Windows Server 2012

Erweiterte Netzwerk-administration

Martin Dausch

1. Ausgabe, April 2013

W2012EN

HERDT

4 Router einrichten

In diesem Kapitel erfahren Sie

- wie Sie LAN-Router unter Windows Server 2012 einrichten
- wie Sie virtuelle Netze mit Hyper-V konfigurieren
- wie Sie Routen hinzufügen
- wie Sie eine Regel der Windows-Firewall definieren
- wie Sie Routing im Netzwerk überprüfen

Voraussetzungen

- Grundlagen von Netzwerkprotokollen
- Grundkenntnisse in Netzwerkkonfiguration unter Windows Server 2012
- Grundkenntnisse in Hyper-V 2.0

4.1 Router planen

Standorte und Server in der Testumgebung

In der Testumgebung sollen zwei Standorte eingerichtet werden, Berlin und Regensburg. Diese sollen jeweils über einen Domänencontroller mit zusätzlichen Netzwerkdiensten und einen Fileserver verfügen, der außerdem die Funktion des Routers übernimmt. Zusätzlich werden für die Konfiguration drei Netzwerke benötigt. Ein lokales Netzwerk für die jeweiligen Standorte und eines, um die beiden Standorte miteinander zu verbinden.

In der Praxis würde man aus Kosten- und Effizienzgründen sicherlich eher einen Hardware-Router einsetzen, als diese Aufgabe mit Windows-Server-Betriebssystemen zu lösen. Die Kosten für einen Server, die Effektivität beim Routing und Sicherheitserwägungen sprächen gegen eine solche Softwarelösung. Dennoch sollten Sie die Möglichkeiten kennen, Routing mit Windows-Bordmitteln einzurichten.

4.2 Virtuelle Testumgebung einrichten

Testumgebung übernehmen

Im Folgenden wird davon ausgegangen, dass Sie die Testumgebung aus dem HERDT-Buch *Windows Server 2012 - Netzwerkadministration* nachgestellt haben. Aus der alten Testumgebung können Sie die Server *B-DC01* und *B-FS01* übernehmen. Da es beim Umbenennen von DCs zu unerwarteten Problemen kommen kann, sollten Sie den Server *B-DC02* nicht einfach umbenennen. Nehmen Sie stattdessen den sicheren Weg, bei dem Sie zuerst den zweiten Domänencontroller zu einem normalen Mitgliedsserver herabstufen und ihn aus der Domäne entlassen. Damit haben Sie dafür gesorgt, dass das Active Directory weiterhin intakt ist, auch wenn es den Server *B-DC02* nicht mehr gibt.

Zweiten DC herabstufen und aus der Domäne entfernen

Das aus früheren Server-Versionen bekannte Kommandozeilentool *DCPromo* kann auch bei Server 2012 noch verwendet werden, allerdings empfiehlt Microsoft den Weg über einen Assistenten. Sie können einen DC herunterstufen, indem Sie die Serverrolle *AD-Domänendienste* entfernen.

Domänencontroller entfernen

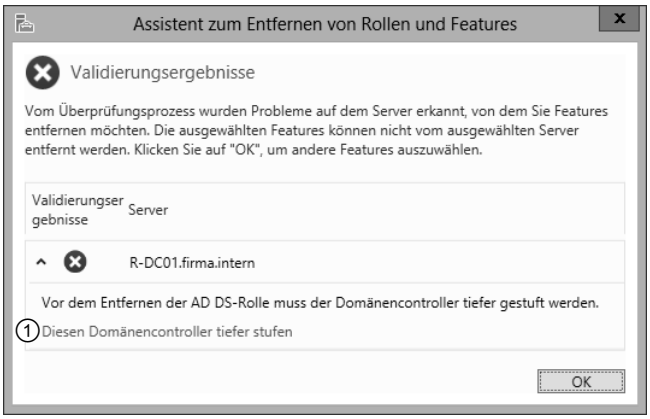
Um einen Domänencontroller stillzulegen, wird der Assistent zum Entfernen von Rollen und Features verwendet.

- Klicken Sie im Server-Manager auf *Verwalten - Rollen und Funktionen entfernen*.

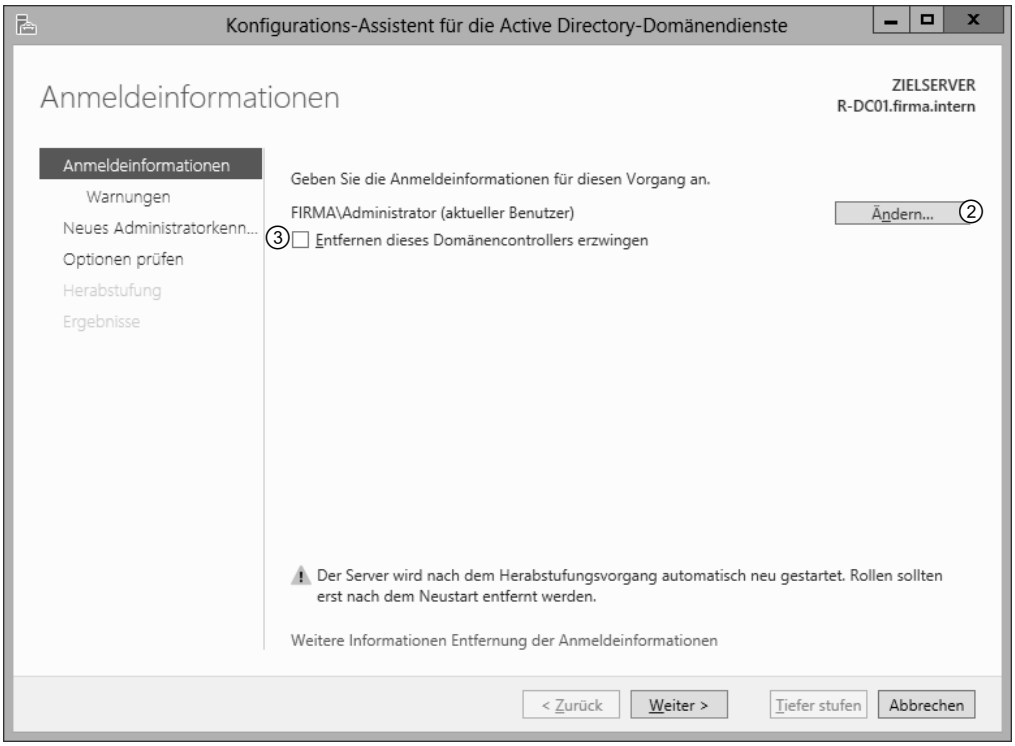
  Es öffnet sich der Assistent zum Entfernen von Rollen und Features.
- Wählen Sie in der Serverauswahl den Server aus und klicken Sie auf *Weiter*.
- Deaktivieren Sie die Serverrolle *Active Directory-Domänendienste* und bestätigen Sie die Entfernung der zugehörigen Features.

  Nach einer Prüfung erscheint eine Fehlermeldung, die besagt, dass der Server erst tiefergestuft werden muss.
- Klicken Sie auf den Link *Diesen Domänencontroller tiefer stufen* ①.

  Der *Konfigurations-Assistent für die Active Directory-Domänendienste* wird geöffnet.



Der DC muss tiefergestuft werden, bevor das AD entfernt werden kann



Anmeldeinformationen prüfen und das Entfernen erzwingen

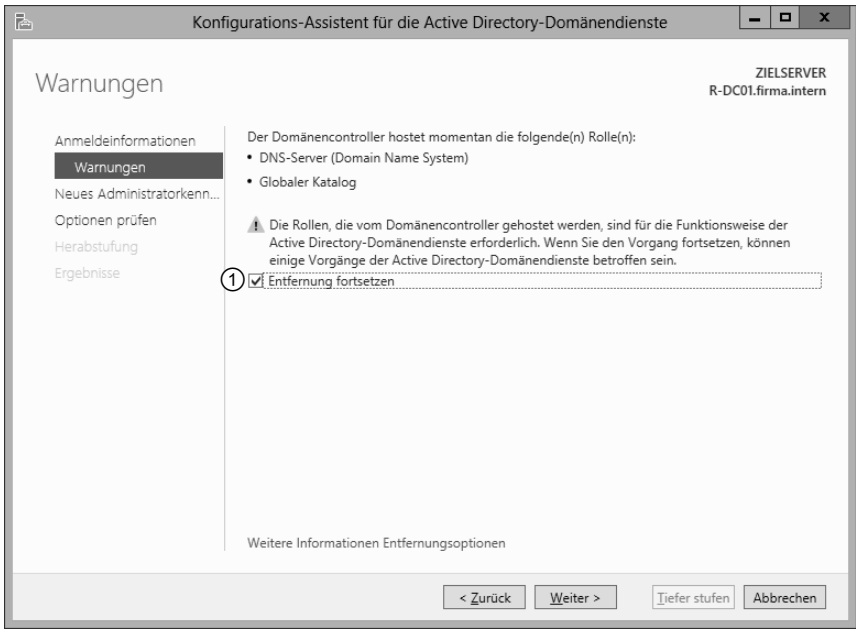
- Überprüfen Sie, ob die Anmeldeinformationen korrekt sind, und ändern Sie sie gegebenenfalls ②.

Bei Problemen beim Entfernen des letzten DCs einer Domäne können Sie die Option *Entfernen dieses Domänencontrollers erzwingen* ③ aktivieren, ansonsten sollten Sie diese Option nur in Notfällen verwenden.

Das Erzwingen entspricht dem von früher bekannten `dcpromo /forceremoval`. Dabei wird zwar der DC vom Server entfernt, nicht jedoch aus dem Active Directory, was zu zahlreichen Problemen führt. In einem solchen Fall können die verwaisten Einträge in der Konsole *AD-Benutzer und Computer*, dem Kommandozeilentool NTDSUtil oder einem Skript entfernen. Eine Anleitung dazu finden Sie unter *http://technet.microsoft.com/en-us/library/cc816907%28WS.10%29.aspx*.

Auf der Seite *Warnungen* werden alle wichtigen Rollen im Active Directory angezeigt, die der DC innerhalb der Domäne innehat.

- Lesen Sie sich die Auflistung durch und überlegen Sie bei jedem Punkt, ob Sie an alle Auswirkungen gedacht haben, die eine Entfernung nach sich zieht.
- Um den Vorgang fortzusetzen, müssen Sie die Option *Entfernung fortsetzen* ① aktivieren und auf *Weiter* klicken.



Entfernung des DCs mit allen Rollen im AD bestätigen

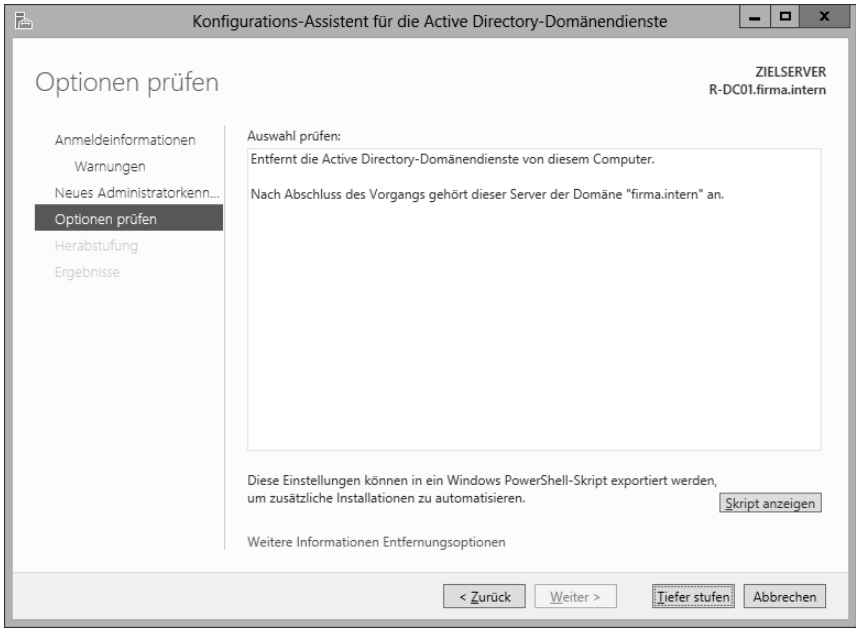
Auf der Seite *Entfernungsoptionen* können Sie auswählen, ob alle DNS-Zonen und alle Anwendungspartitionen des Active Directory entfernt werden sollen.

- Klicken Sie auf *Weiter*.
- Geben Sie auf der nächsten Seite zweimal ein neues Kennwort für den lokalen Administrator des Computers ein und klicken Sie auf *Weiter.*

Auf der Seite *Optionen prüfen* wird nochmals zusammengefasst, dass die Domänendienste entfernt werden sollen und dass der Server nach der Herabstufung weiterhin Mitglied der Domäne ist. Der letzte DC einer Domäne wird zu einem Mitglied einer Arbeitsgruppe.

- Klicken Sie auf *Tiefer stufen*, um die Deinstallation des DCs auszuführen.

Nach einem Neustart ist der ehemalige DC nur noch ein Mitgliedsserver. Sicherheitshalber sollten Sie ihn nun auch noch aus der Domäne entfernen.



Letzte Bestätigung und Ausführen der Deinstallation

Computer aus Domäne entlassen

- ▶ Klicken Sie im Server-Manager auf der Seite *Lokaler Server* auf den Domänennamen.

oder Öffnen Sie mit ⊞ Pause die Systeminformationen und klicken Sie auf *Einstellungen ändern*.

- ▶ Klicken Sie in den erweiterten Systemeigenschaften auf dem Register *Computername* auf *Ändern*.
- ▶ Aktivieren Sie die Option *Arbeitsgruppe*, wählen Sie einen Namen für die Gruppe und klicken Sie auf *OK*.

Nach einem Neustart ist der Computer nicht mehr Mitglied der Domäne und im Active Directory ordnungsgemäß abgemeldet.

Hinweis zu Testumgebungen

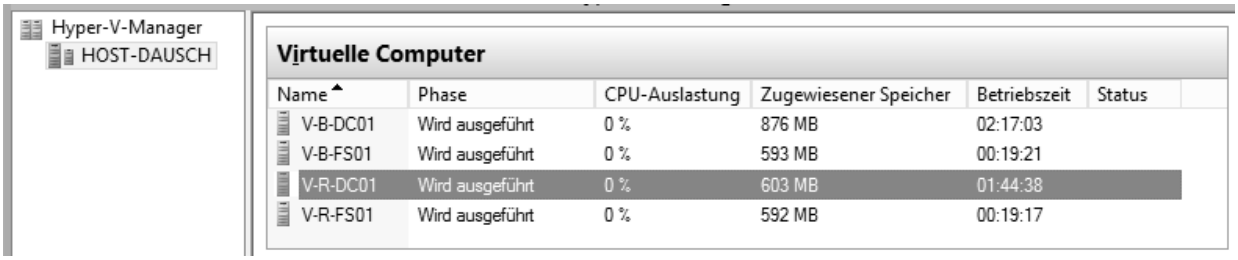
Haben Sie etwas Geduld, nachdem Sie den DC herabgestuft haben, denn es kann einige Minuten dauern, bis die Änderungen im Active Directory repliziert wurden. In der Testumgebung aus dem Vorgängerbuch gab es nur einen Standort, daher sollte die Änderung spätestens nach 5 Minuten im AD bekannt sein. Bei mehreren Standorten kann die Replikation erheblich länger dauern (in manchen Fällen mehrere Stunden). Warten Sie einige Minuten, bevor Sie nach dem Neustart den Computer anderweitig einsetzen.

Neuinstallation ist sicherer als Umbenennung

Prinzipiell könnten Sie nun den Server *B-DC02* in *R-DC01* umbenennen und ihn wieder zum DC machen, davon ist allerdings im Interesse einer sauberen Testumgebung abzuraten. Empfehlenswert ist, eine neue VM zu erstellen und Windows neu zu installieren. Damit ersparen Sie sich möglicherweise zeitaufwendige Fehlersuchen, die durch fehlerhafte DNS- und Active Directory-Einträge verursacht werden.

Beachten Sie, dass Sie den bestehenden Server *B-DC01* nur dann weiterverwenden können, wenn Sie vorher den zweiten Domänencontroller *B-DC02* ordnungsgemäß zu einem normalen Mitgliedsserver heruntergestuft und am besten ganz aus der Domäne herausgenommen haben. Anderenfalls haben Sie später mit verwaisten Einträgen im Active Directory und DNS zu kämpfen.

Falls auf dem Hostcomputer der Festplattenplatz zur Neige geht, können Sie Speicherplatz zurückgewinnen, indem Sie nicht mehr benötigte VMs (z. B. *B-DC02*) und einige Zwischen-Snapshots löschen. Vergessen Sie nicht, anschließend auch den Papierkorb zu leeren. Weiterer Speicherplatz lässt sich durch das Löschen von Systemwiederherstellungspunkten und durch eine Datenträger- und Systemdatenbereinigung zurückgewinnen. Dies gilt sowohl für den Host als auch für die VMs.



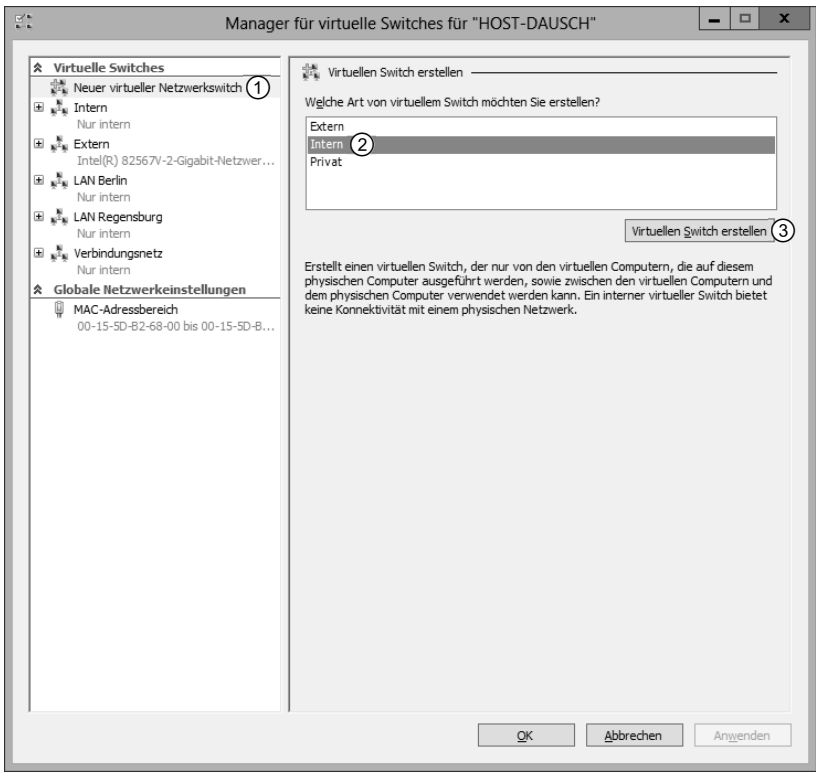
Server in der erweiterten Testumgebung

Sie benötigen insgesamt vier virtuelle Server, je einen DC und ein Fileserver/Router pro Standort. Jede VM benötigt insgesamt etwa 30 GB Festplattenspeicher. Berücksichtigen Sie dies bei der Wahl des Speicherorts für die VMs und die virtuellen Festplattendateien. Vor der Einrichtung der VMs und der Windows-Installation ist es sinnvoll, im Hyper-V-Manager die virtuellen Netzwerke einzurichten wie im folgenden Abschnitt beschrieben.

Virtuelle Netzwerke einrichten

Als Erstes sollten Sie auf dem Hostserver drei virtuelle interne Netzwerkswitches installieren, und zwar ein lokales Netz für jeden Standort sowie ein Verbindungsnetzwerk zwischen den Standorten. Dieses Verbindungsnetz entspricht einem WAN bzw. dem Internet. Sie benötigen außerdem einen externen Netzwerkswitch für die Windows-Aktivierung der virtuellen Server. Gehen Sie wie folgt vor:

- Klicken Sie im Tools-Menü des Server-Managers auf *Hyper-V-Manager* oder geben Sie im Startbildschirm `Hyper` ein und wählen Sie *Hyper-V-Manager*.
- Markieren Sie im Hyper-V-Manager den Hostserver.
- Wählen Sie unter *Aktionen* den *Manager für virtuelle Switches*.
- Klicken Sie im Manager für virtuelle Netzwerke auf *Neuer virtueller Netzwerkswitch* ①, markieren Sie *Intern* ② und klicken Sie auf *Virtuellen Switch erstellen* ③.
- Tragen Sie unter *Namen* `LAN Berlin` ein und bestätigen Sie mit *OK*.
- Wiederholen Sie die letzten Schritte zweimal für `LAN Regensburg` und `Verbindungsnetz`.
- Falls noch nicht vorhanden, erstellen Sie auf die gleiche Weise einen externen Switch und nennen Sie ihn `Extern`.



Virtuelle Netzwerke verwalten

Wenn Sie aus der Testumgebung des Vorgängerbuchs über einen weiteren Switch *Intern* verfügen, sollten Sie ihn erst entfernen, wenn er von keiner VM mehr verwendet wird. Anderenfalls lassen sich die entsprechenden VMs nicht mehr starten. Benennen Sie keine Switches um, da dies in einigen Fällen zu merkwürdigen Fehlern in der virtuellen Netzwerkumgebung führt.

Durch den ausgewählten Netzwerktyp *Intern* haben Sie sichergestellt, dass Verbindungen nur zwischen den virtuellen Systemen untereinander und dem Hostserver möglich sind. So können alle Schulungsteilnehmer die gleichen IP-Adressen verwenden, da die virtuellen Server nicht über Hostgrenzen im physischen Netzwerk miteinander kommunizieren können.

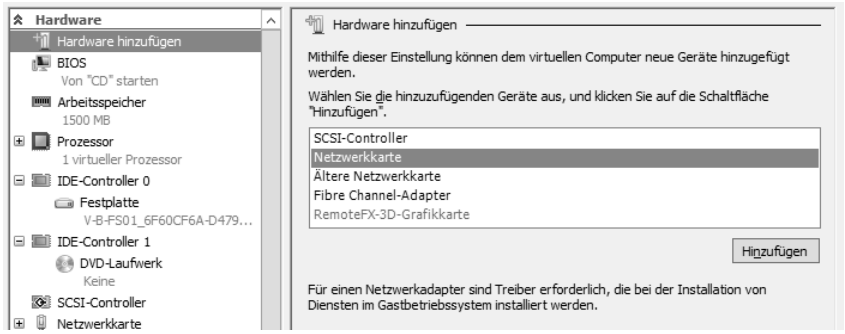
Installieren Sie nun alle vier benötigten Server.

- Verwenden Sie für die VMs die Namen *V-B-DC01*, *V-B-FS01*, *V-R-DC01* und *V-R-FS01*.
- Übernehmen Sie die Standardgröße für die VHDX-Datei.
- Wählen Sie als Netzwerkverbindung *Extern*, falls die virtuellen Server automatisch über DHCP eine Netzwerkadresse erhalten dürfen und sich sofort mit dem Internet verbinden sollen. Wählen Sie *Nicht verbunden*, um eine automatische Verbindung zu verhindern.

Beachten Sie bei der Einrichtung externer Verbindungen die Vorgaben des Schulungsleiters und des zuständigen Netzwerkbetreuers.

Zweite virtuelle Netzwerkkarte für das Routing hinzufügen

- Bevor Sie die virtuellen Server *V-B-FS01* und *V-R-FS01* zum ersten Mal starten, klicken Sie im Hyper-V-Manager mit der rechten Maustaste darauf und wählen Sie *Einstellungen*.
- Klicken Sie in den Einstellungen der VM auf *Hardware hinzufügen* und wählen Sie *Netzwerkkarte*. Klicken Sie auf *Hinzufügen*.



Bei ausgeschalteter VM eine zweite Netzwerkkarte hinzufügen

- Wählen Sie für den zweiten virtuellen Switch zunächst *Nicht verbunden* aus, um später bei der Vergabe der IP-Adressen Verwechslungen der Netzwerke zu vermeiden. Nachdem Windows aktiviert wurde, können Sie die erste Netzwerkverbindung auf das entsprechende LAN Berlin oder LAN Regensburg umstellen und die IP-Adresse `192.168.1.1` bzw. `192.168.2.1` zuweisen. Erst danach stellen Sie den zweiten virtuellen Switch auf *Verbindungsnetz* und weisen die Adressen `10.0.10.1` und `10.0.10.2` zu.

Alle virtuellen Server benötigen anfangs für kurze Zeit einen Internetzugang, damit sich Windows automatisch aktivieren kann. Weisen Sie daher bei der Erstellung der VM die Netzwerkverbindung *Extern* zu. Falls in Ihrer realen Netzwerkumgebung DHCP verfügbar ist, wird bereits während der Installation eine IP-Adresse vergeben und die virtuelle Maschine verfügt über einen funktionierenden Internetzugang. Sobald die Aktivierung erfolgreich war, können Sie das Netzwerk in den Hyper-V-Einstellungen auf das jeweilige LAN umstellen.

IP-Adressen planen

Für die drei Netzwerke benötigen Sie jeweils eindeutige Netzwerkadressen. Da es sich bei der Testumgebung um ein internes virtuelles Netzwerk handelt, kann jeder Kursteilnehmer dieselben IP-Adressen verwenden. Sie müssen sich nur bei einer externen Konfiguration mit dem Kursleiter und anderen Teilnehmern absprechen, um Adresskonflikte zu verhindern. Beachten Sie, dass Windows auf allen virtuellen Maschinen über das Internet aktiviert worden sein muss, bevor die Netzwerkverbindung von extern auf die lokalen LANs und das Verbindungsnetz umgestellt werden kann und die aufgeführten IP-Einstellungen verwendet werden können.

Die IPv6-Einstellungen sind für die Übungen in der Testumgebung optional.

Servername	**IPv4**	**IPv6**
Hostcomputer	Interner Adapter: Verbindungsnetz IP-Adresse: 10.0.10.3 Subnetzmaske: 255.255.255.0 Standardgateway: keines DNS-Server: keiner	Interner Adapter: Verbindungsnetz IP-Adresse: fc01::10:0:10:3 Subnetzpräfixlänge: 64 Standardgateway: keines DNS-Server: keiner
	Externer Adapter: physisches Ethernet IP-Adresse: passend zur Umgebung Subnetzmaske: 255.255.255.0 Standardgateway: z. B. Internetrouter DNS-Server: z. B. Internetrouter	Externer Adapter: physisches Ethernet IP-Adresse: passend zur Umgebung Subnetzpräfixlänge: 64 Standardgateway: z. B. Internetrouter DNS-Server: z. B. Internetrouter

Servername	IPv4	IPv6
B-DC01	Interner Adapter: LAN Berlin IP-Adresse: 192.168.1.2 Subnetzmaske: 255.255.255.0 Standardgateway: 192.168.1.1 DNS-Server: 192.168.1.2	Interner Adapter: LAN Berlin IP-Adresse: fc01::192:168:1:2 Subnetzpräfixlänge: 64 Standardgateway: fc01::192:168:1:1 DNS-Server: fc01::192:168:1:2
B-FS01	Interner Adapter: LAN Berlin IP-Adresse: 192.168.1.1 Subnetzmaske: 255.255.255.0 Standardgateway: keines DNS-Server: 192.168.1.2	Interner Adapter: LAN Berlin IP-Adresse: fc01::192:168:1:1 Subnetzpräfixlänge: 64 Standardgateway: keines DNS-Server: fc01::192:168:1:2
	Externer Adapter: Verbindungsnetz IP-Adresse: 10.0.10.1 Subnetzmaske: 255.255.255.0 Standardgateway: keines DNS-Server: keiner	Externer Adapter: Verbindungsnetz IP-Adresse: fc01::10:0:10:1 Subnetzpräfixlänge: 64 Standardgateway: keines DNS-Server: keiner
R-DC01	Netzwerkadapter: LAN Regensburg IP-Adresse: 192.168.2.2 Subnetzmaske: 255.255.255.0 Standardgateway: 192.168.2.1 DNS-Server: 192.168.2.2	Netzwerkadapter: LAN Regensburg IP-Adresse: fc01::192:168:2:2 Subnetzpräfixlänge: 64 Standardgateway: fc01::192:168:2:1 DNS-Server: fc01::192:168:2:2
R-FS01	Interner Adapter: LAN Regensburg IP-Adresse: 192.168.2.1 Subnetzmaske: 255.255.255.0 Standardgateway: keines DNS-Server: 192.168.2.2	Interner Adapter: LAN Regensburg IP-Adresse: fc01::192:168:2:1 Subnetzpräfixlänge: 64 Standardgateway: keines DNS-Server: fc01::192:168:2:2
	Externer Adapter: Verbindungsnetz IP-Adresse: 10.0.10.2 Subnetzmaske: 255.255.255.0 Standardgateway: keines DNS-Server: keiner	Externer Adapter: Verbindungsnetz IP-Adresse: fc01::10:0:10:2 Subnetzpräfixlänge: 64 Standardgateway: keines DNS-Server: keiner

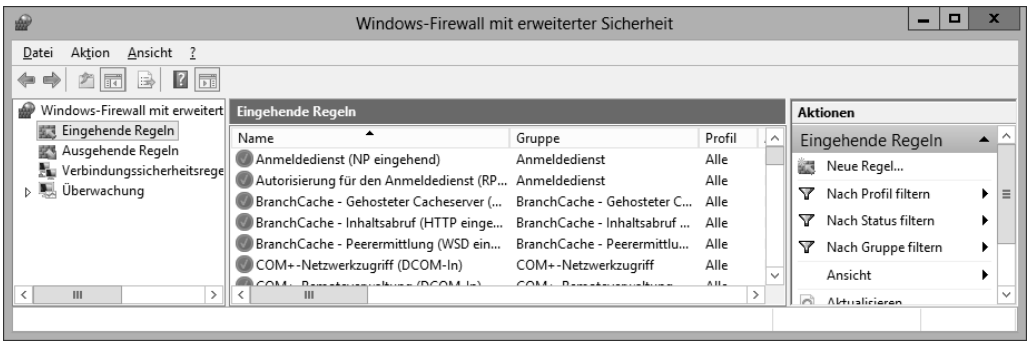
Gegen Ende des Buches wird ein zusätzlicher Windows-8-Client benötigt, den Sie jetzt aber noch nicht einrichten sollten. Die nötigen Einstellungen werden im entsprechenden Kapitel angegeben.

4.3 Firewall konfigurieren

Neue Firewallregel erstellen

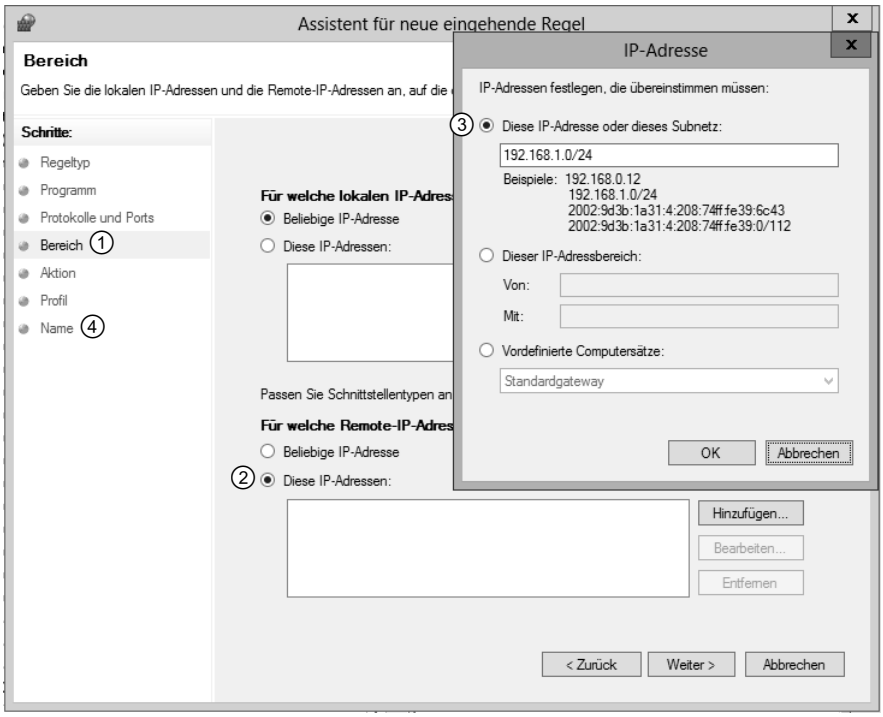
Als nächsten Schritt sollten Sie die Firewall des Routers so konfigurieren, dass Pakete zwischen den Netzwerken der Testumgebung ausgetauscht werden können. Gehen Sie dazu folgendermaßen vor:

- Geben Sie im Startbildschirm `firewall` ein und klicken Sie auf *Windows-Firewall mit erweiterter Sicherheit*. Alternativ können Sie die erweiterten Firewall-Einstellungen auch über das Tools-Menü im Server-Manager oder die Systemsteuerung erreichen.
- Klicken Sie auf *Erweiterte Einstellungen* und dann auf den Knoten *Eingehende Regeln*.



Firewall überprüfen

- Klicken Sie nun unter *Aktionen* auf *Neue Regel*.
  Der Assistent für neue eingehende Regeln wird geöffnet.

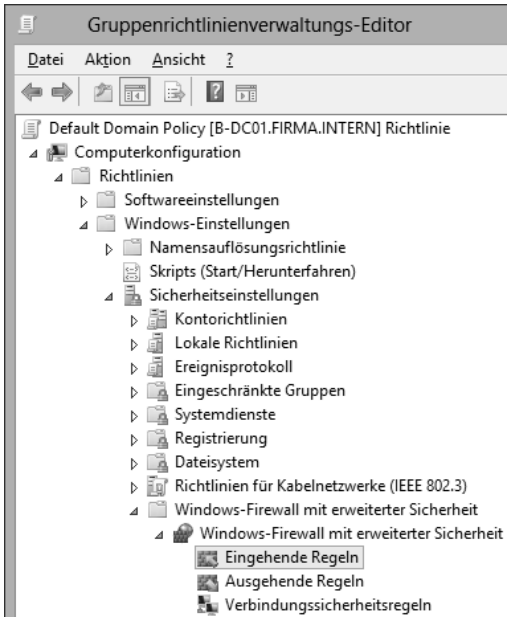


Neue Firewall-Regel erstellen

- Wählen Sie den Regeltyp *Benutzerdefiniert* und klicken Sie auf *Bereich* ①.
- Aktivieren Sie bei Remote-IP-Adressen *Diese IP-Adressen* ② und klicken Sie auf *Hinzufügen*.
- Geben Sie unter *Diese IP-Adresse oder dieses Subnetz* ③ die Netzwerkadresse des Standortes *Berlin* an (192.168.1.0/24) und bestätigen Sie mit *OK*.
- Fügen Sie auf gleiche Weise das IPv6-Subnetz (fc01::192:168:1:0/64) hinzu.
- Erstellen Sie weitere eingehende Regeln für das LAN des Standortes *Regensburg* (192.168.2.0/24 und fc01::192:168:2:0/64) und für das Verbindungsnetz (10.0.10.0/24 und fc01::10:0:10:0/64) und klicken Sie auf *Weiter*.
- Stellen Sie sicher, dass die Verbindungen zugelassen sind, und klicken Sie auf *Name* ④.
- Geben Sie einen aussagekräftigen Namen für die neue Regel ein, z. B. `Routing Test-umgebung`, und betätigen Sie *Fertig stellen*.

Wiederholen Sie die Konfiguration auf allen anderen Servern. Hier erstellen Sie ebenfalls eingehende Regeln für das LAN Berlin und das LAN Regensburg sowie für das Verbindungsnetz.

Firewall-Einstellungen über Gruppenrichtlinien



Die virtuellen Server sind zu diesem Zeitpunkt noch nicht miteinander und mit der Domäne verbunden. Für die Firewall-Einstellung können Sie z. B. die Default Domain Policy verwenden. In der Gruppenrichtlinienverwaltung können Sie die Default Domain Policy über einen Rechtsklick bearbeiten. Der Gruppenrichtlinienverwaltungs-Editor wird geöffnet. Sie finden die Einstellungen für die erweiterte Windows-Firewall unter *Computerkonfiguration - Richtlinien - Softwareeinstellungen - Windows-Einstellungen - Sicherheitseinstellungen - Windows-Firewall mit erweiterter Sicherheit*. Hier können Sie wie oben beschrieben eine neue eingehende oder ausgehende Regel erstellen, die anschließend von jedem Computer der Domäne angewendet wird.

Wenn Sie möchten, können Sie dieses Verfahren später nach der erfolgreichen Einrichtung des Routings für die Testumgebung ausprobieren. Die Gruppenrichtlinie könnte z. B. bei der fünften virtuellen Maschine eingesetzt werden, wo nach der Aufnahme in die Domäne automatisch die Firewallregel aktiv wäre.

Firewall über die Kommandozeile konfigurieren

Die Firewall lässt sich auch über die Kommandozeile und das mächtige Netsh-Tool (Network Shell) steuern. Auf diese Weise können Sie z. B. mehrere Regeln in einem Skript sammeln und per E-Mail versenden.

- Öffnen Sie eine Administrator-Eingabeaufforderung und geben Sie `netsh` ↵ und anschließend `advfirewall firewall` ↵ ein.

  Sie befinden sich nun in der Befehlsebene für die erweiterte Firewall. Alternativ können Sie auch jedem Befehl ein `netsh advfirewall firewall` voranstellen.

Im folgenden Beispiel soll eine eingehende Regel (`dir=in`; "dir" bedeutet "direction", also 'Richtung') für ein Programm (Programm.exe) mit dem unter `name` angegebenen Namen erstellt werden. Die Regel soll den Zugriff erlauben (`action=allow`) und sofort aktiv sein (`enable=yes`). Sie soll für die aufgeführten IP-Adressen und Bereiche gelten, die jeweils mit einem Komma abgetrennt sind. In vielen Fällen reicht hier auch die Angabe von `LocalSubnet`. Zum Schluss können Sie optional ein Profil angeben, für das die Regel gelten soll. Wenn unter `profile` nichts angegeben wird, ist die Regel für alle drei Profile (privat, öffentlich und domänenweit) wirksam.

```
netsh advfirewall firewall add rule name="Neue Regel" dir=in action=<allow | block>
program="c:\Programme\Programm.exe" enable=<yes | no>
remoteIP=192.168.1.0/24,192.168.2.1,LocalSubnet profile=<private | public | domain>
```

Über die Parameter `protocol` und `localport` können Sie die Regel auf bestimmte Protokolle oder Ports eingrenzen. Mit den Befehlen `set rule` können Sie eine bestehende Regel verändern, mit `delete rule` löschen Sie sie.

Zu Testzwecken können Sie die Windows-Firewall mit dem Befehl `netsh advfirewall set allprofiles state on | off` komplett ein- oder ausschalten und mit `netsh advfirewall reset` auf die Standardeinstellungen zurücksetzen.

Sie können bestehende Firewall-Einstellungen exportieren, um sie später auf demselben oder anderen Computern zu importieren. Dies erreichen Sie durch die Befehle `netsh advfirewall export "<Pfad zur .wfw-Datei>"` bzw. `netsh advfirewall import <Pfad zur .wfw-Datei>`.

Sie können auch die Firewall-Regeln innerhalb eines Gruppenrichtlinienobjekts erstellen und bearbeiten. Dazu müssen Sie zuerst den Kontext herstellen, indem Sie die Domäne und den Namen des GPOs angeben:

```
netsh advfirewall set store gpo=<Domäne>\<GPO-Name>
```

Anschließend können Sie die Befehle einsetzen wie oben beschrieben.

Firewall über die PowerShell konfigurieren

Die Firewall lässt sich auch über die PowerShell bedienen. Hier können Sie im selben Befehl auch gleich das GPO und die Domäne angeben:

```
New-NetFirewallRule -DisplayName "<Name der Regel>" -Direction <Outbound | Inbound> -
Program "<Programmpfad>" –Protocol <Protokoll> –LocalPort <Portnummer> -Action <Block
| Allow> –PolicyStore <Domäne>\<GPO-Name>
```

Genau wie bei Netsh können Sie einzelne Teile einer bestehenden Regel verändern:

```
Set-NetFirewallRule –DisplayName "<Name der Regel>" -RemoteAddress 192.168.0.2
```

Bei Netsh müssen Sie zwingend den Namen einer Regel kennen und angeben, während Sie mit der PowerShell auf vielfältige Weise nach bestimmten Merkmalen suchen und die Ergebnisse über eine Pipe an den nächsten Befehl übergeben können. Nützliche Informationen zu diesem Thema finden Sie, wenn Sie im TechNet nach den Begriffen `PowerShell` und `Firewall` suchen oder unter *http://technet.microsoft.com/de-de/library/hh831755.aspx.*

4.4 Routing und RAS aktivieren

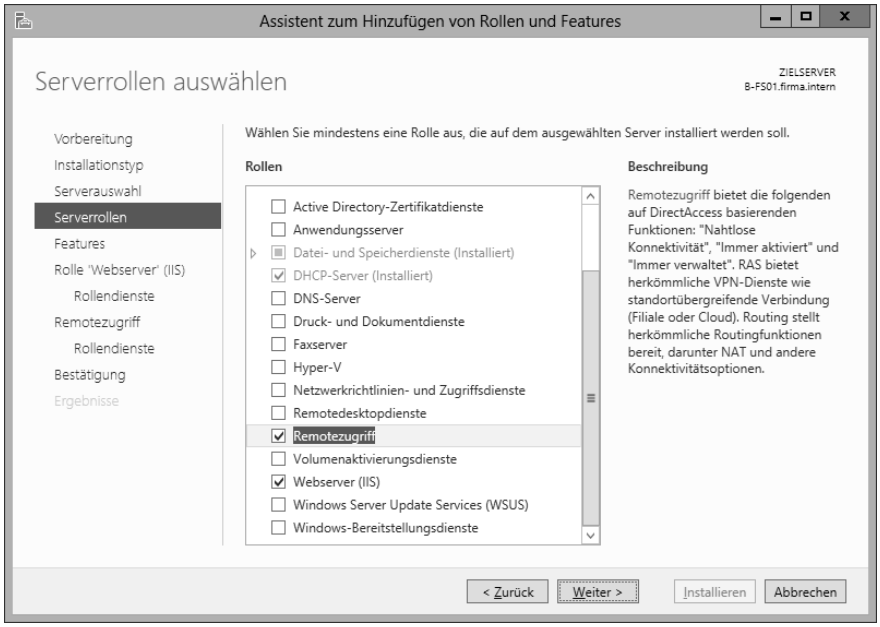
Serverrolle *Remotezugriff* hinzufügen

Für einfaches LAN-Routing wie in der Testumgebung müssen theoretisch keine zusätzlichen Serverrollen oder Features installiert werden, für erweiterte Konfigurationen ist dies jedoch zwingend erforderlich. Im Vergleich zum Vorgänger hat sich bei Windows Server 2012 bei der Verwaltung des Routings einiges verändert. Dies ist darauf zurückzuführen, dass einfaches Routing nur in Ausnahmefällen von einem Windows Server übernommen wird. Solche Aufgaben können effizienter und besser von spezialisierten Hardware-Routern übernommen werden. Routing unter Windows Server 2012 findet fast ausschließlich im Zusammenhang mit VPN-Zugriffen mit DirectAccess und dem Netzwerkzugriffsschutz NAP statt, daher wurden alle beteiligten Mechanismen in der neuen Serverrolle *Remotezugriff* zusammengefasst. Alle dafür notwendigen Serverrollen, Features und Verwaltungstools werden installiert, sobald die Serverrolle *Remotezugriff* hinzugefügt wird.

Für die Konfiguration des Routings über die grafische Benutzeroberfläche ist die Installation der Serverrolle *Remotezugriff* mit allen angegliederten Komponenten zwingend erforderlich. Dazu zählt auch der Webserver. Ohne vollständige Installation ist die RRAS-Konsole nicht verfügbar und in der Computerverwaltung bricht die Konfiguration von RRAS mit einer Fehlermeldung ab, dass DirectAccess nicht verfügbar sei.

- Stellen Sie eine Verbindung mit *B-FS01* her.
- Klicken Sie im Server-Manager auf *Verwalten - Rollen und Features hinzufügen*.
- Aktivieren Sie die Serverrolle *Remotezugriff* und klicken Sie anschließend auf *Features hinzufügen*.

Dadurch werden neben zahlreichen Remoteserver-Verwaltungstools auch die Gruppenrichtlinienverwaltung und der Webserver IIS installiert, die für die Verwendung von DirectAcess benötigt werden.



Hinzufügen der Serverrolle "Remotezugriff"