und möglicherweise auch verschiedener Features kann der Server seiner Bestimmung gerecht werden.

In diesem Kapitel lernen Sie alle Rollen, Rollendienste und Features kennen. Außerdem stellen wir die verschiedenen Editionen vor, und Sie erfahren, welche Installationsmöglichkeiten zur gewünschten Funktion auf Ihrem Server führen.

2.1 Rollen und Rollendienste

Eine *Rolle* beschreibt die Aufgabe, die der Server übernehmen wird. Durch die Installation der Rolle wird der Server auf seine Aufgabe vorbereitet. Aufgaben, für die ein Windows Server unter anderem eingesetzt werden kann, sind *Verzeichnisdienst-Funktionen*, *Dateidienst-Aufgaben* oder *Webserver*; aber er kann auch als *DHCP-Server*, *DNS-Server* oder *Hyper-V-Host* dienen (siehe Abbildung 2.1). Er kann für die Verteilung von Updates als *WSUS-Server* verwendet werden oder als *KMS* die Produktschlüssel für die Aktivierung aller Clients im Netzwerk zentral verwalten. Im Folgenden finden Sie zu jeder Rolle eine Kurzbeschreibung. Ein Großteil dieser Rollen wird in eigenen Kapiteln detailliert beschrieben.

Die möglichen *Rollendienste*, die während der Installation zu manchen Rollen aufgelistet werden, sind Einzelkomponenten einer Rolle. Ein Rollendienst ist eine Teilkomponente, die zu einer Rolle gehört und bei Bedarf ausgewählt und installiert werden kann (siehe Abbildung 2.2).

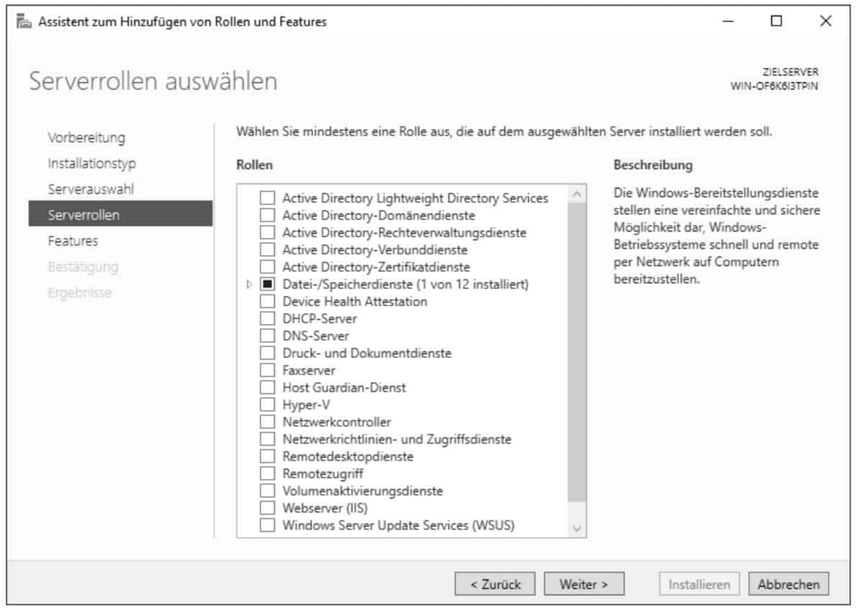


Abbildung 2.1 Assistent zum Hinzufügen von Rollen und Features – Rollenauswahl

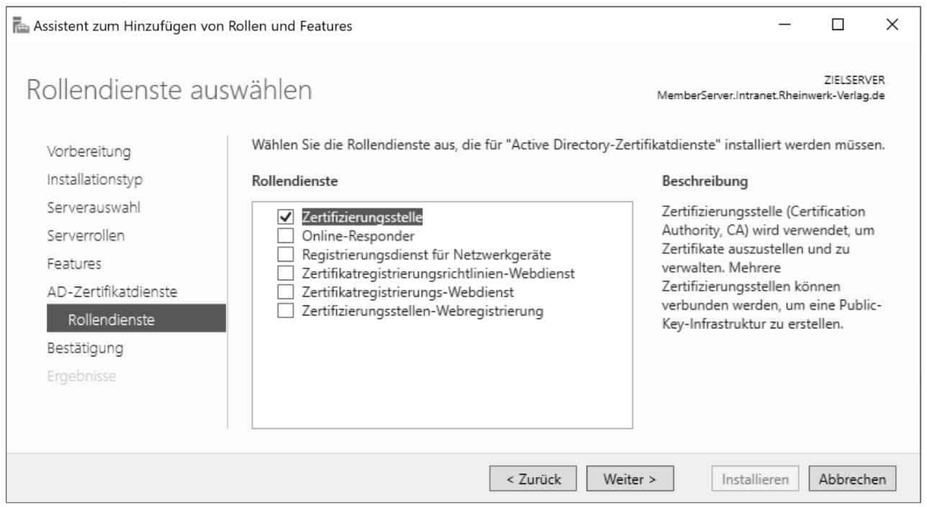


Abbildung 2.2 Rollendienst – Auswahl während der Installation einer Rolle

Das unterscheidet den Rollendienst auch von einem *Feature*, das unabhängig von Rollen die Serverfunktionen erweitert. Falls ein Rollendienst zum Betreiben einer Rolle unabdingbar

ist, wird er während der Rolleninstallation automatisch aktiviert. Weitere Rollendienste können je nach Bedarf auch später hinzugefügt werden, insofern sie benötigt werden.

Ein Windows Server 2019 hat – ohne installierte Zusatzpakete – die Möglichkeit, 21 verschiedene Rollen plus deren Rollendienste auszuführen. Im Folgenden werden wir Ihnen diese vorstellen.

2.2 Die Rollen im Überblick

Dieser Abschnitt liefert Ihnen eine Übersicht über alle verfügbaren Rollen inklusive einer Kurzbeschreibung, wie sie auch im Installationsassistenten des Servers zu finden ist. Diese Liste soll Ihnen einen Überblick geben. Abgerundet wird die Vorstellung der Rollen und ihrer Rollendienste durch kleine Darstellungen, damit Sie die Elemente im Server leichter wiederfinden, und Bemerkungen über Besonderheiten. So können Sie einfach und schnell alle Möglichkeiten des Servers erkennen. Welche Funktionen sich hinter den einzelnen Rollen verbergen, lesen Sie im Folgenden.

2.2.1 Active Directory Lightweight Directory Services

Die erste Rolle, die zu den Verzeichnisdiensten gehört, heißt *Active Directory Lightweight Directory Services* (AD LDS). Bis Windows Server 2003 trug diese Rolle noch den Namen *Active Directory Application Mode* (ADAM).

AD LDS stellt einen Datenzugriff per *LDAP(S)* bereit. Er bietet für verzeichnisdienstfähige Anwendungen die Möglichkeit, deren Daten in einen dafür bereitgestellten Speicher zu legen. Man könnte ihn auch als »Low-End-Variante« des Active Directory bezeichnen. Mit AD LDS können auch mehrere, verschiedene Instanzen auf einem Server parallel betrieben werden. Dies bietet zum Beispiel den Vorteil, dass die verschiedenen Instanzen nicht das gleiche Schema benutzen müssen. Die Daten der Applikation werden in separaten Ordnern gespeichert und bereitgestellt. Einen Domänencontroller muss man beim Einsatz dieser Rolle nicht extra betreiben.

Nachdem Sie die Rolle installiert haben, können Sie eine AD LDS-Instanz konfigurieren. Der Setup-Assistent benötigt folgende Informationen:

- die **Art der Instanz** – EINDEUTIG (eine neue Instanz) oder REPLIKAT (Kopie einer bestehenden Instanz)
- einen **Namen**
- den **Anschluss-Port** – Achten Sie darauf, dass es ein freier und verfügbarer Port ist!
- eine Entscheidung, ob eine **Anwendungspartition** erstellt werden soll oder ob die Anwendung selbst eine solche erstellt
- den **Speicherort** für die mit der Instanz verknüpften Daten

- das **Dienstkonto**, unter dessen Berechtigung die Instanz betrieben wird
- die Auswahl, welche **LDIF-Dateien** importiert werden, um bestimmte Konfigurationen anwenden zu können

Vor der Installation der Instanz zeigt der Setup-Assistent eine Zusammenfassung aller Konfigurationen an (siehe Abbildung 2.3).

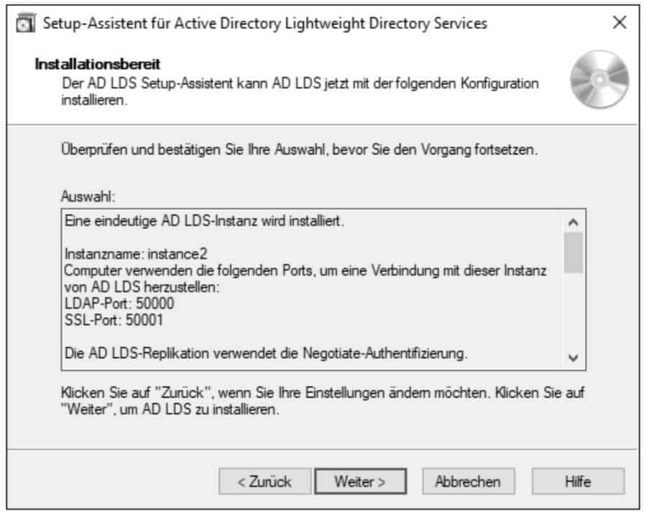


Abbildung 2.3 Zusammenfassung im Setup-Assistenten für eine neue AD LDS-Instanz

Diese Rolle ist nicht von anderen Rollen abhängig und könnte auch mit anderen Rollen betrieben werden. Die Installation dieser Rolle erfordert keinen Neustart.

Entfernen können Sie die Rolle erst, wenn zuvor alle AD LDS-Instanzen entfernt wurden. Diese Aktion fordert ebenfalls keinen Neustart.

2.2.2 Active Directory-Domänendienste

Die Rolle *Active Directory-Domänendienste* (AD DS) stellt einen Informationsspeicher im Netzwerk bereit, in dem Administratoren (oder andere privilegierte Benutzer) beispielsweise Benutzer- oder Computer-Objekte anlegen und zentral verwalten können. Nachdem die Rolle installiert wurde, muss der Server zum *Domänencontroller* hochgestuft werden, damit er diese Rolle ausführen kann. Er authentifiziert dann z. B. Benutzer im Netzwerk, sobald sie sich anmelden. Nach erfolgreicher Authentifizierung ermöglicht der Domänencontroller ihnen den Zugriff auf zugelassene Ressourcen, wie Dateien auf Dateiservern oder Netzwerk-Drucker. Einen tieferen Einblick in dieses Thema erhalten Sie in Kapitel 6 und in Kapitel 7.

Eine beliebte klassische Verwaltungskonsole für die Domänendienste ist das MMC-Snap-In *Active Directory Benutzer und -Computer*, das für die Konfiguration von Domäneneinstellungen verwendet wird (siehe Abbildung 2.4).

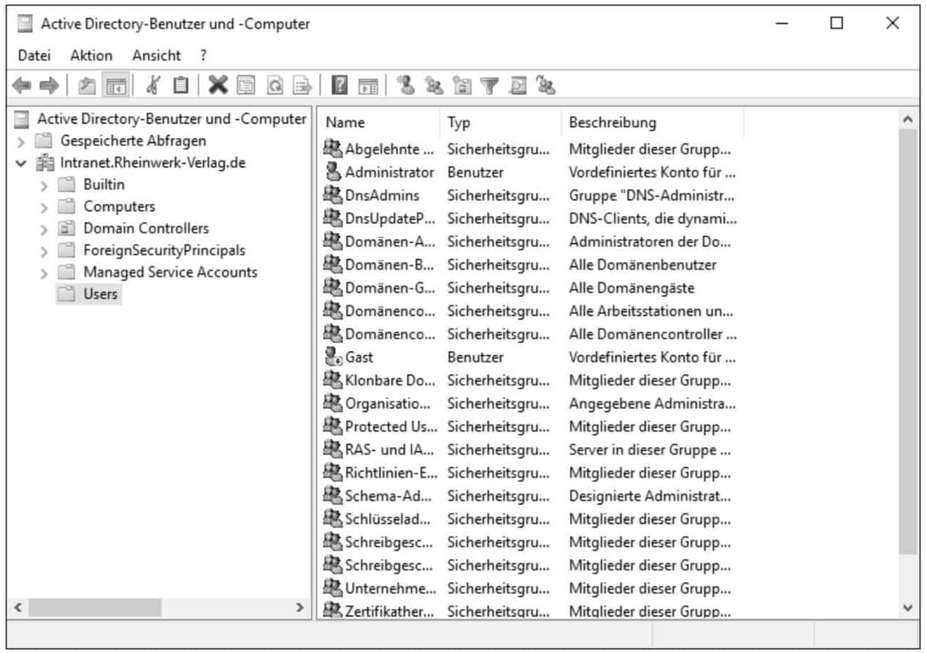


Abbildung 2.4 Active Directory Benutzer und Computer – Verwaltungskonsole

Da die klassische *Microsoft Management Console (MMC*) nicht mehr weiterentwickelt wird, können Sie zur Verwaltung auch das Active Directory-Verwaltungscenter verwenden, das Sie in Abbildung 2.5 sehen.

Die Installation der Rolle selbst erfordert keinen Neustart. Wenn allerdings nach der Rolleninstallation der Domänencontroller konfiguriert wurde, führt der Server automatisch einen Neustart durch, auf den hingewiesen wird. Danach ist eine Anmeldung nur noch mit einem Domänen-Benutzer möglich, der über administrative Rechte verfügt. Eine Ausnahme bildet hier der *Directory Service Restore Mode (DSRM)*, der unter anderem für die Domänencontroller-Wiederherstellung verwendet wird.

Aufgrund der Sicherheitsrelevanz wird empfohlen, einen Domänencontroller als einzige Rolle auf einem Server zu betreiben. Die einzige Ausnahme stellt der DNS-Service dar, insofern dieser AD-integriert konfiguriert wurde.

Möchten Sie die AD DS-Rolle wieder entfernen, müssen Sie den Domänencontroller erst wieder herabgestufen. Die Herabstufung benötigt einen Neustart.

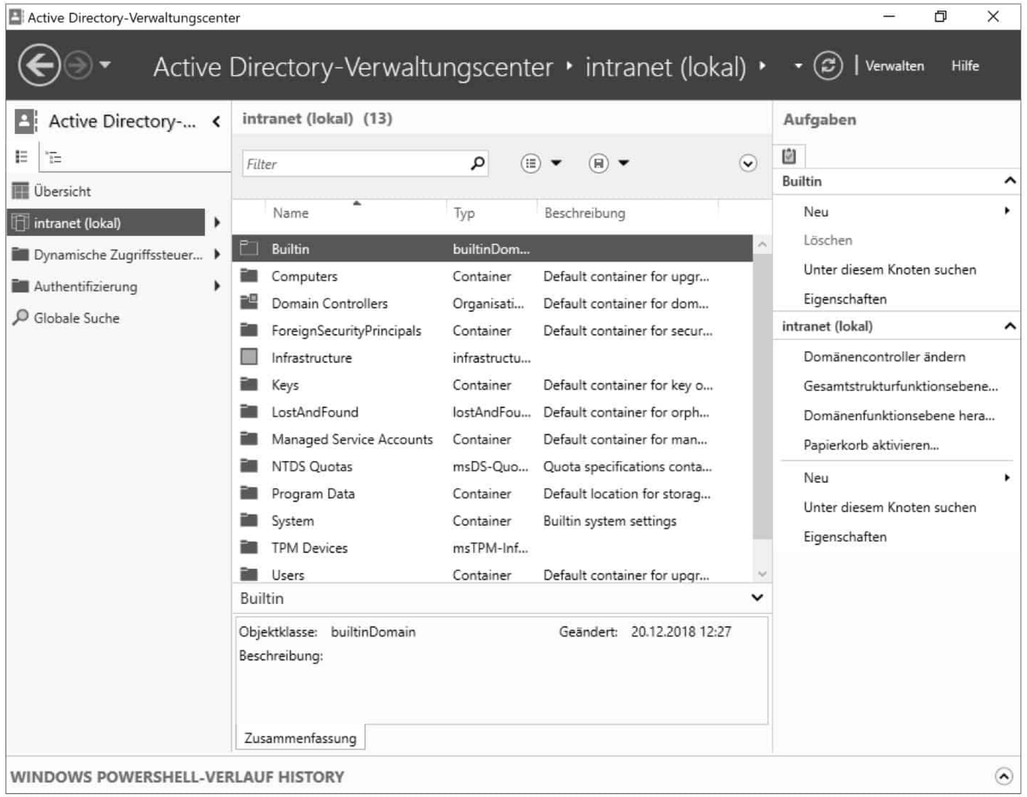


Abbildung 2.5 Active Directory-Verwaltungscenter

Entfernen der Rolle AD DS

Sollte es sich um den letzten Domänencontroller in der Umgebung handeln, entfernen Sie mit dieser Aktion Ihre AD- Gesamtstruktur!

Bitte beachten Sie, dass nach dem Entfernen der Rolle *AD DS* die im Standardfall ebenfalls vorhandene Rolle *DNS-Server* immer noch installiert bleibt. Sie muss separat entfernt werden, sollten Sie sie ebenfalls nicht mehr benötigen.

2.2.3 Active Directory-Rechteverwaltungsdienste

Der *AD Right-Management-Service (AD RMS)* ist eine Datenschutztechnologie, die – mit anderen Anwendungen – dazu beitragen kann, digitale Informationen vor Missbrauch zu schützen. Eingesetzt wird sie daher, wenn Sie Ihre Daten vor unautorisiertem Gebrauch schützen wollen.

Sie können sich das so vorstellen: Sie möchten einem Kollegen eine Datei schicken, aber verhindern, dass er die Datei weiterleiten oder ausdrucken kann. Mit den klassischen Mitteln einer Rechtevergabe im Dateisystem ist so etwas unmöglich. Wenn Sie aber einen AD RMS-Server im Netzwerk einsetzen, werden die Dokumente verschlüsselt auf dem RMS-Cluster abgespeichert. Nur wenn Ihr Kollege dort entsprechende Rechte besitzt, schaltet der AD RMS-Server den Zugriff frei (siehe Abbildung 2.6).

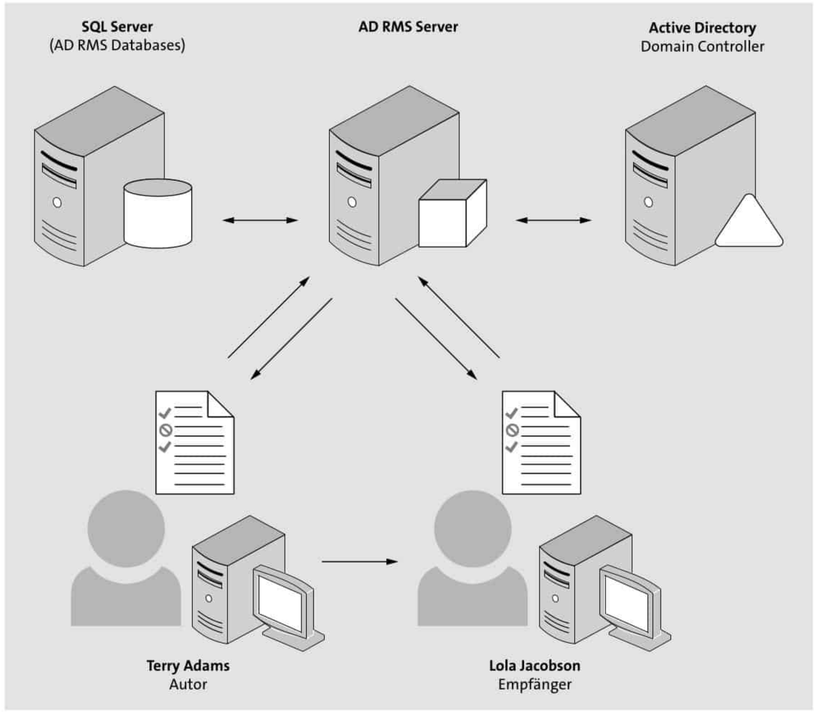


Abbildung 2.6 Beispiel einer möglichen AD RMS-Infrastruktur
(Quelle: https://i-technet.sec.s-msft.com/dynimg/IC603502.jpeg)

Wenn Sie die AD RMS-Rolle zur Installation auswählen, schlägt der Installationsassistent Ihnen vor, die darüber hinaus benötigten Rollendienste und Features gleich mit zu installieren. Dies betrifft Teile aus dem Bereich der .NET-Funktionen, der Webserver-Rollendienste und -Features und der Windows-Prozessaktivierungsdienste. Außerdem wird die Verwal-

tungskonsole für AD-Rechteverwaltungsdienste aus dem Feature-Bereich der Remoteserver-Verwaltungstools aktiviert.

AD RMS ist die erste Rolle in unserer Reihe, die während der Installation auch Rollendienste zur Installation auflistet.

Für AD RMS sind folgende Rollendienste gelistet:

- *Active Directory-Rechteverwaltungsserver* – Hierbei handelt es sich um den Rollendienst für die AD RMS-Rolle selbst.
- *Unterstützung für den Identitätsverbund* – Dieser Rollendienst nutzt Partnervertrauensstellungen zwischen Ihrer Organisation und anderen Organisationen, um Benutzeridentitäten nachzuweisen und um Zugriff auf geschützte Informationen beider Organisationen zu gewähren.

Da AD RMS auch Teile des Webservers (IIS) benötigt, werden auch davon Rollendienste und Features installiert, die der Assistent automatisch vorauswählt.

Name der Domain nicht ändern

Der Domänenname, in der der AD RMS-Server konfiguriert wird, darf sich anschließend nicht mehr ändern!

Unterstützt wird diese Technik nur von aktuellen MS Office-Versionen. Die Konfiguration der Rolle ist komplex und das Rechtekonstrukt unterscheidet sich sehr von der derzeit gewohnten Rechtevergabe auf Dateiebene.

AD RMS benötigt eine Active Directory im Netzwerk, also eine Domänenumgebung, die die Autorisierungen prüft. Außerdem muss ein Datenbankserver vorhanden sein, der als Informationsspeicher dient. Sollen Benutzer, die sich außerhalb der eigenen Infrastruktur befinden, ebenfalls zugreifen und Rechte abrufen können, muss der RMS-Server über das Internet erreichbar sein.

Mit Windows Server 2012 wurde eine neue Technik vorgestellt: *Dynamic Access Control* (DAC). Damit können Sie in einer Domäne die Berechtigungen und Zugriffe über AD-Attribute steuern. AD RMS ist hierfür die Grundlage.

2.2.4 Active Directory-Verbunddienste

Mit den *Active Directory-Verbunddiensten* (AD FS, *AD Federation Service*) wird ein vereinfachter und gesicherter Identitätsverbund sowie die Funktion für die einmalige browserbasierte Anmeldung bereitgestellt.

Wenn Sie vorhaben, in Ihrem Unternehmen einen internen Verbund zwischen verschiedenen Identitätsbereichen zu erstellen oder sogar Cloud-Plattformen mit Ihrem Unternehmen zu verbinden, ist der AD FS eine gute Wahl.

Mit den Verbunddiensten wird es Ihnen ermöglicht, die im AD gespeicherten Identitätsinformationen eines Benutzers gesichert zu verwenden, um über den Verbund auch auf andere Bereiche zuzugreifen. Der Benutzer braucht sich dadurch nicht mehrfach anzumelden. Der Vorteil für die Administration besteht darin, dass zusätzliche Benutzerkonten eingespart werden, und die digitalen Identitäten und Zugriffsrechte der Benutzer an vertrauenswürdige Partner weitergegeben werden. Die Verwaltung der Identitäten in der Partnerumgebung muss nicht aus der Hand gegeben werden, wenn eine Verbund-Vertrauensstellung diese Autorisierung übernimmt. Der Zugriff auf Ressourcen Ihrer Partner ist mit dieser Technik möglich, ohne dass es eine AD-Vertrauensstellung geben muss und Sie die Kennwörter Ihrer Benutzer an Ihre Partner liefern müssen. Der Einsatz dieser Rolle vereinfacht die Zusammenarbeit mit Verbundpartnern erheblich. Gerade in der heutigen Zeit, in der Cloud-Strategien immer relevanter werden, wächst die Bedeutung dieser Rolle.

Ein Beispiel für eine AD FS-Infrastruktur finden Sie in Abbildung 2.7.

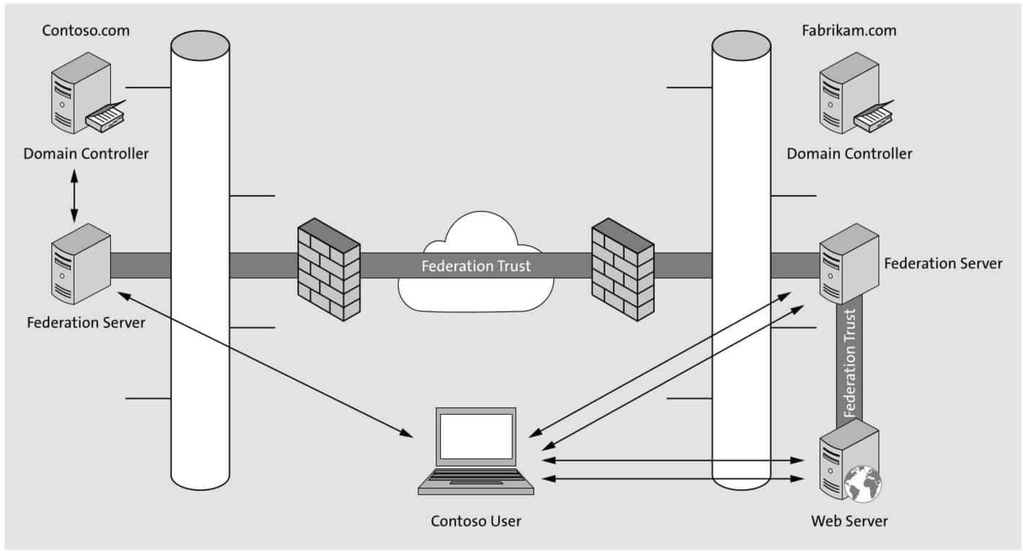


Abbildung 2.7 AD FS-Infrastruktur-Beispiel (Quelle: http://i1.wp.com/www.netwatch.me/wp-content/uploads/2015/07/ADFS-overview.png)

Ab Windows Server 2016 können Benutzerkonten, die in einer AD LDS-Instanz gespeichert sind, ebenfalls in einem Verbund authentifiziert werden.

Der Server muss Teil einer Domäne sein, wenn die AD FS-Rolle installiert wird. Außerdem kommt der Webanwendungsproxy-Rollendienst zum Einsatz. Er darf nicht auf demselben Computer installiert sein wie der Verbunddienst.

Die Installation der AD FS-Rolle erfordert keinen Neustart.

Nach der Rolleninstallation startet ein Konfigurationsassistent. Er zeigt Ihnen auf, welche Voraussetzungen es für die Installation eines Verbundservers gibt. Beispielsweise benötigen Sie unter anderem ein öffentliches Zertifikat für die SSL-Serverauthentifizierung, ein Dienstkonto und einen Datenbankspeicher.

2.2.5 Active Directory-Zertifikatdienste

Haben Sie sich schon mal Gedanken darüber gemacht, sich mit einer Chip-Karte, einer sogenannten Smart-Card, zu authentifizieren? Oder wollten Sie Ihre eigene öffentliche Unternehmenswebsite mit einem Vertrauenssiegel versehen? Dann müssen Sie sich mit dem Einsatz von Zertifikaten vertraut machen. Die Servereinheit, die solche Zertifikate erstellt und verwaltet, ist eine Zertifizierungsstelle. Diese kann eingesetzt werden, wenn Sie die Rolle *Active Directory-Zertifizierungsdienste* (AD CS, *AD Certification Service*) installieren. Wenn Sie im Unternehmen eine eigene Zertifizierungsstelle (*Certificate Authority*, *CA*) bereitstellen, kann diese die Zertifikate für eine Vielzahl von Anwendungen ausstellen. Einige Beispiele sind Datei- oder E-Mail-Verschlüsselung, Smart-Card-Authentifizierung oder Internetprotokollsicherheit (IPSec).

Der Aufbau einer CA-Infrastruktur, die Teil einer *Public-Key-Infrastruktur* (*PKI*) ist, sollte mehrere Zertifizierungsstellen-Ebenen vorsehen, um in erster Linie den Ursprung der Vertrauenskette zu schützen. Wenn wir zum Beispiel eine dreistufige Hierarchie betrachten (siehe Abbildung 2.8) würde diese sich wie folgt erklären:

- Den Ursprung bildet eine *Root-CA* oder *Stammzertifizierungsstelle*, die nach der Konfiguration und dem Ausstellen der benötigten Root-Zertifikate ausgeschaltet und sicher verwahrt werden sollte, damit die Vertrauenswürdigkeit der gesamten PKI gewährleistet bleibt. Diese Offline-Root-CA bildet den Anfang der Vertrauenskette der Zertifikate. Vertraut man dem Root-Zertifikat, vertraut man allen danach ausgestellten Zertifikaten ebenfalls.
- Unterhalb dieser Root-CA werden dann *Richtlinien-CAs* erstellt, mit deren Hilfe verschiedene Bereiche der PKI unterteilt werden können.
- Auf dritter Ebene werden *ausstellende CAs* aufgebaut. Beteiligte Geräte oder Benutzer wenden sich an eine ausstellende CA, um sich eines der zuvor definierten Zertifikate zuteilen zu lassen.

Beim Planen einer PKI sind Vorgaben wie die zukünftige Gültigkeitsdauer von Zertifikaten oder die Lebensdauer der Zertifizierungsstellen-Hardware sehr relevant und müssen mit betrachtet werden.

Konfiguration der AD CS-Rolle

Den Computernamen und die Domäneneinstellungen des Servers, auf dem die AD CS-Rolle installiert wird, können Sie anschließend nicht mehr ändern.

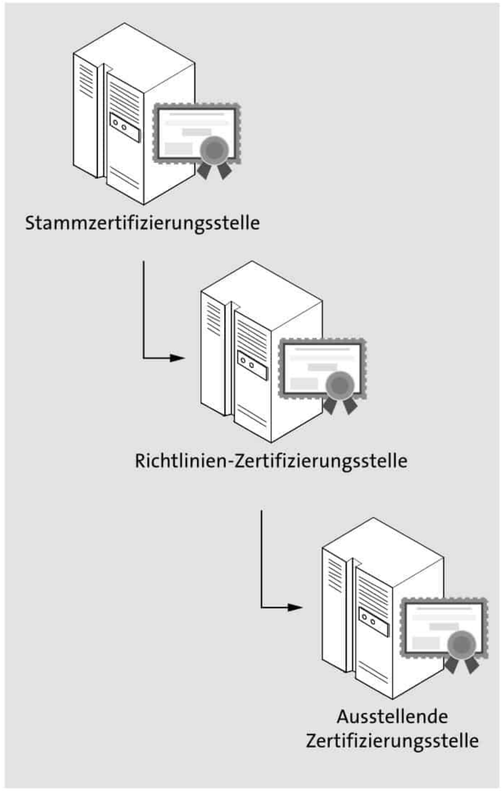


Abbildung 2.8 Aufbau einer dreistufigen Zertifizierungsstellenhierarchie

Während der Rolleninstallation werden folgende Rollendienste zur Installation angeboten, wobei der erste Dienst bereits aktiviert ist:

- *Zertifizierungsstelle* – Hierbei handelt es sich um den Rollendienst der Zertifizierungsstelle selbst.
- *Online-Responder* – Dieser Rollendienst ermöglicht Clients in komplexen Netzwerkumgebungen den Zugriff auf Daten der Zertifikatsperrüberprüfung.
- *Registrierungsdienst für Netzwerkgeräte* – Er verwendet *Simple Certificate Enrollment Process* (*SCEP*) und dient zum Ausstellen und Verwalten von Zertifikaten für Router und andere Netzwerkgeräte.
- *Zertifikatregistrierungsrichtlinien-Webdienst (CEP)* – Mit dem CEP können Benutzer und Computer Informationen der Zertifikatregistrierungsrichtlinien abrufen, auch wenn der Computer kein Mitglied der Domäne ist. Dieser Rollendienst arbeitet mit dem Zertifikatregistrierungs-Webdienst zusammen, um eine richtlinienbasierte automatische Zerti-

fikatregistrierung für diese Benutzer und Computer bereitzustellen. CEP können Sie verwenden, um Clients Zertifikate bereitzustellen, die nicht über einen *Remote Procedure Call (RPC)* mit der Zertifizierungsstelle kommunizieren können oder sollen. Das Gleiche gilt auch für den nächsten Rollendienst CES.

- *Zertifikatregistrierungs-Webdienst (CES)* – Mit diesem Rollendienst können Benutzer und Computer sich für Zertifikate registrieren und Zertifikate verlängern, auch wenn keine Domänenmitgliedschaft vorliegt. CES arbeitet mit dem Zertifikatregistrierungsrichtlinien-Webdienst (CEP) zusammen, um eine richtlinienbasierte automatische Zertifikatregistrierung für diese Benutzer und Computer bereitzustellen.

  Durch den Einsatz von CEP und CES können Clients, die sich in einem geschützten Bereich wie einer *Demilitarisierten Zone (DMZ)* befinden, Zertifikate von einer internen Zertifizierungsstelle abrufen.

  Der CES kann hierbei als eine Art RPC-Proxy eingesetzt werden, der die Anfragen der Clients annimmt und dann die Verbindung zur Zertifizierungsstelle per RPC aufbaut.

- *Zertifizierungsstellen-Webregistrierung* – Der letzte angebotene Rollendienst stellt eine einfache Webschnittstelle bereit, die Benutzern das Ausführen von Aufgaben ermöglicht, beispielsweise das Anfordern von Sperrlisten (CRLs) oder das Registrieren von Smartcard-Zertifikaten.

Je nach Rollendienstauswahl wird auch der CA-Konfigurationsassistent, der nach Abschluss der Rolle ausgeführt werden kann, die Konfiguration der einzelnen Rollendienste anbieten. Er erweitert sich interaktiv nach Aktivierung des jeweiligen Rollendienstes.

Vor der Aktivierung eines Rollendienstes zeigt der Assistent die Punkte aus Abbildung 2.9 an.

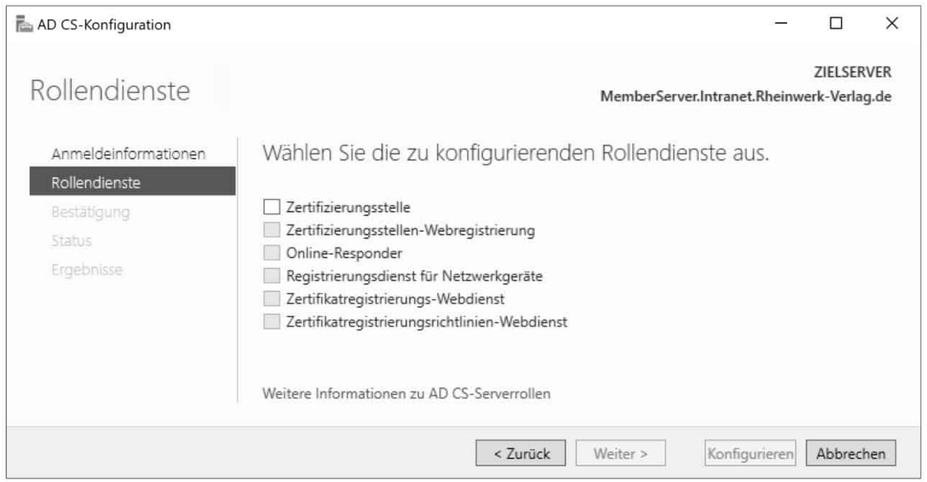


Abbildung 2.9 Der AD CS-Konfigurationsassistent vor der Aktivierung des Rollendienstes

Nach Aktivierung des Rollendienstes erweitert sich die Ablaufleiste so wie in Abbildung 2.10.

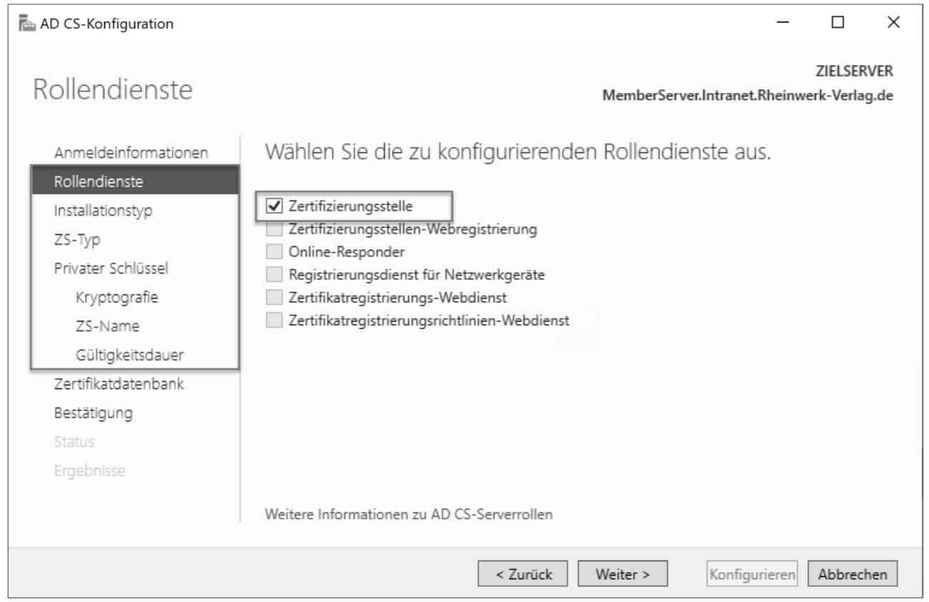


Abbildung 2.10 Der AD CS-Konfigurationsassistent nach Aktivierung des Rollendienstes

Natürlich sind im Assistenten nur die Rollendienste aktivierbar, die auch bei der Rolleninstallation ausgewählt wurden.

Sollten Sie nachträglich noch Rollendienste benötigen, können Sie diese über den gleichen Weg wie eine Rolleninstallation auswählen und hinzufügen.

Mehr zum Thema PKI finden Sie in Kapitel 17.

2.2.6 Datei-/Speicherdienste

Die *Datei-/Speicherdienste* bieten eine Vielzahl an Rollen und Diensten, die dem Server Dateiverwaltungsfunktionen bereitstellen. Eine Übersicht finden Sie in Abbildung 2.11.

Im Sammelpunkt DATEI- UND ISCSI-DIENSTE verbergen sich Technologien, mit deren Hilfe Sie Dateiserver und Speicher verwalten, die Datenträgerauslastung reduzieren, Dateien in Filialen replizieren und zwischenspeichern, eine Dateifreigabe auf einen anderen Clusterknoten verschieben oder einen Failover auf einen anderen Clusterknoten ausführen und Dateien mithilfe des NFS-Protokolls freigeben können. Aktivieren Sie diesen Sammelpunkt, wird automatisch die erste untergeordnete Rolle, DATEISERVER, ausgewählt.

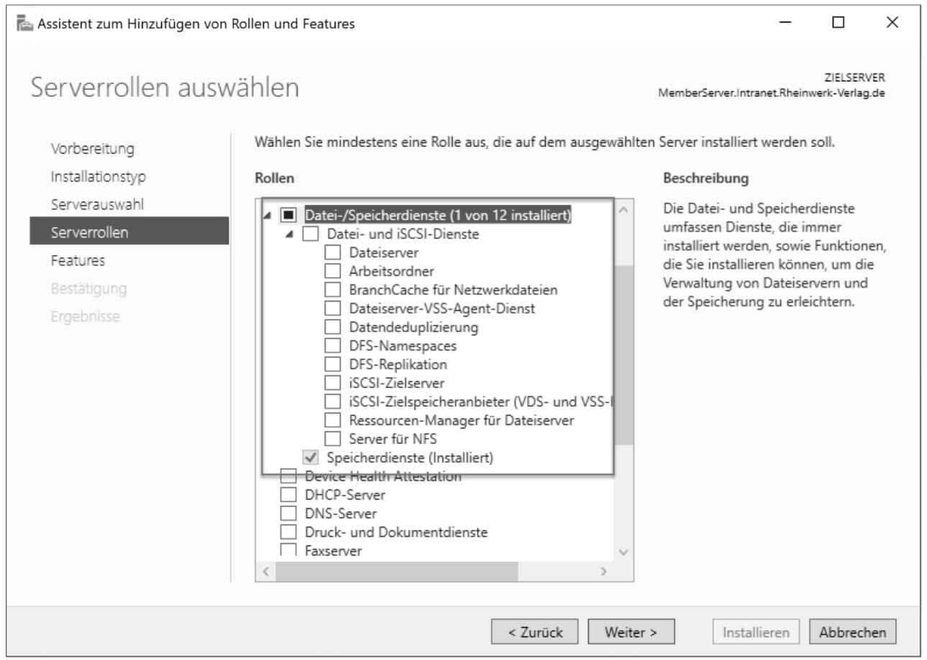


Abbildung 2.11 Liste der Datei-/Speicherdienste im Rolleninstallationsassistenten

Die Rolle *Dateiserver* bietet die Möglichkeit, freigegebene Ordner zu verwalten, und Benutzern Zugriff auf Dateien zu ermöglichen, die auf dem Server gespeichert sind.

Diese Rolle ist für alle anderen Rollen dieses Sammelpunktes notwendig. Sobald Sie eine der anderen Datei-/Speicherdienst-Rollen auswählen, weist der Assistent darauf hin, dass die Rolle Dateiserver ebenfalls benötigt und daher mitinstalliert wird.

Die Installation der Rolle benötigt keinen Neustart. Nach der Rolleninstallation hat sich zwar die Anzahl der vorhandenen Tools nicht verändert, aber Sie finden im *Server-Manager* unter dem Auswahlpunkt DATEI-/SPEICHERDIENSTE die neu hinzugefügten Themen FREIGABEN, ISCSI und ARBEITSORDNER (siehe Abbildung 2.12).

Da aktuell nur die *Dateiserver*-Rolle installiert wurde, werden Sie feststellen, dass die Punkte ISCSI und ARBEITSORDNER zwar schon vorhanden sind, aber bei Auswahl darauf hinweisen, dass die jeweilige Rolle noch installiert werden muss (siehe Abbildung 2.13).

Ihnen wird des Öfteren auffallen, dass Konfigurationsoberflächen bereits auf dem Server vorhanden sind, aber noch nicht benutzt werden können, weil die dazu notwendigen Rollen fehlen. Aber keine Sorge, die Assistenten oder Hilfetexte weisen darauf hin und erleichtern Ihnen meist per Link die Aktivierung der benötigten Rolle.

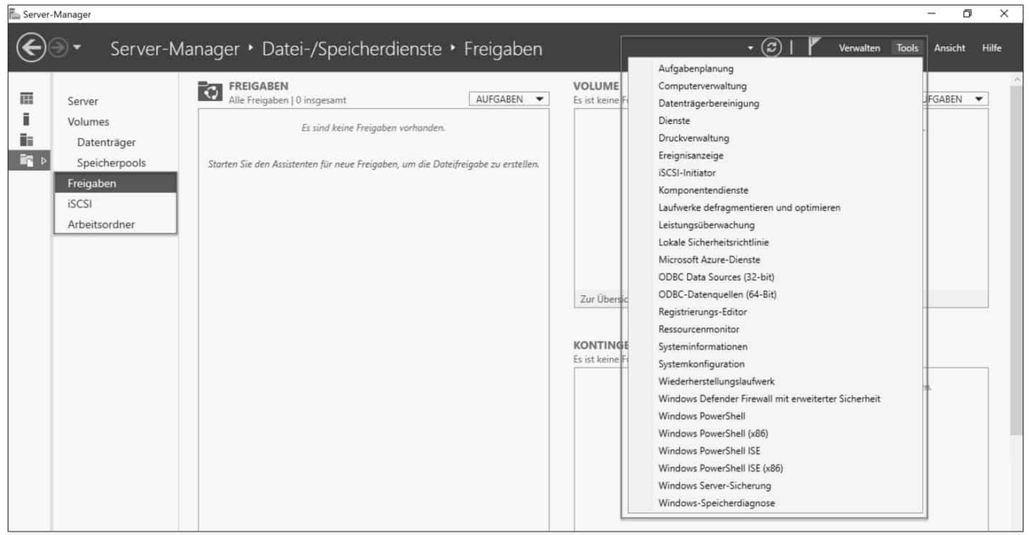


Abbildung 2.12 Server-Manager mit installierter Dateiserver-Rolle



Abbildung 2.13 Server-Manager mit Hinweis zur Rolleninstallation

Zurück zur Dateiserver-Rolle und ihrer Oberfläche zur Konfiguration von Freigaben, die Sie im Server-Manager finden: Wenn Sie eine Freigabe konfigurieren möchten, werden Sie auch hier von einem Assistenten unterstützt (siehe Abbildung 2.14).

Entscheiden Sie sich dafür, die Rolle *Arbeitsordner* zu aktivieren, wird der Assistent Sie darauf hinweisen, dass auch das Feature *Hostfähiger Webkern für Internetinformationsdienste* installiert wird. Arbeitsordner ermöglichen die Verwendung von Arbeitsdateien auf verschiedenen Computern, einschließlich Arbeitsgeräten und persönlichen Geräten.

Sie können mithilfe von Arbeitsordnern Benutzerdateien hosten und synchronisieren. Nachdem die Rolle installiert wurde, können Arbeitsordner auch über den Server-Manager eingerichtet werden (siehe Abbildung 2.15).



Abbildung 2.14 Der Assistent zur Erstellung von Freigaben auf einem Dateiserver

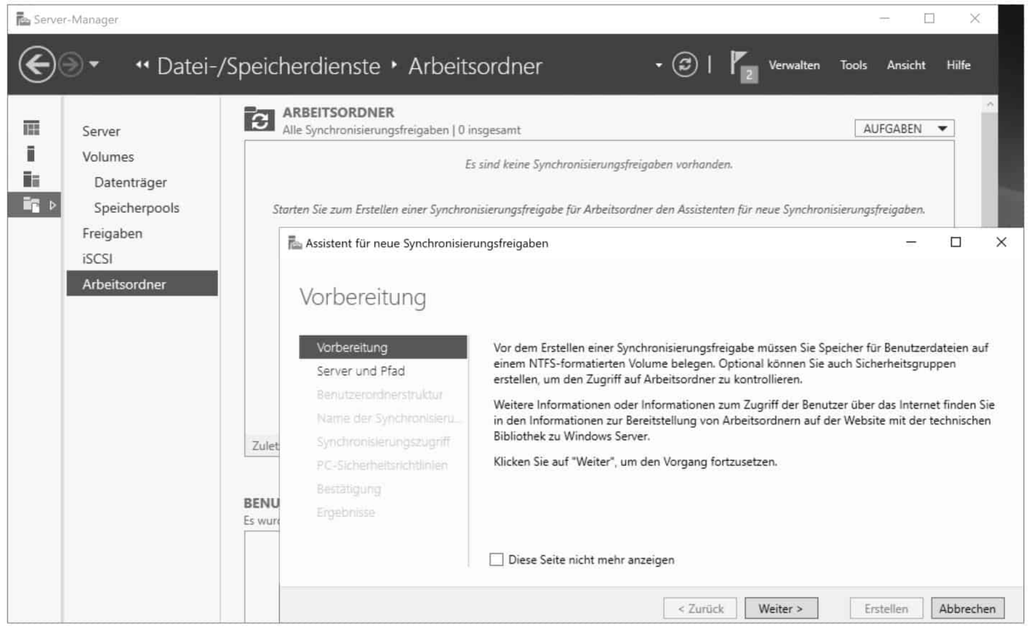


Abbildung 2.15 Assistent zur Erstellung von Arbeitsordnern

Diese Rolle kann ohne Neustart installiert und deinstalliert werden. Die Ansicht der Server-Manager-Konsolen im Bereich ARBEITSORDNER wird nach der Deinstallation allerdings erst nach einem Neustart wieder aktualisiert.

Die Rolle *BranchCache für Netzwerkdateien* stellt auf einem Dateiserver eine Bandbreitenoptimierungstechnologie für Fernnetze, sogenannte *Wide Area Networks (WANs)*, bereit. Dadurch ist die Zwischenspeicherung von Daten möglich, die in den Filialstandorten benötigt werden, aber im zentralen Rechenzentrum gespeichert sind. Für einen Benutzer optimiert das den Zugriff auf diese Daten. Nachdem die Rolle installiert wurde, müssen die gewünschten Verzeichnisse freigegeben und die Hashgenerierung aktiviert werden, damit die Daten zwischengespeichert werden können. Diese Einstellungen setzen Sie per Gruppenrichtlinie oder lokaler Richtlinie (siehe Abbildung 2.16 und Abbildung 2.17).

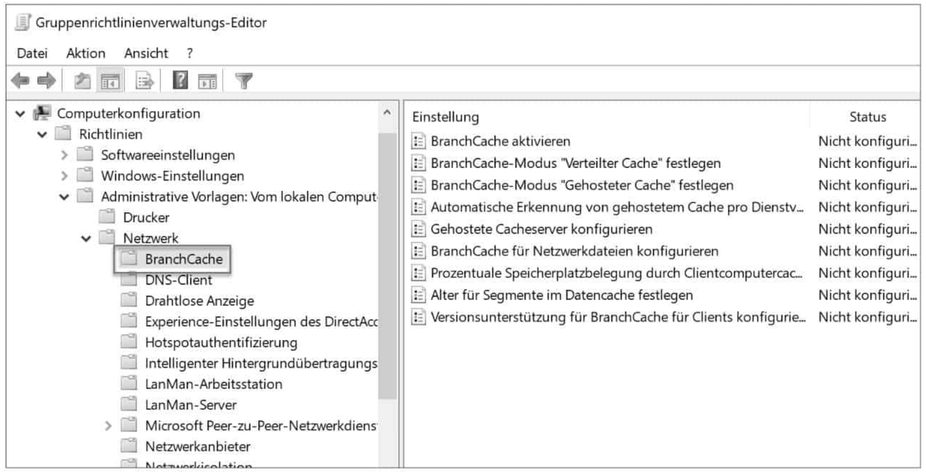


Abbildung 2.16 Richtlinien-Einstellungen für BranchCache-Dateiserver

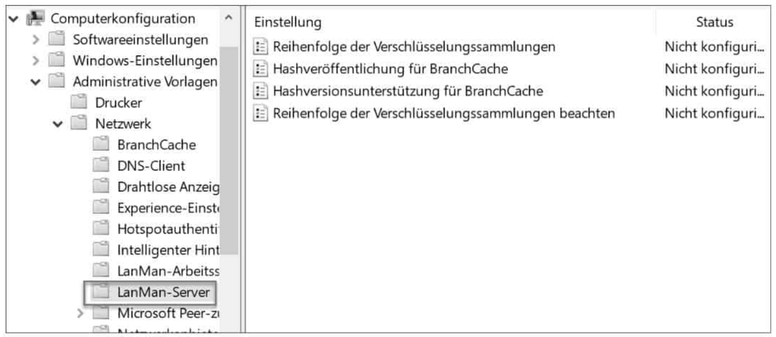


Abbildung 2.17 Richtlinien-Einstellungen für die Hashgenerierung der BranchCache-Dateiserver

Die Installation dieser Rolle erfordert keinen Neustart, das Entfernen der Rolle allerdings schon.

Die nächste Rolle in der Liste ist der *Dateiserver-VSS-Agent-Dienst*. VSS steht für *Volume-Shadow-Copy Service* oder *Volumenschattenkopie*. Mit dieser Technik werden Änderungen an Dateien aufgezeichnet, sodass bei Bedarf auf entsprechende Vorgängerversionen zurückgegriffen werden kann. Nach der Installation dieser Rolle erscheint der Microsoft-Schattenkopie-Agent-Dienst für Dateiserver in der Liste der installierten Dienste (siehe Abbildung 2.18). Er interagiert mit dem VSS-Dateiserver-Agent des Dateiservers. VSS-fähige Anwendungen können ihre Datendateien in Dateifreigaben auf dem Dateiserver speichern, und dieser Dienst verwaltet die Schattenkopien der Volumes auf dem Dateiserver, auf dem die Dateifreigaben liegen.

Manager-Dienst für den Funktionszugriff	Stellt Funktionen bereit, mit denen der Zugriff von UWP-Apps auf App-Funktio...		Manuell	Lokales System
Microsoft App-V Client	Manages App-V users and virtual applications		Deaktivi...	Lokales System
Microsoft iSCSI-Initiator-Dienst	Verwaltet Internet SCSI (iSCSI)-Sitzungen, die es zwischen diesem Computer und i...		Manuell	Lokales System
Microsoft Passport	Stellt die Prozessisolation für kryptografische Schlüssel bereit, die zur Authentifiz...		Manuell ...	Lokales System
Microsoft Passport-Container	Verwaltet lokale Benutzeridentitätsschlüssel, um Benutzer für Identitätsanbieter ...		Manuell ...	Lokaler Dienst
Microsoft Store-Installationsdienst	Bietet Infrastrukturunterstützung für den Microsoft Store. Der Dienst wird bei Be...		Manuell	Lokales System
Microsoft-Schattenkopie-Agent-Dienst für Dateiserver	Verwaltet die Schattenkopie von Dateifreigaben, die vom VSS-Dateiserver-Agent...		Manuell ...	Lokales System
Microsoft-SMP für Speicherplätze	Hostdienst für den Microsoft-Verwaltungsanbieter für Speicherplätze. Wird dies...		Manuell	Netzwerkdienst
Microsoft-Softwareschattenkopie-Anbieter	Verwaltet softwarebasierte Volumeschattenkopien des Volumeschattenkopie-Die...	Wird ausgeführt	Manuell	Lokales System
Net.Tcp-Portfreigabedienst	Ermöglicht es, TCP-Ports über das Protokoll "Net.Tcp" freizugeben.		Deaktivi...	Lokaler Dienst
Netzwerkeinrichtungsdienst	Der Netzwerkeinrichtungsdienst verwaltet die Installation von Netzwerktreibern ...	Wird ausgeführt	Manuell ...	Lokales System
Netzwerkkonnektivitäts-Assistent	Stellt die DirectAccess-Statusbenachrichtigung für Benutzeroberflächenkompon...		Manuell ...	Lokales System
Netzwerklistendienst	Identifiziert die Netzwerke, mit denen der Computer eine Verbindung hergestellt...	Wird ausgeführt	Manuell	Lokaler Dienst
Netzwerkspeicher-Schnittstellendienst	Dieser Dienst stellt Netzwerkbenachrichtigungen (z. B. beim Hinzufügen/Löschen...	Wird ausgeführt	Automat...	Lokaler Dienst
Netzwerkverbindungen	Verwaltet Objekte im Ordner "Netzwerk- und Wählverbindungen", in dem LAN- ...		Manuell	Lokales System

Abbildung 2.18 Ausschnitt aus der Liste der Dienste auf dem Windows Server 2019

Weder die Installation noch die Deinstallation dieser Rolle erfordert einen Neustart.

Mit der Rolle *Datendeduplizierung* können Sie auf Ihrem Dateiserver Speicherplatz einsparen, indem nur eine Kopie identischer Daten auf einem Volume gespeichert wird. Die Deduplizierung ist eine Alternative zur Komprimierung von Daten, um Speicherplatz auf einer Festplatte einzusparen. Um wirklich effektiv Datenspeicher freizugeben, wird der Dienst standardmäßig erst aktiv, wenn eine Datei größer als 64 KB und älter als 3 Tage ist. Diese Werte können Sie entsprechend anpassen. Vorrangige Einsatzgebiete der Deduplizierung sind die Datensicherung (Backup), die Datenspeicherung, die Archivierung und der Datentransfer. Das Verfahren eignet sich jedoch grundsätzlich für jeden Einsatzfall, bei dem Daten (oder Teile davon) mehrfach auf einem Server vorhanden sind.

Mit der Installation der Rolle werden zwei Dienste hinzugefügt und gestartet:

- *Datendeduplizierungsdienst*
- *Datendeduplizierung – Volumenschattenkopie-Dienst*

Nachdem Sie die Rolle installiert haben, können Sie die Deduplizierungstechnik auf dem Volume wie in Abbildung 2.19 aktivieren und konfigurieren.

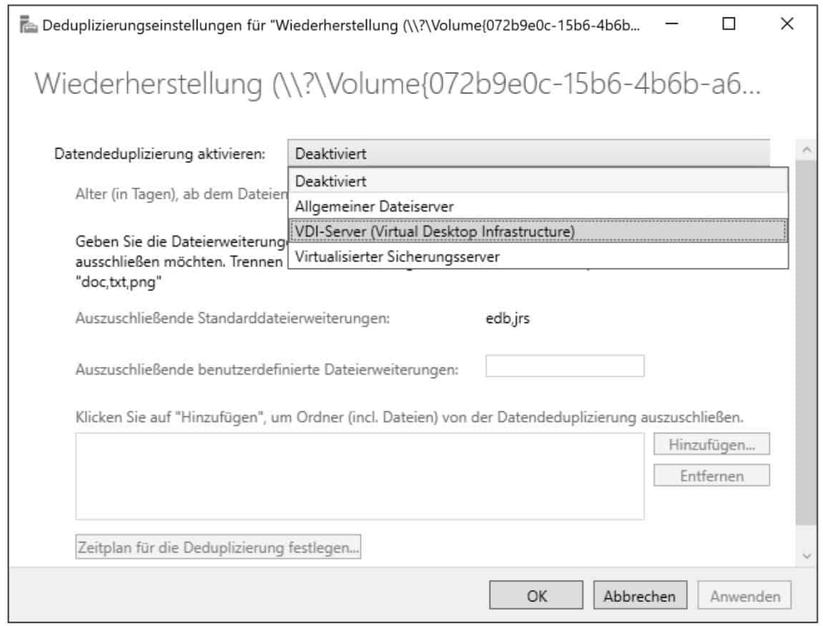


Abbildung 2.19 Optionen der Deduplizierung für das Volume, über den Server-Manager geöffnet

Die Installation der Rolle erfordert keinen Neustart, die Deinstallation allerdings schon.

Mithilfe der Rolle *DFS-Namespace* (*Distributed File System*, dt. »verteiltes Dateisystem«) können Sie freigegebene Ordner von verschiedenen Dateiservern in logisch strukturierte DFS-Namespaces gruppieren. Das kann hilfreich sein, wenn Sie Ihren Anwendern eine immer gleichbleibende, bekannte Ordnerstruktur bereitstellen möchten, obwohl die Daten, die sich darin verbergen, auf verschiedenen Dateiservern gespeichert sind. Der Anwender braucht nicht zu wissen, auf welchen Dateiservern die Daten abgespeichert wurden, da diese über die logisch dargestellte Verzeichnisstruktur, den DFS-Namespace, für den Benutzer einfach und gleichbleibend zu finden sind. Selbst bei einem Hardware-Austausch der Dateiserver-Infrastruktur bleibt die bekannte Struktur für den Anwender erhalten.

Ein gutes Beispiel für den Einsatz eines DFS-Namespaces ist eine Projektarbeit, deren Teilnehmer über viele Standorte verteilt sind bzw. bei der die Projektdaten auf verschiedenen Dateiservern abgelegt werden. Ein neuer DFS-Namespace für die Projektdaten wird unter dem Namen *Projekte* angelegt. Der Pfad, um zum Beispiel mit dem Namespace *Projekte* zu arbeiten, könnte so aussehen: *\\intranet.rheinwerk-verlag.de\Projekte*. Hier findet der Anwender nun alle Projektdaten – ganz unabhängig davon, ob der Dateiserver, mit dem die Verzeichnisse verbunden werden, am Standort A oder Standort B betrieben wird. Dies bleibt dem Benutzer genauso unbekannt wie die Namen der verwendeten Dateiserver selbst. Nur die Administratoren, die die logische Struktur mit den tatsächlichen Dateiservern verbin-

den, müssen natürlich die Infrastruktur kennen, die hinter der sichtbaren Verzeichnisstruktur steht, und diese im DFS-Namespace verknüpfen.

Wenn Sie diese Funktion installieren, wird der Assistent Sie darauf hinweisen, dass er auch die Verwaltungsoberfläche *DFS-Verwaltung* installiert, die für die Administration der DFS-Namespaces wichtig ist (siehe Abbildung 2.20).

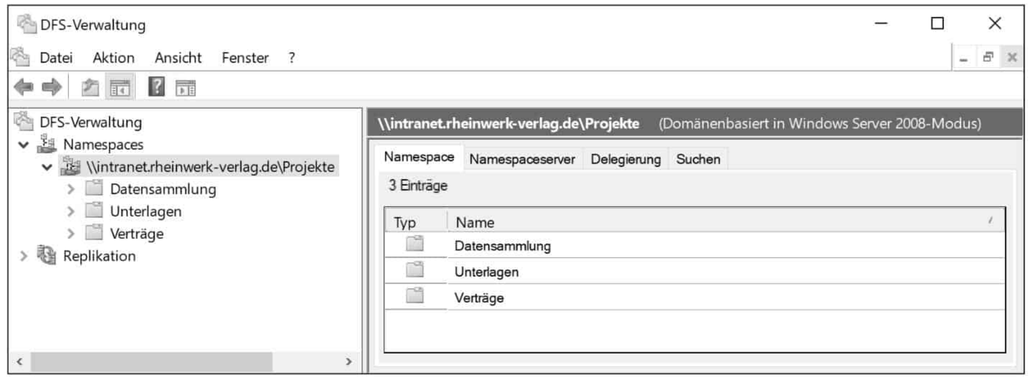


Abbildung 2.20 DFS-Management-Konsole mit einem DFS-Namespace namens »Projekte«

Die Installation der Rolle erfordert keinen Neustart. Wollen Sie die Rolle entfernen, weist der Assistent Sie darauf hin, dass zuerst alle DFS-Namespaces entfernt werden müssen (siehe Abbildung 2.21).

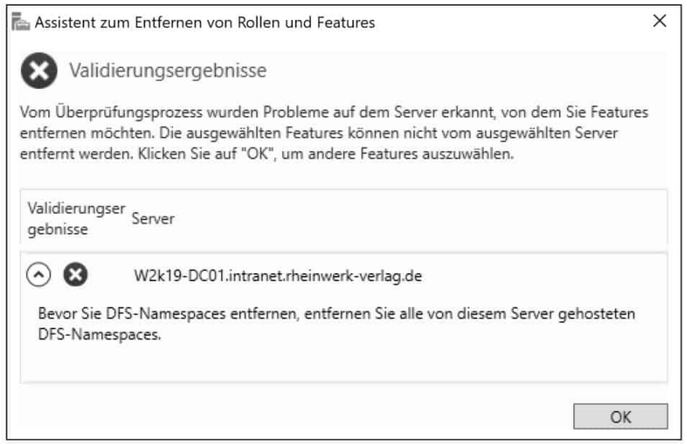


Abbildung 2.21 Hinweis beim Entfernen der DFS-Namespace Rolle

Ein Namensverwandter ist die Rolle *DFS-Replikation (DFS-R)*. Doch obwohl beide Rollen mit den drei gleichen Buchstaben beginnen und sogar in derselben Verwaltungskonsole administriert werden, haben sie nichts miteinander gemeinsam. Die Funktion, die sich hinter der Rolle DFS-Replikation befindet, hilft Ihnen dabei, Daten zwischen zwei oder mehreren Dateiservern zu replizieren.

Sie dient dazu, Daten beispielsweise aus den Filialen an einen zentralen Ort zu replizieren, um eine Datensicherung der gesammelten Daten durchführen zu können. Umgekehrt lassen sich auch Daten von einem zentralen Punkt an andere Orte verteilen. Ein gutes Beispiel dafür ist ein zentral verwaltetes Vorlagenverzeichnis, das Sie an die Filialstandorte verteilen.

FRS – Eine Ära geht zu Ende

Bevor Daten mit DFS-R repliziert wurden, erledigte der *FRS-Dienst (File Replication Service)* diese Aufgabe. Das älteste Beispiel für einen replizierten Ordner im Windows-Domänenumfeld ist das *SYSVOL-Verzeichnis*, das die Vorlagen für Gruppenrichtlinien und Anmeldeskripte beinhaltet. Es muss auf allen Domänencontrollern vollständig vorhanden sein, damit die Anmeldedienste konsistent arbeiten können. Deshalb war SYSVOL der erste vom Domänendienst automatisch eingerichtete replizierte Ordner.

Jedoch verlangte FRS einen höheren administrativen Aufwand und war fehleranfälliger als sein Nachfolger DFS-R. Auch wenn die Replikation des SYSVOL-Inhaltes mit der Verwendung von DFS-R noch warten musste, bis der Domänenlevel auf Windows Server 2008 umgestellt wurde, konnte für alle anderen Dateiverzeichnisse bereits ab Windows Server 2003 R2 die Replikationstechnik FRS durch DRS-R ersetzt werden.

Eine Migration muss immer manuell durchgeführt werden. Der FRS-Dienst kann noch bis Windows Server 2016 für bestehende Replikationen verwendet werden, wird aber seit Windows Server 2019 nicht mehr unterstützt.

FRS-Dienst und Windows Server 2019

Denken Sie daran, Ihre mit dem FRS-Dienst replizierten Dateninhalte (auch SYSVOL!) auf die DFS-R-Technik zu migrieren, bevor Sie Windows Server 2019 einsetzen.

Nun stellt sich die Frage, was die beiden Rollen *DFS-Namespaces* und *DFS-Replikation* so verbindet, dass sie in derselben Verwaltungskonsole auftauchen.

Technisch gesehen, verbindet sie gar nichts. Wie bereits erwähnt, handelt es sich um komplett eigenständige, voneinander unabhängige Technologien. Allerdings können die beiden Techniken kombiniert eingesetzt werden. Das bedeutet, dass Sie einen freigegebenen Ordner, der logisch mit einem DFS-Namespace verbunden und für die Benutzer somit veröffentlicht wurde, zusätzlich dazu noch mit DFS-Replikation auf verschiedene Server kopieren können. Damit erreichen Sie, dass Ihre Anwender an Standort A an der gleichen Stelle im DFS-Namespace-Verzeichnisbaum die augenscheinlich gleichen Daten sehen wie die Anwender in Standort B. Beide Anwender werden über den DFS-Namespace jeweils mit einem

lokal replizierten Datenbereich verbunden, dessen Inhalt durch DFS-Replikation identisch gehalten werden könnte.

Falls Sie planen, diese Technik einzusetzen, müssen Sie bedenken, dass es sich dabei nicht um eine Echtzeit-Replikation handelt: Änderungen an replizierten Daten werden erst nach dem Schließen einer Datei vom DFS-R-Dienst übertragen. Sollte eine replizierte Datei unschönerweise zur gleichen Zeit an ihren verschiedenen Orten modifiziert werden, wird der DFS-Dienst für eine Lösung dieses Replikationsproblems sorgen: Die Änderungen an einer der beiden Dateien werden verloren gehen. Im besten Fall wird die Datei, die gelöscht wird, in einen separaten Speicherbereich verschoben; im schlechtesten Fall werden die Änderungen einfach überschrieben. Welcher Fall eintrifft, hängt von der Konfiguration der Replikationszeitpläne ab. Diese Technik ist, wie Sie erkennen, nicht für den Echtzeit-Zugriff an verschiedenen Lokationen gedacht, sondern eher um Datensammlungen (z. B. für Datensicherungen) oder die Datenverteilung (z. B. zur Erstellung von verteilten Vorlagenverzeichnissen) zu ermöglichen.

Die Installation dieser Rolle erfordert keinen Neustart. Wollen Sie die Rolle entfernen, müssen Sie vorher alle DFS-Replikationsgruppen entfernen.

SYSVOL

Sollten Sie die Rolle auf einem Domänencontroller installiert haben und anschließend wieder entfernen wollen, ist dies nicht mehr möglich. Der Inhalt des auf einem Domänencontroller freigegebenen Verzeichnisses *SYSVOL*, das relevante Daten für den Domänenbetrieb beinhaltet, wird zwischen Domänencontrollern mit dieser DFS-R-Technik repliziert. Diese systemrelevante Replikationsgruppe kann nicht entfernt werden und somit auch die DFS-R-Rolle nicht mehr.

Trotzdem gilt: Wenn ein Domänencontroller aufgesetzt wird, arbeitet das System für die Replikation der SYSVOL-Dateien mit dem DFS-R-Dienst, auch wenn die eigentliche Rolle *DFS-Replikation* nicht aktiviert wurde bzw. als installiert dargestellt wird.

Der *iSCSI-Zielserver* ist die nächste Rolle in der Liste der Datei- und iSCSI-Dienste. Sie stellt Dienste und Verwaltungstools für iSCSI-Ziele bereit.

Die Installation der Rolle benötigt keinen Neustart, die Deinstallation allerdings schon.

Die Rolle *iSCSI-Zielspeicheranbieter* ermöglicht es Anwendungen, die mit einem iSCSI-Ziel verbunden sind, Volumenschattenkopien von Daten auf virtuellen iSCSI-Datenträgern zu erstellen. Darüber hinaus bietet Sie Ihnen die Möglichkeit, virtuelle iSCSI-Datenträger mit älteren Anwendungen zu verwalten, die einen *VDS-Hardwareanbieter (Virtual Disk Service)* erfordern (z. B. der Befehl `Diskraid`).

Für diese iSCSI-Komponente ist weder nach der Installation noch nach dem Entfernen ein Neustart erforderlich.

Die Installation der nächsten Rolle, des *Ressource-Manager für Dateiserver*, unterstützt Sie bei der Verwaltung von Dateien und Ordnern auf Ihrem Dateiserver. Außerdem können mit ihr Berichte erstellt werden, die Ihnen helfen, Ihren Dateiserver zu verstehen. Mit dieser Rolle können Sie Folgendes tun:

- Dateiverwaltungsaufgaben und Speicherberichte planen
- Dateien und Ordner klassifizieren
- Ordnerkontingente konfigurieren
- Dateiprüfungsrichtlinien definieren

Während der Installation dieser Rolle wird Ihnen angeboten, auch die Verwaltungskonsole aus den Features *Rollenverwaltungstools* dafür hinzuzufügen.

Die letzte der gelisteten Rollen im Bereich DATEI- UND ISCSI-DIENSTE ist die Rolle *Server für NFS*. Diese Funktion ermöglicht es dem Server, Dateien für UNIX-basierte Computer und andere Computer freizugeben, die das Protokoll *NFS* (*Network File System*) verwenden.

Die Aktivierung dieser Rolle fügt während der Installation automatisch noch das benötigte Administrations-Tool *Dienste für das Netzwerkdateisystem* hinzu. Dieses Tool ist nach Abschluss der Installation als Konsole DIENSTE FÜR NFS verfügbar. Nach dem Start zeigt es Ihnen eine Übersicht und eine Checkliste zum Einrichten für NFS an, wie Sie in Abbildung 2.22 erkennen können.

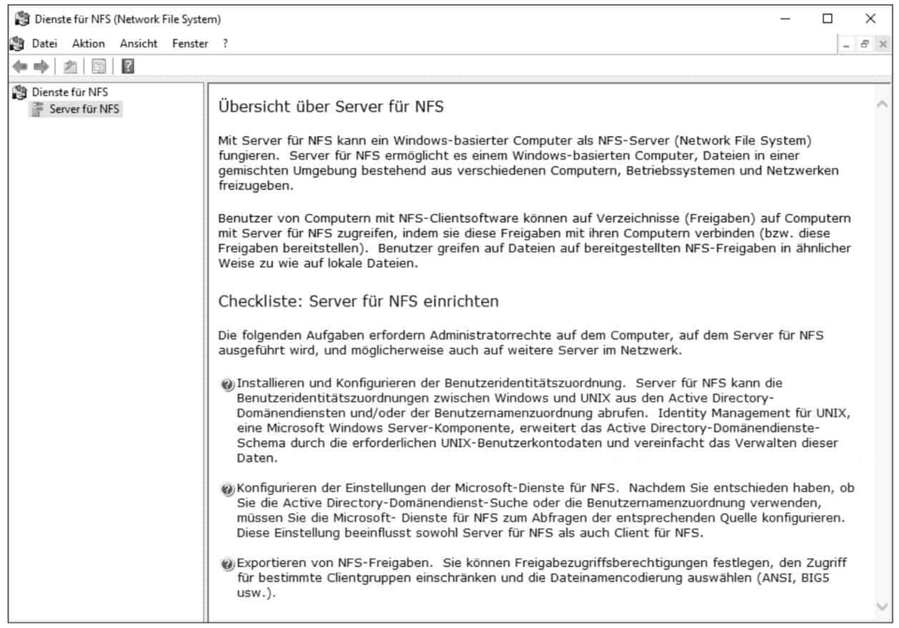


Abbildung 2.22 Dienste für NFS – Verwaltungskonsole

Die Installation der Rolle erfordert keinen Neustart. Wenn Sie die Rolle wieder entfernen, müssen Sie den Server neu starten.

Die am Ende gelisteten, bereits installierten *Speicherdienste* sind von Beginn an aktiviert, weil sie zum Betrieb des Betriebssystems benötigt werden. Sie bieten Speicherverwaltungsfunktionen und können nicht entfernt werden.

2.2.7 Device Health Attestation

Die Rolle *Device Health Attestation (DHA Service)* wurde mit Windows Server 2016 eingeführt. Sie ermöglicht Ihnen die Verwaltung von Geräten (die mindestens unter Windows 10 laufen müssen) in Ihrem Unternehmen durch den Integritätsnachweisdienst für Windows-Clients. Wird sie eingesetzt, können Sie die Integrität von Geräten überprüfen und administrieren, die *Trusted Platform Module (TPM)* 1.2 oder 2.0 unterstützen. Ein Beispiel für den Einsatz ist die Überprüfung, ob auf allen verwalteten Geräten die BitLocker-Funktion aktiviert ist.

Dieser Dienst empfängt Werte und Messungen von diversen Sicherheitsparametern der Clients (den Status von »Sicherer Start« oder einer aktivierten BitLocker-Festplattenverschlüsselung), die von TPM gemessen und signiert werden, und gibt daraufhin eine Bestätigung über den nachgewiesenen Integritätsstatus des Clients zurück. Der Client übergibt diese Bestätigung dann an eine Auswertungsinstanz wie die *MDM-Software* (*Mobile Device Management*), um die Geräteintegrität für Szenarien wie den bedingten Zugriff auf Unternehmensressourcen auszuwerten.

Wenn die Rolle installiert ist, müssen Sie den Dienst initialisieren und konfigurieren. Anschließend müssen diverse Zertifikate für die Signierung und Verschlüsselung erstellt und festgelegt werden. Diese Konfiguration findet durch PowerShell-Befehle statt.

Wenn Sie diese Rolle installieren, werden Ihnen noch das Feature *.NET-Framework 4.7*, der Prozessaktivierungsdienst und Teile des Webservers IIS zur Installation angeboten. Weder die Installation noch die Deinstallation benötigt einen Neustart.

Abbildung 2.23 zeigt Ihnen die Installation der Rolle.

Hochverfügbarkeit

Um Hochverfügbarkeit sicherzustellen, ist es ratsam, mehrere Instanzen der Rolle DHA Service zu installieren.

Die Verwaltung über den Server-Manager finden Sie in Abbildung 2.24.

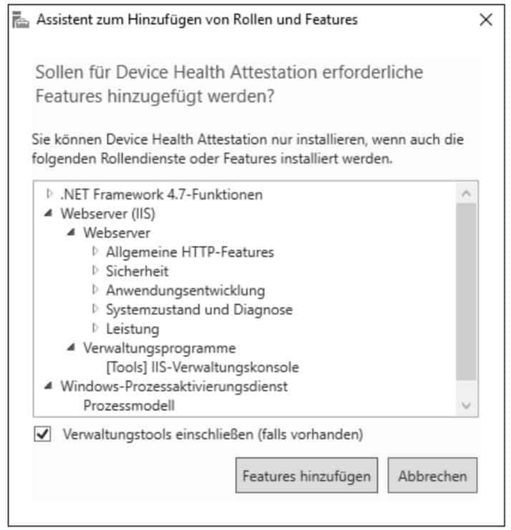


Abbildung 2.23 Installation der Rolle »DHA Service« und benötigte Features

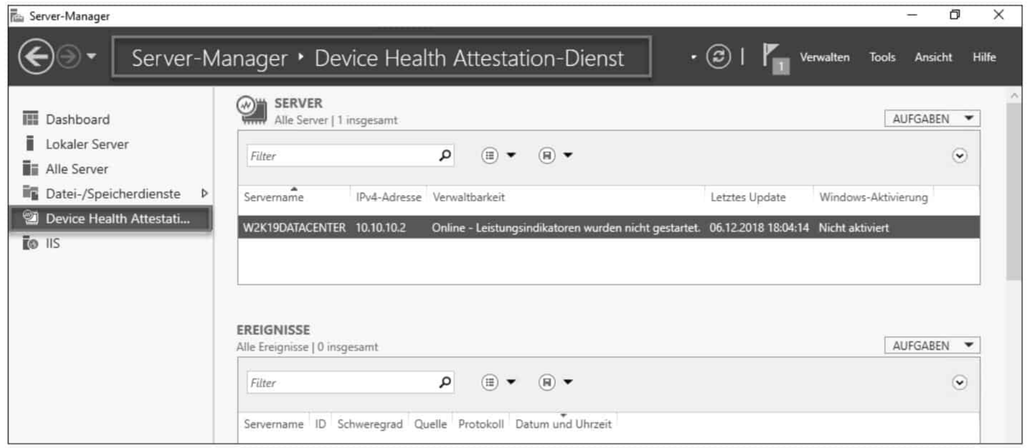


Abbildung 2.24 Verwaltungsoberfläche für »DHA Service« im Server-Manager

Um diesen Dienst zu installieren, müssen Sie Mitglied der lokalen Administratorgruppe sein. Nach der Installation muss der Dienst mithilfe der bereitgestellten PowerShell-Cmdlets wie in Abbildung 2.25 initialisiert und konfiguriert werden.

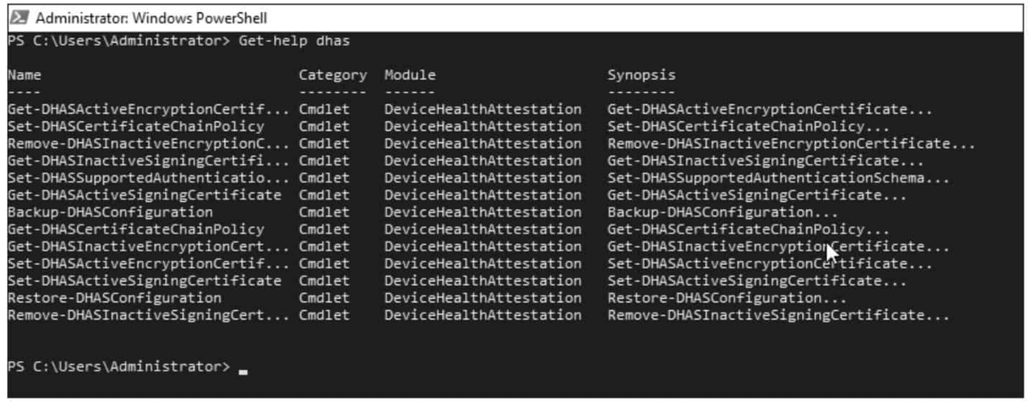


Abbildung 2.25 Cmdlets für das Modul Device Health Attestation

2.2.8 DHCP-Server

Möchten Sie mit Ihrem Server IP-Adressen in Ihrem Unternehmen zentral verwalten, bietet sich die Rolle des DHCP-Servers an. Der *Dynamic Host Configuration Protokoll*-Server ermöglicht die zentrale Konfiguration, Verwaltung und Bereitstellung von IPv4- und IPv6-Adressen und liefert darüber hinaus weitere Informationen wie DNS-Server-IP-Adressen, Router-Informationen, Zeitserver-Informationen und viele mehr, die über diesen Dienst an den Clientcomputer übergeben werden können. Das servergestützte Zuweisen von IP-Adressen an Clientcomputer oder TCP/IP-basierte Netzwerkgeräte wird auch *Leasen* genannt. Durch die Verwendung von IP-Adressen können Geräte Verbindungen zu anderen Netzwerkressourcen wie DNS-Servern und Routern herstellen.

Wird der Dienst installiert, wird auch das zugehörige Verwaltungstool *DHCP-Servertool* für die Installation vorgeschlagen, das Sie natürlich ebenfalls installieren sollten.

Nach Abschluss der Installation weist der Assistent darauf hin, dass der DHCP-Nachinstallationsassistent gestartet werden soll, um die DHCP-Konfiguration abzuschließen. Wird dieser Assistent ausgeführt, werden die benötigten Sicherheitsgruppen *DHCP-Administratoren* und *DHCP-Benutzer* angelegt. Danach muss der DHCP-Dienst neu gestartet werden, damit die Installation abgeschlossen wird.

Die Installation dieser Rolle benötigt keinen Neustart des Servers. Möchten Sie die Rolle entfernen, wird der Assistent Sie darauf hinweisen, dass dies ein wenig Zeit in Anspruch nehmen kann. Sie müssen den Server zum Abschluss der Deinstallation neu starten.

In der DHCP-Verwaltungskonsole können Sie nun alle gewünschten Konfigurationen zur IP-Adressverwaltung einstellen (siehe Abbildung 2.26).



Abbildung 2.26 Die DHCP-Verwaltungskonsole

Stellen Sie sicher, dass in der Netzwerkkonfiguration des DHCP-Servers eine feste IP-Adresse eingetragen wurde. Ist das nicht der Fall, startet der DHCP-Dienst nicht.

Um eine Infrastruktur aufzubauen, die sich gut verwalten lässt, sollten Sie die Subnetze, DHCP-Bereiche und gegebenenfalls Ausschlüsse für Ihr DHCP-Netz planen, bevor Sie es tatsächlich anlegen.

Wenn Ihr DHCP-Server Mitglied Ihrer Domäne ist, muss der DHCP-Server erst im Active Directory autorisiert werden, bevor er IP-Adressen an die Clients verteilen kann. Das verhindert, dass unbeabsichtigt mehrere Windows-DHCP-Server gleichzeitig IP-Adressen verteilen und es dadurch zu Netzwerk-Kommunikationsproblemen wegen doppelter IP-Adressvergabe kommt. Die Autorisierung eines DHCP-Servers kann nur ein Benutzer durchführen, der Mitglied der Gruppe der *Organisations-Admins* ist. Diese Aktion benötigt diese hohen Rechte, weil die Information der autorisierten DHCP-Server in einem Bereich der AD-Datenbank geschrieben wird, die unternehmensweit repliziert und verwendet werden kann.

2.2.9 DNS-Server

Um in einem Netzwerk Ressourcen über den Namen ansprechen zu können, müssen diese Namen in IP-Adressen aufgelöst werden. Dazu benötigen Sie einen Namensauflösungsdienst. Wird die Rolle des DNS-Servers installiert, kann der Server diese Aufgabe übernehmen. Für eine Active Directory-Domäne ist ein DNS-Server zwingend erforderlich. Sollten Sie sich dazu entschließen, die DNS-Daten AD-integriert abzuspeichern, muss der DNS-Server auf dem Domänencontroller installiert werden. Während der Promotion eines Domänencontrollers werden Sie durch den Assistenten darauf hingewiesen, und die DNS-Rolle wird mitinstalliert, falls sie noch nicht vorhanden ist.

Um die Eindeutigkeit der verwendeten Namen im Netzwerk zu gewährleisten, stellt DNS einen hierarchischen Namensraum zur Verfügung. Eine mögliche Zusammenarbeit mit dem DHCP-Dienst nimmt Ihnen die Arbeit ab, dass beim Erstellen neuer Geräte deren Namen manuell eintragen werden müssen.

Abbildung 2.27 zeigt Ihnen die DNS-Management-Konsole.

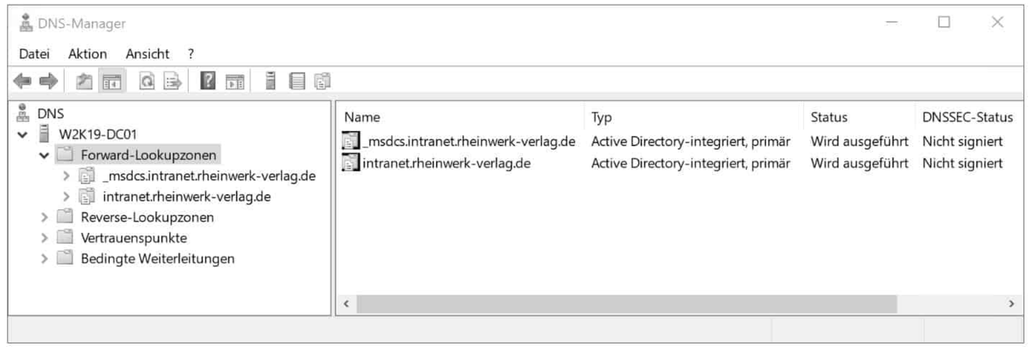


Abbildung 2.27 Die Management-Konsole für DNS

Sollte der DNS-Dienst auf dem Domänencontroller installiert worden sein, weil Sie sich für AD-integrierte Konfiguration entschieden haben, werden alle DNS-Zonen und deren Inhalte in der Active Directory-Verzeichnisdatenbank abgespeichert. Somit erreichen Sie durch die AD-Datenbank-Replikation über die Domänencontroller-Infrastruktur eine optimale Verteilung der DNS-Informationen für die Namensauflösung.

2.2.10 Druck- und Dokumentendienste

Mit der Installation der Druck- und Dokumentendienste entsteht die Grundlage für den Betrieb eines Druckservers. Wenn Sie diese Rolle auf einem Server aktivieren, können Sie damit die Verwaltungsaufgabe für den Netzwerk-Druck zentralisieren. Während der Rolleninstallation wird auch das Feature *Tools für Druck- und Dokumentenmanagementdienste* zur Installation vorgeschlagen. Für die Verwaltung sollten Sie diese Konsolen natürlich auch aktivieren.

Sobald Sie über den Server-Manager die Rolle zur Installation aktiviert haben, werden im Installationsassistenten die Rollendienste *Druckserver*, *Internetdrucken* und *LPD-Druck* hinzugefügt.

Der Rollendienst *Druckserver* enthält das *Druckverwaltungs-Snap-In*, mit dem Sie mehrere Drucker oder Druckerserver verwalten und Drucker von anderen oder auf andere Windows-Druckserver migrieren können. Dieser Rollendienst wird während der Rolleninstallation immer aktiviert. Die beiden folgenden Rollendienste können additiv hinzugefügt werden.

Mithilfe des zweiten Rollendienstes, *Internetdrucken*, wird für die Verwaltung von Druckaufträgen eine Webseite auf diesem Server bereitgestellt. Mithilfe der Webseite können die Benutzer die Druckaufträge dann verwalten. Darüber hinaus haben Benutzer mit installiertem Internetdruckclient die Möglichkeit, eine Verbindung mit freigegebenen Druckern des Servers herzustellen sowie auf diesen Druckern mithilfe eines Webbrowers zu drucken. Verwendet wird dazu das *Internet Printing Protocol (IPP)*.

Wird dieser Rollendienst während der Rolleninstallation ausgewählt, werden auch .NET 4.7-Funktionen und Teile des Webservers benötigt und ebenfalls installiert.

Der letzte Rollendienst, *LPD-Dienst*, wird benötigt, wenn UNIX-basierte Computer oder andere Computer, die den LPD-Dienst nutzen, auf freigegebenen Druckern auf diesem Server zugreifen wollen.

Wenn die Rolle installiert wurde, erscheint im Server-Manager ein neuer Einstiegspunkt für die Druckdienste (siehe Abbildung 2.28).

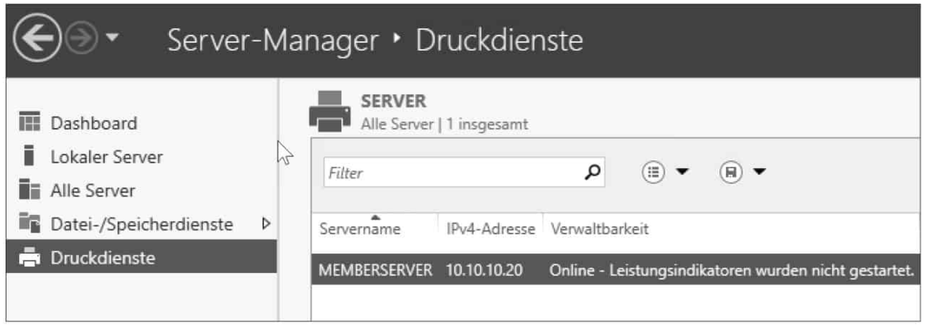


Abbildung 2.28 Der Menüpunkt »Druckdienste« im Server-Manager

Außerdem finden Sie unter TOOLS die Verwaltungsoberfläche für die Konfiguration (siehe Abbildung 2.29).



Abbildung 2.29 Druckverwaltung-Managementtool

Druckertreiber gibt es in verschiedenen Modellen bzw. Typen. Windows Server 2019 unterstützt die Druckwarteschlangen mit Druckertreibern des Typs 3 oder 4. Während der Installation wird ebenfalls darauf hingewiesen, dass es empfohlen ist, den Typ 4 zu verwenden. Mit diesem Typ können Benutzer, die nicht Mitglied der lokalen Admin-Gruppe sind, standardmäßig eine Verbindung mit dem Drucker herstellen.

Für den Betrieb dieser Rolle müssen signierte, paketierfähige Treiber verwendet werden, damit Clients eine Verbindung mit den freigegebenen Druckerwarteschlangen herstellen können, die den Druckertreiber des Typs 3 auf dem Druckerserver unterstützen. Falls keine signierten oder paketfähigen Treiber vorhanden sind, müssen Clientbenutzer entweder als lokaler Admin angemeldet sein oder Sie haben die Gruppenrichtlinien für *Computer\Administrative Vorlagen\Drucker\Point-and-Print-Einschränkungen* bereits für Sicherheitseingabeaufforderungen konfiguriert.

Zu guter Letzt wird noch darauf hingewiesen, dass für 32-Bit-Clients die 32-Bit-Versionen der Druckertreiber installiert sein müssen, falls Sie diese Technik einsetzen.

Die Installation und dieser Rolle und ihrer Rollendienste erfordert keinen Neustart. Falls Sie die Rolle und ihre Rollendienste entfernen, müssen Sie den Server neu starten.

2.2.11 Faxserver

Soll Ihr Server Faxe senden und empfangen können, müssen Sie die Rolle *Faxserver* installieren. Sie können damit zum Thema Fax außerdem Aufgaben definieren, Einstellungen setzen und ändern, Berichte erstellen oder die Faxgeräte in Ihrem Netzwerk verwalten. Ein Faxserver dient dazu, Faxressourcen im Netzwerk an einer zentralen Stelle freizugeben und auch dort zu verwalten. Während der Konfiguration des Faxservers können Sie auch Routingrichtlinien und Faxregeln definieren, die Verwaltung des Zugriffs auf gesendete oder empfangene Faxe steuern, und die Aktivitäten protokollieren, um die Nutzung der Faxressourcen nachzuverfolgen. Der Faxdienst-Manager stellt die Oberfläche und die Werkzeuge bereit, mit denen die Faxgeräte installiert, angezeigt und verwaltet werden können.

Wird diese Rolle über den Server-Manager aktiviert, weist der Assistent Sie darauf hin, dass der Rollendienst *Druckserver* aus der Rolle *Druck- und Dateidienste* ebenfalls benötigt wird. Für die Verarbeitung der Faxe wird die Technologie des Druck-Spoolers verwendet. Deshalb wird dieser Rollendienst ebenfalls benötigt.

Den Faxdienst-Manager und die Konfigurationsmöglichkeiten der Faxdienste sehen Sie in Abbildung 2.30 und Abbildung 2.31.

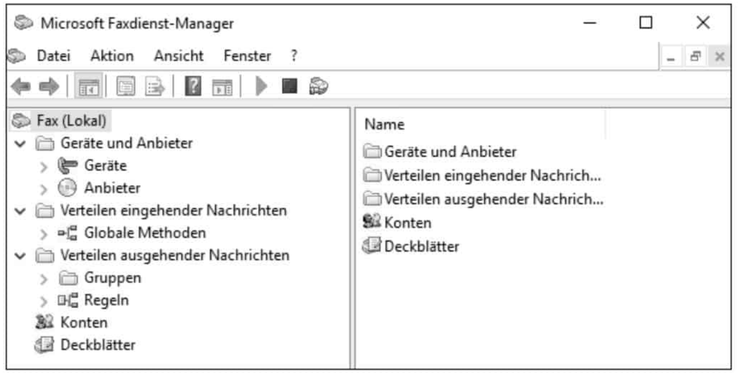


Abbildung 2.30 Der Microsoft Faxdienst-Manager nach der Installation der Rolle »Faxdienste«

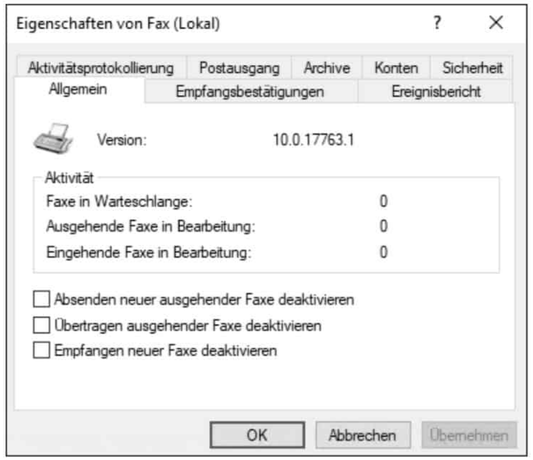


Abbildung 2.31 Konfigurationsmöglichkeiten der Faxdienste über die »Eigenschaften«-Seite

Die Installation der Rolle und des zusätzlich benötigten Druck-Rollendienstes erfordert keinen Neustart. Allerdings ist nach der Rolleninstallation die Konfiguration erforderlich. Darauf weist der Installationsassistent Sie hin. Nach der Auswahl des Konfigurationshinweises öffnet sich die Konsole FAXDIENST-MANAGER, über die alle Einstellungen gesetzt werden können, wie Sie in Abbildung 2.30 erkennen können.

Möchten Sie den Faxserver wieder entfernen, wird nicht automatisch auch der Rollendienst *Druckserver* mit entfernt. Dies muss manuell ausgewählt und sollte nicht vergessen werden, da der Rollendienst sonst unnötig weiter auf dem Server ausgeführt wird. Nachdem der Assistent die Rollen entfernt hat, muss der Server neu gestartet werden.

2.2.12 Host Guardian-Dienst

Der *Host Guardian-Dienst (HGS)* stellt Nachweis- und Schlüsselschutzdienste bereit, die die Ausführung abgeschirmter virtueller Computer auf *Guarded Hosts* ermöglichen, also auf überwachten Hostmaschinen. Der Nachweisdienst, der mit dieser Rolle installiert wird, überprüft die Identität und die Konfiguration der Guarded Hosts. Vereinfacht gesagt, können Sie durch HGS erreichen, dass Ihre virtuellen Maschinen so abgeschirmt betrieben werden, dass sie vor dem Zugriff durch Hyper-V-Administratoren geschützt sind.

Wenn Sie diese Rolle über den Assistenten aktivieren, wird eine große Anzahl an weiteren Rollen und Features aufgelistet, die ebenfalls benötigt werden. Dazu zählen das .NET Framework, der Active Directory-Domänendienst, das Failoverclustering, Teile des Webservers IIS und der Windows-Prozessaktivierungsdienst. Darüber hinaus wird noch eine ganze Handvoll Verwaltungsoberflächen für die genannten Rollen aktiviert.

Das automatische Hinzufügen der AD DS-Rolle macht deutlich, dass der Server, der die HGS-Rolle ausführen wird, einen neuen eigenen AD-Forest erstellt. Zum Installieren dieser Rolle benötigen Sie lokale administrative Rechte auf dem Server. Da allerdings aus diesem Server der Domänencontroller des neuen Forests entstehen muss, wofür Sie ebenfalls die benötigten Rechte besitzen müssen, handelt es sich somit bei lokalen administrativen Rechten um AD-Gesamtstruktur-Admin-Rechte. Sie können sich während der Konfiguration entscheiden, ob Sie für die HGS-Umgebung eine eigene AD-Gesamtstruktur aufbauen wollen (was der Empfehlung entspricht) oder ob Sie sich Ihrer bestehenden anschließen. Je nach Entscheidung sind administrative Domänenrechte in der vorhandenen oder der neuen AD-Gesamtstruktur erforderlich.

Die zweite Besonderheit ist hier, dass der Server ebenfalls Teil eines Failover-Clusters wird. Wichtig ist, dass der Failover-Dienst niemals den Domänendienst betreffen wird, sondern in diesem Fall ausschließlich die HGS-Dienste. Domänendienste sind Multimaster-Dienste und werden niemals geclustert.

Damit abgeschirmte virtuelle Computer bei einem Serverausfall auf Guarded Hosts ausgeführt werden können, müssen Sie mindestens drei Instanzen der Serverrolle des Host Guardian-Diensts installieren. Zu guter Letzt ist noch zu beachten, dass der Server bei der Rolleninstallation automatisch mit dem Profil Minimale Administration konfiguriert und bei vordefinierten Active Directory-Benutzergruppen registriert wird.

Die Konfiguration des HGS findet hauptsächlich über die PowerShell statt.

Diese Rolle gibt es seit Windows Server 2016, aber mit Windows Server 2019 wurden einige Features verbessert:

- *Host Key Attestation* ist der neueste Bescheinigungsmodus, der die Ausführung abgeschirmter VMs vereinfacht, wenn für Ihre Hyper-V-Hosts keine TPM-2.0-Geräte für die TPM-Attestierung verfügbar sind. Host Key Attestation verwendet Schlüsselpaare, um Hosts mit HGS zu authentifizieren. Dadurch müssen Hosts keiner Active Directory-Domäne beitreten, die AD-Vertrauensstellung zwischen HGS und der Unternehmensstruktur wird aufgehoben und die Anzahl der offenen Firewall-Ports reduziert. Die Hostschlüssel-Attestierung ersetzt die Active Directory-Attestierung, die in Windows Server 2019 nicht mehr unterstützt wird.
- *V2-Attestierungsversion* – Um die Host-Key-Attestierung und neue Funktionen in Zukunft zu unterstützen, wurde die Versionierung von HGS eingeführt. Eine Neuinstallation von HGS unter Windows Server 2019 führt dazu, dass der Server die Attestierung der Version 2 verwendet. Dies bedeutet, dass sowohl die Host-Key-Attestierung für Windows Server 2019-Hosts als auch weiterhin die Hosts der Version 1 unter Windows Server 2016 unterstützt werden können. In-Place-Upgrades bis 2019 erhalten Version 1, bis Sie manuell Version 2 aktivieren. Die meisten PowerShell-Cmdlets verfügen jetzt über einen Parameter `-HgsVersion`, mit dem Sie angeben können, ob Sie mit älteren oder modernen Attestierungsrichtlinien arbeiten möchten.
- *Unterstützung für geschirmte Linux-VMs* – Hyper-V-Hosts unter Windows Server 2019 können geschirmte Linux-VMs ausführen. Während es seit Windows Server 1709 geschützte VMs gibt, ist Windows Server 2019 die erste Version des Long-Term-Service-Channels, die sie unterstützt.
- *Verbesserungen in Zweigstellen* – Die Ausführung von abgeschirmten VMs in Zweigstellen mit Unterstützung für abgeschirmte Offline-VMs und Fallback-Konfigurationen auf Hyper-V-Hosts wurde vereinfacht.
- *TPM-Hostbindung* – Für sicherste Workloads, für die eine abgeschirmte VM nur auf dem ersten Host ausgeführt werden soll, auf dem sie erstellt wurde, aber auf keinem anderen, können Sie die VM jetzt mithilfe des TPM des Hosts an diesen Host binden.

Nach der Installation der Rolle *HGS* und der Konfiguration aller zusätzlichen Dienste und Features sind mehrere Neustarts notwendig – der erste gleich nach der Rolleninstallation. Sollten Sie die Rolle wieder entfernen, müssen Sie auch hier alle Komponenten manuell auswählen, die entfernt werden sollen. Danach ist ein Neustart erforderlich.

2.2.13 Hyper-V

Wenn Sie planen, virtuelle Maschinen auf Ihrem Server zu betreiben, dann ist die Rolle *Hyper-V* die richtige Wahl. Diese Rolle stellt Dienste bereit, die Sie zum Erstellen und Verwalten der virtuellen Maschinen und von deren Ressourcen verwenden können. Eine *virtuelle Maschine* ist ein Computersystem, das in einer isolierten Ausführungsumgebung betrieben wird. Dadurch können Sie gleichzeig mehrere Betriebssysteme auf einem physischen Server parallel betreiben. Diese Rolle kann nur auf einem physischen Server installiert werden. Versuchen Sie die Installation auf einer virtuellen Maschine, werden Sie scheitern, wie in Abbildung 2.32 zu erkennen ist. Eine Hyper-V-Infrastruktur für Virtualisierungen ist in einer bereits virtuellen Umgebung nicht möglich.

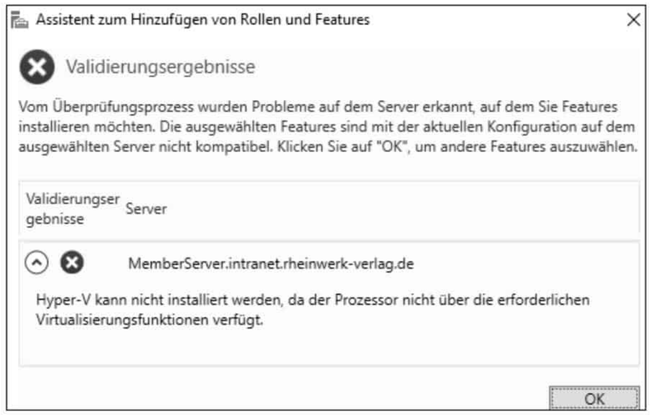


Abbildung 2.32 Die Rolle »Hyper-V« kann nur auf physischen Servern installiert werden.

Wenn Sie die Rolle im Installationsassistenten aktivieren, werden die Verwaltungstools vorgeschlagen, die Sie zur Installation benötigen. Installieren Sie diese ebenfalls.

Dem Thema Hyper-V ist ein eigenes Kapitel gewidmet, nämlich Kapitel 13.

2.2.14 Netzwerkcontroller

Die Rolle *Netzwerkcontroller* stellt eine hochgradig skalierbare und hochverfügbare Automatisierung bereit und ist nur in der *Datacenter-Edition* vorhanden. Sie ist innerhalb eines Rechenzentrums erforderlich, und zwar für die kontinuierliche Konfiguration, Überwachung und Diagnose von:

- virtuellen Netzwerken
- physischen Netzwerken
- Netzwerkdiensten
- Netzwerktopologien
- Adressverwaltung usw.

Mit dieser Rolle können Sie virtuelle Infrastrukturen, wie z. B. virtuelle Hyper-V-Switches programmieren und überwachen. Außerdem werden auch physische Infrastrukturen (wie Switches und Router) und Hardwarelösungen (wie Lastenausgleichmodule, dedizierte Firewalls und VPN-Server) für die Verwaltung eingebunden.

Während der Rolleninstallation wird die Verwaltungskonsole Network Controller Management ebenfalls für die Installation vorgeschlagen.

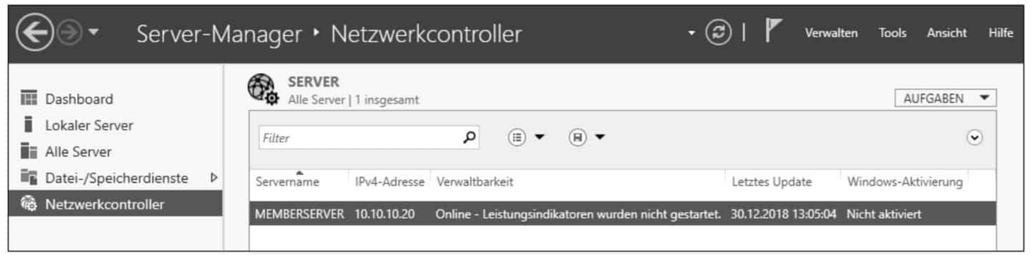


Abbildung 2.33 Server-Manager mit installierter Rolle »Netzwerkcontroller«

Die Rolle *Netzwerkcontroller* (siehe Abbildung 2.33) bietet die Möglichkeit, das von ihr gesteuerte Netzwerk mithilfe von Verwaltungs-Tools und anderen netzwerkfähigen Anwendungen wie dem *System Center Virtual Machine Manager (SCVMM)* und dem *System Center Operation Manager (SCOM)* zu verwalten.

Nach der Installation der Rolle muss der Server nicht neu gestartet werden. Nach der Deinstallation dieser Rolle fordert der Assistent allerdings einen Neustart.

2.2.15 Netzwerkrichtlinien- und Zugriffsdienste

Durch die Installation der Rolle *Netzwerkrichtlinien- und Zugriffsdienste* erstellen Sie auf Ihrem Windows Server 2019-Server einen *Netzwerkrichtlinienserver* (NPS), der die Sicherheit des Netzwerks gewährleisten wird. Mit Unterstützung dieser Dienste können Sie Richtlinien für den Netzwerkzugriff definieren. Außerdem ist es möglich, Richtlinien für die Authentifizierung und Autorisierung zu konfigurieren.

Nach der Installation finden Sie die Verwaltungskonsole Netzwerkrichtlinienserver im Menü Tools des Server-Managers (siehe Abbildung 2.34). Diese Verwaltungskonsole erklärt erste Schritte und hilft Ihnen bei der weiteren Konfiguration dieser Rolle und ihrer Möglichkeiten.

Sie können den NPS als RADIUS-Server und -Proxy bereitstellen. RADIUS steht für *Remote Authentication Dial-In User Service* und ermöglicht die Authentifizierung, Autorisierung sowie das Accounting für RADIUS-Clients. Dazu zählen allerdings keine Clientbetriebssysteme oder Laptops, sondern die Komponenten, die für die Einwahl zur Verfügung stehen. Dazu zählen WLAN-Geräte, Switches, DFÜ-Remotezugriffe und VPN-Server. Nachdem Sie den NPS mit diesem Assistenten installiert haben, können Sie ihn mit der NPS-Konsole über die Konsolen-Startseite konfigurieren.

Weder die Installation dieser Rolle noch die Deinstallation erfordert einen Neustart des Servers.

Mehr zum Thema RADIUS finden Sie in Kapitel 19, das die Einrichtung eines VPNs beschreibt.

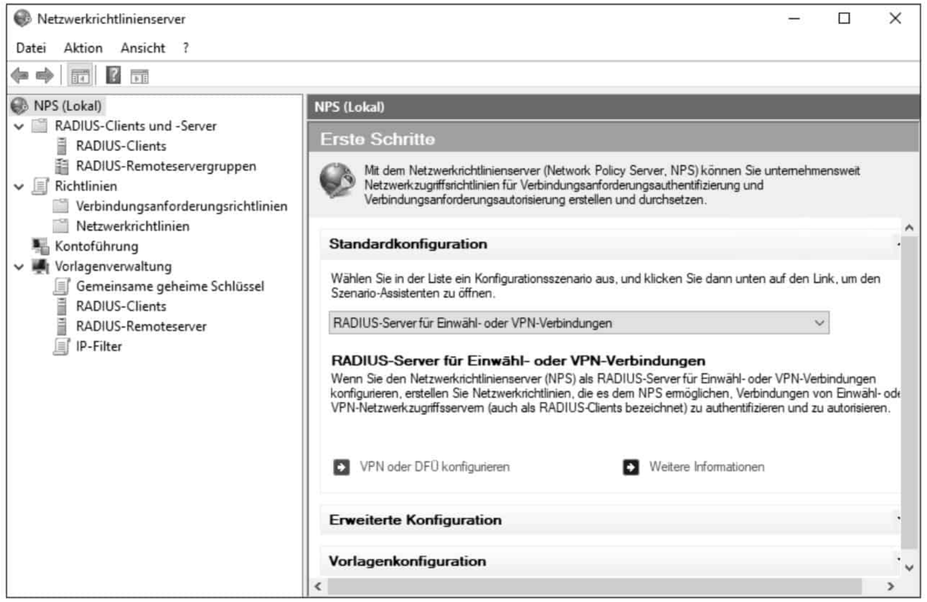


Abbildung 2.34 Verwaltungskonsole für »Netzwerkrichtlinien- und Zugriffsdienste«

2.2.16 Remotedesktopdienste

Wenn Sie Ihren Benutzern in Ihrer Infrastruktur den Zugriff auf virtuelle Desktops, sitzungsbasierte Desktops und RemoteApp-Programme ermöglichen möchten, müssen Sie die Rolle *Remotedesktopdienste* aktivieren. Mit dieser Technik können Sie eine auf virtuellen Computern basierende oder sitzungsbasierte Desktopbereitstellung konfigurieren. Die Aktivierung der Rolle im Installationsassistenten fügt die Auswahl der möglichen Rollendienste hinzu (siehe Abbildung 2.35).

In der Auswahl finden Sie folgende Remotedesktop-Rollendienste:

- *Remote Desktop Session Host* – Dieser Rollendienst ermöglicht es diesem Server, RemoteApp-Programme oder sitzungsbasierte Desktops bereitzustellen. Anwendungen werden auf dem Server ausgeführt.
- *Remotedesktopgateway* – Dieser Rollendienst ermöglicht es autorisierten Benutzern, eine Verbindung über das Internet mit virtuellen Desktops, RemoteApp-Programmen und sitzungsbasierten Desktops in Ihrem Unternehmensnetzwerk herzustellen.
- *Remotedesktoplizenzierung* – Mit diesem Rollendienst verwalten Sie Ihre Lizenzen, die erforderlich sind, um eine Verbindung mit einem Remotedesktop-Sitzungshostserver oder

einem virtuellen Desktop herstellen zu dürfen. Sie können damit Lizenzen installieren und ausstellen sowie ihre Verfügbarkeit nachverfolgen.

- *Remotedesktop-Verbindungsbroker* – Wenn Ihre Anwender Verbindungen zu vorhandenen virtuellen Desktops, Remote-App-Programmen und sitzungsbasierten Desktops herstellen können sollen, sollten Sie diesen Rollendienst installieren. Er stellt eine gleichmäßige Lastenverteilung zwischen den Remotedesktop-Sitzungshostservern in einer Sitzungssammlung oder zwischen den virtuellen Desktops einer virtuellen Desktopsammlung bereit, die in einem Pool zusammengefasst ist.
- *Remotedesktop-Virtualisierungshost* – Dieser Rollendienst ermöglicht es Ihren Anwendern, mithilfe von Remote-App- und Remotedesktop-Verbindungen Verbindungen mit virtuellen Desktops herzustellen. Die Anwendungen werden auf einem unter Hyper-V virtualisierten Client bereitgestellt.
- *Web Access für Remotedesktop* – Mit diesem Rollendienst wird es Ihren Anwendern ermöglicht, über das Startmenü oder einen Webbrowser auf RemoteApp- und andere Desktopverbindungen zuzugreifen. Das bietet Ihren Benutzern eine angepasste Ansicht von RemoteApp-Programmen, sitzungsbasierten Desktops und virtuellen Desktops.

Je nach Auswahl des Rollendienstes werden gegebenenfalls noch weitere Rollen aktiviert. So werden z. B. beim Remotedesktopgateway Teile der Rolle *Webserver IIS* und der Rolle *Netzwerkrichtlinienserver* aktiviert, bei der Rolle *Remotedesktop-Virtualisierungshost* kommen Hyper-V-Komponenten hinzu; andere Rollendienste wiederum benötigen keine gesonderte weitere Rollenaktivierung.

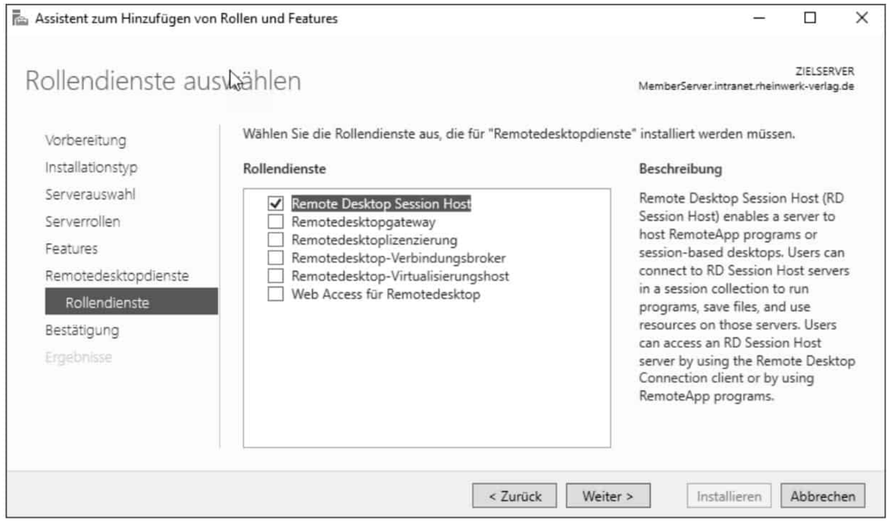


Abbildung 2.35 Rollendienst-Auswahl während der Installation der Remotedesktopdienste

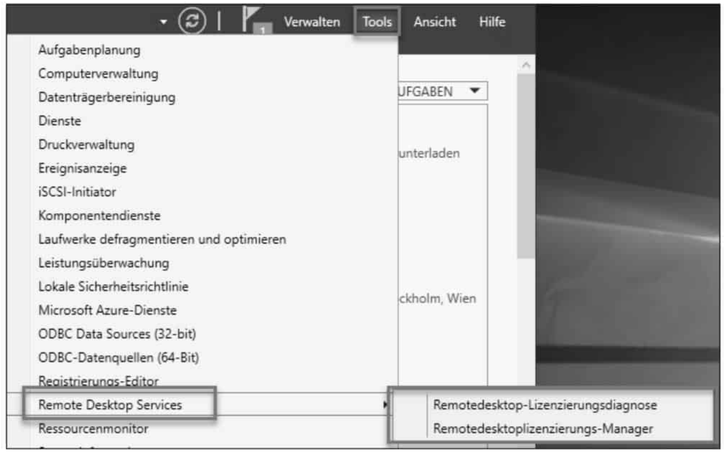


Abbildung 2.36 Verwaltungskonsolen für das Lizenzmanagement

Nach der Installation der Rolle finden Sie im Server-Manager unter TOOLS die Verwaltungskonsolen für das Lizenzmanagement für die REMOTE DESKTOP SERVICES (siehe Abbildung 2.36). Die Installation dieser Rolle und ihrer Rollendienste benötigt mindestens einen Neustart. Das Entfernen der verschiedenen Elemente erfordert meist einen Neustart.

Mehr zu diesem Thema erfahren Sie in Kapitel 18.

2.2.17 Remotezugriff

Die Rolle *Remotezugriff* stellt die Verbindungsmöglichkeit über *DirectAccess*, *VPN* und *Webanwendungsproxy* bereit. Wenn Sie diese Rolle auswählen, werden drei Rollendienste zur Aktivierung angeboten und anschließend in einer einzigen Verwaltungskonsole integriert verwaltbar gemacht.

Durch *DirectAccess (DA)* können Ihre verwalteten Domänencomputer als DA-Clients eine Verbindung mit Ihrem internen Netzwerk aufbauen. Die Konnektivität ist nahtlos, transparent und jederzeit verfügbar, sofern der jeweilige Client mit dem Internet verbunden ist. DA-Administratoren können Clients remote verwalten und so sicherstellen, dass mobile Computer stets über die neuesten Sicherheitsupdates verfügen und die Anforderungen ihres Unternehmens erfüllen. Mit *VPN* haben Sie die Möglichkeit, den Clientcomputern, die DA nicht unterstützen oder einer Arbeitsgruppe angehören (also nicht Ihrer Active Directory-Domäne), einen Remotezugriff auf Ihr Unternehmensnetzwerk über eine VPN-Verbindung zu ermöglichen.

Der zweite auswählbare Rollendienst ist *Routing*. Dieser bietet die Unterstützung für NAT-Router, LAN-Router mit BGP (*Border Gateway Protocol*), RIP (*Routing Information Protocol*) und multicastfähige Router, z. B. IGMP-Proxys (Internet Group Management Protocol).

Mit dem dritten Rollendienst, *Webanwendungsproxy*, können Sie ausgewählte HTTP- und HTTPS-basierte Anwendungen aus Ihrem internen Netzwerk für Clients extern veröffentlichen. Zum Veröffentlichen von internen Anwendungen (z. B. Webseiten, OWA) kann der Webanwendungsproxy als Reverse-Proxy verwendet werden. Mit AD FS können Sie Ihre Benutzer vor dem Zugriff darauf auch authentifizieren lassen.

Der RAS-Verbindungsmanager wird während der Installation hinzugefügt. Sie können die Routing- und RAS-Konfiguration über die Konsole ROUTING UND RAS bearbeiten, die Sie nach der Rolleninstallation unter TOOLS finden (siehe Abbildung 2.37).



Abbildung 2.37 Routing und RAS-Verwaltungskonsole für den Rollendienst »Routing«

Nach der Installation werden Sie noch im Installationsassistenten darauf hingewiesen, dass Sie den Remotezugriff konfigurieren müssen (siehe Abbildung 2.38). Es wird sogar ein Link zum Starten des Assistenten angeboten, was den Start des Assistenten erleichtert (siehe Abbildung 2.39).



Abbildung 2.38 Assistent zum Einrichten des Remotezugriffs

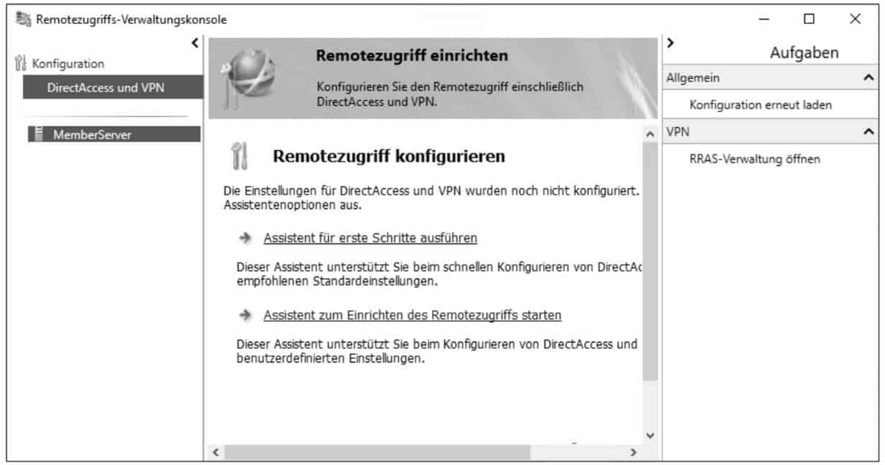


Abbildung 2.39 Die Verwaltungskonsole für den Remotezugriff

Die Installation erfordert keinen Neustart, aber nach der Rolleninstallation wird die Konfiguration des Remotezugriffs gefordert. Wenn Sie die Rolle wieder entfernen, müssen Sie die zusätzlichen Komponenten (wie Teile des Webservers IIS) ebenfalls manuell zum Entfernen aktivieren, sofern diese nicht mehr für anderen Aufgaben benötigt werden. Anschließend ist auch ein Neustart erforderlich. Mehr zu diesem Thema erfahren Sie in Kapitel 18.

2.2.18 Volumenaktivierungsdienste

Ein System, auf dem ein aktuelles Microsoft-Betriebssystem installiert ist, muss während der Installation oder in einem definierten Zeitraum nach der Installation mit einem gültigen Lizenzschlüssel aktiviert werden, damit es ohne Einschränkungen betrieben werden kann. Wenn Sie also ein System neu aufsetzen, ist das manuelle Eintragen des Schlüssels kein Problem. Verwalten Sie allerdings viele Maschinen, ist es sinnvoll, die Schlüsselverteilung zur Lizenzaktivierung Ihrer Systeme von einem Server übernehmen zu lassen.

Mit der Installation der Rolle *Volumenaktivierungsdienste* erschaffen Sie eine Umgebung in Ihrem Netzwerk, in der die Maschinen nicht mehr manuell aktiviert werden müssen. Damit können Sie die Verwaltung von KMS-Hostschlüsseln und der Infrastruktur der Volumenschlüsselaktivierung für ein Netzwerk automatisieren und vereinfachen. Mit diesem Dienst installieren und verwalten Sie einen *Schlüsselverwaltungsdienst-Host* (*Key Management Service, KMS*) oder konfigurieren die Microsoft Active Directory-basierte Aktivierung, um die Volumenaktivierung für Systeme bereitzustellen, die Mitglied Ihrer AD-Domäne sind. Ausführlichere Informationen dazu finden Sie in Kapitel 1.

Nach der Rolleninstallation startet der Assistent aus Abbildung 2.40, der Sie durch die Konfiguration führt.

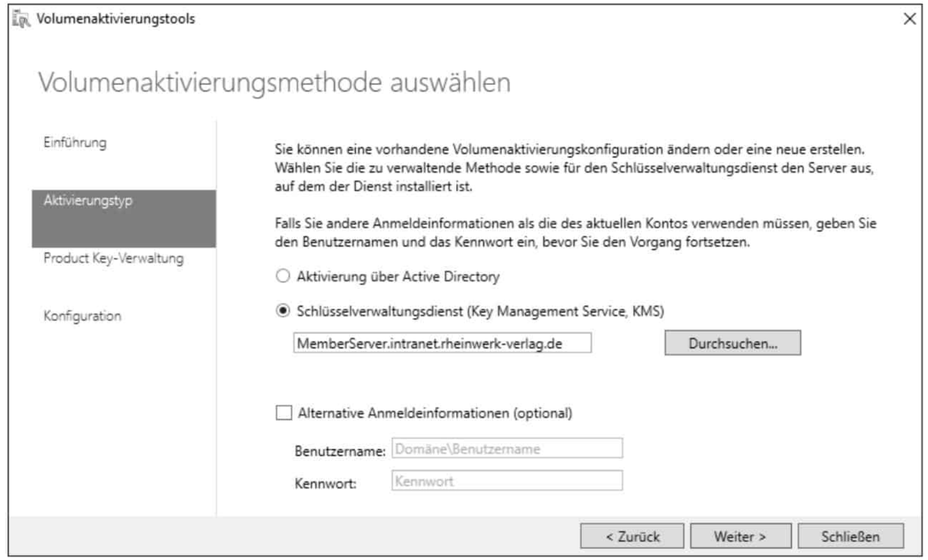


Abbildung 2.40 Der Assistent zum Konfigurieren eines KMS-Dienstes

Bevor Sie diese Rolle installieren, müssen Sie den richtigen Volumenaktivierungsschlüssel beschaffen, der zum Betrieb des KMS-Servers benötigt wird. Um diese Rolle zu installieren und zu aktivieren, müssen Sie Mitglied in der lokalen Administratorengruppe des Servers sein. Die Installation dieser Rolle erfordert keinen Neustart. Sie können die (nicht konfigurierte) Rolle auch wieder ohne Neustart entfernen.

2.2.19 Webserver (IIS)

Wenn Sie webseitenbasierte Informationen veröffentlichen möchten – z. B. im Internet, aber auch innerhalb Ihres Netzwerks im Intranet oder eventuell in einem Extranet –, dann benötigen Sie zum Bereitstellen dieser Inhalte einen Webserver. Mit der Installation der Rolle *Webserver (IIS)* wird Ihr Windows Server 2019 zum Webserver.

Die Rolle *Webserver (IIS)* umfasst die meisten hinzufügbaren Rollendienste. Passen Sie die vorausgewählten Features nicht an, beinhaltet die Standardinstallation alle Techniken, die zum Bereitstellen von statischen Inhalten benötigt werden, die Sie auch komprimieren können. Kleine Anpassungen können vorgenommen werden. Außerdem kann die Serveraktivität überwacht und protokolliert werden.

Da die Liste der möglichen Rollendienste und deren Erweiterungen so lang ist, hilft Ihnen die folgende Auflistung dabei, sich einen Überblick zu verschaffen. Um leichter zu erkennen, welche Vorauswahl bereits bei der Standardinstallation gesetzt ist (siehe auch Abbildung 2.41), wurden diese hier **fett** formatiert.

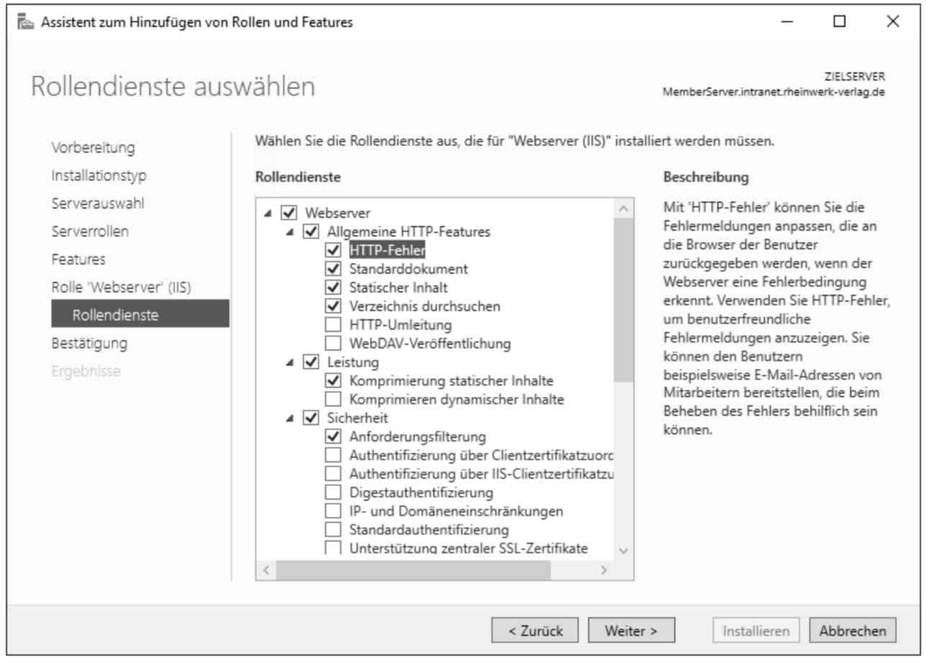


Abbildung 2.41 Auswahl der Rollendienste während der Konfiguration zur Webserver-Installation

Die Rolle *Webserver (IIS)* umfasst folgende Rollendienste:

- **Allgemeine HTTP-Features** – Unterstützung grundlegender HTTP-Funktionen, z. B. Bereitstellen von Standarddateiformaten und Konfigurieren von benutzerdefinierten Servereigenschaften. Sie können allgemeine HTTP-Funktionen verwenden, um benutzerdefinierte Fehlermeldungen zu erstellen, einige Anforderungen automatisch an einen anderen Speicherort weiterzuleiten oder um zu konfigurieren, wie der Server auf Anforderungen ohne Dokumentangabe reagieren soll.

  Untergeordnet ist folgende Auswahl möglich:

  - **HTTP-Fehler** – Erstellen benutzerfreundlicher Fehlermeldungen im Browser
  - **Standarddokument** – Konfiguration einer Standarddatei
  - **Statischer Inhalt** – Verwendung von statischen Webdateiformaten
  - **Verzeichnis durchsuchen** – Anzeigen von Inhalten auf dem Webserver
  - *HTTP-Umleitung* – Unterstützung beim Umleiten an ein neues Ziel (z. B. beim Umzug einer Webseite)

  - *WebDAV-Veröffentlichung* – WebDAV (*Web Distributed Authoring and Versioning*) ermöglicht das Veröffentlichen von Dateien von und auf einem Webserver mithilfe des HTTP-Protokolls.
- **Leistung** – stellt die Infrastruktur zur Zwischenspeicherung der Ausgaben bereit.
  - **Komprimierung statischer Inhalte**
  - *Komprimierung dynamischer Inhalte*
- **Sicherheit** – stellt die Infrastruktur zum Sichern des Webservers durch verschiedene Authentifizierungsmethoden bereit.
  - **Anforderungsfilterung** – Einsatz von Filtern, um bösartige Anforderungen zu erkennen
  - *Authentifizierung über Clientzertifikatzuordnung*
  - *Authentifizierung über IIS-Clientzertifikatzuordnung*
  - *Digestauthentifizierung* – Authentifizierung über den Domänencontroller mithilfe eines Kennwort-Hashs
  - *IP- und Domäneneinschränkungen* – Zulassen oder Ablehnen von Inhalten basierend auf IP-Quelladresse oder Quelldomänennamen
  - *Standardauthentifizierung* – gut geeignet für kleine Netze, starke Browserkompatibilität
  - *Unterstützung zentraler SSL-Zertifikate* – zentrale Verwaltung von SSL-Serverzertifikaten über eine Dateifreigabe
  - *URL-Autorisierung* – Zugriffseinschränkung auf Webinhalte mithilfe von Regeln, die an Benutzer, Gruppen oder HTTP-Headerverben gebunden werden
  - *Windows-Authentifizierung* – ermöglicht es in einer AD-Domäne, die Domänenifrastruktur zum Authentifizieren von Benutzern zu verwenden.
- **Systemzustand und Diagnose** – stellt eine Infrastruktur bereit, um Webserver, Websites und Anwendungen zu überwachen, zu verwalten und um Probleme mit der Integrität zu behandeln.
  - **HTTP-Protokollierung** – ermöglicht das Protokollieren der Websiteaktivität
  - *Ablaufverfolgung* – stellt Infrastruktur für Diagnose und Problembehandlung bereit.
  - *Anforderungsüberwachung* – stellt Infrastruktur zum Überwachen der Integrität bereit.
  - *Benutzerdefinierte Protokollierung* – unterstützt die Protokollierung mit eigens erstellten Modulen, die sich erheblich von den IIS-Protokollen unterscheiden.
  - *ODBC-Protokollierung* – unterstützt das Protokollieren der Webserveraktivitäten in eine ODBC-kompatible Datenbank.
  - *Protokollierungstools* – stellt eine Infrastruktur zum Verwalten von Webserverprotokollen und zum Automatisieren von allgemeinen Protokollierungsaufgaben bereit.

- *Anwendungsentwicklung* – Damit können Sie Webanwendungen entwickeln und hosten.

  Unter diesem Punkt werden folgende Optionen zur Aktivierung angeboten: *.NET-Erweiterbarkeit 3.5*, *.NET-Erweiterbarkeit 4.7*, *Anwendungsinitialisierung*, *ASP*, *ASP.NET 3.5*, *ASP.NET 4.7*, *CGI*, *ISAPI-Erweiterung*, *ISAPI-Filter*, *serverseitige Include-Dateien* und *WebSocket-Protokoll*.

Zusätzlich zur Webserver-Rolle und ihren soeben aufgezeigten Rollendiensten wird auch der FTP-Server mit den Rollendiensten *FTP-Dienst* und *FTP-Erweiterbarkeit* angeboten und wie bei anderen Rollen auch Teile der Verwaltungsprogramme, nämlich:

IIS-Verwaltungsprogramme

- IIS-Verwaltungsskripts und -tools
- Kompatibilität mit der IIS 6-Verwaltung
- IIS 6-Metabasiskompatibilität
- IIS 6-Skripttools
- IIS 6-Verwaltungskonsole
- Kompatibilität mit WMI für IIS 6
- Verwaltungsdienst

Die Installation der Rolle erfordert in ihrer Standardeinstellung keinen Neustart. Nach der Installation finden Sie unter TOOLS die Verwaltungsoberfläche INTERNETINFORMATIONSDIENSTE (IIS)-MANAGER, wie Sie in Abbildung 2.42 sehen können.

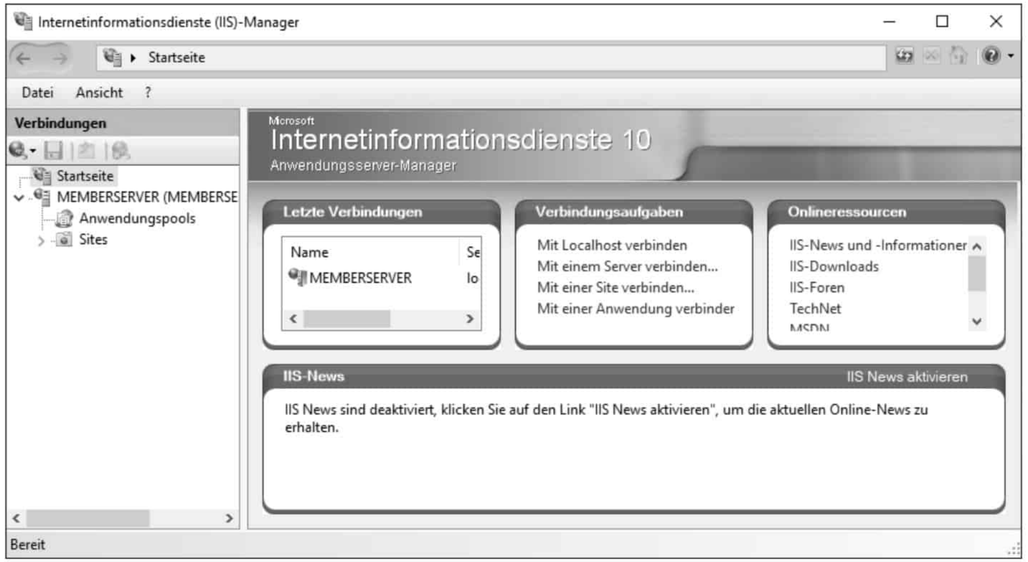


Abbildung 2.42 Verwaltungsoberfläche für den IIS

Beim Entfernen der Rolle müssen Sie den Server zum Abschluss neu starten.

Weitere Information zum Webserver finden Sie in Kapitel 15.

2.2.20 Windows Server Update Services (WSUS)

Die Rolle *Windows Server Update Services (WSUS)* für den Update-Service unterstützt Sie beim Laden, Prüfen, Sortieren und Verteilen von Microsoft-Updates auf die Maschinen in Ihrem Unternehmen.

Über die Verwaltungsoberfläche von WSUS können Sie Bereiche von Computern gruppieren, um Installationsphasen bestimmen zu können, z. B. anhand von Betriebssystemen oder für Pilotphasen. Außerdem unterstützt dieses Produkt Sie beim Erstellen von Berichten über den Paketierungsstatus der Computer und der zu installierenden Updates.

Wenn Sie diese Rolle auswählen, werden ebenfalls .NET-Framework 4.7-Funktionen installiert und Teile des Webservers mit aktiviert.

Die Rolle *WSUS* beinhaltet drei Rollendienste:

- *WID Connectivity* – installiert die von WSUS verwendete Datenbank in WID (*Windows Internal Database*).
- *WSUS Services* – beinhaltet alle verwendeten WSUS-Dienste: *Updatedienst*, *Berichtserstattungswebdienst*, *API-Remoting-Webdienst*, *Clientwebdienst*, *Webdienst für die einfache Webauthentifizierung*, *Serversynchronisierungsdienst* und *DSS-Authentifizierungswebdienst*.
- *SQL Server Connectivity* – Dieser Dienst kann optional gewählt werden und installiert dann die Funktionen, durch die die WSUS-Verbindung mit einer SQL-Server-Datenbank aktiviert wird.

Während der Installation der Rolle werden Sie darauf hingewiesen, dass Sie – je nach verfügbarem Plattenplatz auf dem WSUS-Server – die Updates lokal speichern können, um Ihren Clients eine rasche Installation anzubieten, oder dass die Clients ihre Updates bei Bedarf selbst vom Microsoft Update Server aus dem Internet herunterladen können (siehe Abbildung 2.43). Die Voraussetzungen zum Download sind mindestens 6 GB freier Speicherplatz und ein NTFS-formatiertes Laufwerk.

Den Speicherort für die Updates können Sie an dieser Stelle direkt während der Installation definieren. Diese Option kann auch deaktiviert werden, wie Sie in der Darstellung erkennen können. Wenn Sie den Haken entfernen, müssen Sie es Ihren Clients aber ermöglichen, den Windows Update Service zu erreichen, um eigenständig die benötigten Updates zu laden.

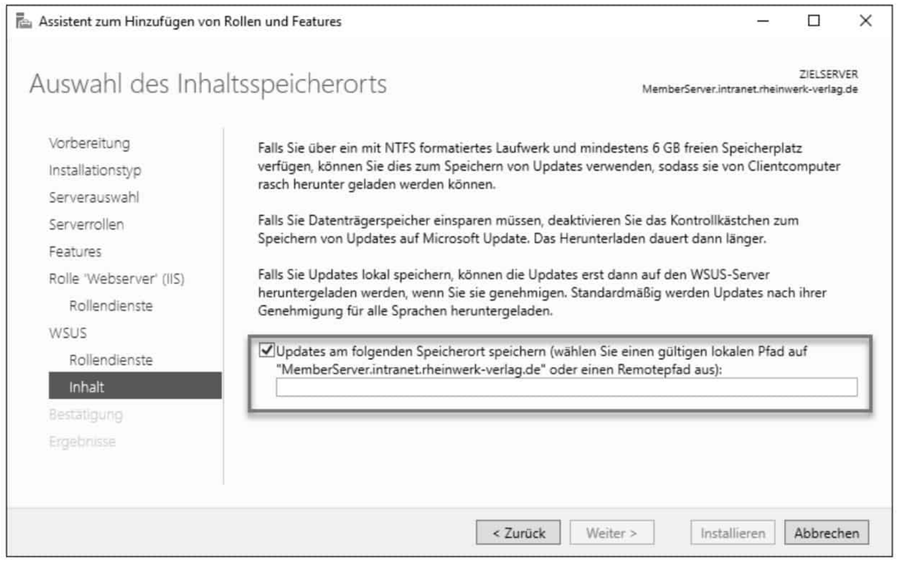


Abbildung 2.43 Rolleninstallation von WSUS – Auswahl des Inhaltsspeicherorts

Nach Abschluss der Rolleninstallation weist der Installationsassistent Sie darauf hin, dass der WSUS-Server konfiguriert werden muss, und bietet noch im Installationsfenster einen Link dafür an. Wenn Sie den Link anklicken, wird der Server im Hintergrund automatisch konfiguriert. Danach wird eine Abschlussmeldung wie in Abbildung 2.44 angezeigt.

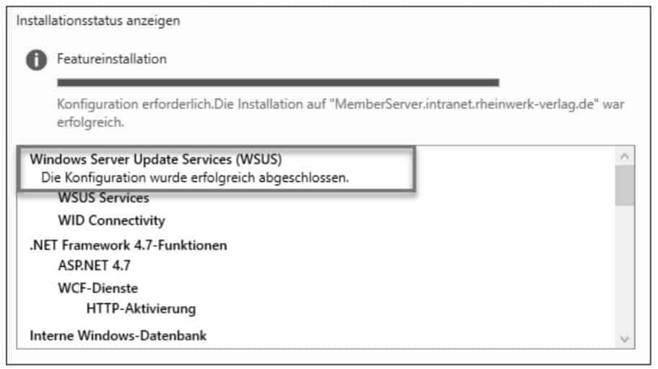


Abbildung 2.44 WSUS-Installation: Die Konfiguration wurde abgeschlossen.

Wenn Sie nun unter Tools erstmalig die Windows Server Update Service-Verwaltungsoberfläche öffnen, startet der Konfigurationsassistent aus Abbildung 2.45, der Ihnen bei allen notwendigen Schritten Unterstützung bietet.

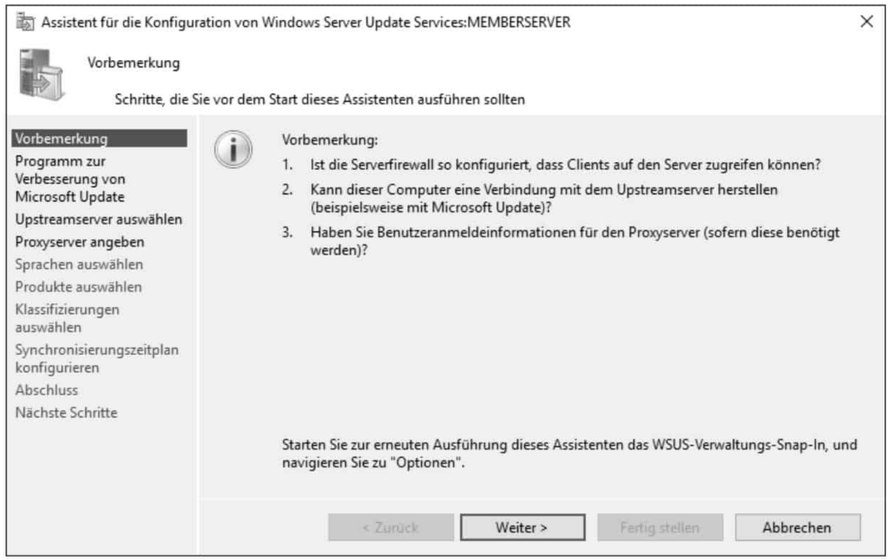


Abbildung 2.45 WSUS-Konfigurationsassistent

Haben Sie die Konfiguration abgeschlossen, können Sie Ihre Umgebung mit der Oberfläche aus Abbildung 2.46 verwalten.

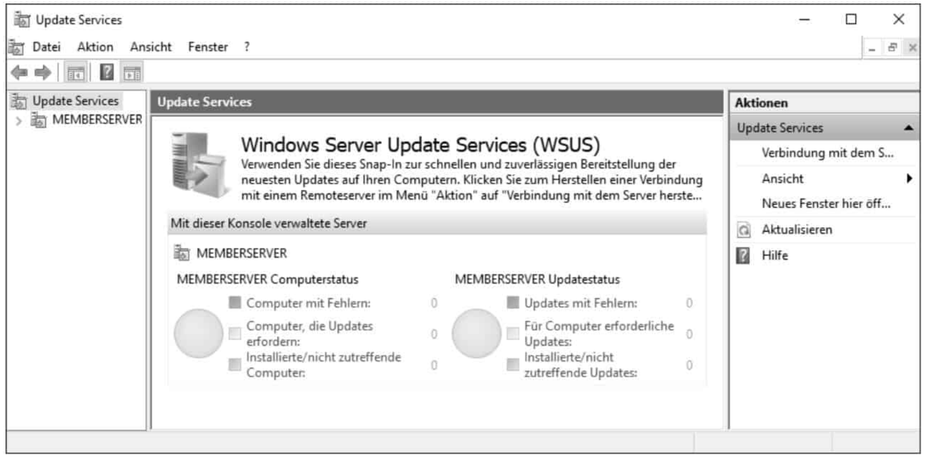


Abbildung 2.46 Verwaltungsoberfläche für WSUS

Mindestens ein WSUS-Server in Ihrer Umgebung muss in der Lage sein, die Updates über das Internet von Microsoft Update herunterzuladen. Ist das nicht der Fall, müssen Sie dafür sorgen, dass der Content anderweitig in Ihrer Umgebung bereitgestellt wird, zum Beispiel als

Offline-Inhalt auf einem Windows-Client. Sie müssen dann allerdings (manuell) dafür sorgen, dass der Offline-Inhalt immer die aktuellsten Updates enthält. Der Rest der WSUS-Server (sollten mehrere vorhanden sein) kann dann die Daten von dem ersten WSUS-Server beziehen oder aber auch direkt von der Microsoft-Update-Quelle. Die Kommunikationsverbindungen von WSUS-Servern untereinander oder von dem WSUS-Server und seinem Client sollten mithilfe von SSL (*Secure Socket Layer*) eingerichtet und abgesichert werden.

Nach der Rolleninstallation ist kein Neustart erforderlich. Wenn Sie WSUS wieder entfernen möchten, müssen Sie den Server anschließend neu starten.

Falls Sie einen WSUS-Server abbauen möchten, der in Betrieb war, denken Sie bitte daran, dass Sie neben dem Entfernen der Rolle auch andere Bereinigungen vornehmen müssen. Dazu zählen das Entfernen der zugehörigen SQL-Datenbank und der Update-Pakete sowie das Bereinigen der Gruppenrichtlinieneinstellungen.

WSUS beschreiben wir ausführlich in Kapitel 17.

2.2.21 Windows-Bereitstellungsdienste

Ganz unten in der Rollen-Liste steht noch die Rolle *Windows Deployment Services (WDS)*. Sie bietet eine vereinfachte und sichere Methode, um Windows-Betriebssysteme schnell und remote über Ihr Netzwerk für Ihre Windows-Maschinen bereitzustellen.

Sie können diese Rolle einsetzen, um auf PXE-fähigen Computern Betriebssysteme zu installieren und konfigurieren. *Preboot Execution Environment (PXE)* ist ein Verfahren, um netzwerkfähige Rechner von einem Server ausgehend über das Netzwerk starten zu können. Sollten Ihre Computer nicht PXE-fähig sein, kann auch *Windows PE* (die Windows-Vorinstallationsumgebung) unterstützend verwendet werden.

Die WDS-Rolle ersetzt die RIS-Dienste (*Remoteinstallationsdienste*). Die Verwaltung und Konfiguration findet über das für die Bereitstellungsdienste hinzugefügte MMC-Snap-In statt.

Während der Installation der Rolle werden die beiden Rollendienste *Bereitstellungsserver* und *Transportserver* installiert. Der *Bereitstellungsserver* bietet die vollständige Funktionalität der WDS, die Sie zum Konfigurieren und für die Remoteinstallation Ihrer Windows-Clients benötigen. Mit diesem Rollendienst können Sie Images erstellen und anpassen. Für die Bereitstellung dieser Images benötigen Sie den zweiten Rollendienst, den *Transportserver*. Er enthält die Kernnetzwerkbestandteile, die Sie zum Übertragen Ihrer Daten mithilfe von Multicast oder Unicast auf einem eigenständigen Server verwenden können.

Für den Einsatz von WDS müssen im Netzwerk auch ein DHCP-Server und ein DNS-Dienst vorhanden sein. Außerdem benötigen Sie für den Bereitstellungs- und den Transportserver NTFS-Partitionen für den Datenspeicher (siehe Abbildung 2.47).

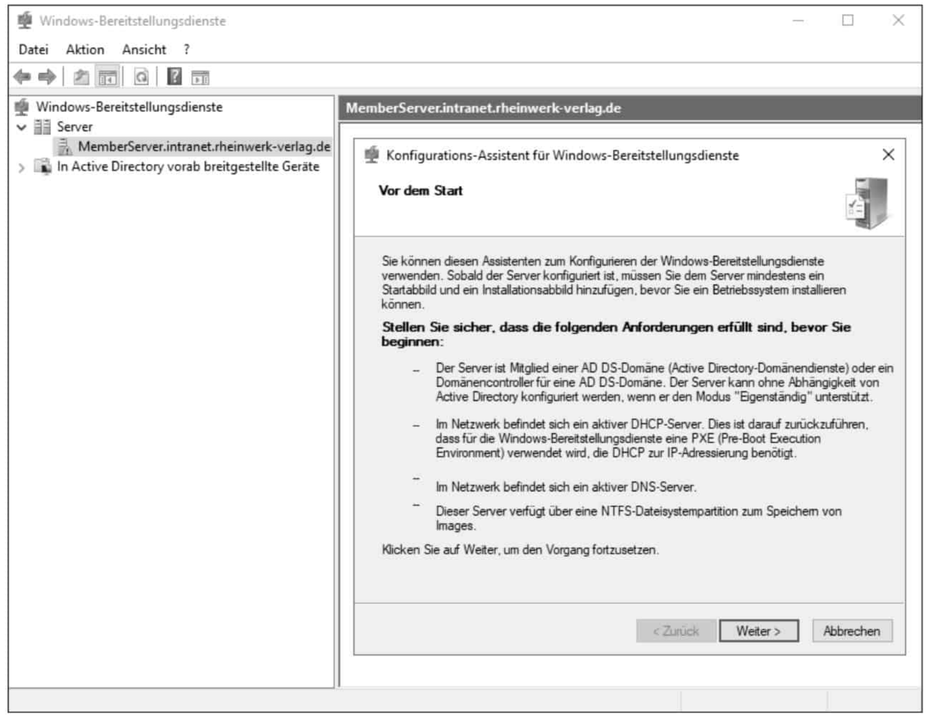


Abbildung 2.47 Das WDS-MMC-Snap-In mit gestartetem Konfigurationsassistenten

WDS muss vor der Bereitstellung durch die Ausführung des Konfigurationsassistenten oder mit dem Tool `WDSutil.exe` konfiguriert werden. Das Bereitstellen eines Startabbildes und eines Installationsabbildes ist ebenfalls erforderlich, bevor Sie starten können.

Ein *Startabbild* ist zum Beispiel *Windows PE*, also das Betriebssystem, mit dem Sie starten.

Ein *Installationsabbild* beinhaltet das Zielbetriebssystem mit den gewünschten Anwendungen und benötigten Treibern.

Weder für die Installation noch zum Entfernen der Rolle WDS muss der Server neu gestartet werden.

2.3 Features

Neben den Rollen und ihren Rollendiensten finden Sie noch die sogenannten *Features*. Microsoft unterscheidet somit zwischen den primären Funktionen (den Rollen) und Zusatzdiensten (den Features).

Features sind kleine, zum Teil eigenständige Funktionen und Bausteine, die den Server beim Ausführen seiner Aufgaben um weitere Möglichkeiten erweitern. Bei der Installation einer Rolle sorgt der Installationsassistent meist dafür, dass Features, die für den Betrieb einer Rolle unabdingbar sind, bereits vorgeschlagen und aktiviert werden. Hierauf weist der Assistent Sie hin und er zeigt die Auswahl an (siehe Abbildung 2.48).

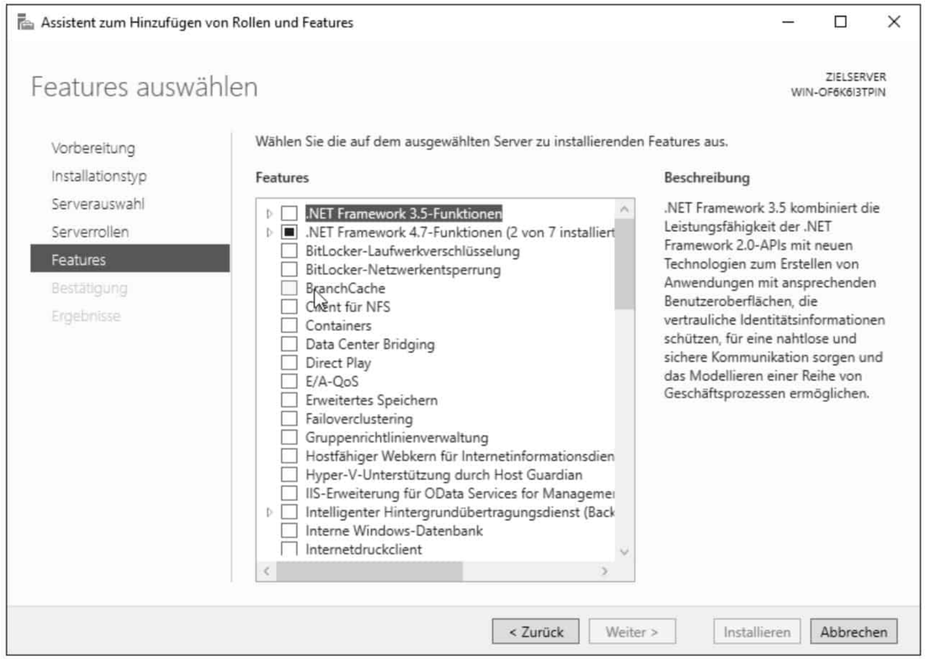


Abbildung 2.48 Der »Assistent zum Hinzufügen von Rollen und Features« – Features

Die vorhandenen 21 Rollen und ihre Rollendienste werden ergänzt durch über 80 Features, die wir Ihnen jetzt vorstellen.

.NET Framework 3.5-Funktionen

Dieses Feature erweitert die .NET Framework 2.0-APIs um neuere Technologien. Damit können Anwendungen mit ansprechenden Benutzeroberflächen erschaffen werden, die vertrauliche Identitätsinformationen schützen. Das dient zur nahtlosen und sicheren Kommunikation und kann zur Erstellung einer Reihe von Geschäftsprozessen verwendet werden.

.NET-Framework

Beachten Sie bei der Installation dieses Features, dass diese alten .NET-Framework-Dateien nicht mehr in den Quelldateien des Betriebssystems vorhanden sind.

Deshalb müssen Sie bei der Installation den Quellpfad der Dateien angeben (z. B. vom Installationsdatenträger im Verzeichnis *\Sources\SxS*). Der Server-Manager weist auf diesen Umstand während der Feature-Installation hin (siehe Abbildung 2.49 und Abbildung 2.50).

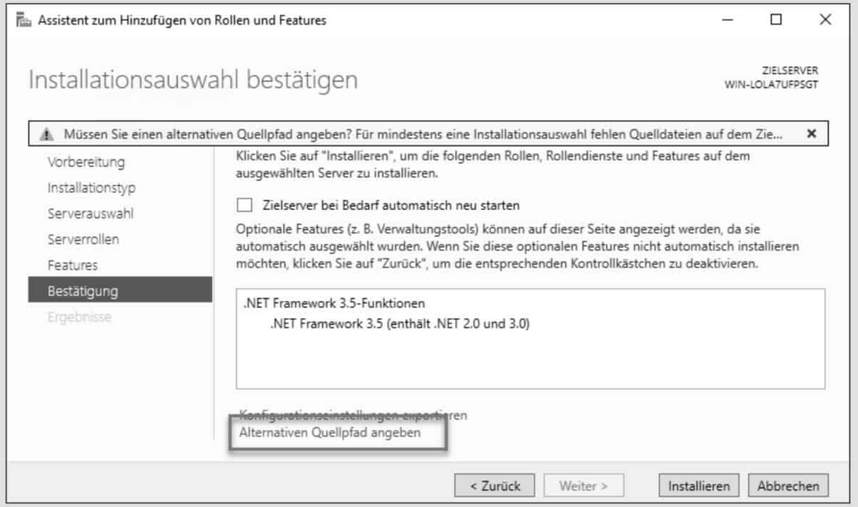


Abbildung 2.49 .NET Framework 3.5-Installation



Abbildung 2.50 .NET Framework 3.5-Installation – alternativen Quellpfad angeben

.NET Framework 4.7-Funktionen

Die Weiterentwicklung des .NET-Frameworks ist seit Windows Server 2012 im Einsatz. Sie bietet ein umfassendes und konsistentes Programmiermodell zum schnellen und einfachen Erstellen und Ausführen von Anwendungen für verschiedene Plattformen. Dazu zählen Desktop-PCs, Server, Smartphones und die öffentliche und private Cloud.

Dieses Feature ist bereits installiert. Es beinhaltet noch weitere, ungeordnete Features wie ASP.NET 4.7 und WCF-Dienste:

- *ASP.NET 4.7* wird für die Ausführung eigenständiger ASP.NET 4.7-Anwendungen benötigt sowie für Anwendungen, die in IIS integriert sind.
- Der Sammelpunkt *Windows Communication Foundation (WCF)-Dienste* ist untergliedert in *Pipe-Aktivierung*, *HTTP-Aktivierung*, *Message Queuing (MSMQ)-Aktivierung*, *TCP-Aktivierung* und in das vorinstallierte Feature *TCP-Portfreigabe*. Im Rahmen dieses Feature-Bundles wird der Windows-Prozessaktivierungsdienst genutzt, um Anwendungen mithilfe der genannten Protokolle über das Netzwerk aufzurufen. Dies ermöglicht Ihnen das dynamische Starten und Stoppen von Anwendungen als Reaktion auf eingehende Arbeitsaufgaben und somit ein stabiles, verwaltbares und effizientes Anwendungshosting.

BitLocker-Laufwerkverschlüsselung

Mit dem Feature *BitLocker-Laufwerkverschlüsselung* können Sie Ihre lokalen Festplatten verschlüsseln. Damit schützen Sie Ihre Daten gegen ungewollten Zugriff, falls sie verloren gehen, gestohlen werden oder unsachgemäß außer Dienst genommen werden. Einen Zugriff auf Daten, die sich auf verschlüsselten Platten befinden, erhalten Sie nur, wenn die Startkomponenten in Ihrem System erfolgreich überprüft wurden und sich das Laufwerk im originalen Computer befindet.

Diese Technik bietet an, nur benutzte Bereiche der Festplatte zu verschlüsseln. Kommen neue Daten hinzu, wird die Verschlüsselung dafür erweitert. Microsoft empfiehlt, die komplette Festplatte zu verschlüsseln. Für die Integritätsprüfung ist ein kompatibles *Trusted Platform Module* (TPM) erforderlich. Wenn Sie TPM nicht verwenden (können), haben Sie trotzdem die Möglichkeit, die Bitlocker-Verschlüsselung einzusetzen. Dazu benutzen Sie einen USB-Stick, auf den Sie den symmetrischen Schlüssel speichern. Der Stick muss dann beim Starten eingesteckt sein, sonst fährt die Maschine nicht hoch.

BitLocker-Netzwerkentsperrung

Die *BitLocker-Netzwerkentsperrung* ermöglicht es, dass die BitLocker-Schlüsselinformationen Ihrer Domänencomputer zentral im Active Directory gespeichert werden. Die Verwendung dieser netzwerkbasierten Schlüsselschutzvorrichtung zur automatischen Entsperrung eines mit BitLocker geschützten Betriebssystemlaufwerks eines Domänenrechners sorgt zum Beispiel dafür, dass Administratoren Wartungsarbeiten, die einen Neustart des Computers erfordern, auch außerhalb der regulären Arbeitszeit durchführen können.

BranchCache

Das Feature *BranchCache* installiert Dienste, die es Ihnen ermöglichen, bereits geladene Daten auf diesem Computer zu speichern, um diese Daten vor Ort den Benutzern von Windows 7-Clients (und neuer) schneller verfügbar zu machen, falls sich die Originaldaten auf einem zentralen Server an einer anderen Lokation befinden. Der Computer fungiert dann als gehosteter Cacheserver oder BranchCache-aktivierter Inhaltsserver.

Für die Bereitstellung muss dieser Computer dann als HTTP-Webserver oder BITS-basierter (*Background Intelligent Transfer Service* – intelligenter Hintergrundübertragungsdienst) Anwendungsserver konfiguriert werden. Um dieses Feature benutzen zu können, müssen Sie auch die zugehörige Serverrolle *Dateidienste* und die ihr untergeordnete Serverrolle *BranchCache für Netzwerkdateien* installieren. Mehr zum Thema finden Sie in Kapitel 14 über Dateidienste.

Client für NFS

Wenn Sie Dateien auf UNIX-basierten NFS-Servern hosten und diese für den Zugriff von diesem Computer freigeben möchten, benötigen Sie das Feature *Client für NFS*. Es ermöglicht Ihnen, dass eine Verbindung mit der UNIX-NFS-Freigabe hergestellt wird, bei der ein anonymer Zugriff akzeptiert wird.

Container

Das Feature *Container* stellt Dienste und Werkzeuge bereit, um *Windows Server Container* und ihre Ressourcen zu erstellen und zu verwalten.

Die auf *Server Core* basierenden Containerimages in Windows Server 2019 unterstützen Entwickler in der Modernisierung bestehender Anwendungen, die Container-Technologien verwenden. Diese Technik macht es möglich, das Image auf etwa ein Drittel seiner derzeitigen Größe zu reduzieren und damit die Downloadzeiten stark zu verringern. Mit Windows Server 2019 wird Ihnen auch ein neues Image namens *Windows* bereitgestellt. Im Vergleich zu den bereits bekannten Images *Nanoserver* und *WindowsServerCore* bietet das neue Image einen stark erweiterten Funktionsumfang, mit dem sich nahezu alle Windows-Programme nutzen lassen.

Windows Server 2019 unterstützt ebenfalls *Kubernetes*. Google Kubernetes ist Googles Open-Source-System zum Management von Linux-Containern über Privat-, Public- und Hybrid-Clouds. Damit lassen sich auch hybride Container-Umgebungen betreiben.

Mehr zu diesem Thema finden Sie in Kapitel 8.

Data Center Bridging

Durch die Installation des Features *Data Center Bridging* wird eine Auswahl von technischen Standardisierungen der IEEE aktiviert, die zur Verbesserung der Steuerung von großen Netz-

werken beitragen. Der Einsatz von hardware-basierter Bandbreitenzuweisung ist nur ein Vorteil. Unterstützt Ihr Netzwerk-Adapter CNA (*Converged Netwerk Adapter*), lassen sich auch Daten wie iSCSI und RDMA besser nutzen.

DirectPlay

Das Feature *DirectPlay* installiert die *DirectPlay*-Komponente. Mit diesem Protokoll können verschiedene Transport- und Übertragungsaufgaben zwischen Servern realisiert werden. Diese Technik kommt sinnvoll auf Remotedesktop-Servern zum Einsatz.

E/A-QoS

Das Feature *Eingabe/Ausgabe-Quality of Service* ermöglicht die Konfiguration dieser Komponente. Damit können Sie zum Beispiel E/A- und Bandbreitengrenzwerte für Anwendungen bestimmen.

Erweitertes Speichern

Wird das Feature *Erweitertes Speichern* aktiviert, ermöglicht es Ihnen den Zugriff auf zusätzliche Funktionen, die von erweiterten Speichergeräten bereitgestellt werden. Erweiterte Speichergeräte bieten integrierte Sicherheitsfeatures, mit denen gesteuert werden kann, wer auf die Daten auf dem Gerät zugreifen darf. Die Zusammenarbeit Ihres Servers mit dem externen Speichergerät wird verbessert, indem beteiligte Komponenten Berechtigungen austauschen.

Failoverclustering

Wenn Sie vorhaben, einen Dienst hochverfügbar anzubieten, kann das Feature *Failoverclustering* Sie dabei unterstützen. Es installiert die Clusterfähigkeit des Servers und ermöglicht somit die Zusammenarbeit mehrerer Server zum Bereitstellen einer hochverfügbaren Serverrolle. Diese Technik wird häufig beim Clustern von Dateiservern, Datenbank- und E-Mail-Anwendungen eingesetzt.

> **Clusterfähigkeit der Dienste**
>
> Bitte informieren Sie sich, welche Dienste bzw. welche Hard- und Software clusterfähig ist, bevor Sie deren Einsatz planen. Sie können dazu die HCL (Hardware-Kompatibilitätsliste) konsultieren.

Gruppenrichtlinienverwaltung

Die grafische Verwaltungskonsole, die mit der Installation des Features *Gruppenrichtlinienverwaltung* verfügbar gemacht wird, unterstützt Sie beim Verwalten der Gruppenrichtlinien

Ihres Active Directorys. Nach der Installation finden Sie die *Microsoft Management Console* (MMC) in den administrativen Tools oder auch als Snap-In. Abgekürzt wird diese Konsole oft als *GPMC* bezeichnet (*Group Policy Management Console*).

Auf Domänencontrollern wird dieses Snap-In während der Installation der Rolle *Active Directory-Domänendienste* automatisch aktiviert; auf anderen Management-Maschinen können Sie es bei Bedarf für administrative Zwecke einzeln zusätzlich installieren. Die Installation auf einem Core-System ist nicht möglich.

Hostfähiger Webkern für Internetinformationsdienste

Dieses Feature macht es möglich, dass Serveranwendungen eigene Konfigurationsdateien für IIS verwenden können. Es wird als HWC (*Hosted Web Core*) abgekürzt. Dadurch kann die Anwendung HTTP-Anforderungen verarbeiten und eigene Konfigurationsdateien wie *applicationHost.config* und *root web.config* verwenden. Die HWC-Anwendungserweiterung ist in der Datei *hwebcore.dll* enthalten.

Hyper-V-Unterstützung durch Host Guardian

Dieses Feature stellt Funktionen bereit, die von einem Hyper-V-Server zur Bereitstellung abgeschirmter virtueller Computer benötigt werden. Es ist sozusagen das Gegenstück, die Client-Komponente, zur *Host Guardian Dienst-Rolle*. Die mit Windows Server 2019 verbesserten HGS-Funktionen werden damit unterstützt.

IIS-Erweiterung für OData Services for Management

Dieses Framework unterstützt die Bereitstellung von Windows-PowerShell-Cmdlets über einen ODATA-basierten Webdienst, der unter dem IIS ausgeführt wird. Nach der Aktivierung des Features muss neben weiteren Konfigurationsschritten auch eine Schemaerweiterung eingespielt werden, damit dieser Webdienst funktionsfähig wird.

Intelligenter Hintergrundübertragungsdienst (BITS)

Mit dem Feature *BITS* kann ein Server im Hintergrund Daten empfangen, ohne die Bandbreite im Vordergrund zu beeinträchtigen. Andere Netzwerkanwendungen können so auf einem Server weiterhin über die volle Netzwerkperformance verfügen. Dies hilft Ihrem System, die Reaktionsfähigkeit anderer Netzwerkanwendungen beizubehalten. Auch werden Dateiübertragungen fortgesetzt, nachdem eine Trennung vom Netzwerk stattgefunden hat oder der Server neu gestartet wurde. Der *Windows Update Service* zum Beispiel benutzt die BITS-Komponente auf dem Client, um darüber wegen der Updates zu kommunizieren. Das ist sozusagen das Pendant für einen Server, der Daten bereitstellt, die übertragen werden sollen oder müssen.

BITS beinhaltet außerdem noch zwei untergeordnete Features:

- *IIS-Servererweiterung* – Damit kann der Server Dateien empfangen, die von Clients hochgeladen wurden, auf denen das BITS-Uploadprotokoll implementiert ist.
- *Compact-Server* – Dieses Feature bietet einen eigenständigen HTTPS-Dateiserver, mit dem eine begrenzte Anzahl großer Dateien asynchron zwischen Computern in der gleichen Domäne oder in Domänen übertragen werden kann, die sich gegenseitig vertrauen.

Interne Windows-Datenbank

Diese kostenfreie Datenbank, die Ihnen das System als Feature anbietet, ist ein relationaler Datenspeicher, der nur von Windows-Rollen und -Funktionen verwendet werden kann. Dienste wie der Active Directory-Rechteverwaltungsdienst AD RMS oder der Windows-Update-Dienst WSUS können ihre Daten darin ablegen. Die interne Windows-Datenbank ist somit nicht für Drittherstellerprodukte geeignet.

Internetdruckclient

Der *Internetdruckclient* bietet Ihren Anwendern über das *Internet Printing Protocol (IPP)* die Möglichkeit, eine Verbindung mit Netzwerk- und/oder Internetdruckern herzustellen und Druckaufträge zu initiieren. Er ist somit das Pendant zur Rolle *Interdruckdienst*. Für mobile Mitarbeiter, die Dokumente von unterwegs in der Firma ausdrucken möchten, kann dieses Feature hilfreich sein.

IP-Adressverwaltungsserver (IPAM-Server)

Um eine zentrale Verwaltungsoberfläche für Ihr gesamtes IP-Management zu erhalten, können Sie dieses Feature einsetzen. Es stellt ein zentrales Framework bereit, über das Ihre IP-Adressräume und die entsprechenden Infrastrukturserver, wie DHCP- und DNS-Server, verwaltet werden können. Auch wenn die klassischen Verwaltungskonsolen für DHCP und DNS weiterhin vorhanden sind und auch für gewisse Konfigurationen benötigt werden, bietet IPAM folgende Möglichkeiten in einer gemeinsamen Oberfläche:

- eine automatische Erkennung von Infrastrukturservern in der gesamten AD-Gesamtstruktur
- die Verwaltung dynamischer und statischer IPv4- und IPv6-Adressräume
- die Nachverfolgung von IP-Adressverwendungstrends
- das Erstellen von Berichten der IP-Infrastruktur
- Überwachungs- und Verwaltungsmöglichkeiten von DNS- und DHCP-Diensten im Netzwerk

iSNS-Serverdienst

iSNS steht für *Internet Storage Name Server*. Dieses Feature benötigen Sie, wenn Sie iSCSI-Geräte als Speichergeräte einsetzen. Er hilft iSNS-Initiatoren (Clients), über Namen iSNS-Ziele auf iSNS-Targets zu finden. Es stellt Erkennungsdienste für iSCSI-SANs bereit und verarbeitet Registrierungsanforderungen, Registrierungsaufhebungsanforderungen und Anfragen von iSCSI-Clients.

Der Vorteil von Geräten, die mit iSCSI angebunden werden, ist, dass diese Art der Anbindung nicht über LAN erfolgt. iSCSI ermöglicht den Zugriff auf NAS-Systeme mit dem bei lokalen Datenträgern üblichen Weg als normales lokales Laufwerk. Der blockbasierte Zugriff auf Dateien über die iSCSI-Technologie fällt manchen Anwendungen leichter als der Netzwerkzugriff auf Datenspeicher, die über eine IP-Adresse bereitgestellt werden.

LPR-Portmonitor

Benötigt der von Ihnen angeschlossene Drucker das LPT-Protokoll, müssen Sie dieses Feature installieren. Der LPT-Anschlussmonitor (*Line Printer Remote*) ermöglicht das Drucken auf Druckern, die mithilfe des LPD-Dienstes (*Line Printer Deamon*) freigegeben wurden.

Der LPD-Dienst wird häufig von UNIX-basierten Computern und Geräten für die Druckerfreigabe verwendet. LPD-Ports werden auf Windows-basierten Computern wie lokale Anschlüsse behandelt. Deshalb werden auch Drucker, die über das LPD-Protokoll angesprochen werden, wie lokale Drucker behandelt.

Media Foundation

Das Feature *Media Foundation* bietet Ihnen mit *Windows Media Foundation*, *Windows Media Format SDK* und einer Teilmenge von *DirectShow für Server* die erforderliche Infrastruktur, damit Ihre Anwendungen und Dienste Miniaturansichten für Mediendateien transcodieren, analysieren und generieren können. Für dieses Feature ist die Desktopdarstellung erforderlich. Ein Betrieb mit Windows Server Core ist somit nicht möglich. Der Einsatz auf einem Remotedesktop-Server ist sinnvoll.

Message Queuing

Die Funktion *Message Queuing* unterstützt den gesicherten und überwachten Austausch von Daten zwischen Applikationen auf dem Server. Sie bietet garantierte Nachrichtenübermittlung, effizientes Routing, Sicherheit und prioritätsbasiertes Messaging zwischen Anwendungen.

Die Nachrichtenübermittlung zwischen Anwendungen wird auch verwaltet, wenn diese auf verschiedenen Betriebssystemen, in unterschiedlichen Netzwerkinfrastrukturen, zeitweise offline oder auch zu unterschiedlichen Zeiten stattfindet.

Dieses Feature wird für die detaillierte Installation in weitere Kategorien mit Unterpunkten aufgeteilt:

- Der *Message Queuing-Dienst* enthält:
  - *Message Queuing-Server* – kann zum Implementieren von Lösungen für asynchrone und synchrone Messagingszenarien verwendet werden.
  - *HTTP-Unterstützung* – ermöglicht das Senden von Nachrichten über HTTP.
  - *Message Queuing-Trigger* – ermöglicht den Aufruf einer COM-Komponente oder einer ausführbaren Datei in Abhängigkeit von den Filtern, die Sie für die eingehenden Nachrichten in einer bestimmten Warteschlange definieren.
  - *Multicasting-Unterstützung* – ermöglicht das Einreihen in eine Warteschlange und das Senden von Multicastnachrichten an eine IP-Multicastadresse.
  - *Routingdienst* – leitet Nachrichten zwischen verschiedenen Webseiten und innerhalb einer Webseite weiter.
  - *Verzeichnisdienstintegration* – ermöglicht das Veröffentlichen von Warteschlangeneigenschaften im Verzeichnis sowie die Authentifizierung und Verschlüsselung von Nachrichten mithilfe von Zertifikaten, die im Verzeichnis registriert sind, sowie das Routing von Nachrichten über Verzeichniswebseiten hinweg
- *Message Queuing-DCOM-Proxy* – Durch den DCOM-Proxy kann dieser Computer als DCOM-Client eines Message-Queuing-Remoteservers fungieren.

Multipfad-E/A

Durch den Einsatz des Features *Multipfad-E/A* wird die Verfügbarkeit des Servers erhöht. Mehrere Pfade inklusive Pfad-Failover werden dadurch vom Server zum Speichersubsystem zugelassen.

Unterstützt ein Server im *Storage Area Network* (*SAN*, Speichernetzwerk) diese Multipfad-E/A-Funktion, können Sie mehrere Pfade zum Lesen und Schreiben für eine *Logical Unit Number* (*LUN*, logischer Speicherbereich, der aus einem physischen Festplattenspeicher erstellt wird) aktivieren, indem Sie auf dem Server mehrere Fibrechannel-Ports oder iSCSI-Adapter derselben LUN zuweisen.

> **Multipfad-E/A**
> Um Datenverlust zu vermeiden, stellen Sie bitte sicher, dass der Server oder der Cluster die Funktion *Multipfad-E/A* unterstützt.

MultiPoint Connector

Das Feature *MultiPoint Connector* ermöglicht es mehreren Anwendern, sich diesen Computer mit unterschiedlichen Anwendererfahrungen zu teilen.

In Windows Server 2016 finden Sie diese Funktion als Rolle, die den *MultiPoint Server* als eigenständiges Produkt abgelöst hat. In Windows Server 2019 wurde die Rolle zum Feature. Dieses Feature enthält zwei separate Installationsoptionen:

- *MultiPoint Connector Dienste*
- *MultiPoint-Manager* und *MultiPoint Dashboard (GUI-Verwaltungstools)*

Netzwerklastenausgleich

Network Load Balancer (NLB) ist der bekanntere Name dieses Features. Es verteilt mithilfe des TCP/IP-Netzwerkprotokolls den aufkommenden Datenverkehr auf mehrere Server. Mit NLB können Sie sicherstellen, dass Anwendungen durch Hinzufügen von mehreren Servern bei zunehmender Last skalierbar sind. Das dynamische Umverteilen der Last beim Verändern der Anzahl der teilnehmenden Server ist einer der Vorteile. Applikationen, für die diese Technik eingesetzt werden kann, sind Webserver, Remotedesktopserver, virtuelle private Netzwerke, Windows-Media-Server und viele andere mehr.

Netzwerkvirtualisierung

Dieses Feature bietet Hyper-V-Netzwerkvirtualisierung an. Damit bietet sich Ihnen die Möglichkeit, überlagernde virtuelle Netzwerke für virtuelle Maschinen im selben physischen Netzwerk zu betreiben. Die Netzwerkvirtualisierung entkoppelt virtuelle Netzwerke von der physikalischen Netzwerkinfrastruktur. Diese Flexibilität erleichtert es Ihnen, zu *IaaS-Clouds* (*IaaS* – Infrastrucure as a Service) zu wechseln. Den Administratoren ist es damit möglich, die erforderliche Isolation zwischen den Instanzen bereitzustellen, ohne die Sicherheitsanforderungen zu übergehen.

Peer Name Resolution-Protokoll

Durch Verwendung dieses Protokolls, kurz PNRP, können Anwendungen ihre Namen auf dem Computer registrieren und in eine IPv6-Adresse und Portnummer auflösen, was die Kommunikation anderer Computer mit diesen Anwendungen ermöglicht. Dieser Dienst baut auf IPv6 auf.

RAS-Verbindungs-Manager-Verwaltungskit (CMAK)

Mithilfe dieses Verwaltungskits können Sie Profile für die Verbindung zu Remoteservern und Remotenetzwerken erstellen. Daraus können dann ausführbare Dateien erstellt werden, in denen die Einstellungen für das Herstellen von Verbindungen enthalten sind. Diese Dateien können Sie dann auf Ihren Clientcomputern anwenden, um deren Verbindungen zu den Remotenetzwerken zu konfigurieren. Weitere Informationen finden Sie in Kapitel 19, »Virtuelles privates Netzwerk und Netzwerkrichtlinienserver«.

Remotedifferenzialkomprimierung

Das Feature *Remotedifferenzialkomprimierung (RDC)* unterstützt Sie bei einer optimierten Übertragung von geänderten Daten über das Netzwerk. RDC berechnet und überträgt die Unterschiede zwischen zwei Datei-Objekten bei minimaler Bandbreitenbeanspruchung. Diese Technik ist ein Bestandteil der Rolle *DFS-Replikation* und optimiert die Netzlast.

Remoteserver-Verwaltungstools (RSAT)

Im Untermenü dieses Sammelpunktes befinden sich viele Tools und Snap-Ins, die zur Verwaltung von Serverfunktionen über das Netzwerk von diesem Windows Server 2019 aus umgesetzt werden können. Das Feature *Remoteserver-Verwaltungstools* teilt sich auf in FEATUREVERWALTUNGSTOOLS (siehe Abbildung 2.51) und in ROLLENVERWALTUNGSTOOLS (siehe Abbildung 2.52).



Abbildung 2.51 Server-Manager: Liste der möglichen Featureverwaltungstools



Abbildung 2.52 Server-Manager: Liste der möglichen Rollenverwaltungstools

Remoteunterstützung

Das Feature *Remoteunterstützung* ermöglicht es dem Benutzer, Hilfe von seinem Administrator oder Mitarbeiter im technischen Support anzufordern. Diese Kollegen können sich dann per Remotedesktop auf den betroffenen Rechner aufschalten, um den Benutzer bei Fragen oder Problemen zu unterstützen.

Der Verbindungsaufbau kann dabei über das Netzwerk, das Internet oder eine Telefonleitung mit angeschlossenem Modem durchgeführt werden. Häufiger findet diese Art der Unterstützung auf einer Arbeitsstation als auf einem Server statt. Auf einem Remotedesktopserver kann es aber durchaus sinnvoll sein, dieses Feature zu installieren, damit es zur Unterstützung zur Verfügung steht.

RPC-über-HTTP-Proxy

Das Feature *RPC-über-HTTP-Proxy* verpackt Datenverkehr, der über *Remote Procedure Calls (RPC)* erfolgt, in *HTTP(S)*-Pakete. Wenn Anwender über das Internet auf Applikationen zugreifen müssen, kann diese Technik sie dabei unterstützen. Sie kommt zum Beispiel beim Zugriff von Outlook über das Internet auf einen internen Exchange-Server zum Einsatz. Dies ist eine Alternative zu den Clients, die über eine VPN-Verbindung auf den Server zugreifen.

Sammlung von Setup- und Startereignissen

Mit diesem Feature können Sie Setup- und Startereignisse von anderen Computern im Netzwerk sammeln und protokollieren.

Simple TCP/IP Services

Die einfachen TCP/IP-Dienste stellen Ihrem Server noch einige zusätzliche Dienste für TCP/IP zur Verfügung. Dieses Feature unterstützt folgende TCP/IP-Dienste:

- *Character Generator* (*Zeichengenerator*) – Er sendet Daten, die sich aus einer Folge von 95 druckbaren ASCII-Zeichen zusammensetzen. Eingesetzt wird er als Debugging-Tool zum Testen und bei der Problemanalyse von Zeilendruckern.
- *Daytime* – Wie der Name vermuten lässt, zeigt dieses Protokoll Meldungen mit Wochentag, Monat, Tag, Jahr, aktueller Uhrzeit im Format `HH:MM:SS` sowie Informationen zur Zeitzone an.
- *Discard* – Dieses Protokoll verwirft alle über diesen Anschluss empfangenen Daten, ohne eine Antwort zu senden. Es wird als Nullanschluss während der Netzwerkinstallation und -konfiguration eingesetzt.
- *Echo* – Damit werden Echorückmeldungen zu allen über diesen Serveranschluss empfangenen Nachrichten erzeugt.
- *Quote of the Day* – Das »Zitat des Tages« gibt ein zufälliges Zitat in Form eines ein- oder mehrzeiligen Textes zurück. Der Inhalt der Zufallsausgabe wird von der Datei *C:\Windows\System32\Drivers\Etc\Quotes* bestimmt.

SMB 1.0/CIFS File Sharing Support

Diese Technik unterstützt die Protokolle *SMB 1.0/CIFS-Dateifreigabe* und *Computer Browsing*. Unter dem Sammelpunkt befinden sich zwei separat aktivierbare Teile. Der erste ist der *SMB 1.0/CIFS Client* und der zweite der *SMB 1.0/CIFS Server*. Mit dem Client können Sie auf ältere Server zugreifen, die nur SMB 1.0 verwenden. Aktivieren Sie das Server-Feature, bietet Ihr Server das SMB 1.0-Protokoll für Datenfreigaben für ältere Clients an und benutzt es zum Browsen durchs Netzwerk.

Bitte bedenken Sie, dass es nicht mehr empfohlen ist, SMB 1.0 zu verwenden, da es Schadsoftware gibt (zum Beispiel die Schadsoftware *WannaCry*), die Schwächen dieser Technik ausnutzt, um in Ihr System einzudringen. Wenn es Ihnen möglich ist, entfernen Sie dieses Protokoll komplett aus Ihrem System!

SMB-Bandbreitengrenzwert

Wollen Sie den SMB-Datenverkehr pro Kategorie nachverfolgen oder die Menge der Bandbreite begrenzen, sollten Sie das Feature *SMB-Bandbreitengrenzwert* aktivieren. Zu den Kategorien, die Sie verfolgen können, zählen *Standard*, *Hyper-V* und *Life-Migration*. Meist wird dieses Feature eingesetzt, um die von der Life-Migration verwendete Bandbreite für SMB zu beschränken.

SMTP-Server

Mit dem Feature *SMTP-Server* (*Simple Mail Transfer Protocol*) unterstützen Sie den Transfer von E-Mail-Nachrichten zwischen einem Mailserver und Ihrem Windows Server 2019. Aktuelle Exchange Server-Versionen bringen allerdings ihren eigenen SMTP-Dienst mit und benötigen dieses lokale Feature nicht. Falls Sie ältere Mail-Relay-Anwendungen verwenden, kann dieser lokale SMTP-Dienst noch benötigt werden.

SNMP-Dienst

Das *Simple Network Management Protocol (SNMP)*. Dieser Dienst bietet Ihnen Agenten, mit denen Sie die Aktivität von Netzwerkgeräten überwachen können. Darüber hinaus können Sie damit Berichte für die Netzwerkarbeitsstation erstellen.

Zum Einsatz kommt diese Technik vor allem bei Überwachungsprogrammen von Servern. Dieser Dienst ist eine optionale Erweiterung einer erfolgreich abgeschlossenen TCP/IP-Konfiguration und stellt einen SNMP-Agenten bereit, der eine zentrale Remoteverwaltung von Computern ermöglicht.

Software Load Balancer

Der *Software Load Balancer (SLB)* ermöglicht einen Lastenausgleich zwischen Netzwerkressourcen. Dieses Feature bietet Cloud-Dienstanbietern und Unternehmen, die *Software Defined Networking (SDN)* bereitstellen, die Möglichkeit, Mandanten- und Netzwerkdatenverkehr zwischen Ressourcen im virtuellen Netzwerk gleichmäßig zu verteilen. SLB ermöglicht hohe Verfügbarkeit und Skalierbarkeit mit mehreren Servern zum Hosten derselben Workloads. Es ist seit Windows Server 2016 verfügbar.

Speicherreplikat

Mit der Aktivierung des Features *Speicherreplikat* erhalten Sie zum einen die Möglichkeit, Daten über eine synchrone Replikation auf Blockebene zwischen Servern oder Clustern für die Notfallwiederherstellung einzusetzen. Eine andere Einsatzmöglichkeit ist der *Failovercluster* zwischen Standorten. Die synchrone Replikation ermöglicht die Spiegelung von Daten an physischen Standorten mit ausfallsicheren Volumes, um auf Dateisystemebene sicherzustellen, dass kein Datenverlust auftritt. Die asynchrone Replikation ermöglicht die Standorterweiterung über regionale Bereiche hinaus, wobei jedoch Datenverluste auftreten können. Dieses Feature bietet Verbesserungen der Protokollierungsleistung für Speicherreplikate und unterstützt das *Windows Admin Center*.

Standardbasierte Windows-Speicherverwaltung

Wenn Sie auf Ihrem Server-Verwaltungsschnittstellen den *SMI-S*-Standard (*Storage Management Initiative – Specification*) zum Erkennen, Verwalten und Überwachen von Hardwarespeichergeräten einsetzen möchten, können Sie mithilfe dieser Technik diese Geräte mit Windows-Tools verwalten.

SMI-S gilt als Standardbasis für zukünftige Management-Umgebungen bei Speichernetzwerken (SAN). Diese Funktionalität wird als Gruppe von *Windows Management Instrumentation (WMI)*-Klassen und Windows-PowerShell-Cmdlets verfügbar gemacht.

Storage Migration Service

Das Feature *Storage Migration Service* koordiniert die Speichermigration, indem es den Speichermigrations-Proxy-Dienst aufruft. Der Speichermigrationsdienst ist eine neue Technologie in Windows Server 2019, mit der Server leichter auf eine neuere Version von Windows Server migriert werden können. Er bietet ein grafisches Tool, das Daten auf Servern inventarisiert, Daten und die Konfiguration auf neuere Server überträgt und dann optional die Identitäten der alten Server auf die neuen Server überträgt, sodass Apps und Benutzer nichts ändern müssen.

Storage Migration Service Proxy

Dieser Proxy-Dienst unterstützt den Speichermigrationsdienst beim Ausführen der Inventarisierung, Übertragung und Übernahme von Daten für die Speichermigration. Sollen Daten von einem Server auf einen anderen Server übertragen werden, kann das über einen *Storage Migration Proxy* erfolgen. Wird dieses Feature aktiviert, wird der Dienst selbst über *Storage Migration Service* installiert. Weitere Informationen finden Sie in Kapitel 12.

System Data Archiver

Der *System Data Archiver* bietet Dienste an, mit denen Windows Server-Systemdaten gesammelt und archiviert werden. Das Feature ist neu in Windows Server 2019, und es ist auf einem neuen System bereits installiert.

System Insights

Das in Windows Server 2019 neue Feature *System Insights* erweitert Ihr System um noch mehr Überwachungsfunktionen. Es bietet lokale vorausschauende Analysefunktionen auf dem Server. Dazu werden unter anderem Leistungsindikatoren und Ereignisse mit einbezogen. Alle Daten werden lokal direkt gesammelt, gespeichert und analysiert. Mithilfe der Vorhersagen, die *System Insights* liefert (z. B. Daten zur Auslastung, zum Netzwerkverkehr und zur Datenspeicherung), können Sie Ihren Windows Sever effektiver betreiben.

Die Installation des neuen *Windows Admin Center*, mit dem Sie Windows Server 2016 und Windows Server 2019 in einer webbasierten Oberfläche verwalten können, ist eine Voraussetzung für den Einsatz von *System Insights*. Im Admin Center finden Sie dieses Feature unter dem Namen SYSTEMDATEN. Weiterführende Informationen zum Windows Admin Center finden Sie in Kapitel 10.

Wenn Sie System Insights installieren, wird automatisch die PowerShell-Schnittstelle mit zur Installation angeboten. Damit können Sie über die grafische Verwaltung, die im Admin Center umgesetzt wird, Automatisierungen entwickeln und steuern.

Telnet-Client

Mit der Aktivierung des Telnet-Clients ist es Ihnen möglich, mit dem Telnet-Protokoll remote Verbindung zu einem Telnet-Server aufzubauen, um Anwendungen auf dem Zielserver zu betreiben. Das Feature, mit dem Sie Ihren Windows Server zu einem Telnet-Server machen können, ist seit der Version Windows Server 2016 kein Bestandteil des Betriebssystems mehr. Sie sollten dieses alte Protokoll nicht mehr nutzen.

TFTP-Client

TFTP steht für *Trivial File Transfer Protocol*. Dieses Protokoll benutzt ein Client, um von einem TFTP-Server Daten zu lesen oder um Daten dorthin zu schreiben. TFTP wird hauptsächlich von Geräten oder Systemen verwendet, die während des Startvorgangs Firmware, Konfigurationsinformationen oder ein Systemabbild von einem TFTP-Server abrufen.

Verbessertes Windows-Audio-/Video-Streaming

Der Windows-Dienst *qWave* ist eine Netzwerkplattform für Audio/Video-Streaminganwendungen in IP-Heimnetzwerken. *qWave* stellt die Netzwerk-*QoS* (*Quality of Service*) für die Audio/Video-Anwendungen sicher und verbessert so deren Streamingleistung und -zuverlässigkeit. Der Dienst stellt Mechanismen für Zugangssteuerung, Laufzeitüberwachung und Laufzeiterzwingung, Anwendungsfeedback sowie Datenverkehrspriorisierung bereit.

Auf Windows Server-Plattformen sind für *qWave* nur Übertragungsraten- und Priorisierungsdienste verfügbar.

VM-Abschirmungstools für die Fabricverwaltung

Dieses Feature stellt Hilfsprogramme für abgeschirmte VMs bereit, die von Fabricverwaltungslösungen verwendet werden und auf dem Fabricverwaltungsserver installiert werden sollten.

Azure Service Fabric ist eine Plattform für verteilte Systeme, die das Packen, Bereitstellen und Verwalten skalierbarer und zuverlässiger Microservices und Container vereinfacht. Entwickler und Administratoren können komplexe Infrastrukturprobleme vermeiden und sich auf das Implementieren geschäftskritischer, anspruchsvoller Workloads konzentrieren, die skalierbar, zuverlässig und einfach zu verwalten sind.

WebDAV-Redirector

Mit der *Web Distributed Authoring and Versioning (WebDAV)-Redirector*-Technik wird es Ihren Windows-basierten Programmen ermöglicht, internetbasierte Dateien zu erstellen, darauf zuzugreifen und diese zu ändern. Wenn Sie den WebDAV-Redirector aktivieren, können Autoren von Webinhalten Content auf einer vorhandenen Website veröffentlichen, auf der das WebDAV-Modul installiert ist.

Windows Defender Antivirus

Der *Windows Defender Antivirus* hilft Ihnen dabei, Ihren Windows Server 2019 vor Schadsoftware zu schützen. Dieses Feature ist bereits bei der Installation des Servers aktiviert. Wenn Sie einen anderen Virenscanner auf Ihrem System einsetzen, sollten Sie den Defender deaktivieren.

> **Vorsicht bei Core-Systemen**
>
> Bitte beachten Sie, dass bei deaktiviertem *Windows Defender Antivirus* die Komponenten auf einen Windows Server Core-System nicht aktualisiert werden. Somit könnten diese dann angreifbar werden und ein Sicherheitsrisiko darstellen.

Windows Identity Foundation 3.5

Das *Windows Identity Foundation 3.5 (WIF 3.5)* beinhaltet eine Sammlung von .NET Framework-Klassen, die zum Implementieren von Claim-basierten Identitäten verwendet werden. Claim-basierte Identitäten sind solche Identitäten, die anhand von Attributen anstatt von Gruppenzugehörigkeiten authentifiziert werden. WIF 3.5 wurde durch WIF-Klassen abgelöst,

die in .NET 4.5 enthalten sind. Planen Sie den Einsatz von Claim-basierten Identitäten, sollten Sie .NET 4.5 für die Entwicklung Ihrer Anwendungen verwenden.

Windows PowerShell

Windows PowerShell ist eine auf dem .NET Framework basierende Skriptsprache, die das Automatisieren der lokalen Verwaltung und der Remoteverwaltung von Windows ermöglicht. Sie enthält hunderte von integrierten Befehlen und bietet Ihnen die Möglichkeit, eigene Befehle und Skripte zu schreiben und zu verteilen. Dieses Feature bietet fünf untergeordnete Installationsmöglichkeiten, die Sie in Abbildung 2.53 sehen.

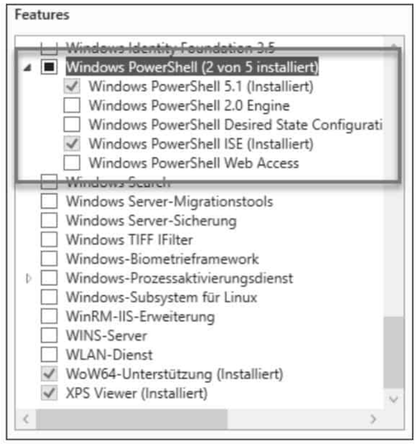


Abbildung 2.53 Server-Manager – PowerShell-Features

Das Feature *Windows PowerShell 5.1* und die *Windows PowerShell ISE* sind bereits installiert. Mit *Integrated Scripting Environment* können Sie in einer grafischen Oberfläche Skripte erstellen, bearbeiten und debuggen. Darüber hinaus ist es möglich, mehrzeilige Teile eines vorhandenen Skripts aufzurufen. Zu den Vorzügen von ISE zählen *IntelliSense*, die Vervollständigung mit ⇆, Ausschnitte, farbkodierte Syntax, Zeilennummerierung, selektive Ausführung, grafisches Debuggen, Rechts-nach-links-Sprache und Unicode-Unterstützung.

Zur Gewährleistung der Abwärtskompatibilität finden Sie in den Unterpunkten auch die *Windows PowerShell 2.0 Engine*.

Der Dienst *Windows PowerShell Desired State Configuration* unterstützt die Konfigurationsverwaltung mehrerer Knoten über ein einziges Repository.

Mit dem Feature *Windows PowerShell Web Access* ist es Ihnen möglich, den Server als Web-Gateway einzusetzen. Benutzer können dann damit auf Remotecomputern das Ausführen von Windows PowerShell-Sitzungen in einem Webbrowser verwalten. Die Gatewaykonfiguration muss nach der Installation von *Windows PowerShell Web Access* von einem Administrator in der *Webserver (IIS)*-Verwaltungskonsole vorgenommen werden.

Mehr zum Thema PowerShell finden Sie in Kapitel 11.

Windows Search

Mit der *Windows-Suche* werden schnelle Dateisuchvorgänge auf Ihrem Server von Clients aus bereitgestellt, die mit diesem Feature kompatibel sind. Diese Funktion eignet sich für die Desktopsuche, die Verwendung auf Remotedesktop-Servern oder kleinen Dateiservern, auf denen indexierte Dateien für Ihre Anwender bereitgestellt werden müssen. Sie ist jedoch eher ungeeignet für komplexere Szenarien.

Windows Server-Migrationstools

Wie der Name schon andeutet, unterstützt dieses Feature Sie bei Migrationen von früheren Versionen von Windows Server. Die Aktivierung dieser Funktion stellt PowerShell-Cmdlets bereit, die die Migration von Serverrollen, Betriebssystemeinstellungen und Dateien und Freigaben von Computern erleichtern. Für eine Migration muss das Feature auch auf dem Quellserver aktiviert werden, von dem die Daten migriert werden sollen.

Windows Server-Sicherung

Mit dem Datensicherungsprogramm *Windows Server-Sicherung* können Sie Ihr Betriebssystem, Anwendungen und Daten sichern und wiederherstellen. Die grafische Oberfläche, die von Beginn an vorhanden ist, weist Sie beim ersten Öffnen darauf hin, dass Sie das Feature erst installieren müssen, um es verwenden zu können. Anschließend können Sie damit den Status der durchgeführten Sicherungen erkennen. Außerdem ist es möglich, eine Sicherungsaufgabe zu planen, um Daten oder den ganzen Server mithilfe des Assistenten wiederherstellen zu können. Selbst die Verwaltung von Datensicherungen anderer Server ist mit der *Windows Server-Sicherung* möglich. Neben der grafischen Konsole gibt es auch ein Befehlszeilentool `wbadmin`, das Sie zur Verwaltung Ihrer Sicherungsaufgaben einsetzen können.

Windows TIFF IFilter

Den *Tagged Image File Format Index Filter (TIFF IFilter)* benötigen Sie für die OCR-Erkennung von eingescannten TIFF 6.0-kompatiblen Dokumenten mit der Indexierung und der Windows-Suche. Die Dateien können die Dateiendung TIF oder TIFF verwenden.

Windows-Biometrieframework

Möchten Sie Anmeldungen an Windows-Maschinen anhand von Fingerabdrücken möglich machen, hilft Ihnen dieses Feature weiter. *Windows-Biometrieframework (WBF)* bringt die Komponenten mit, die Sie zur Verwendung von Fingerabdruckgeräten benötigen, um Identitäten zu bestimmen und zu überprüfen.

Windows-Prozessaktivierungsdienst

Der Windows-Prozessaktivierungsdienst (*Windows Process Activation Service*, *WPAS)* verallgemeinert das IIS-Prozessmodell und entfernt die Abhängigkeit von HTTP. Alle Funktionen, die zuvor nur für HTTP-Anwendungen verfügbar waren, sind nun für *Windows Communication Foundation* (*WCF)*-Anwendungshostingdienste mithilfe von Nicht-HTTP-Protokollen verfügbar. IIS 10.0 verwendet WPAS außerdem für die nachrichtenbasierte Aktivierung über HTTP.

Das Feature WPAS besitzt noch drei Unter-Features:

- Das *Prozessmodell* fungiert als Host für Web- und WCF-Dienste und wurde erstmals in IIS 6.0 eingesetzt. Das Prozessmodell ist eine neue Architektur, die einen schnellen Ausfallschutz, Integritätsüberwachung und Recycling ermöglicht. Das Prozessmodell des WPAS beseitigt die Abhängigkeit von HTTP.
- Die *.NET-Umgebung 3.5* unterstützt die Aktivierung in verwaltetem Code im Prozessmodell. Mithilfe der Konfigurations-APIs können Anwendungen, die mit dem .NET Framework erstellt wurden, von WPAS programmgesteuert konfiguriert werden. So können Entwickler veranlassen, dass die Einstellungen des WPAS beim Ausführen einer Anwendung automatisch konfiguriert werden und die Konfiguration nicht vom Administrator manuell durchgeführt werden muss.

Windows-Subsystem für Linux

Das neu entwickelte *Windows-Subsystem für Linux (WSL)* umfasst Dienste und Umgebungen zum Ausführen von Linux-Shells und -Tools unter Windows. Das Windows-Subsystem für Linux ist nur auf 64-Bit-Versionen ab Windows 10 oder dem Windows Server 2019 verfügbar.

WinRM-IIS-Erweiterung

Die IIS-Erweiterung für die *Windows-Remoteverwaltung (WinRM)* ermöglicht es einem Server, Verwaltungsanforderungen eines Clients mithilfe der Webserver-Verwaltungskonsole zu empfangen. WinRM ist die Microsoft-Implementierung des Webserver-Verwaltungsprotokolls, das einen sicheren Kommunikationsweg zwischen lokalen Computern und Remotecomputern mithilfe von Webdiensten bereitstellt.

WINS-Server

Auch in Windows Server 2019 ist der Dienst *Windows Internet Naming Service (WINS)* wieder verfügbar. Die mit diesem Server bereitgestellte verteilte WINS-Datenbank beinhaltet die registrierten dynamischen NetBIOS-Namenszuordnungen für Computer und kann somit NetBIOS- und WINS-Abfragen beantworten und auflösen. Dieser Dienst ordnet NetBIOS-Namen IP-Adressen zu und behebt die Probleme, die auf die NetBIOS-Namensauflösung in Routingumgebungen zurückzuführen sind.

WLAN-Dienst

Ein WLAN befindet sich heutzutage fast in jedem privaten Haushalt, und auch in Firmenumgebungen findet dieses Funknetzwerk seinen Einsatz. Möchten Sie Ihren Windows Server 2019 auch kabellos in Ihr WLAN-Netzwerk einbinden, müssen Sie dieses Feature installieren. Das Feature *WLAN-Dienst* startet und konfiguriert außerdem den WLAN-Autokonfigurationsdienst unabhängig davon, ob der Windows Server über einen Funkadapter verfügt. Die integrierte Autokonfiguration listet die verfügbaren Funkadapter auf und verwaltet sowohl Funkverbindungen als auch Funkprofile. Funkprofile enthalten die Einstellungen, die zum Konfigurieren eines WLAN-Clients notwendig sind, damit er eine Verbindung zum WLAN herstellen kann.

WoW64-Unterstützung

WOW64 (*Windows-On-Windows 64-Bit*) ist ein Subsystem des Windows-Betriebssystems, das in der Lage ist, 32-Bit-Anwendungen auszuführen. WOW64 ist in allen 64-Bit-Versionen von Windows seit Windows 2000 und Microsoft Windows XP enthalten.

Das Feature *WoW64-Unterstützung* ist bereits von Beginn an aktiviert und unterstützt die Ausführung von 32-Bit-Anwendungen auf Ihrem Windows Server 2019. Es enthält das gesamte WoW64 zum Ausführen von 32-Bit-Anwendungen auf einem Server Core.

XPS Viewer

Das letzte Feature in der Liste ist der *XPS-Viewer*. Er wird benötigt, um Dateien im XPS-Format lesen zu können. XPS steht für *XML Paper Specification* und ist ein Dateiformat von Windows. Ähnlich wie beim weit verbreiteten PDF-Format wird eine XPS-Datei formatgetreu auf allen Geräten dargestellt und gedruckt. Das Dokument sieht somit immer gleich aus, egal mit welchem Gerät Sie es ansehen. Dieses Feature ist von Beginn an aktiviert.

2.4 Editionen und ihre Möglichkeiten

Sie haben in Kapitel 1 bereits erfahren, dass es für das aktuelle Windows Server-Betriebssystem verschiedene Editionen und Installationspfade gibt, zwischen denen Sie sich entscheiden müssen. Neben dem *Windows Server 2019 Long Term Servicing Channel (LTSC)*, den es in verschiedenen Editionen gibt (von *Essential* über *Standard* bis *Datacenter*, und dann auch als *Core*) gibt es auch den sogenannten *Installations-Pfad* für *Windows Server Semi Annual Channel (SAC)*.

LTSC-Versionen enthalten alle Installationsmöglichkeiten. Dazu zählen der altbekannte Server mit dem Windows-Desktop, der Core-Server und der Nano-Server. SAC-Versionen enthalten nur die Optionen *Server Core für Container-Host und -Image* und Nano-Server-Containerimage. Ein vollständiger Windows Server inklusive grafischer Oberfläche ist im SAC nicht enthalten.

LTSC-Versionen sind die Basis für traditionelle Applikationen wie Dateiserver, Druckserver, Domänencontroller, Exchange, SQL-Server oder virtuelle Infrastrukturen. SAC-Versionen enthalten keine grafische Oberfläche und werden üblicherweise im Rahmen von *DevOps* für Container- und Cloud-Apps produktiv genutzt.

DevOps ist ein Kunstwort aus den Begriffen *Development* (dt. *Entwicklung*) und *IT-Operations* (dt. *IT-Betrieb*) und beschreibt einen Prozessverbesserungsansatz aus den Bereichen der Softwareentwicklung und der Systemadministration.

Wir erklären Ihnen im Folgenden die Unterschiede. Bei den Überlegungen, welche die richtige Version ist, geraten Sie sonst leicht in eine Sackgasse. Entscheiden Sie sich von Beginn an für die passende Version und Edition, die alle Rollen und Features bereitstellen, die Sie einsetzen möchten.

2.4.1 Windows Server 1809 SAC

Sollten Sie sich für das SAC-Installations- und Update-Modell entscheiden wollen, haben Sie wie bereits erwähnt keine grafische Oberfläche und auch nicht die gleichen Optionen wie bei der vollen Installation der Desktop-Version eines Windows Server 2019. Allerdings können Sie auch hier aktuell zwischen den Installationsvarianten *Standard* und *Datacenter* wählen (siehe Abbildung 2.54).

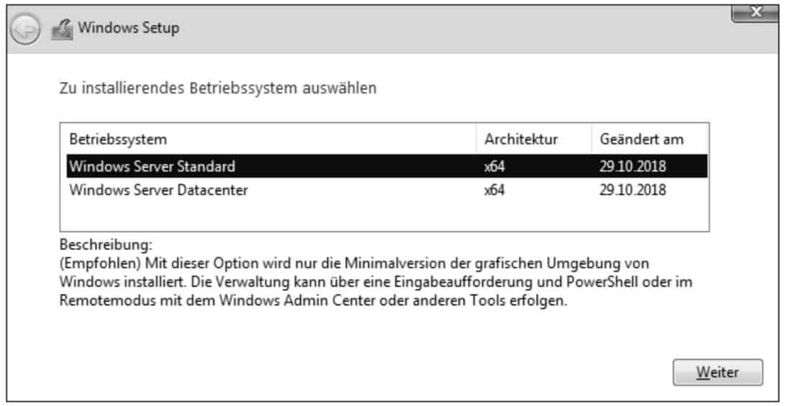


Abbildung 2.54 SAC-Windows-Setup: Windows Server 1809 – Betriebssystemauswahl

Versionsnummern

Die Nummer im Namen des SAC-Windows Server steigt scheinbar in zufälligen Versionsnummer-Schritten an, ist aber eigentlich sprechend: Sie steht für das Jahr und den Monat der SAC-Ausgabe. Im aktuellen Fall ist das der September 2018.

Ein aktueller Vergleich zeigt, dass der einzige Unterschied zwischen der *Windows Server 1809 – Datacenter-Edition* und der *Windows Server 2019 – Datacenter Core Edition* das Vorhandensein des Features *Netzwerkcontroller* und des zugehörigen Management-Tools ist.

In zukünftigen Versionen kann sich das natürlich wieder ändern.

2.4.2 Windows Server 2019 LTSC – Essential

Die Edition *Essentials* ist für kleine Unternehmen mit maximal 25 Mitarbeitern (50 Geräten) sinnvoll. Der Essential-Server ist der Nachfolger des *Small Business Servers* (allerdings ohne Zusatzdienste wie Exchange und SharePoint) und wahrscheinlich auch mit der Version 2019 der letzte seiner Art. Sollte die Funktion des Domänencontrollers eingesetzt werden, darf jede Organisation nur einen einzigen *Windows Server 2019 Essentials* einsetzen. Die Einhaltung des Limits von 25 Benutzern und 50 Geräten wird über den Domänencontroller sichergestellt. Die Essentials-Edition kann damit nur in kleineren Organisationen und Umgebungen eingesetzt werden.

Windows Server 2019 Essentials verfügt über die gleichen Lizenzmerkmale und technischen Merkmale wie sein Vorgänger, *Windows Server 2016 Essentials*. Wenn Windows Server 2019 Essentials als Domänencontroller konfiguriert ist, muss dieser der einzige Domänencontroller sein und alle *Flexible Single Master Operations*-(FSMO-)Rollen ausführen, und er darf keine bidirektionalen Vertrauensstellungen mit anderen Active Directory-Domänen haben.

Windows Server 2019 Essentials enthält die neue Hardware-Unterstützung sowie Funktionen und Verbesserungen wie Windows Server 2019 Standard, einschließlich Speichermigrationsdiensten, Systeminformationen und viele mehr.

Windows Server 2019 Essentials wird keine *Essentials Experience*-Rolle enthalten. Die Essentials Experience diente in erster Linie der vereinfachten Dateifreigabe und Geräteverwaltung. Eine verbesserte Verwaltungserfahrung bietet jetzt das *Windows Admin Center*.

2.4.3 Windows Server 2019 LTSC – Standard oder Datacenter, Core oder Desktop

Gleich zu Beginn einer neuen Server-Installation wird der Windows-Setup-Assistent Sie wie in Abbildung 2.55 nach dem Installations-Key fragen, um Windows zu aktivieren.

Haben Sie keinen Key zur Hand, können Sie an dieser Stelle trotzdem fortfahren und Windows später aktivieren. In diesem Fall bekommen Sie bei der Auswahl für das zu installierende Betriebssystem alle Möglichkeiten angezeigt (siehe Abbildung 2.56).

- Windows Server 2019 Standard – als Core oder in der Desktop-Variante
- Windows Server 2019 Datacenter – als Core oder in der Desktop-Variante



Abbildung 2.55 Windows-Setup: Windows aktivieren

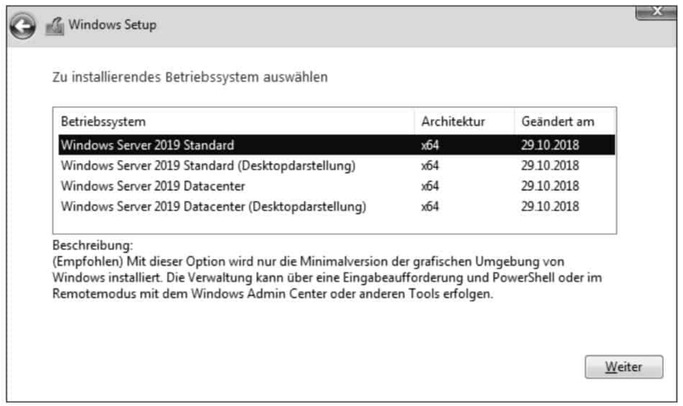


Abbildung 2.56 Windows-Setup: Installationsauswahl ohne Key-Eingabe

Haben Sie allerdings einen Installations-Key vorliegen, entscheidet sich mit Eingabe des Keys bereits die Auswahl der Version *Standard* oder *Datacenter*.

Nach der Eingabe eines Keys, den Sie für eine *Standard*-Version gekauft haben, erhalten Sie daher die Auswahl aus Abbildung 2.57.

Sollten Sie sich für die Lizenz einer Datacenter-Installation entschieden haben, sehen Sie auch dies nach der Eingabe des Keys (siehe Abbildung 2.58).

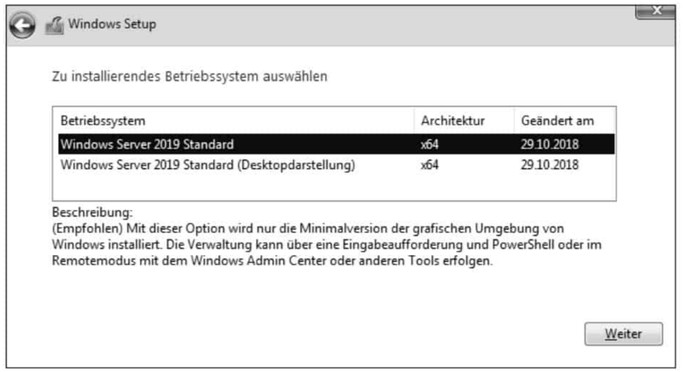


Abbildung 2.57 Windows-Setup nach Eingabe eines gültigen Standard-Version-Keys

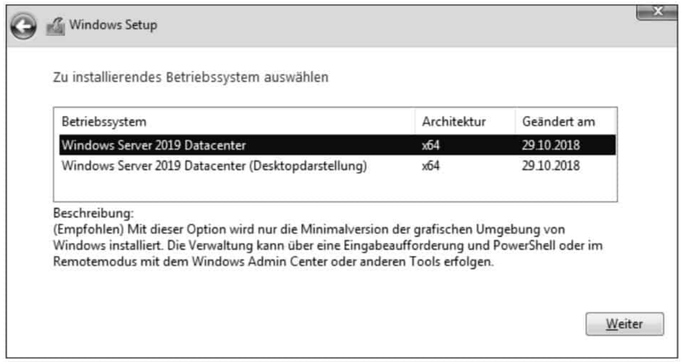


Abbildung 2.58 Windows-Setup nach Eingabe eines gültigen Datacenter-Versions-Keys

2.4.4 Vergleichen Sie die Editionen

Wenn Sie die *Windows Server 2019 Standard*- und die *Datacenter*-Edition (inklusive der Desktop- und Core-Varianten) vergleichen, bemerken Sie diverse Unterschiede bei den vorhandenen und aktivierten Funktionen. Nutzen Sie die PowerShell, um sich die aktivierten Funktionen auflisten zu lassen und die Dateien zu vergleichen.

Die vorhandenen Funktionen eines Servers und deren Installationsstatus können Sie mit folgendem Befehl abfragen:

```
Get-WindowsFeatures
```

Einen Ausschnitt der Ausgabe sehen Sie in Abbildung 2.59. Der Inhalt hängt natürlich von der jeweiligen Edition ab, für die der Befehl ausgeführt wurde.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\Administrator> Get-WindowsFeature

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[ ] Active Directory Lightweight Directory Services     ADLDS                          Available
[X] Active Directory-Domänendienste                     AD-Domain-Services             Installed
[ ] Active Directory-Rechteverwaltungsdienste           ADRMS                          Available
    [ ] Active Directory-Rechteverwaltungsserver        ADRMS-Server                   Available
    [ ] Unterstützung für Identitätsverbund             ADRMS-Identity                 Available
[ ] Active Directory-Verbunddienste                     ADFS-Federation                Available
[ ] Active Directory-Zertifikatdienste                  AD-Certificate                 Available
    [ ] Zertifizierungsstelle                           ADCS-Cert-Authority            Available
    [ ] Online-Responder                                ADCS-Online-Cert               Available
    [ ] Registrierungsdienst für Netzwerkgeräte         ADCS-Device-Enrollment         Available
    [ ] Zertifikatregistrierungsrichtlinien-Webdienst   ADCS-Enroll-Web-Pol            Available
    [ ] Zertifikatregistrierungs-Webdienst              ADCS-Enroll-Web-Svc            Available
    [ ] Zertifizierungsstellen-Webregistrierung         ADCS-Web-Enrollment            Available
[X] Datei-/Speicherdienste                              FileAndStorage-Services        Installed
    [X] Datei- und iSCSI-Dienste                        File-Services                  Installed
        [X] Dateiserver                                 FS-FileServer                  Installed
        [ ] Arbeitsordner                               FS-SyncShareService            Available
        [ ] BranchCache für Netzwerkdateien             FS-BranchCache                 Available
        [ ] Dateiserver-VSS-Agent-Dienst                FS-VSS-Agent                   Available
        [ ] Datendeduplizierung                         FS-Data-Deduplication          Available
        [X] DFS-Namespaces                              FS-DFS-Namespace               Installed
        [X] DFS-Replikation                             FS-DFS-Replication             Installed
        [ ] iSCSI-Zielserver                            FS-iSCSITarget-Server          Available
        [ ] iSCSI-Zielspeicheranbieter (VDS- und VSS... iSCSITarget-VSS-VDS            Available
        [ ] Ressourcen-Manager für Dateiserver          FS-Resource-Manager            Available
        [ ] Server für NFS                              FS-NFS-Service                 Available
    [X] Speicherdienste                                 Storage-Services               Installed
```

Abbildung 2.59 Ausgabe des PowerShell-Befehls für vorhandene Windows-Features

Die Ausgabe dieser Abfrage speichern Sie in einer Textdatei ab. Das gleiche Vorgehen führen Sie auf dem zweiten Server durch, den Sie mit dem ersten vergleichen wollten. Beide Textdateien legen Sie in ein gemeinsames Verzeichnis.

Mit dem folgenden PowerShell-Befehl können Sie anschließend die beiden Textdateien der verschiedenen Installationsvarianten vergleichen und die Unterschiede erkennen:

```
Compare-Object (Get-Content ".\Feature-Liste_Datacenter.txt") `
  (Get-Content ".\Feature-Liste-Standard.txt")
```

In diesem Beispiel werden die Features der *Standard*-Installation in der Textdatei *Feature-Liste-Standard.txt* ausgegeben und die Features der Datacenter-Version *Liste_Datacenter.txt* abgespeichert. Anschließend werden beide Dateien miteinander verglichen und in die Ausgabe aus Abbildung 2.60 geschrieben.

In der Ausgabe können Sie erkennen, dass das Feature *PowerShell-V2* in der *Standard*-Variante vorhanden und nicht aktiviert ist. Zu erkennen ist das daran, dass der Pfeil hinter AVAILABLE (dt. *verfügbar*) nach rechts zeigt. Im ausgeführten Befehl, mit dem beide Versionen miteinander verglichen wurden, stand der Standard-Server auch rechts (siehe Abbildung 2.61).


```
Vergleich-Standard-Datacenter.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
InputObject                                                                SideIndicator
-----------                                                                -------------
    [ ] Windows PowerShell 2.0 Engine                PowerShell-V2          Available =>
[ ] Netzwerkcontroller                               NetworkController      Available <=
        [ ] Network Controller Management Tools      RSAT-NetworkController Available <=
[ ] Software Load Balancer                           SoftwareLoadBalancer   Available <=
    [ ] Windows PowerShell 2.0 Engine                PowerShell-V2            Removed <=
```

Abbildung 2.60 Ausgabe eines Vergleichs von Textdateien

```
Windows PowerShell
PS C:\> Compare-Object (Get-Content ".\Feature-Liste_Datacenter.txt") (Get-Content ".\Feature-Liste-Standard.txt")
```

Abbildung 2.61 Vergleich von zwei Textdateien – »Standard« steht rechts.

In der *Datacenter*-Variante ist das PowerShell-V2-Feature allerdings mit REMOVED (dt. *entfernt*) gekennzeichnet. Der Pfeil zeigt nach links und kennzeichnet somit den Datacenter-Server, der im Befehlsaufruf an erster Stelle stand, also links (siehe Abbildung 2.62).

```
Windows PowerShell
PS C:\> Compare-Object (Get-Content ".\Feature-Liste_Datacenter.txt") (Get-Content ".\Feature-Liste-Standard.txt")
```

Abbildung 2.62 Vergleich von zwei Textdateien – »Datacenter« steht links.

Mit diesem Wissen erkennen Sie aus dem Output in Abbildung 2.60, dass in der Datacenter-Variante auch das Feature *Netzwerkcontroller*, das zugehörige Management-Tool und der *Software Load Balancer* für die Installation verfügbar sind. Alle drei sind gemäß dieser Ausgabe somit in der *Standard*-Variante nicht vorhanden, weil sie nicht mit einem Pfeil nach rechts gelistet werden.

Mit dieser Möglichkeit können Sie bei Bedarf Versionen miteinander vergleichen und sich einen Überblick über die Unterschiede der verschiedenen Servertypen verschaffen.

2.5 Platzierung

Auch wenn ein Server viele Rollen gleichzeitig übernehmen könnte, ist es aus vielen Gründen ratsamer und sinnvoller, genau zu planen, welche und wie viele Rollen auf einer einzelnen Maschine laufen werden. Grundsätzlich und aufgrund der Tatsache, dass Server virtualisiert betrieben werden können, lautet die Empfehlung, so wenige Rollen wie möglich auf ein und derselben Maschine zu installieren.

Im laufenden Betrieb stellt sowohl die Verwaltung als auch die Wartung einer Maschine mit mehreren Rollen eine Herausforderung dar. Manche Rollen sind darüber hinaus gänzlich ungeeignet, um parallel mit anderen Rollen auf derselben Maschine installiert zu werden, oder sie werden gar nicht erst unterstützt.

Bitte setzen Sie sich vor der Inbetriebnahme einer Rolle damit auseinander, ob diese allein oder mit anderen Rollen oder Aufgaben auf einem einzelnen Windows Server 2019 laufen soll.

Klären Sie dabei folgende Fragen:

- Welcher Personenkreis wird den Server verwalten, und welche Rechte sind dazu notwendig?
- Gibt es Abhängigkeiten zu anderen Rollen, die zu beachten sind?
- Sprechen technische Details gegen eine Inbetriebnahme der verschiedenen Rollen auf einem Server?
- Wie viele Server werden benötigt, und an welchen Lokationen müssen diese platziert werden, um den Anforderungen zu entsprechen?

Wenn Sie nun entschieden haben, welche Rollen Sie auf welchen Servern in Ihrem Netzwerk installieren werden, können Sie mit der Installation beginnen.

Auf einen Blick

1 Windows Server 2019 27

2 Rollen und Features 59

3 Netzwerkgrundlagen und -Topologien 135

4 IP-Adressmanagement 157

5 Authentifizierungsprotokolle 233

6 Active Directory 257

7 Benutzer, Gruppen & Co im Active Directory 335

8 Virtualisierung 381

9 Dateiserver 413

10 Verwaltung 459

11 Windows PowerShell 531

12 Migration verschiedener Serverdienste auf Windows Server 2019 567

13 Hyper-V 635

14 Dateidienste 691

15 Internetinformationsdienste-Server (IIS) 753

16 PKI und Zertifizierungsstellen 795

17 Patchmanagement mit WSUS 859

18 Remotedesktopdienste 913

19 Virtuelles privates Netzwerk und Netzwerkrichtlinienserver 981

20 Integration in Azure 1059

21 Troubleshooting im Windows Server 2019 1117

22 Security in und mit Windows Server 2019 1171

Inhalt

Vorwort der Autoren 21

1 Windows Server 2019 27

1.1 What's new? 28

1.2 Die verschiedenen Editionen 30
1.2.1 Windows Server Standard 31
1.2.2 Windows Server Datacenter 31

1.3 Long Term Services Channel vs. Semi-Annual Channel 31

1.4 Lizenzierung 32
1.4.1 Verschiedene Lizenzierungsarten 32
1.4.2 Lizenzprogramme (KMS und MAK) 32
1.4.3 Active Directory Based Activation (ADBA) 36
1.4.4 VM-Based Activation 37

1.5 Systemanforderungen 37

1.6 Installation von Windows Server 2019 37
1.6.1 Installation mit grafischer Oberfläche 39
1.6.2 Windows Server Core 44
1.6.3 Nach der Installation 45

1.7 Die Installation automatisieren 47
1.7.1 Windows Assessment and Deployment Kit (ADK) 47
1.7.2 Abbildverwaltung (Deployment Image Servicing and Management) 51
1.7.3 Sysprep 53

1.8 Update-Strategie 57

2 Rollen und Features 59

2.1 Rollen und Rollendienste 59

2.2 Die Rollen im Überblick 61
2.2.1 Active Directory Lightweight Directory Services 61
2.2.2 Active Directory-Domänendienste 62
2.2.3 Active Directory-Rechteverwaltungsdienste 65

2.2.4 Active Directory-Verbunddienste ... 66
2.2.5 Active Directory-Zertifikatdienste ... 68
2.2.6 Datei-/Speicherdienste ... 71
2.2.7 Device Health Attestation ... 82
2.2.8 DHCP-Server ... 84
2.2.9 DNS-Server ... 85
2.2.10 Druck- und Dokumentendienste ... 86
2.2.11 Faxserver ... 88
2.2.12 Host Guardian-Dienst ... 90
2.2.13 Hyper-V ... 91
2.2.14 Netzwerkcontroller ... 92
2.2.15 Netzwerkrichtlinien- und Zugriffsdienste ... 93
2.2.16 Remotedesktopdienste ... 94
2.2.17 Remotezugriff ... 96
2.2.18 Volumenaktivierungsdienste ... 98
2.2.19 Webserver (IIS) ... 99
2.2.20 Windows Server Update Services (WSUS) ... 103
2.2.21 Windows-Bereitstellungsdienste ... 106

2.3 Features ... 107

2.4 Editionen und ihre Möglichkeiten ... 127
2.4.1 Windows Server 1809 SAC ... 128
2.4.2 Windows Server 2019 LTSC – Essential ... 129
2.4.3 Windows Server 2019 LTSC – Standard oder Datacenter, Core oder Desktop ... 129
2.4.4 Vergleichen Sie die Editionen ... 131

2.5 Platzierung ... 133

3 Netzwerkgrundlagen und -Topologien 135

3.1 Was ist ein Netzwerk? Diese Begriffe sollten Sie kennen ... 135

3.2 Welche Topologien gibt es und welche werden heute in der Praxis noch genutzt? ... 137
3.2.1 Bus-Topologie ... 137
3.2.2 Ring-Topolgie ... 138
3.2.3 Stern-Topologie ... 139
3.2.4 Hierarchische Topologie ... 139
3.2.5 Vermaschte Topologie ... 140

3.3 Referenzmodelle ... 141
3.3.1 ISO-OSI-Referenzmodell ... 142
3.3.2 TCP/IP-Referenzmodell ... 152
3.3.3 Gegenüberstellung der beiden Modelle ... 153

3.4 Übertragungsmethoden ... 154
3.4.1 Unicast ... 154
3.4.2 Multicast ... 154
3.4.3 Broadcast ... 155

4 IP-Adressmanagement 157

4.1 Was ist eine MAC-Adresse? ... 157

4.2 Was ist TCP/IP? ... 159

4.3 Das IP-Protokoll genauer erklärt ... 161
4.3.1 IP Version 4 ... 161
4.3.2 ARP ... 168
4.3.3 Subnetting ... 171
4.3.4 IP Version 6 (IPv6) ... 173
4.3.5 Aufbau eines IP-Pakets ... 181

4.4 Wie kommuniziert ein Computer mit einem Netzwerk? ... 184
4.4.1 Kabelverbindungen ... 185
4.4.2 WLAN und Mobilfunk ... 186

4.5 Netzwerkkonfiguration unter Windows ... 188

4.6 Namensauflösung ... 194
4.6.1 DNS-Namensauflösung ... 195
4.6.2 NetBIOS ... 203

4.7 DHCP ... 205
4.7.1 Was ist DHCP? ... 205
4.7.2 Wie funktioniert die Vergabe von IP-Adressen mit DHCP und wie werden die IP-Adressen erneuert? ... 205
4.7.3 Automatische Vergabe von privaten IP-Adressen (APIPA) ... 206
4.7.4 Aufbau eines DHCP-Datenpakets ... 207
4.7.5 Installation eines DHCP-Servers unter Windows Server 2019 ... 208
4.7.6 Konfiguration eines DHCP-Servers nach der Installation der Rolle ... 213
4.7.7 Konfiguration eines DHCP-Failovers ... 225

4.8 IPAM ... 227
4.8.1 Vorteile des IPAM ... 227

4.8.2 Installation des IPAM ... 227
4.8.3 Konfiguration des IPAM-Servers ... 228
4.8.4 Mögliche Anpassungen des IPAM-Servers und Hinweise für den Betrieb ... 231

5 Authentifizierungsprotokolle 233

5.1 Domänenauthentifizierungsprotokolle ... 233
5.1.1 LanManager (LM) ... 234
5.1.2 NTLM ... 235
5.1.3 Kerberos ... 235
5.1.4 Ansprüche (Claims) und Armoring ... 251
5.1.5 Sicherheitsrichtlinien ... 254

5.2 Remotezugriffsprotokolle ... 255
5.2.1 MS-CHAP ... 255
5.2.2 Password Authentication Protocol (PAP) ... 255
5.2.3 Extensible Authentication Protocol (EAP) ... 255

5.3 Webzugriffsprotokolle ... 256

6 Active Directory 257

6.1 Geschichte des Active Directorys ... 257

6.2 Was ist neu im Active Directory in Windows Server 2019? ... 258

6.3 Die Datenbank von Active Directory ... 259

6.4 Die Komponenten des Active Directorys ... 260
6.4.1 Logischer Aufbau ... 260
6.4.2 Physischer Aufbau ... 264
6.4.3 Globaler Katalog ... 264
6.4.4 FSMO (Flexible Single Master Operations) bzw. Betriebsmaster ... 265
6.4.5 Standorte ... 267
6.4.6 Distinguished Name ... 267
6.4.7 Canonical Name ... 267
6.4.8 Common Name ... 267

6.5 LDAP ... 268

6.6 Schema ... 268

6.7 Replikation ... 269
6.7.1 Steuerung der AD-Replikation ... 269
6.7.2 Tool für die Überprüfung des Replikationsstatus ... 272

6.8 Read-Only-Domänencontroller (RODC) ... 272
6.8.1 Voraussetzungen für den Einsatz eines RODC ... 273
6.8.2 Funktionalität ... 274
6.8.3 RODC-Attributsatzfilter ... 274
6.8.4 Wie funktioniert eine RODC-Anmeldung? ... 275
6.8.5 Einen schreibgeschützten Domänencontroller installieren ... 275

6.9 Vertrauensstellungen ... 282
6.9.1 Eigenschaften der Domänenvertrauensstellungen ... 284
6.9.2 Vertrauensstellungstypen ... 286
6.9.3 Vertrauensstellung in Windows-Domänen ab Windows Server 2003 ... 286
6.9.4 Authentifizierungsvarianten in Vertrauensstellungen ab Windows Server 2003 ... 287
6.9.5 Fehlerhafte Vertrauensstellungen ... 288
6.9.6 Eine Gesamtstrukturvertrauensstellung einrichten ... 288

6.10 Offline-Domänenbeitritt ... 296

6.11 Der Papierkorb im Active Directory ... 297

6.12 Der Wiederherstellungsmodus des Active Directorys ... 299
6.12.1 Nicht-autorisierende Wiederherstellung ... 300
6.12.2 Autorisierende Wiederherstellung ... 300
6.12.3 Garbage Collection ... 301
6.12.4 Active Directory Database Mounting Tool ... 301

6.13 Active Directory-Verbunddienste (AD FS) ... 302
6.13.1 Die Komponenten des AD FS ... 302
6.13.2 Was ist eine Verbundvertrauensstellung? ... 303

6.14 Installation des Active Directory ... 304
6.14.1 Den ersten DC in einer Domäne installieren ... 304
6.14.2 Weiteren DC in einer Domäne installieren ... 315
6.14.3 Installation des ersten DC in einer Subdomäne der Gesamtstruktur ... 317
6.14.4 Einen DC aus einer Domäne entfernen ... 319
6.14.5 Einen defekten oder nicht mehr erreichbaren DC aus einer Domäne entfernen ... 323
6.14.6 Die Domäne entfernen ... 326

6.15 Wartungsaufgaben innerhalb des Active Directorys ... 329
6.15.1 Übertragen oder Übernehmen der FSMO ... 329

6.15.2 Wartung der AD-Datenbank ... 330
6.15.3 IFM-Datenträger ... 331

7 Benutzer, Gruppen & Co im Active Directory 335

7.1 Container ... 335
7.1.1 Administrative Konten und Sicherheitsgruppen im Container »Builtin« ... 337
7.1.2 Administrative Konten und Sicherheitsgruppen aus dem Container »Users« ... 340
7.2 Organisationseinheiten ... 342
7.2.1 Objektverwaltung delegieren ... 343
7.3 Benutzer ... 346
7.4 Computer ... 346
7.4.1 Sicherheitseinstellungen für den Domänenbeitritt von neuen Computern ... 347
7.5 Gruppen ... 349
7.5.1 Arten von Sicherheitsgruppen ... 351
7.5.2 Protected Users Group ... 352
7.6 MSA und gMSA ... 352
7.6.1 Managed Service Account (MSA) ... 352
7.6.2 Group Managed Service Account (gMSA) ... 353
7.7 Password Settings Objects (PSOs) ... 356
7.7.1 Voraussetzungen für das Anwenden der PSOs ... 357
7.7.2 PSOs erstellen ... 357
7.8 Gruppenrichtlinienobjekte (GPO) ... 360
7.8.1 Allgemeines zu Gruppenrichtlinien ... 362
7.8.2 Bestandteile einer GPO und die Ablageorte ... 363
7.8.3 Aktualisierungsintervalle von GPOs ... 364
7.8.4 GPOs erstellen und löschen ... 365
7.8.5 Sicherheitsfilter der GPOs ... 367
7.8.6 Administrative Vorlagen und Central Store ... 367
7.8.7 Der Central Store ... 369
7.8.8 Clientseitige Erweiterungen ... 371
7.8.9 Softwareinstallation über GPOs ... 371
7.8.10 Sicherheitseinstellungen innerhalb der GPOs ... 372
7.9 msDs-ShadowPrincipal ... 376
7.9.1 msDS-ShadowPrincipalContainer ... 377
7.9.2 Die Klasse msDS-ShadowPrincipal ... 377

7.9.3 Die SID msDS-ShadowPrincipal ... 377
7.9.4 Shadow Principals nutzen ... 377
7.10 Freigegebene Ordner ... 378
7.11 Freigegebene Drucker ... 379

8 Virtualisierung 381

8.1 Hypervisoren ... 381
8.1.1 Hypervisor-Typen ... 382
8.1.2 Hypervisor-Design ... 383
8.2 Hyper-V ... 385
8.2.1 Hyper-V-Hypervisor ... 385
8.2.2 Hyper-V-Architektur ... 395
8.2.3 Hyper-V-Anforderungen ... 397
8.3 Das ist neu in Windows Server 2019 ... 405
8.4 Virtual Desktop Infrastructure (VDI) ... 407
8.5 Container ... 409
8.5.1 Windows-Container ... 411
8.5.2 Hyper-V-Container ... 412

9 Dateiserver 413

9.1 Grundlagen des Dateisystems ... 413
9.1.1 Datenträger und Volumes ... 413
9.1.2 iSCSI ... 421
9.1.3 Schattenkopien ... 424
9.1.4 Freigaben ... 427
9.1.5 NTFS und Freigaben-Berechtigungen ... 432
9.1.6 Offlinedateien ... 439
9.1.7 Datendeduplizierung ... 442
9.2 Distributed File System (DFS) ... 444
9.2.1 DFS-N (Distributed File System Namespace) ... 444
9.2.2 DFS-R (Distributed File System Replication) ... 449
9.3 Hochverfügbarkeit (HA-Anforderungen) ... 453
9.4 Neuerungen in Windows Server 2019: Server Storage Migration Service ... 455

10 Verwaltung 459

10.1 Windows Admin Center (WAC) 459
10.1.1 Bereitstellungsszenarien 460
10.1.2 Voraussetzungen 462
10.1.3 Die Installation des Windows Admin Centers vorbereiten 463
10.1.4 Windows Admin Center installieren 466
10.1.5 Für Hochverfügbarkeit sorgen 469
10.1.6 Einstellungen des Windows Admin Centers 472
10.1.7 Berechtigungen konfigurieren 475
10.1.8 Erweiterungen 477
10.1.9 Systeme verwalten 481

10.2 Server-Manager 498
10.2.1 Lokalen Server verwalten 498
10.2.2 Servergruppen erstellen 500
10.2.3 Remote-Server verwalten 502

10.3 Remote Server Administration Tools (RSAT) 502
10.3.1 Installation auf Windows 10 503

10.4 PowerShell 507
10.4.1 Anforderungen 508
10.4.2 Beispiele für die Verwaltung 509

10.5 WinRM und WinRS 511
10.5.1 Windows Remote Management (WinRM) 511
10.5.2 Windows Remote Shell (WinRS) 513

10.6 Windows Server-Sicherung 514
10.6.1 Die Windows Server-Sicherung installieren 515
10.6.2 Backup-Jobs erstellen 516
10.6.3 Windows Server-Sicherung auf Remote-Servern 521
10.6.4 Einzelne Dateien wiederherstellen 523
10.6.5 Recovery-Medium nutzen 526

11 Windows PowerShell 531

11.1 Windows PowerShell und PowerShell Core 531

11.2 Grundlagen zur PowerShell 541
11.2.1 Aufbau der PowerShell-Cmdlets 543
11.2.2 Skripte ausführen 545

11.2.3 Offline-Aktualisierung der PowerShell und der Hilfedateien 546

11.3 Sicherheit rund um die PowerShell 547
11.3.1 Ausführungsrichtlinien (Execution Policies) 548
11.3.2 Die PowerShell remote ausführen 550
11.3.3 Überwachung der PowerShell 553

11.4 Beispiele für die Automatisierung 555

11.5 Just enough Administration (JEA) 559
11.5.1 Einsatzszenarien 559
11.5.2 Konfiguration und Verwendung 559

11.6 Windows PowerShell Web Access 565

12 Migration verschiedener Serverdienste auf Windows Server 2019 567

12.1 Einen Read-only-Domain-Controller (RODC) löschen 567
12.1.1 Einen produktiven und erreichbaren RODC aus der Domäne entfernen 567
12.1.2 Einen RODC entfernen, der kompromittiert wurde bzw. einer Gefahr ausgesetzt war 568

12.2 Migration von AD-Objekten aus einem Active Directory in ein anderes Active Directory 570
12.2.1 Installation von ADMT auf einem Windows Server 2012 R2 570
12.2.2 ADMT für die Nutzermigration verwenden 571

12.3 Upgrade eines Active Directory von Windows Server 2016 auf Windows Server 2019 580

12.4 Migration eines DHCP-Servers 586
12.4.1 Migration des DHCP-Servers auf klassische Weise 586
12.4.2 Migration des DHCP-Server mithilfe des Failover-Features 586

12.5 Migration eines Druckerservers 593
12.5.1 Migration der vorhandenen Drucker vom alten Druckerserver mithilfe des Assistenten 593
12.5.2 Migration der gesicherten Drucker auf den neuen Druckerserver mithilfe des Assistenten 595
12.5.3 Anpassung einer eventuell vorhandenen GPO für die Druckerzuweisung 598

12.6 Migration eines Dateiservers 601
12.6.1 Vorbereitungen für die Migration des Dateiservers 601
12.6.2 Daten mithilfe von robocopy auf einen neuen Dateiserver migrieren 602

12.6.3 Daten zwischen virtuellen Dateiservern migrieren ... 603
12.6.4 Weitere Schritte nach der Migration der Daten ... 603
12.6.5 Einen Dateiserver über die Domänen hinaus migrieren ... 604
12.6.6 Dateiserver mit dem Storage Migration Service auf Server 2019 umziehen ... 604

12.7 Migration eines Hyper-V-Servers ... 614
12.7.1 Migration einer virtuellen Maschine durch Exportieren und Importieren ... 615
12.7.2 Migration einer virtuellen Maschine mithilfe der PowerShell ... 620

12.8 Migration eines Failoverclusters ... 622
12.8.1 Migration des Failoverclusters mit neuer Hardware ... 623
12.8.2 Migration eines Failoverclusters auf Windows Server 2019 ohne neue Hardware ... 632

13 Hyper-V 635

13.1 Bereitstellung von Hyper-V ... 635
13.1.1 Hyper-V installieren ... 636
13.1.2 Das Hyper-V-Netzwerk konfigurieren ... 637
13.1.3 Hyper-V konfigurieren ... 648
13.1.4 Virtuelle Maschinen bereitstellen ... 653

13.2 Hochverfügbarkeit herstellen ... 658
13.2.1 Installation des Failoverclusters ... 658
13.2.2 Den Cluster erstellen ... 658
13.2.3 Cluster-Storage ... 663
13.2.4 Das Quorum konfigurieren ... 665
13.2.5 Das Cluster-Netzwerk konfigurieren ... 668
13.2.6 Hochverfügbare virtuelle Maschinen erstellen ... 668

13.3 Replikation für Hyper-V ... 671
13.3.1 Den Replikatserver konfigurieren ... 672
13.3.2 Replikation für virtuelle Maschinen starten ... 674
13.3.3 Die Konfiguration der virtuellen Maschine anpassen ... 676
13.3.4 Testfailover ... 677
13.3.5 Geplante Failovers ... 678
13.3.6 Desasterfall ... 679

13.4 Den Host Guardian Service bereitstellen ... 680
13.4.1 Installation ... 681
13.4.2 Initialisieren des Host Guardian Service ... 682
13.4.3 Den Host Guardian Service für HTTPS konfigurieren ... 683

13.4.4 Redundante Host Guardian Services bereitstellen ... 684
13.4.5 Anpassungen in der Hyper-V-Infrastruktur ... 685

14 Dateidienste 691

14.1 Die Dateiserver-Rolle installieren ... 691
14.1.1 Installation mit dem Server-Manager ... 691
14.1.2 Dateifreigaben anlegen ... 692

14.2 DFS-Namespaces ... 694
14.2.1 DFS installieren ... 694
14.2.2 Basiskonfiguration ... 695
14.2.3 DFS-Ordnerziele erstellen ... 698
14.2.4 Redundanzen der Namespaceserver ... 699

14.3 DFS-Replikation ... 701
14.3.1 DFS-R installieren ... 702
14.3.2 Die Replikation einrichten und konfigurieren ... 702

14.4 Ressourcen-Manager für Dateiserver ... 705
14.4.1 Installation des Ressourcen-Managers ... 707
14.4.2 Kontingente ... 708
14.4.3 Die Dateiprüfungsverwaltung verwenden ... 713

14.5 Dynamische Zugriffssteuerung (Dynamic Access Control, DAC) ... 718

14.6 Hochverfügbare Dateiserver ... 727
14.6.1 Bereitstellung über einen Failovercluster ... 733
14.6.2 Einrichten eines Speicherreplikats ... 741
14.6.3 Einrichten von »direkten Speicherplätzen« (Storage Spaces Direct, S2D) ... 746

15 Internetinformationsdienste-Server (IIS) 753

15.1 Installation der IIS-Rolle ... 753
15.1.1 Installation auf einem Client ... 753
15.1.2 Installation auf einem Serverbetriebssystem ... 757
15.1.3 Remoteverwaltung des IIS ... 767

15.2 Konfiguration des IIS ... 773
15.2.1 Erstellen von Websites und virtuellen Verzeichnissen ... 778

15.3 Absichern des Webservers ... 783
15.3.1 Authentifizierungsprotokolle ... 783
15.3.2 Einsatz von SSL ... 784
15.3.3 Überwachung und Auditing ... 789
15.4 Sichern und Wiederherstellen ... 790
15.5 Hochverfügbarkeit ... 792

16 PKI und Zertifizierungsstellen 795

16.1 Was ist eine PKI? ... 795
16.1.1 Zertifikate ... 796
16.1.2 Verschlüsselung und Signatur ... 796
16.2 Aufbau einer CA-Infrastruktur ... 803
16.2.1 Installation der Rolle ... 811
16.2.2 Alleinstehende »Offline« Root-CA ... 815
16.2.3 Untergeordnete Zertifizierungsstelle als »Online«-Sub-CA ... 832
16.3 Zertifikate verteilen und verwenden ... 838
16.3.1 Verteilen von Zertifikaten an »Clients« ... 839
16.3.2 Remotedesktopdienste ... 841
16.3.3 Webserver ... 843
16.3.4 Clients ... 848
16.3.5 Codesignatur ... 849
16.4 Überwachung und Troubleshooting der Zertifikatdienste ... 853

17 Patchmanagement mit WSUS 859

17.1 Einführung ... 859
17.1.1 Patching in der Windows-Welt ... 859
17.1.2 Geschichte von WSUS ... 860
17.1.3 Patch Tuesday ... 860
17.1.4 Best Practices für das Patching ... 861
17.1.5 Begriffe im Microsoft-WSUS-Umfeld ... 863
17.2 Eine WSUS-Installation planen ... 865
17.2.1 Systemvoraussetzungen ... 866
17.2.2 Bereitstellungsoptionen ... 867
17.2.3 Installationsoptionen ... 869

17.3 Installation und Konfiguration von WSUS-Server ... 870
17.3.1 Konfigurationsassistent ... 873
17.3.2 Den Abruf von Updates über WSUS konfigurieren ... 881
17.3.3 Reporting-Funktionalität aktivieren ... 884
17.4 Die Administration des WSUS-Servers ... 884
17.4.1 Die WSUS-Konfigurationskonsole ... 884
17.4.2 Der WSUS-Webservice ... 894
17.4.3 Updates freigeben ... 895
17.4.4 Computer-Reports ... 897
17.4.5 Erstellen von zeitgesteuerten Update-Phasen ... 899
17.4.6 Vom Netzwerk getrennte WSUS-Server ... 903
17.4.7 Verschieben des WSUS-Repositorys ... 904
17.5 Automatisierung ... 905
17.5.1 E-Mail-Benachrichtigungen ... 905
17.5.2 Installation und Konfiguration mit der PowerShell ... 906
17.5.3 WSUS-Automatisierung mit der Kommandozeile ... 908

18 Remotedesktopdienste 913

18.1 Remotedesktopdienste vs. RemoteAdminMode ... 914
18.1.1 Remotedesktop aktivieren ... 919
18.1.2 Installation der einzelnen Rollendienste ... 923
18.1.3 Bereitstellung einer Remotedesktop-Umgebung ... 926
18.2 Eine Sammlung von Anwendungen bereitstellen ... 934
18.2.1 Erstellen einer RD-Sammlung ... 935
18.2.2 RemoteApps verwenden ... 940
18.2.3 Den HTML5-Webclient verwenden ... 947
18.3 Absichern einer Remotedesktop-Umgebung ... 951
18.3.1 Einsatz von Zertifikaten ... 951
18.3.2 Verwaltung der Umgebung mithilfe von Gruppenrichtlinien ... 956
18.3.3 Ein RD-Gateway verwenden ... 960
18.3.4 Überwachung und Troubleshooting ... 967
18.3.5 Restricted Admin Mode ... 969
18.3.6 Remote Credential Guard ... 970
18.4 Sonstige Konfigurationen ... 971
18.4.1 Implementieren eines RD-Lizenzservers ... 971
18.4.2 Aktivieren der Kennwortwechselfunktion ... 977

19 Virtuelles privates Netzwerk und Netzwerkrichtlinienserver 981

19.1 VPN-Zugang 981
19.1.1 Einrichten des VPN-Servers 981
19.1.2 VPN-Protokolle 1003
19.1.3 Konfiguration des VPN-Servers 1007
19.1.4 Konfiguration der Clientverbindungen 1008
19.1.5 Troubleshooting 1011

19.2 DirectAccess einrichten 1013
19.2.1 Bereitstellen der Infrastruktur 1014
19.2.2 Tunnelprotokolle für DirectAccess 1017

19.3 NAT einrichten 1018

19.4 Netzwerkrichtlinienserver 1022
19.4.1 Einrichtung und Protokolle 1024
19.4.2 RADIUS-Proxy-Server 1032
19.4.3 Das Regelwerk einrichten 1034
19.4.4 Protokollierung und Überwachung 1038

19.5 Den Netzwerkzugriff absichern 1041
19.5.1 Konfiguration der Clients 1042
19.5.2 Konfiguration der Switches 1046
19.5.3 Konfiguration des NPS 1051
19.5.4 Protokollierung und Troubleshooting 1056

20 Integration in Azure 1059

20.1 Hybride Szenarien 1059

20.2 Azure Active Directory 1060
20.2.1 Was ist Azure Active Directory? 1060
20.2.2 Was sind die Azure Active Directory Domain Services? 1061
20.2.3 Was unterscheidet das Active Directory in Windows Server vom Azure Active Directory? 1063
20.2.4 Systemvoraussetzungen für Azure Active Directory 1064
20.2.5 Azure Active Directory initial konfigurieren 1066
20.2.6 Azure AD anpassen 1068
20.2.7 Umsetzung des Zugriffs für hybride Identitäten 1075

20.3 Azure Active Directory Connect installieren 1082

20.4 AD FS-Lab-Installation 1096
20.4.1 Entwurf und Planung einer produktiven AD FS-Umgebung 1109

20.5 Erweitertes Monitoring 1109

20.6 Ausblick: Datacenter-Erweiterung 1115

21 Troubleshooting im Windows Server 2019 1117

21.1 Die Windows-Ereignisanzeige 1117
21.1.1 Konfiguration der Log-Eigenschaften 1124
21.1.2 Eine Überwachung einrichten 1127
21.1.3 Verwenden des Windows Admin Centers 1131

21.2 Die Leistungsüberwachung 1132
21.2.1 Ressourcenmonitor 1137
21.2.2 Leistungsindikatoren und die »üblichen Verdächtigen« 1139
21.2.3 CPU 1142
21.2.4 Arbeitsspeicher 1144
21.2.5 Datenträger 1145
21.2.6 Netzwerk 1146
21.2.7 Datensammlersätze 1147

21.3 Erstellen und Auswerten eines Startvorgangs 1149

21.4 Erstellen und Lesen eines Netzwerktraces 1152
21.4.1 Beziehen einer IP-Adresskonfiguration 1157
21.4.2 Anmeldung eines Benutzers an einem System 1159
21.4.3 Zugriff auf einen Webdienst 1161

21.5 Debugging 1162
21.5.1 Aktivieren der zusätzlichen Protokollierungsoptionen 1163
21.5.2 Erzeugen und Prüfen von Memory-Dumps 1165

22 Security in und mit Windows Server 2019 1171

22.1 Sicherheitsprinzipien 1171
22.1.1 Protect, Detect, Respond 1171
22.1.2 Das Least-Privilege-Prinzip 1172

22.1.3 Berechtigungssysteme innerhalb von Windows ... 1173
22.1.4 Stellenwert von Identitäten ... 1174
22.1.5 Härtung von Systemeinstellungen und Anwendungen ... 1176
22.1.6 Das Clean-Source-Prinzip ... 1177
22.1.7 Trusted Platform Modul, UEFI Secure Boot und virtualisierungsbasierte Sicherheit ... 1179

22.2 Tier-Modell ... 1183
22.2.1 Pass the Hash und Pass the Ticket ... 1183
22.2.2 Schutz von privilegierten Usern durch ein Ebenenmodell ... 1183
22.2.3 Logon-Beschränkungen ... 1188
22.2.4 Security Baselines anwenden ... 1192
22.2.5 Protected Users ... 1197
22.2.6 Organisationseinheiten (OUs) und Delegationen erstellen ... 1199

22.3 Praxisbeispiele, mit denen Sie die Sicherheit in Windows Server 2019 erhöhen ... 1203
22.3.1 Installation und Konfiguration von LAPS ... 1203
22.3.2 Windows Event Forwarding zur Zentralisierung von Log-Informationen ... 1216
22.3.3 Die Verwendung von Standardgruppen einschränken ... 1226
22.3.4 Gruppenverwaltete Dienstkonten ... 1227
22.3.5 Security Center in Windows Server 2019 ... 1229

22.4 Erweiterte Maßnahmen zum Schutz von Windows-Umgebungen ... 1232
22.4.1 Sicherer Zugriff auf Windows Server 2019 durch Privilege Access Workstations ... 1232
22.4.2 Authentication Policys und Silos ... 1234
22.4.3 Ausblick auf Red Forest ... 1239
22.4.4 Ausblick: Microsoft Advanced Threat Analytics ... 1242

Glossar ... 1247
Index ... 1271