KAPITEL 6

Einrichten von Netzwerkdiensten und Netzwerkzugriff

Auch das Thema »Einrichten von Netzwerkdiensten und Netzwerkzugriff« der Prüfung 70-417 umfasst nur ein einziges Lernziel, nämlich die Einrichtung von DirectAccess. Dabei handelt es sich um eine verbesserte Alternative zu VPNs, die erstmals in Windows Server 2008 R2 und Windows 7 eingeführt werde. Wenn Sie sich vor der Veröffentlichung von Windows Server 2008 R2 auf Ihre letzte Zertifizierung vorbereitet haben, ist Ihnen diese wichtige neue Technologie womöglich noch nicht vertraut. Doch auch wenn Sie sich mit DirectAccess in Windows Server 2008 R2 auskennen, sollten Sie sich noch einmal damit beschäftigen, da diese Funktion in Windows Server 2012 erheblich geändert wurde.

Lernziele in diesem Kapitel

Lernziel 6.1: Einrichten von DirectAccess

DirectAccess war in Windows Server 2008 R2 und Windows 7 eine viel versprechende Technologie, ließ sich aber nur schwer konfigurieren. In Windows Server 2012 und Windows 8 wurden die Infrastrukturanforderungen für DirectAccess und die Konfiguration vereinfacht und die Funktion erheblich erweitert.

Für die Prüfung 70-417 müssen Sie sich zunächst einmal mit den Prinzipien und Bestandteilen von DirectAccess vertraut machen. Außerdem müssen Sie die Infrastrukturanforderungen für DirectAccess-Clients kennen, die zur Unterstützung verschiedener Funktionen jeweils notwendig sind, und wissen, wie DirecctAccess zu konfigurieren ist.

In diesem Abschnitt geht es um die folgenden Themen:

- Infrastrukturoptionen für DirectAccess
- Einrichten von DirectAccess-Clients
- Einrichten von DirectAccess-Servern
- Einrichten von DirectAccess-Infrastrukturservern

Was ist DirectAccess?

DirectAccess ist eine Technologie für den Remotedauerzugriff auf der Grundlage von IPv6. Damit kann ein Computer von jedem Ort der Welt aus automatisch, sicher und für den Benutzer unsichtbar Verbindung mit einem privaten Unternehmensnetzwerk aufnehmen, sofern er mit dem Internet verbunden ist. Über eine aktive DirectAccess-Verbindung können Remotebenutzer auf Ressourcen in einem Unternehmensnetzwerk zugreifen, als wären sie vor Ort.

DirectAccess überwindet die Einschränkungen von VPNs und bietet die folgenden Vorteile:

- **Daueranbindung** Anders als ein VPN ist eine DirectAccess-Verbindung immer aktiv, sogar schon, bevor sich der erste Benutzer an seinem Computer anmeldet.
- **Nahtlose Anbindung** Für den Benutzer ist die DirectAccess-Verbindung zum Unternehmensnetzwerk völlig unsichtbar. Bis auf eine Verzögerung durch eine langsame Internetverbindung stellt der Benutzer keinen Unterschied zum direkten Anschluss seines Computers an das Firmennetzwerk fest.
- **Beidseitiger Zugriff** Bei DirectAccess hat nicht nur der Remotecomputer Zugriff auf das Intranet des Unternehmens – auch das Intranet kann den Computer erkennen. Das bedeutet, dass der Remotecomputer mit Gruppenrichtlinien und anderen Verwaltungsinstrumenten (z.B. System Center Configuration Manager [SCCM]) verwaltet werden kann, als gehörte er zum internen Netzwerk.

Außerdem bietet DirectAccess die folgenden Sicherheitsmerkmale:

- DirectAccess authentifiziert sowohl den Computer als auch den Benutzer mithilfe von IPsec. Bei Bedarf kann zur Benutzerauthentifizierung auch eine Smartcard verwendet werden.
- DirectAccess greift auch zur Verschlüsselung der Kommunikation über das Internet auf IPsec zurück.

IPv6 und DirectAccess

Eine DirectAccess-Verbindung von einem Remoteclient zu einer internen Ressource besteht aus zwei Abschnitten. In der ersten Hälfte der Verbindung nutzt der DirectAccess-Client immer IPv6, um Kontakt mit dem DirectAccess-Server aufzunehmen, der sich gewöhnlich am Rand (»Edge«) des privaten Netzwerks befindet. Bei Bedarf werden IPv6-Übergangstechnologien verwendet, um diese Verbindung zu unterstützen. Der zweite Abschnitt liegt zwischen dem DirectAccess-Server und der internen Netzwerkressource. Dieser Teil der Verbindung kann über IPv6 ablaufen, aber auch über IPv4 (nur wenn der DirectAccess-Server Windows Server 2012 ausführt und als NAT64/DNS64-Gerät fungiert).

Abbildung 6.1 zeigt die beiden Abschnitte einer DirectAccess-Verbindung zwischen einem Remoteclient und einer internen Netzwerkressource.

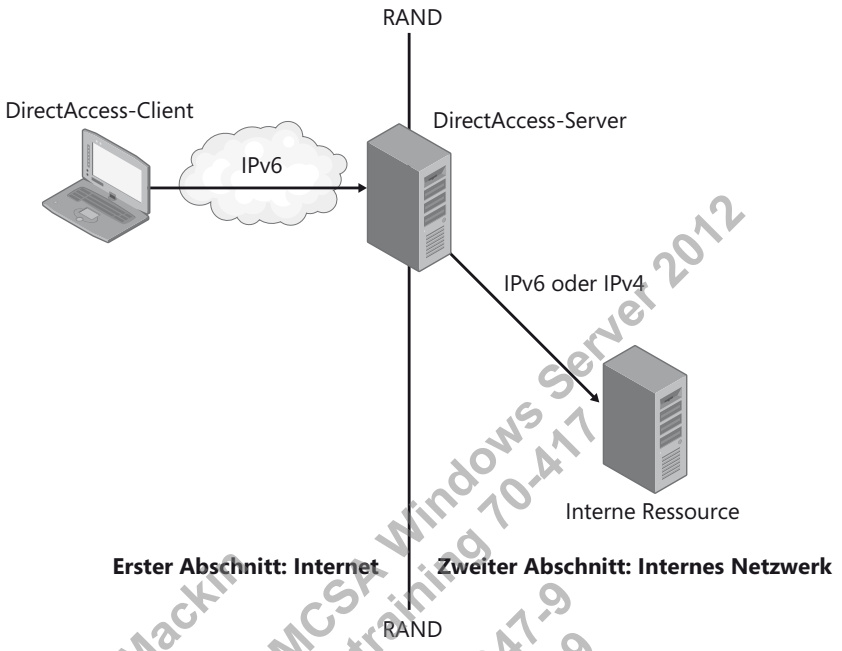

Abbildung 6.1 Eine DirectAccess-Verbindung zu einer internen Ressource

Erster Abschnitt: Vom externen Client zum Rand des privaten Netzwerks

Wenn der DirectAccess-Client eine globale IPv6-Adresse aus seiner Umgebung beziehen kann, erfolgt die Verbindung zum DirectAccess-Server direkt über das IPv6-Internet. Allerdings ist IPv6 in öffentlichen Netzwerken noch nicht weit verbreitet, weshalb zur Einrichtung der IPv6-Verbindung zum DirectAccess-Server drei Übergangstechnologien verwendet werden. Wenn alle drei mithilfe von Gruppenrichtlinien auf dem Client aktiviert sind, wird versucht, sie in der folgenden Reihenfolge anzuwenden:

1. **6to4** Für DirectAccess-Clients mit einer *öffentlichen* IPv4-Adresse kann 6to4 eingesetzt werden, um mit IPv6 über das öffentliche IPv4-Internet Verbindung zum DirectAccess-Server aufzunehmen. Dabei werden IPv6-Daten getunnelt, also in einen IPv4-Header gekapselt. Diese Technik wird als IPv6-über-IPv4 bezeichnet. Für 6to4 müssen alle zwischengeschalteten Router und Firewalls so eingerichtet sein, dass ausgehender Datenverkehr für das Protokoll 41 zugelassen ist. Wenn sich der Client hinter einem NAT-Gerät (Network Address Translation) befindet, kann 6to4 nicht funktionieren.
2. **Teredo** Für DirectAccess-Clients hinter einem NAT-Gerät, die mit einer *privaten* IPv4-Adresse versehen sind, kann Teredo verwendet werden, um mit IPv6 über das öffentliche IPv4-Internet Verbindung zum DirectAccess-Server aufzunehmen. Ebenso wie 6to4 tunnelt Teredo IPv6-Datenverkehr in IPv4. Die zwischengeschalteten Router und Firewalls müssen ausgehenden Datenverkehr über den UDP-Port 3544 zulassen.

3. **IP-HTTPS** Für DirectAccess-Clients, die mithilfe von 6to4 und Teredo keine IPv6-Verbindung zum DirectAccess-Server aufnehmen können, wird IP-HTTPS verwendet. Dabei kapseln die DirectAccess-Clients den IPv6-Datenverkehr in HTTPS. Praktisch alle Router erlauben ausgehenden HTTPS-Datenverkehr, weshalb diese Option fast immer möglich ist.

Hinweis

In Windows Server 2012 und Windows 8 reicht die Leistung von IP-HTTPS nah an die von Teredo heran, da für die HTTPS-Kommunikation eine »Nullverschlüsselung« verwendet wird. In Windows Server 2008 R2 und Windows 7 wird bei IP-HTTPS jedoch zusätzlich zur IPsec-Verschlüsselung noch eine SSL-Verschlüsselung (Secure Sockets Layer) durchgeführt. Diese doppelte Verschlüsselung senkt die Netzwerkleistung erheblich.

Zweiter Abschnitt: Vom Rand des privaten Netzwerks zur internen Ressource

Die Kommunikation zwischen dem Rand des Netzwerks und der internen Ressource kann über IPv6 und über IPv4 erfolgen. In Ihrem internen Netzwerk müssen Sie kein globales IPv6 bereitstellen, da Windows Server 2012 bei der Bereitstellung als DirectAccess-Server am Netzwerkrand als NAT64/DNS64-Gerät fungieren kann. (Ein NAT64/DNS64-Gerät übersetzt zwischen IPv6 und IPv4.) Eine Abwicklung der gesamten Kommunikation über IPv6 ist jedoch zu bevorzugen, da sie die bestmögliche Leistung bietet.

Hinweis

Windows Server 2008 R2 hat keine NAT64/DNS64-Funktion, doch können Sie mit Microsoft Forefront Unified Access Gateway 2010 oder einem Drittanbietergerät für die entsprechende Übersetzung sorgen. Anderenfalls müssen Sie zur Einrichtung von DirectAcess globales IPv6 auf Ihrem internen Netzwrk bereitstellen oder die IPv6-Übersetzungstechnologie ISATAP einsetzen. ISATAP können Sie auch noch in Windows Server 2012 verwenden, was aber nicht empfohlen wird.

Der Verbindungsvorgang von DirectAccess

Eine DirectAccess-Verbindung zur Zielressource im Intranet wird ausgelöst, wenn ein DirectAccess-Client über IPv6 Verbindung mit dem DirectAccess-Server aufnimmt. Client und Server handeln IPSec aus, und schließlich wird die Verbindung zwischen dem Client und der Ressource aufgebaut.

Dieser Vorgang lässt sich in die folgenden Schritte zerlegen:

1. Der DirectAccess-Clientcomputer versucht eine Verbindung zu einem internen Computer herzustellen, der als *Netzwerkadressenserver* konfiguriert ist. Wenn dieser Server erreichbar ist, folgert der DirectAccess-Client, dass er bereits mit dem Intranet verbunden ist, und beendet den DirectAccess-Verbindungsvorgang. Anderenfalls geht der DirectAccess-Client davon aus, dass er mit dem Internet verbunden ist, und setzt den DirectAccess-Verbindungsvorgang fort.

Hinweis

Ein Netzwerkadressenserver ist ein Intranet-Webserver, mit dem ein DirectAccess-Client Verbindung aufzunehmen versucht, um herauszufinden, ob er mit dem Intranet oder dem Internet verbunden ist. Es ist möglich, eine interne Adresse eines DirectAccess-Servers als Netzwerkadressenserver einzurichten, es ist aber besser, einen anderen, hochverfügbaren internen Webserver für diesen Zweck zu verwenden. Wenn Sie einen Webserver als Netzwerkadressenserver einrichten, ist er nicht auf diesen einen Dienst beschränkt.

2. Der DirectAccess-Clientcomputer nimmt über IPv6 und IPsec Verbindung mit dem Direct Access-Server auf. Wenn kein natives IPv6-Netzwerk zur Verfügung steht, richtet der Client mit 6to4, Teredo oder IP-HTTPS einen IPv6-über-IPv4-Tunnel ein. Um diesen Schritt durchzuführen, muss der Benutzer nicht angemeldet sein.
3. Um die IPsec-Sitzung einzurichten, authentifizieren sich DirectAccess-Client und -Server gegenseitig mithilfe von Kerberos oder Computerzertifikaten.
4. Durch eine Überprüfung der Gruppenmitgliedschaften in den Active Directory-Domänendiensten bestätigt der DirectAccess-Server, dass der Clientcomputer und der Benutzer für die Verbindungsaufnahme über DirectAccess autorisiert sind.
5. Wenn der Netzwerkzugriffsschutz (Network Access Protection, NAP) aktiviert und zur Integritätsprüfung eingerichtet ist, erwirbt der DirectAccess-Client ein Integritätszertifikat von einer Integritätsregistrierungsstelle (Health Registration Authority, HRA) im Internet, bevor er sich mit dem DirectAccess-Server verbindet. Die HRA leitet die Integritätsinformationen des Clients an den NAP-Integritätsrichtlinienserver weiter. Dieser Server wiederum verarbeitet die Richtlinien, die vom Netzwerkrichtlinienserver (Network Policy Server, NPS) definiert wurden, und prüft, ob der Client die Systemintegritätsanforderungen erfüllt. Wenn ja, erwirbt die HRA ein Integritätszertifikat für den DirectAccess-Client. Wenn der DirectAccess-Client Verbindung mit dem DirectAccess-Server aufnimmt, reicht er das Integritätszertifikat zur Authentifizierung ein.
6. Der DirectAccess-Server beginnt damit, den Datenverkehr vom DirectAccess-Client zu den Intranetressourcen weiterzuleiten, auf die der Benutzer Zugriff hat.

Infrastrukturoptionen für DirectAccess

Sie können DirectAccess in einer Reihe von Netzwerkkonstellationen bereitstellen, wobei die Skala von einem sehr einfachen bis zu einem sehr komplizierten Aufbau reicht. Einige dieser Möglichkeiten werden in den folgenden Beispielen dargestellt.

Einfache DirectAccess-Infrastruktur

Eine einfache DirectAccess-Infrastruktur enthält einen DirectAccess-Server, der Windows Server 2012 ausführt, am Rand des Netzwerks bereitgestellt ist und als Kerberos-Proxy und als NAT64/DNS64-Übersetzungsgerät fungiert. Für die externe Schnittstelle ist eine öffentliche IP-Adresse eingerichtet. (Für Teredo wären zwei notwendig.) Die interne Adresse wird als Netzwerkadressenserver verwendet.

Innerhalb des internen Netzwerks befindet sich ein kombinierter Domänencontroller und DNS-Server mit mindestens einer internen Netzwerkressource, z.B. einem Datei- oder Anwendungsserver. Beachten Sie, dass bei dieser einfachen Infrastruktur nur Windows 8-Clients zugelassen sind, da Windows 7-Clients keine Kerberos-Authentifizierung für DirectAccess durchführen können.

Abbildung 6.2 zeigt eine solche einfache DirectAccess-Infrastruktur.

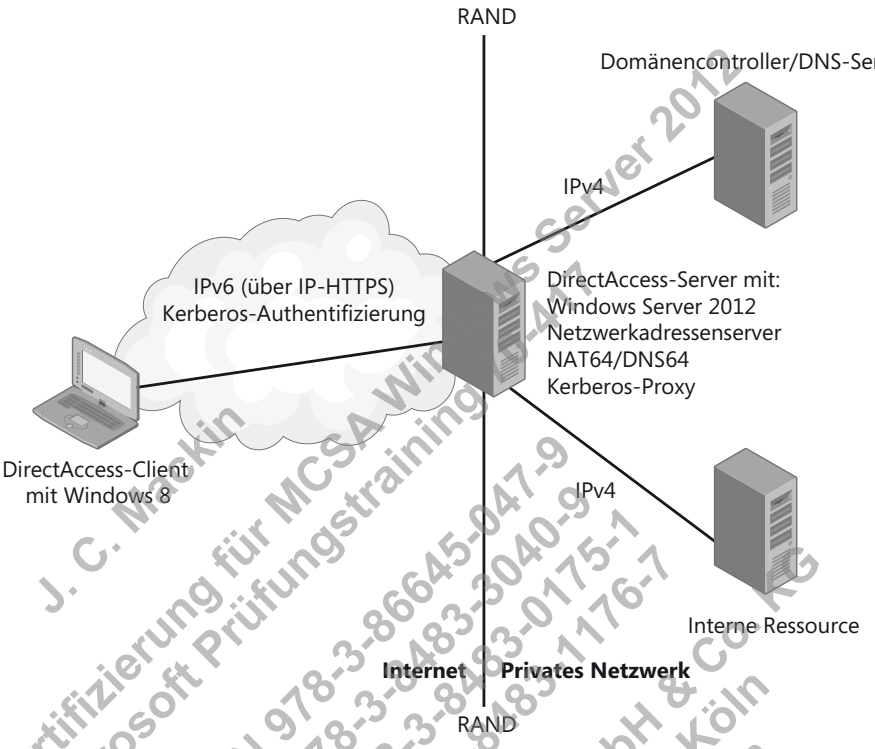

Abbildung 6.2 Eine einfache DirectAccess-Infrastruktur

Prüfungstipp

Denken Sie daran, dass nur Windows Server 2012 und Windows 8 einen Kerberos-Proxy ausführen können, der die Authentifizierung für DirectAccess-Clients stark vereinfacht. Außerdem enthält nur Windows Server 2012 eingebaute Möglichkeiten für die NAT64/DNS64-Übersetzung, mit der Sie DirectAccess in Ihrer vorhandenen internen IPv4-Infrastruktur verwenden können.

DirectAccess-Server hinter NAT

Sowohl in Windows Server 2008 R2 als auch in Windows Server 2012 können Sie einen DirectAccess-Server hinter dem Netzwerkrand in einem Umkreisnetzwerk bereitstellen. Allerdings ist es nur in Windows Server 2012 möglich, ihn hinter einem NAT-Gerät unterzu-

bringen. In einem solchen Fall braucht der DirectAccess-Server nur eine einzige Netzwerkkarte und eine einzige Adresse. Verbindungen von DirectAccess-Clients, die über das NAT-Gerät zu dem DirectAccess-Server laufen, werden mithilfe von IP-HTTPS augebaut.

Abbildung 6.3 zeigt eine DirectAccess-Netzwerktopologie, in der der DirectAccess-Server hinter einem NAT-Gerät liegt.

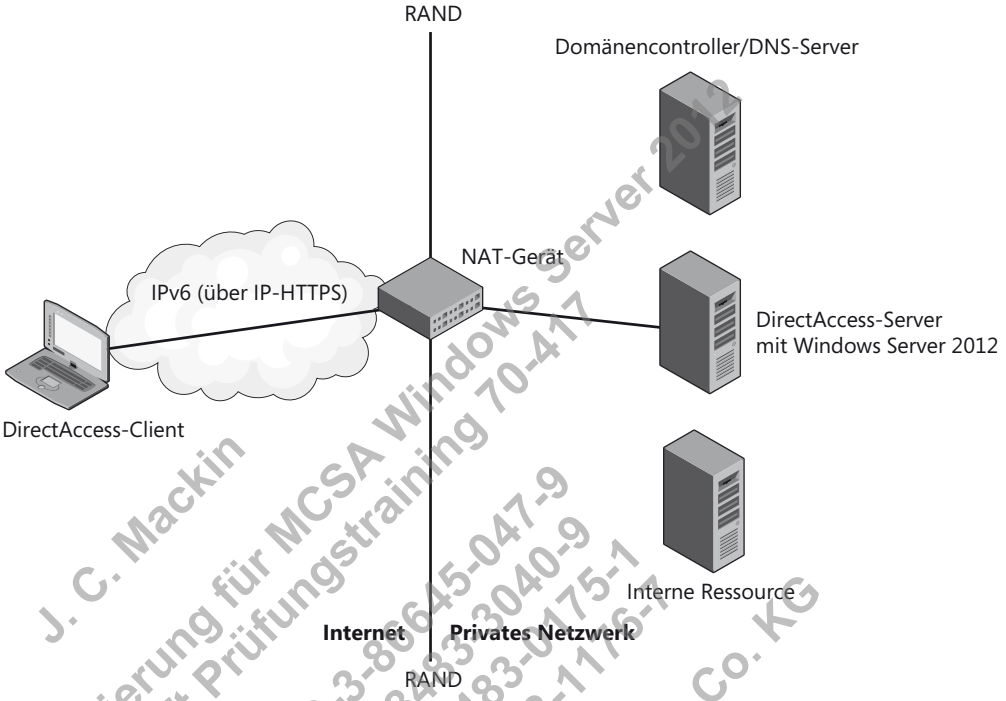

Abbildung 6.3 DirectAccess-Server hinter einem NAT-Gerät

DirectAccess-Infrastruktur mit mehreren Standorten oder Domänen

Eine weitere neue Infrastrukturoption in Windows Server 2012 ist die Möglichkeit, DirectAccess über mehrere Standorte hinweg bereitzustellen. Dazu sind eine Infrastruktur mit öffentlichen Schlüsseln (Public Key Infrastructure, PKI) und eine Computerauthentifizierung über Zertifikate erforderlich. Darüber hinaus ist die Mehrdomänenunterstützung von Windows Server 2012 schon in DirectAccess eingebaut und erfordert keine zusätzliche Konfiguration.

Wenn Sie eine Bereitstellung über mehrere Standorte hinweg einrichten, werden die DirectAccess-Clients mit einer Liste der DirectAccess-Server versehen, die an den einzelnen Standorten als Eintrittspunkte zum privaten Netzwerk dienen. Vor der Verbindungsaufnahme pingen DirectAccess-Clients mit Windows 8 jeden dieser Server an und stellen dann Kontakt mit demjenigen her, der die kürzeste Verzögerung aufweist. (Windows 7-Clients in einer Bereitstellung auf mehreren Standorten verwenden einfach immer dieselbe vorkonfigurierte Adresse für einen DirectAccess-Server.)

Abbildung 6.4 zeigt eine solche DirectAccess-Infrastruktur auf mehreren Standorten.

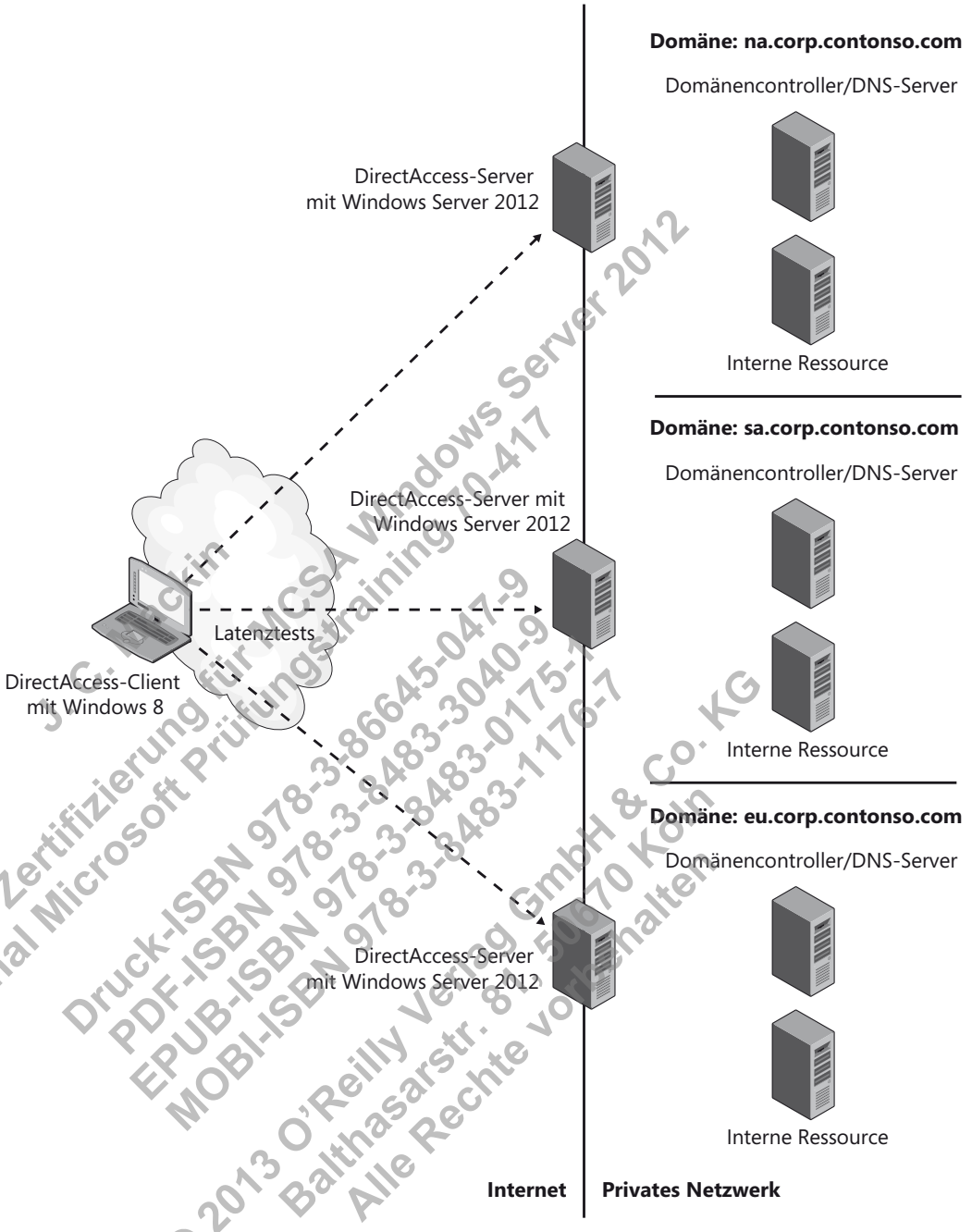

Abbildung 6.4 Eine DirectAccess-Infrastruktur mit mehreren Standorten

Hinweis

Um die Möglichkeiten von DirectAccess für mehrere Standorte zu aktivieren, müssen Sie (wie weiter hinten in Abbildung 6.20 gezeigt) in der Remotezugriffs-Verwaltungskonsole auf *Mehrere Standorte aktivieren* klicken oder das Windows PowerShell-Cmdlet *Enable DAMultiSite* verwenden.

Vielschichtige DirectAccess-Infrastruktur

Windows Server 2012 vereinfacht zwar die grundlegenden Infrastrukturanforderungen für DirectAccess, doch trotzdem kann diese Infrastruktur kompliziert werden, wenn Sie einen Funktionsumfang brauchen, der in der Basiseinrichtung nicht standardmäßig eingeschlossen ist. Beispielsweise ist eine der neuen Funktionen von Windows Server 2012 die Möglichkeit, DirectAccess-Server in Clustern mit Netzwerklastenausgleich (Network Load Balancing, NLB) bereitzustellen. Diese Funktion macht die Infrastruktur komplizierter, ist aber oft erforderlich, wenn Sie viele Remoteclients haben. Eine weitere Forderung, die die Infrastruktur erweitert, ist die Unterstützung von Windows 7-Clients. Solche Computer können DirectAccess-Verbindungen nur mithilfe von Computerzertifikaten authentifizieren, weshalb Sie in diesem Fall auch eine PKI benötigen. Außerdem kann DirectAccess mit NAP bereitgestellt werden, was die Sache ebenfalls komplizierter macht, aber von den IT-Richtlinien Ihrer Organisation möglicherweise verlangt wird. Weitere Funktionen wie etwa eine Zwei-Faktor-Authentifizierung mit Einweg-Kennwörtern erhöhen die Anforderungen an die Infrastruktur noch mehr. Abbildung 6.5 zeigt eine vielschichtigere DirectAccess-Instrstruktur, die alle drei IPv6-Übergangstechnologien unterstützt, die Kapazität durch einen NLB-Cluster verbessert, durch eine PKI mit Zertifizierungsstelle auch Window 7-Clients zulässt, eine NAP-Infrastruktur enthält und einen Netzwerkadressserver außerhalb des DirectAccess-Servers verwendet.

Hinweis

Um den Lastenausgleich in DirectAccess zu aktivieren, müssen Sie (wie weiter hinten in Abbildung 6.20 gezeigt) in der Remotezugriffs-Verwaltungskonsole auf *Lastenausgleich aktivieren* klicken oder die Windows PowerShell-Cmdlet *Set-RemoteAccessLoadBalancer* und *Add-RemoteAccessLoadBalancerNode* verwenden.

Installieren und Konfigurieren von DirectAccess

Die Installation und Konfiguration von DirectAccess wurde in Windows Server 2012 stark vereinfacht. DirectAccess ist jetzt mit herkömmlichen VPNs in der neuen Serverrolle Remotezugriff zusammengefasst. Beide werden mit demselben Werkzeug verwaltet, nämlich der Remotezugriffs-Verwaltungskonsole. Sie können einen Windows Server-Computer jetzt gleichzeitig als DirectAccess- und als herkömmlichen VPN-Server einrichten, was in Windows Server 2008 R2 nicht möglich war. Noch bedeutender als die einheitliche Verwaltung sind die neuen Konfigurations-Assistenten in Windows Server 2012, die die Bereitstellung und Einrichtung von DirectAccess und VPNs relativ einfach machen.

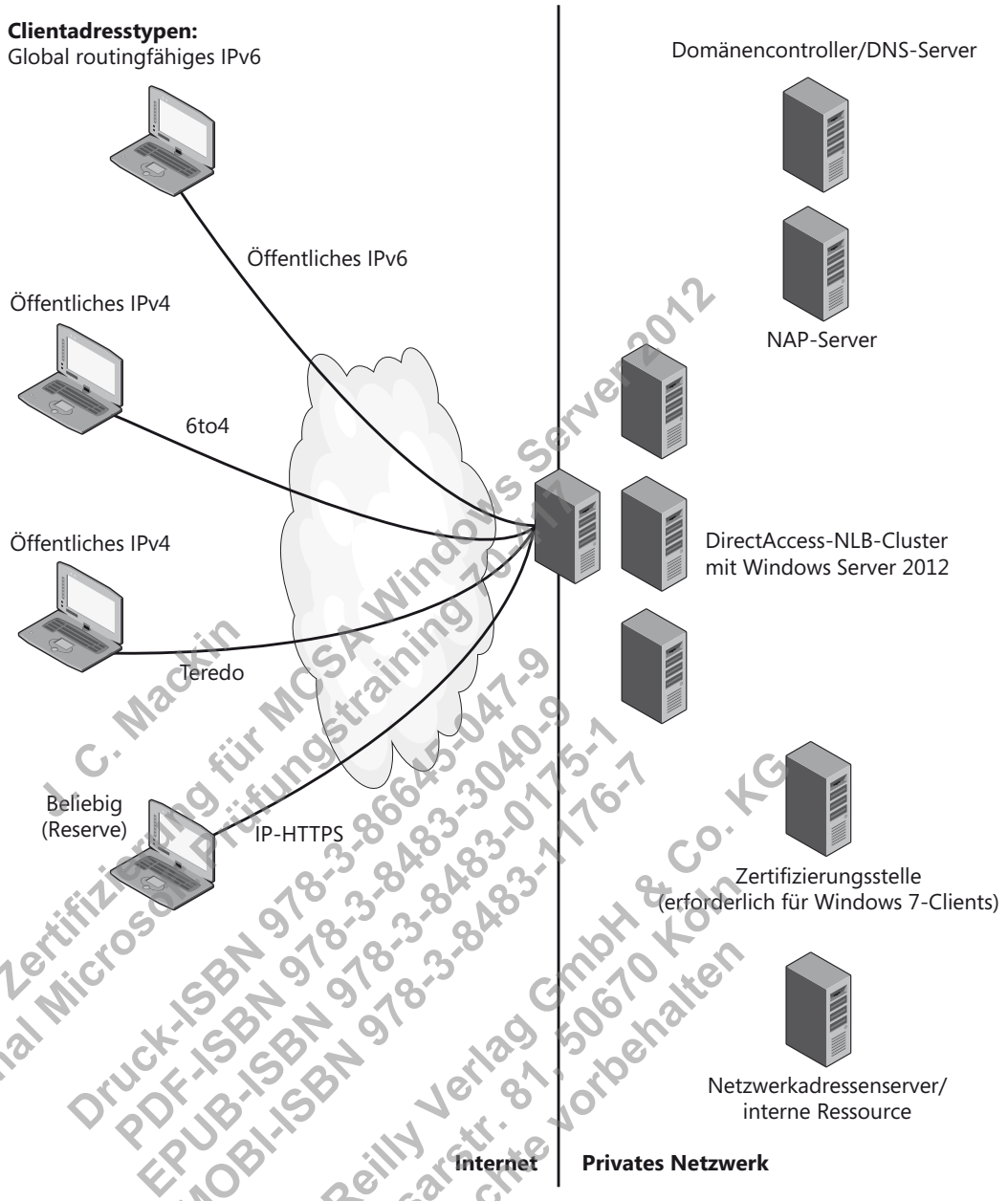

Abbildung 6.5 Eine vielschichtige DirectAccess-Infrastruktur

Installieren des Remotezugriffs

DirectAccess gehört jetzt zur Serverrolle Remotezugriff, die Sie mithilfe des Assistenten zum Hinzufügen von Rollen und Features oder mit folgendem Befehl an einer Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten installieren können:

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

Anschließend können Sie DirectAccess in der Remotezugriffs-Verwaltungskonsole aus Abbildung 6.6 oder mithilfe von Windows PowerShell-Befehlen einrichten.

Hinweis

Weitere Informationen über die Cmdlets zur Konfiguration von DirectAccess erhalten Sie auf *http://technet.microsoft.com/de-de/library/hh918399*. Sie können auch folgenden Befehl an einer Windows PowerShell-Eingabeaufforderung geben:

```
Get-Command -Module RemoteAccess *da*
```

Wenn Sie die Serverrolle Remotezugriff und die zugehörigen Verwaltungswerkzeuge installieren, wird dadurch auch das Windows PowerShell-Modul *DirectAccessClientComponents* mit zusätzlichen Client-Cmdlets hinzugefügt. Eine Liste dieser Cmdlets erhalten Sie auf *http://technet.microsoft.com/de-de/library/hh848426*.

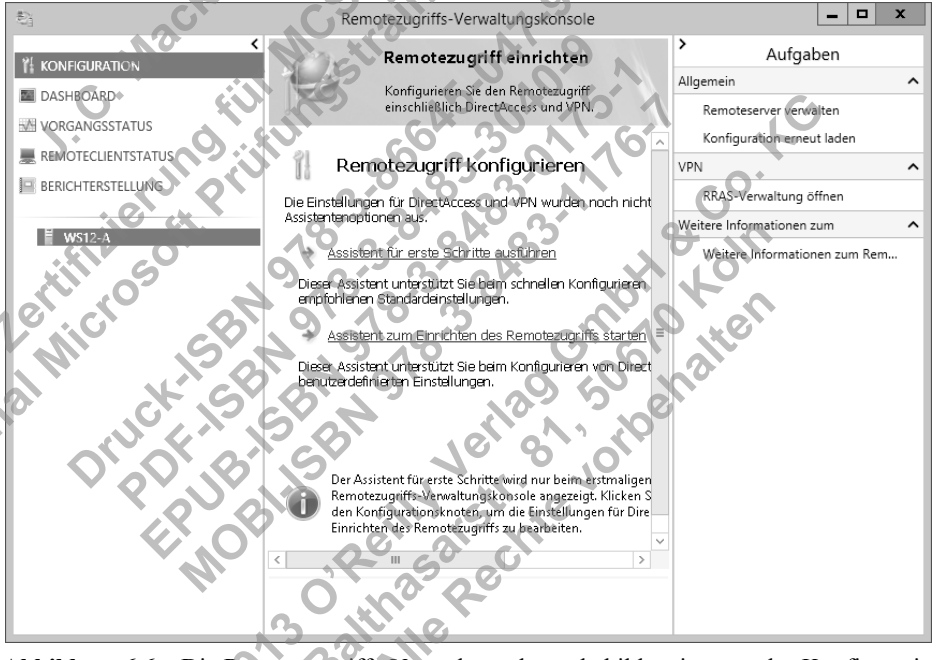

Abbildung 6.6 Die Remotezugriffs-Verwaltungskonsole bildet ein zentrales Konfigurations- und Verwaltungswerkzeug für alle Remotezugriffstechnologien.

Einrichten von DirectAccess

Abbildung 6.6 zeigt die Remotezugriffs-Verwaltungskonsole in dem Zustand, den sie vor der Ausführung irgendwelcher Konfigurationsschritte hat. Im mittleren Bereich stehen der Assistent für erste Schritte und der Assistent zum Einrichten des Remotezugriffs zur Verfügung. Unabhängig davon, für welchen dieser Assistenten Sie sich entscheiden, haben Sie als Nächstes die Wahl, ob Sie nur DirectAccess, nur ein VPN oder beides konfigurieren möchten (siehe Abbildung 6.7).

Abbildung 6.7 Mit dem Assistenten für die Einrichtung des Remotezugriffs können Sie DirectAccess, ein VPN oder beides konfigurieren.

Der Assistent für erste Schritte ist ein hervorragendes neues Werkzeug, um eine Remotezugriffslösung schnell bereitzustellen. Da viele der Konfigurationsoptionen, die Sie für die Prüfung beherrschen müssen, darin jedoch verborgen ist, ist er zum Lernen nicht gut geeignet. Außerdem hat sich die VPN-Konfiguration in Windows Server 2012 nicht auf eine Weise geändert, die für die Prüfung 70-417 maßgeblich wäre. Daher sollten Sie sich zur Vorbereitung auf das Lernziel »Einrichten von DirectAccess« der Prüfung 70-417 auf die Konfigurationsoptionen konzentrieren, die Ihnen angezeigt werden, wenn Sie auf *Assistent zum Einrichten des Remotezugriffs starten* (siehe Abbildung 6.6) und dann auf *Nur DirectAccess bereitstellen* (siehe Abbildung 6.7) klicken.

Wenn Sie das getan haben, wird der mittlere Bereich der Remotezugriffs-Verwaltungskonsole durch ein Bild ersetzt, das ähnlich wie Abbildung 6.8 aussieht. Für die vier Schritte in diesem Diagramm gibt jeweils Konfigurations-Assistenten, die Sie in der richtigen Reihenfolge ausführen müssen. Der erste richtet die DirectAccess-Clients ein, der zweite den DirectAccess-Server,

der dritte die Infrastrukturserver und der vierte die Anwendungsserver (falls gewünscht). Diese Assistenten erstellen und konfigurieren Gruppenrichtlinienobjekte für DirectAccess-Server und -Clients.

In der Prüfung 70-417 werden diese Assistenten nicht namentlich erwähnt. Stattdessen werden Sie über *beliebige Konfigurationsoptionen* befragt, die in diesen Assistenten vorkommen. Diese vier Assistenten bieten eine hervorragende Möglichkeit zur Gliederung der neuen Konfigurationsoptionen, die Sie für die Prüfung 70-417 lernen müssen, weshalb wir sie uns einen nach dem anderen genauer ansehen werden.

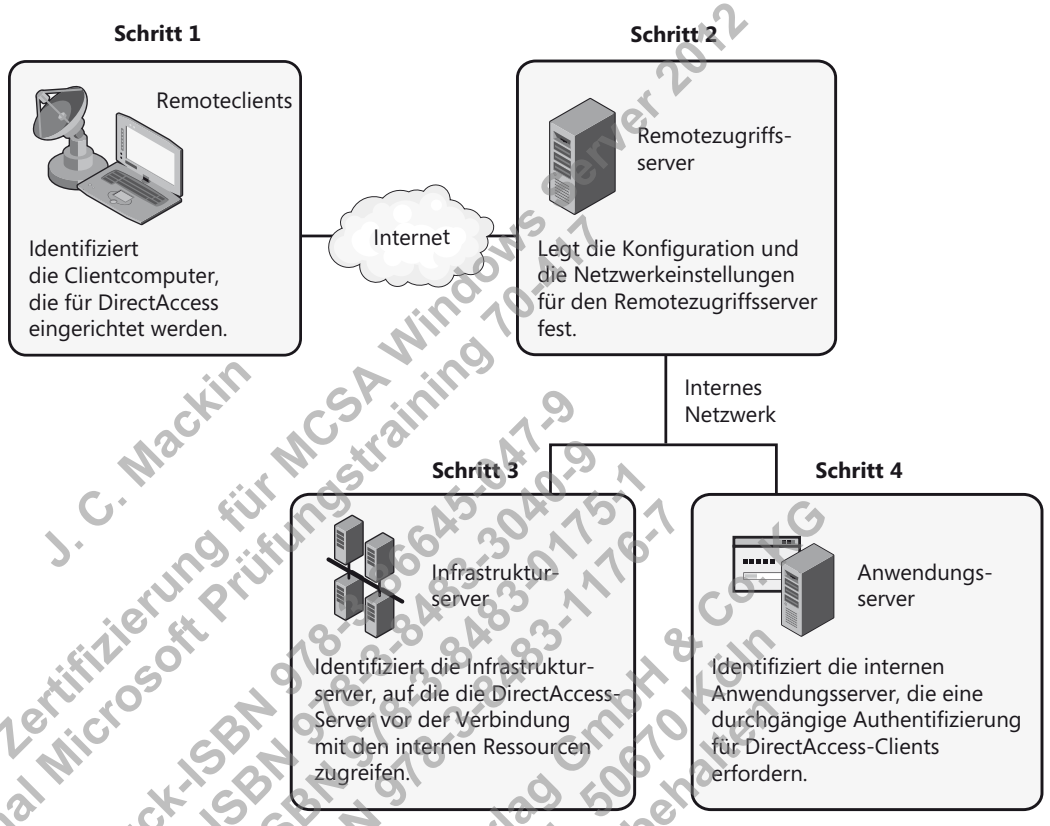

Abbildung 6.8 Die vier Konfigurations-Assistenten für DirectAccess

Schritt 1: DirectAccess-Clientsetup

Die erste Seite des Assistenten für das DirectAccess-Clientsetup sehen Sie in Abbildung 6.9. Sie trägt den Titel *Bereitstellungsszenario* und lässt Ihnen die Wahl, ob Sie DirectAccess-Clients für den Remotezugriff und die Remoteverwaltung oder nur für die Remoteverwaltung einrichten möchten. Die erste Option ist vorab ausgewählt und richtet eine bidirektionale Kommunikation zwischen DirectAccess-Servern und -Clients ein. Wenn Sie sich für die zweite Option entscheiden, können Administratoren DirectAccess-Clients mit Programmen wie SCCM über das Netzwerk verwalten, allerdings ist es den Clients nicht möglich, auf das

interne Unternehmensnetzwerk zuzugreifen. Die zweite Option, die nur die Remoteverwaltung zulässt, ist neu in Windows Server 2012.

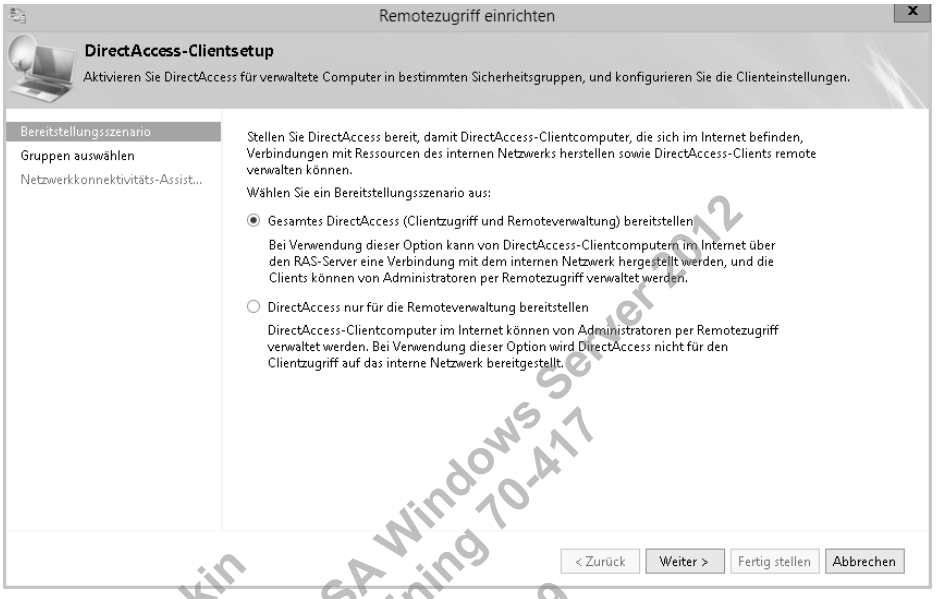

Abbildung 6.9 Die Seite *Bereitstellungsszenario* im Assistenten für das DirectAccess-Clientsetup

Hinweis

Um die Art der Bereitstellung in Windows PowerShell einzurichten, verwenden Sie das Cmdlet *Set-DAServer* mit der Option *-DAInstall* und entweder dem Parameter *FullInstall* oder *ManageOut*. Um beispielsweise eine DirectAccess-Bereitstellung nur für die Remoteverwaltung einzurichten, geben Sie an einer Windows PowerShell-Befehlszeile mit erhöhten Rechten auf dem DirectAccess-Server Folgendes ein:

```
Set-DAServer -DAInstallType ManageOut
```

Die zweite Seite des Assistenten für das DirectAccess-Clientsetup, *Gruppen auswählen*, sehen Sie in Abbildung 6.10. Mit dem ersten Element auf dieser Seite können Sie Sicherheitsgruppen angeben, die Sie für DirectAccess aktivieren möchten. Dies ist ein wichtiger Schritt, den Sie sich unbedingt merken müssen: Wenn Sie einem DirectAccess-Client nicht das Recht einräumen, auf das interne Netzwerk zuzugreifen, kann er dies nicht tun. In Windows PowerShell verwenden Sie hierzu das Cmdlet *Add-DAClient* mit der Option *-SecurityGroupNameList*.

Mit dem zweiten Element auf dieser Seite können Sie DirectAccess ausschließlich für Mobilcomputer aktivieren. Wenn Sie den Assistenten für erste Schritte ausführen, ist diese Option übrigens vorausgewählt. Computer, die über DirectAccess Verbindung aufnehmen, sind höchstwahrscheinlich mobile Rechner, aber es gibt Ausnahmen – und diese Ausnahmen können sehr gut in der Situationsbeschreibung einer Prüfungsfrage erwähnt werden. (Situation:

Einige Benutzer arbeiten an Remotestandorten auf Desktopcomputern, die an die Domäne angeschlossen sind, und erhalten keine Verbindung über DirectAccess. Warum nicht? Die Option zur Aktivierung von DirectAccess ausschließlich für Mobilcomputer wurde gewählt!)

Prüfungstipp

Wenn nur Laptopcomputer über DirectAccess Verbindung erhalten, können Sie diese Einstellung über das Gruppenrichtlinienobjekt für DirectAccess-Clienteinstellungen ändern. Dazu müssen Sie den WMI-Filter *DirectAccess – Laptop Only* entfernen, der in den Sicherheitsfiltereinstellungen mit diesem Gruppenrichtlinienobjekt verknüpft ist.

Die dritte Option auf dieser Seite lautet *Tunnelerzwingung verwenden*. Damit werden DirectAccess-Clients dazu gezwungen, den *gesamten* Netzwerkdatenverkehr ohne Rücksicht auf sein eigentlichen Ziel über das private Netzwerk zu übermitteln. Dies kann beispielsweise dazu verwendet werden, den gesamten Webdatenverkehr von DirectAccess-Clients durch einen internen Webproxyserver zu leiten. In Windows PowerShell richten Sie diese Option mit dem Cmdlet *Set-DAClient* und dem Parameter *-ForceTunnel* ein.

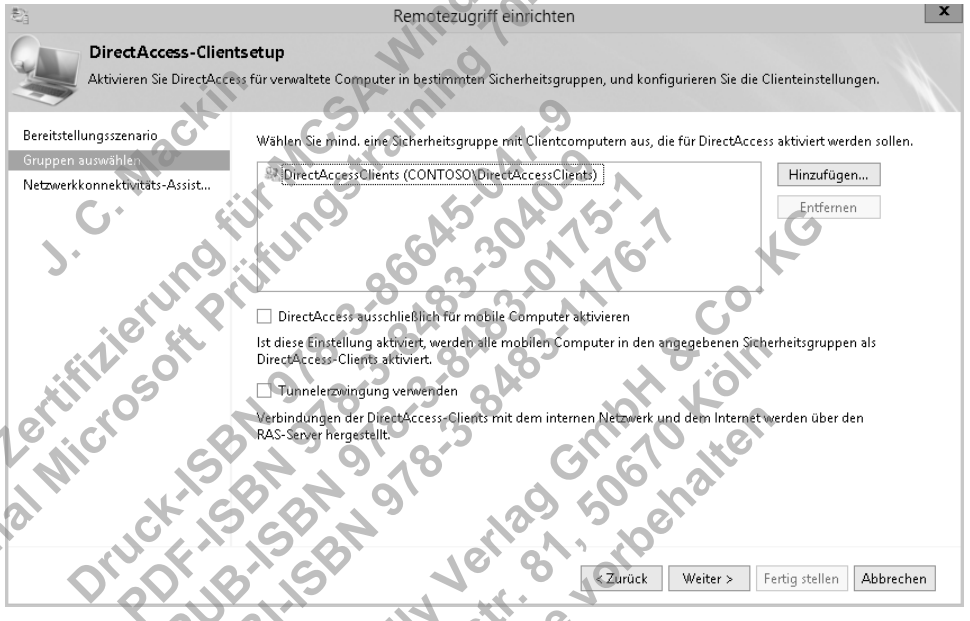

Abbildung 6.10 Die Seite *Gruppen auswählen* im Assistenten für das DirectAccess-Clientsetup

Die letzte Seite des Assistenten für das DirectAccess-Clientsetup, *Netzwerkkonnektivitäts-Assistent*, sehen Sie in Abbildung 6.11.

Oben auf der Seite können Sie die Webtest-Hostadresse angeben. DirectAccess-Clientcomputer überprüfen anhand dieses Webhosts die Anbindung an das interne Netzwerk. Diese Einstellung wird in der Prüfung 70-417 kaum vorgenommen (höchstens als falsche Antwortmöglichkeit).

Wenn Sie die Adresse manuell eingeben müssen, können Sie *http://directaccess-webprobe-host.<IhreDomäne>* verwenden. Der interne DNS-Dienst sollte diese Adresse in die interne IPv4-Adresse des Remotezugriffsservers auflösen (bzw. in die IPv6-Adresse bei einer reinen IPv6-Umgebung).

Die Einstellung auf dieser Seite, zu der am ehesten Prüfungsfragen gestellt werden können, dient dazu, DirectAccess-Clients die lokale Namensauflösung zu erlauben, was in diesem Fall die Broadcast-Protokolle NetBIOS über TCP/IP und LLMNR (Link-Local Multicast Name Resolution) bedeutet. Wenn Sie diese Option aktivieren, dürfen DirectAccess-Clients einteilige Namen wie *App1* lokal auflösen, falls dies über DNS nicht möglich ist. Die lokale Namensauflösung muss auch im Assistenten für das Infrastrukturserversetup eingerichtet werden.

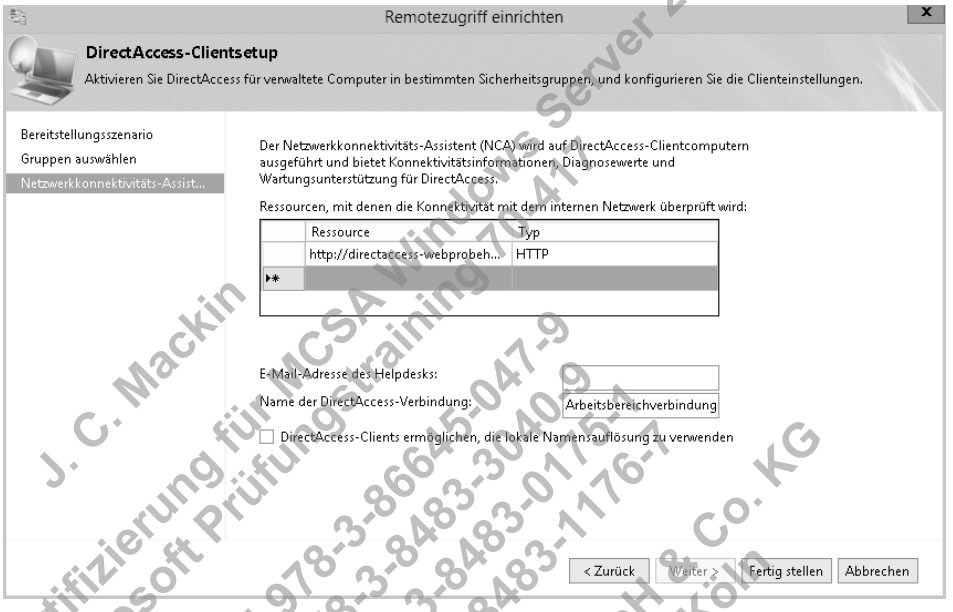

Abbildung 6.11 Die Seite *Netzwerkkonnektivitäts-Assistent* im Assistenten für das DirectAccess-Clientsetup

Schritt 2: RAS-Serversetup

Die erste Seite des Assistenten für das RAS-Serversetup, *Netzwerktopologie*, sehen Sie in Abbildung 6.12. Hier legen Sie fest, an welcher Stelle im Netzwerk Sie den DirectAccess-Server bereitstellen werden.

Die erste Option lautet *Edge* (also »Rand«). Dafür muss der DirectAccess-Server über zwei interne Netzwerkkarten verfügen, von denen die eine mit dem Internet und die andere mit dem internen Netzwerk verbunden ist. Wenn Sie eine Verbindungsaufnahme über Teredo ermöglichen wollen, müssen Sie der externen Schnittstelle zwei aufeinander folgende öffentliche IPv4-Adressen zuweisen.

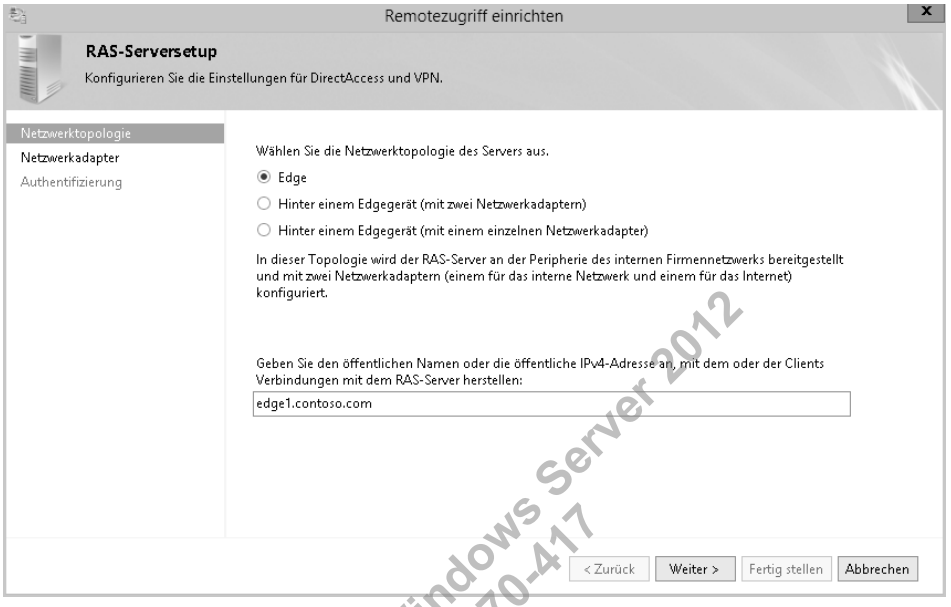

Abbildung 6.12 Die Seite *Netzwerktopologie* des Assistenten für das RAS-Serversetup

Die zweite Option, *Hinter einem Edgegerät (mit zwei Netzwerkadaptern)*, sollten sie wählen, wenn Sie den DirectAccess-Server in einem Umkreisnetzwerk hinter einer Firewall oder einem Router bereitstellen möchten. Bei dieser Topologie werden der Netzwerkkarte am Umkreisnetzwerk eine oder zwei aufeinander folgende öffentliche IPv4-Adressen zugewiesen. Die zweite, an das interne Netzwerk angeschlossene Karte, kann eine private Adresse haben.

Als dritte Option steht *Hinter einem Edgegerät (mit einem einzelnen Netzwerkadapter)*. Wählen Sie diese Option, wenn Sie den DirectAccess-Server hinter einem NAT-Gerät aufstellen wollen. Der Server erhält dabei eine einzige private IP-Adresse.

Auf der Seite *Netzwerktopologie* müssen Sie auch den Namen oder die IPv4-Adresse angeben, über die die DirectAccess-Clients Verbindung mit dem DirectAccess-Server Verbindung aufnehmen. Geben Sie hier einen Namen an, der über öffentliches DNS aufgelöst werden kann, oder eine IPv4-Adresse, die vom öffentlichen Netzwerk aus erreichbar ist.

Die zweite Seite des Assistenten für das RAS-Serversetup, *Netzwerkadapter*, sehen Sie in Abbildung 6.13. Hier müssen Sie je nach gewählter Topologie die Netzwerkkarte für das interne und das externe Netzwerk angeben.

Außerdem ist es erforderlich, ein Zertifikat festzulegen, das der DirectAccess-Server zur Authentifizierung von IP-HTTPS-Verbindungen nutzt. Wenn Ihre Organisation eine PKI bereitgestellt hat, können Sie nach einem Exemplar des Computerzertifikats für den lokalen Server suchen. Wenn nicht, müssen Sie die Option zur Verwendung eines selbstsignierten Zertifikats aktivieren. Diese Option ist neu in Windows Server 2012 und kann daher durchaus die Grundlage für eine Prüfungsfrage bilden.

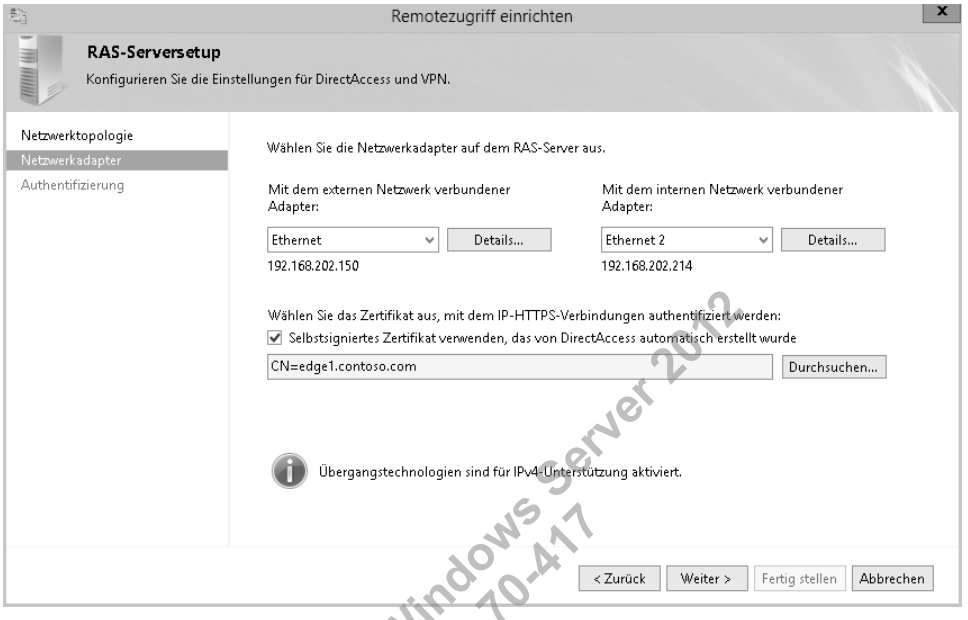

Abbildung 6.13 Die Seite *Netzwerkadapter* des Assistenten für das RAS-Serversetup

Die letzte Seite des Assistenten für das RAS-Serversetup, *Authentifizierung*, sehen Sie in Abbildung 6.14. Hier können Sie die folgenden Einstellungen zur DirectAccess-Clientauthentifizierung vornehmen:

- **Benutzerauthentifizierung** Standardmäßig können sich Benutzer nur mit Active Directory-Anmeldeinformationen authentifizieren. Hier können Sie jedoch auch eine zweistufige Authentifizierung verlangen, wobei die Benutzer gewöhnlich nicht nur ihre Active Directory-Anmeldeinformationen angeben, sondern auch eine Smartcard einführen müssen. In Windows Server 2012 kann das TPM (Trusted Platform Module) von Clientcomputern als virtuelle Smartcard für die zweistufige Authentifizierung fungieren.

  Alternativ können Sie die zweistufige Authentifizierung auch so einrichten, dass die Benutzer neben ihren Active Directory-Anmeldeinformationen auch ein OTP eingeben, wie es beispielsweise RSA SecurID bereitstellt. Für OTP sind eine PKI und ein RADIUS-Server sowie eine Reihe von Konfigurationsschritten erforderlich, die für die Prüfung 70-417 aber nicht von Bedeutung sind. Dazu müssen Sie nur wissen, dass ein OTP als Alternative zu Smartcards für die zweistufige Authentifizierung in DirectAccess verwendet werden kann.
- **Computerzertifikate** Wenn Sie DirectAccess in der grafischen Benutzeroberfläche konfigurieren, werden die Clientcomputer standardmäßig über Kerberos authentifiziert. Allerdings können Sie auch die Computerauthentifizierung über Zertifikate erlangen. Dies ist für die zweistufige Authentifizierung, für eine DirectAccess-Bereitstellung auf mehreren Standorten und für DirectAccess-Clients mit Windows 7 erforderlich.

- **Windows 7-Clients** Standardmäßig können Windows 7-Clientcomputer keine Verbindung zu einer Remotezugriffseinrichtung mit Windows Server 2012 aufnehmen. Diese Möglichkeiten müssen Sie hier ausdrücklich aktivieren.
- **NAP** Hiermit können Sie Integritätsprüfungen der Clientcomputer über NAP verlangen. In Windows PowerShell richten Sie diese Einstellung mit dem Cmdlet *Set-DAServer* und dem Parameter *-HealthCheck* ein.

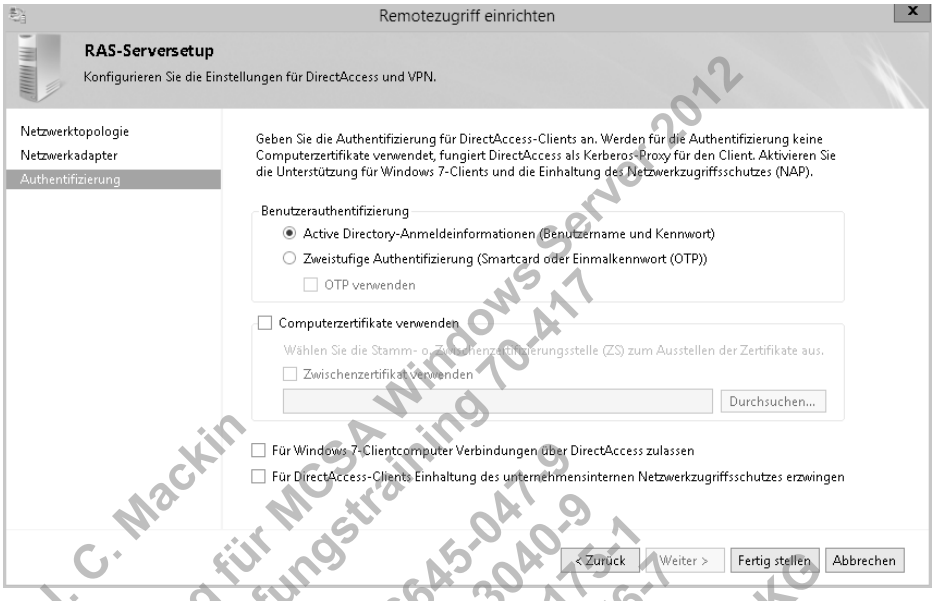

Abbildung 6.14 Die Seite *Authentifizierung* des Assistenten für das RAS-Serversetup

Weitere Informationen

Alle Authentifizierungseinstellungen auf dieser Seite können Sie auch mit *Set-DAServer* vornehmen. Weitere Informationen darüber erhalten Sie über *Get-Help* sowie auf *http://technet.microsoft.com/de-de/library/hh918371*.

Schritt 3: Infrastrukturserver-Setup

Im Assistenten für das Infrastrukturserver-Setup können Sie Einstellungen zum Netzwerkadressenserver, zum DNS-Server und zu Verwaltungsservern, etwa für Aktualisierungen oder zum Schutz gegen Viren, vornehmen.

Die erste Seite dieses Assistenten, *Netzwerkadressenserver*, sehen Sie in Abbildung 6.15. Wie in diesem Kapitel bereits erklärt, ermitteln DirectAccess-Clients mithilfe dieses Servers, ob sie sich im Unternehmensnetzwerk befinden. Es wird empfohlen, für diesen Zweck einen anderen

internen Webserver als den DirectAccess-Server (also den Remotezugriffsserver) zu verwenden. (Die DNS- und die zugehörige IP-Adresse gehören dann natürlich zu der Schnittstelle mit dem internen Netzwerk.) Wenn Sie den DirectAccess-Server als Netzwerkadressenserver verwenden, muss er durch ein Computerzertifikat authentifiziert werden, ggf. durch ein selbstsigniertes. Zur Festlegung des Netzwerkadressenservers in Windows PowerShell verwenden Sie das Cmdlet *Set-DANetworkLocationServer*.

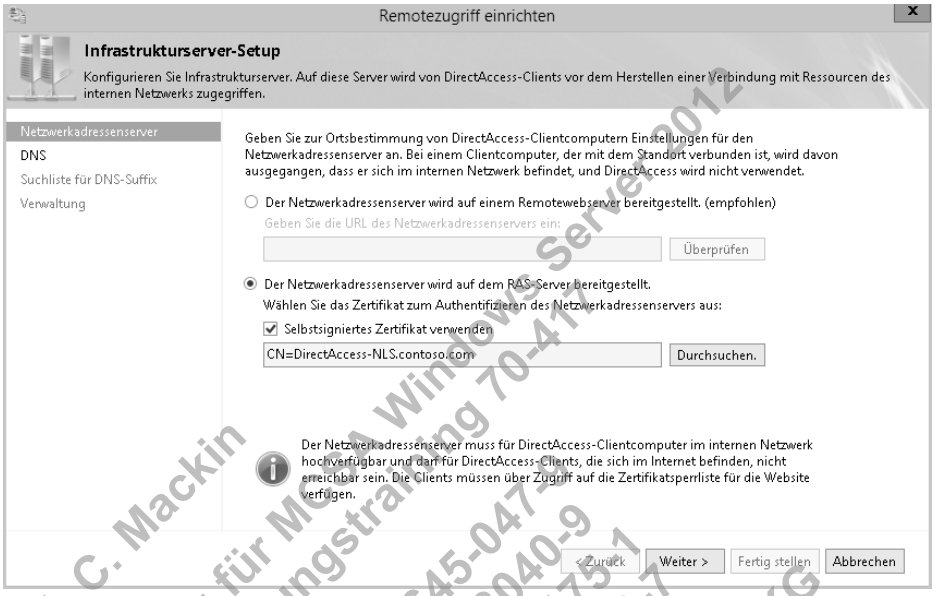

Abbildung 6.15 Die Seite *Netzwerkadressenserver* des Assistenten für das Infrastrukturserver-Setup

Die zweite Seite des Assistenten für das Infrastrukturserver-Setup, *DNS*, sehen Sie in Abbildung 6.16. Der wichtigste Zweck dieser Seite besteht darin, dass Sie hier die Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) ausfüllen können. Die Einträge, die Sie hier einfügen, werden in das Gruppenrichtlinienobjekt zur Konfiguration von DirectAccess-Clients geschrieben.

Anhand dieser Tabelle können DNS-Clients die Adresse eines DNS-Servers zu einzelnen Namensräumen statt zu Schnittstellen zuweisen. Im Grunde genommen enthält die Tabelle eine Liste von Regeln zur Namensauflösung, die über eine Gruppenrichtlinie auf die Clients angewendet werden. Jede dieser Regeln legt einen DNS-Namensraum (einen Domänennamen oder FQDN) und das Verhalten fest, das DNS-Clients für diesen Namensraum an den Tag legen sollen. Die Gesamtheit der Namensauflösungsregeln wird als Namensauflösungsrichtlinie bezeichnet. Jede Anforderung einer Namensabfrage von einem DirectAccess-Client im Internet wird anhand der Regeln in dieser Tabelle überprüft. Bei einer Übereinstimmung wird die Anforderung nach den Einstellungen in der Regel verarbeitet. Die Einstellungen legen fest, an welche DNS-Server die einzelnen Anforderungen gesendet werden. Gibt es für eine Anforderung keinen zugehörigen Namensraum in der Tabelle, wird sie an die DNS-Server gesendet, die in den TCP/IP-Einstellungen für die angegebene Netzwerkschnittstelle eingerichtet sind.

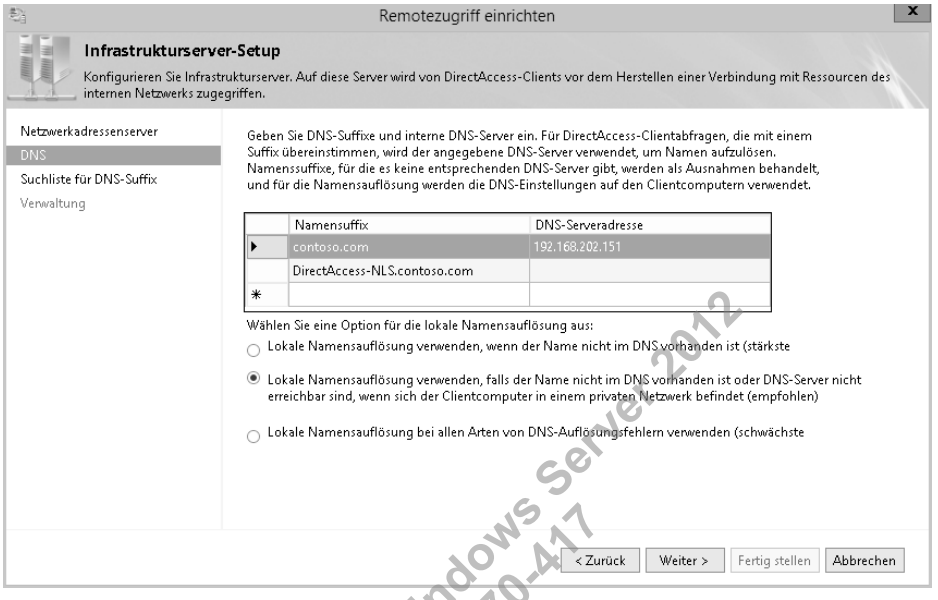

Abbildung 6.16 Die Seite *DNS* des Assistenten für das Infrastrukturserver-Setup

Es kann vorkommen, dass Sie Einträge in der Namensauflösungsrichtlinie vornehmen müssen, wenn Sie DNS-Clients in die Lage versetzen wollen DNS-Suffixe aufzulösen, die es nur in Namensraum des Intranets gibt. Ein weiterer Grund kann darin bestehen, dass Sie eine zweigeteilte öffentliche und private DNS-Umgebung mit einem gemeinsamen Domänennamen haben und sicherstellen müssen, dass DirectAccess-Clients über die DirectAccess-Verbindung nicht in Kontakt mit den öffentlichen Servern (z.B. den Webservern) des Unternehmens treten.

Prüfungstipp

Für die Prüfung 70-417 müssen Sie die Funktion der Namensauflösungsrichtlinie und der Tabelle genau kennen. Um sich die Richtlinientabelle in Windows PowerShell anzusehen, verwenden Sie das Cmdlet *Get-DnsClientNrptPolicy*.

Die zweite Konfigurationsentscheidung, die Sie auf der Seite *DNS* vornehmen, betrifft die Verwendung von lokalen Namensauflösungsmethoden wie NetBIOS und LLMNR durch die DirectAccess-Clients. Mit der Einstellung im Assistenten für das Clientsetup wird die lokale Namensauflösung lediglich zugelassen (also nicht blockiert). Auf dieser Seite jedoch legen Sie fest, wie diese Auflösung durchgeführt werden soll, falls sie erlaubt ist. Dabei haben Sie drei Möglichkeiten. Die restriktivste Option besteht darin, die lokale Namensauflösung nur in den Fällen zuzulassen, in denen der Name in DNS nicht vorhanden ist. Dies gilt als die sicherste Einstellung, da hierbei nicht die Gefahr besteht, dass die Namen der Server im Intranet über die lokale Namensauflösung ins Subnetz durchsickern, wenn die DNS-Server im Intranet nicht erreichbar sind oder irgendwelche anderen DNS-Fehler auftreten. Die zweite, empfohlene

Möglichkeit besteht darin, die lokale Namensauflösung zuzulassen, wenn der Name in DNS nicht vorhanden oder die DNS-Server nicht erreichbar sind und sich der Clientcomputer in einem privaten Netzwerk befindet. Die geringste Einschränkung bietet die dritte Option, bei der die lokale Namensauflösung bei jeder Art von DNS-Fehler verwendet wird. Dies ist die unsicherste Möglichkeit, da die Namen der Server im Intranet dabei über die lokale Namensauflösung im Subnetz bekannt werden können.

Um die lokale Namensauflösung für Clients in Windows PowerShell einzurichten, verwenden Sie das Cmdlet *Set-DAClientDNSConfiguration* mit dem Parameter *-Local*. Die drei Auswahlmöglichkeiten der grafischen Benutzeroberfläche werden durch die Optionen *FallbackSecure*, *FallbackPrivate* und *FallbackUnsecure* bereitgestellt.

Weitere Informationen

Weitere Informationen über das Cmdlet *Set-DAClientDNSConfiguration* erhalten Sie mithilfe von *Get-Help* sowie auf *http://technet.microsoft.com/de-de/library/hh918389*.

Die dritte Seite des Assistenten für das Infrastrukturserver-Setup, *Suchliste für DNS-Suffix*, sehen Sie in Abbildung 6.17.

DirectAccess-Clients nutzen die Liste, die Sie hier anlegen, zur Auflösung von einteiligen Namen wie *http://finance*. Solche Namen können in DNS erst dann aufgelöst werden, wenn der DNS-Client ein Suffix anhängt, wobei standardmäßig das primäre DNS-Suffix des Clientcomputers verwendet wird.

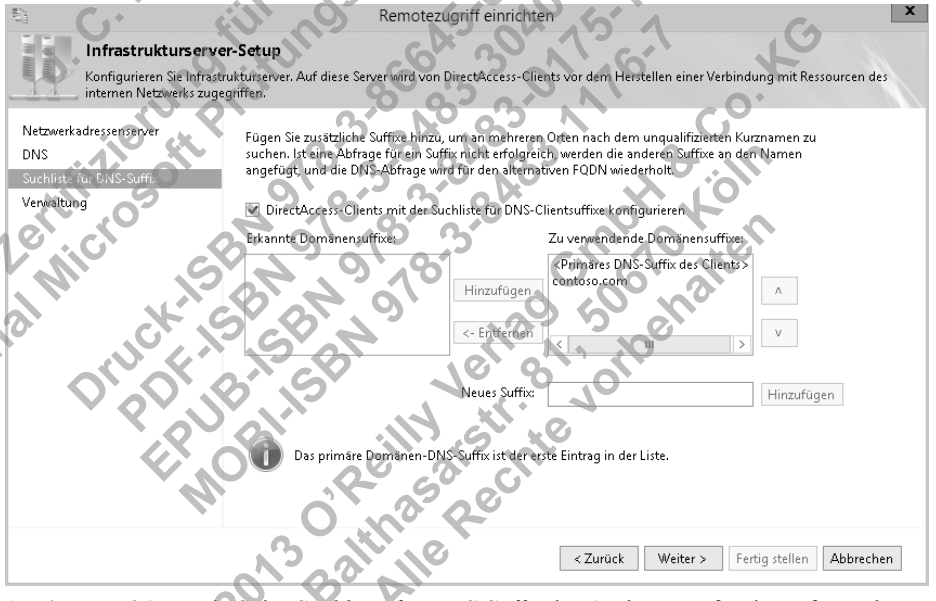

Abbildung 6.17 Die Seite *Suchliste für DNS-Suffix* des Assistenten für das Infrastrukturserver-Setup

Die vierte und letzte Seite des Assistenten für das Infrastrukturserver-Setup, *Verwaltung*, sehen Sie in Abbildung 6.18.

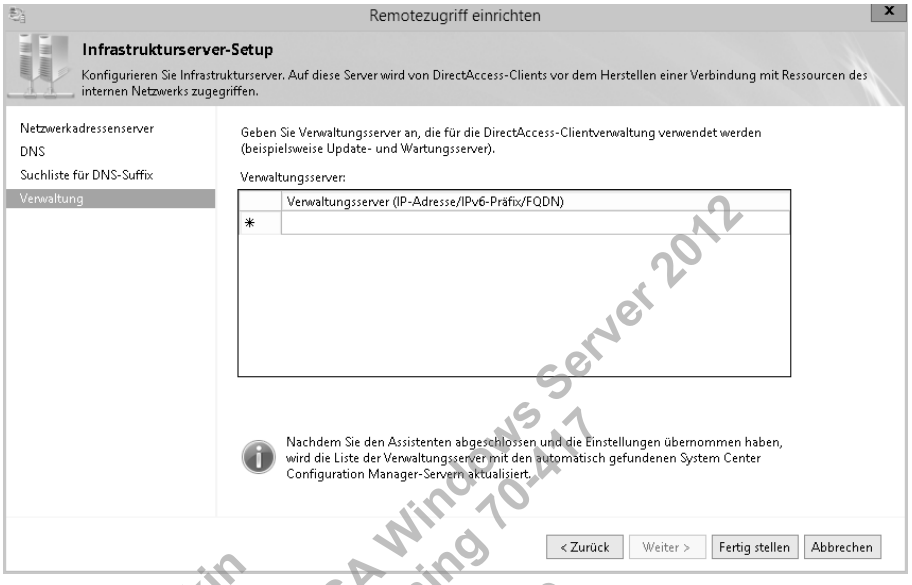

Abbildung 6.18 Die Seite *Verwaltung* des Assistenten für das Infrastrukturserver-Setup

Sie müssen hier keine Domänencontroller und keine SCCM-Server angeben, da sie bei der Erstkonfiguration von DirectAccess automatisch erkannt werden. Tragen Sie stattdessen solche Verwaltungsserver ein, die nicht automatisch erkannt werden können, z.B. WSUS-Aktualisierungsserver oder Antivirusserver. Wenn sich bei den Domänencontrollern oder SCCM-Servern nach der Einrichtung von DirectAccess etwas ändert, müssen Sie in der Remotezugriffs-Verwaltungskonsole lediglich auf *Verwaltungsserver aktualisieren* klicken, um die Liste der Verwaltungsserver auf den richtigen Stand zu bringen.

Es gibt noch einen weiteren Punkt zu beachten: Verwaltungsserver, die Verbindungen zu DirectAccess-Clients einleiten, müssen IPv6 entweder nativ oder über ISATAP unterstützen.

Schritt 4: Setup des DirectAccess-Anwendungsservers

Das Setup des DirectAccess-Anwendungsservers besteht nur aus einer einzigen Konfigurationsseite (siehe Abbildung 6.19). Hier können Sie Anwendungsserver angeben, deren Verbindung mit dem DirectAccess-Server verschlüsselt werden soll. (Der Datenverkehr zwischen dem DirectAccess-Client und dem Server ist natürlich ohnehin standardmäßig verschlüsselt.)

In Windows PowerShell geben Sie diese Anwendungsserver mit *Add-DAAppServer* an.

Schritt 5: Erweiterte Konfigurationsoptionen

Nach dem Setup der DirectAccess-Anwendungsserver sieht die Remotezugriffs-Verwaltungskonsole wie in Abbildung 6.20 aus. Jetzt können Sie weitere Assistenten starten, um die erweiterten Optionen festzulegen, z.B. die Bereitstellung auf mehreren Standorten oder den Lastenausgleich. Klicken Sie dazu im Aufgabenbereich auf die entsprechenden Einträge.

Abbildung 6.19 Setup des DirectAccess-Anwendungsservers

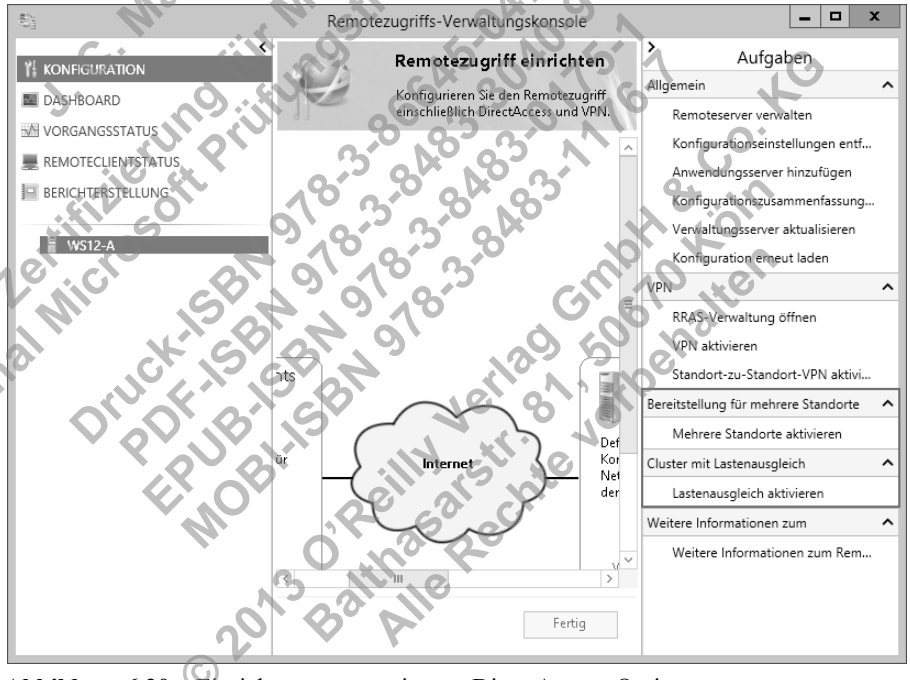

Abbildung 6.20 Einrichten von erweiterten DirectAccess-Optionen

Überprüfen der Konfiguration

Nach Abschluss der Konfiguration können Sie über den Eintrag *Vorgangsstatus* im linken Bereich der Remotezugriffs-Verwaltungskonsole überprüfen, ob DirectAccess betriebsbereit ist. Remoteclients können sich erst dann über DirectAccess mit dem Netzwerk verbinden, wenn der Status aller Komponenten wie in Abbildung 6.21 als *Funktionsfähig* angegeben wird. Es kann nach Abschluss des letzten Konfigurations-Assistenten mehrere Minuten dauern, bis dieser Zustand erreicht ist.

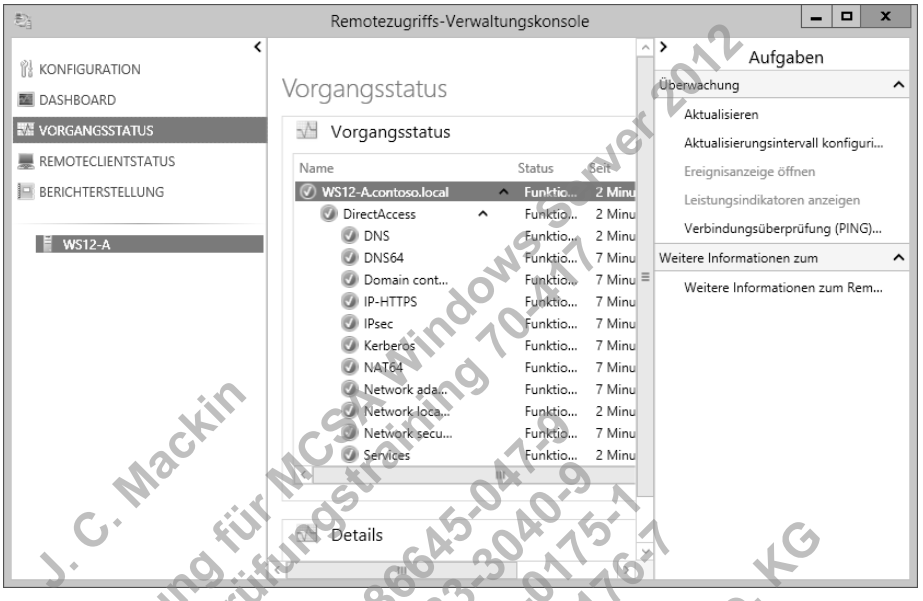

Abbildung 6.21 Vorgangsstatus von DirectAccess

Wenn alle Serverkomponenten funktionieren, können Sie die Verfügbarkeit von DirectAccess vom Client aus überprüfen. Als Erstes bestimmen Sie mit *Get-DAConnectionStatus*, ob DirectAccess den Standort des Clients korrekt ermitteln kann. Abbildung 6.22 zeigt die Windows PowerShell-Konsole auf einem mobilen Client. Zunächst ist er an das Unternehmensnetzwerk angeschlossen. Bei der Ausführung des Cmdlets in diesem Zustand wird gemeldet, dass der Client über eine lokale Verbindung verfügt. Anschließend wird der Laptop von dem Netzwerk getrennt und an eine Internet-Breitbandverbindung angeschlossen. Bei der anschließenden erneuten Ausführung des Cmdlets wird eine Remoteverbindung festgestellt, wobei die Anbindung an das Intranet über DirectAccess erfolgt. Eine weitere Möglichkeit, um das Funktionieren von DirectAccess auf dem Client zu überprüfen, besteht darin, einen Blick auf den Verbindungsstatus in der Netzwerkleiste zu werfen. Wie in Abbildung 6.23 zu sehen ist, wird die DirectAccess-Verbindung hier angezeigt, wenn sie verfügbar ist.

Abbildung 6.22 DirectAccess erkennt automatisch, ob ein Client lokal oder über das Netzwerk Verbindung aufnimmt.

Abbildung 6.23 Eine DirectAccess-Verbindung in der Netzwerkleiste von Windows 8

Das Symbol für die DirectAccess-Verbindung, das Sie in Abbildung 6.23 sehen, stellt einen Server dar, im Gegensatz zu dem VPN-Symbol aus Abbildung 6.24. Diese Symbole wurden in Windows Server 2012 und Windows 8 neu eingeführt. Sie sollten beide für die Prüfung 70-417 kennen.

Abbildung 6.24 Eine VPN-Verbindung in der Netzwerkleiste von Windows 8

Zusammenfassung des Lernziels

- DirectAccess ist eine beidseitige, ständig aktive Alternative zu einem VPN, mit der Clients Verbindung zu Ressourcen im Unternehmensnetzwerk aufnehmen können, wenn sie sich im Internet befinden. DirectAccess wurde in Windows Server 2008 R2 und Windows 7 eingeführt, doch wurde die Bereitstellung in Windows Server 2012 und Windows 8 erheblich vereinfacht.
- In Windows Server 2012 und Windows 8 ist es nicht mehr erforderlich, dass sich DirectAccess-Clients über Computerzertifikate authentifizieren. Stattdessen wird jetzt standardmäßig Kerberos vewendet.
- In Windows Server 2012 wurden verschiedene neue Infrastruktur- und Topologieoptionen für DirectAccess eingeführt, darunter die Unterstützung für mehrere Domänen und mehrere Standorte, die Möglichkeit der Bereitstellung hinter einem NAT-Gerät und der Lastenausgleich in einem NLB-Cluster.
- In Windows Server 2012 sind DirectAccess und VPNs in der neuen Serverrolle Remotezugriff zusammengefasst. Um sie hinzuzufügen, geben Sie an einer Windows PowerShell-Eingabeaufforderung mit erhöhten Rechten folgenden Befehl:

  ```
  Install-WindowsFeature RemoteAccess -IncludeManagementTools
  ```

- Zur Konfiguration von DirectAccess arbeiten Sie vier Assistenten durch, mit denen nacheinander die DirectAccess-Clients, der DirectAccess-Server, die Infrastruktur- und Anwendungsserver eingerichtet werden. Diese Assistenten weisen eine Reihe von Merkmalen und Optionen auf, die in Fragen der Prüfung 70-417 vorkommen können. Daher sollten Sie zur Vorbereitung auf die Prüfung alle Optionen in diesen Assistenten lernen.

Lernzielkontrolle

Beantworten Sie die folgenden Fragen, um zu prüfen, wie gut Sie den Stoff zu diesem Lernziel beherrschen. Antworten auf diese Fragen und Erklärungen darüber, warum eine bestimmte Antwort falsch oder richtig ist, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Was ist erforderlich, um eine DirectAccess-Verbindung zwischen einem Windows 8-Client und einem DirectAccess-Server mit Windows Server 2012 herzustellen?
   a. Ein Computerzertifikat auf dem Client
   b. Ein Benutzerzertifikat auf dem Client
   c. Eine IPv6-Adresse auf dem Client
   d. Eine IPv4-Adresse auf dem Client
2. Sie arbeiten als Administrator für ein Unternehmen, dessen Netzwerk aus einer einzigen Domäne namens *Contoso.com* besteht und 300 Computer mit Windows 8 und 20 Server mit Windows Server 2012 umfasst.

Sie werden beauftragt, DirectAccess mit einer Gruppe von 20 Testbenutzern in Ihrer Organisation auszuprobieren. Dazu stellen Sie einen DirectAccess-Server am Rand des Unternehmensnetzwerks bereit und richten die Computerauthentifizierung über Kerberos ein. Dann bitten Sie die Testbenutzer, von außerhalb des Betriebsgeländes Verbindung mit dem Unternehmensnetzwerk aufzunehmen. Alle diese Verbindungsversuche erfolgen mit Computern, die an die Domäne angeschlossen sind und Windows 8 ausführen. Die meisten der Benutzer konnten zwar Verbindung mit dem Unternehmensnetzwerk bekommen, doch einige, die mit Desktopcomputern oder virtuellen Maschinen arbeiten, waren dazu nicht in der Lage. Natürlich möchten Sie auch diesen Benutzern den Zugriff auf das Unternehmensnetzwerk über DirectAccess einräumen.

Mit welchem der folgenden Windows PowerShell-Befehle können Sie dieses Ziel wahrscheinlich erreichen?

a. *Set-DAClient -OnlyRemoteComputers "Enabled"*

b. *Set-DAClient -OnlyRemoteComputers "Disabled"*

c. *Set-DAClient -ForceTunnel "Enabled"*

d. *Set-DAClient -ForceTunnel "Disabled"*

3. Sie arbeiten als Administrator für ein Unternehmen, dessen Netzwerk aus einer einzigen Domäne namens *Contoso.com* besteht und 500 Computer mit Windows 8 und 30 Server mit Windows Server 2012 umfasst.

   Viele Angestellte arbeiten im Außendienst und besuchen das Betriebsgelände nur selten. Zurzeit sind sie über ein VPN mit dem Unternehmensnetzwerk verbunden. Um Softwarekorrekturen über System Center Configuration Manager anwenden zu können, möchten Sie DirectAccess bereitstellen, allerdings möchten Sie nicht, dass die Computer über die DirectAccess-Verbindung Zugriff auf Ressourcen im Unternehmensnetzwerk bekommen.

   Mit welchem der folgenden Windows PowerShell-Befehle können Sie dies erreichen?

   a. *Set-DAServer -DAInstallType ManageOut*

   b. *Set-DAServer -DAInstallType FullInstall*

   c. *Set-DAServer -HealthCheck "Enabled"*

   d. *Set-DAServer -HealthCheck "Disabled"*

Gedankenexperiment

Sie arbeiten als Netzwerkadministrator für das Unternehmen Fabrikam in Berlin, das eine Filiale in London unterhält. Das Netzwerk der Firma besteht aus drei Active Directory-Domänen, wobei *Fabrikam.com* Ressourcen aus beiden Büros enthält, *de.fabrikam.com* hauptsächlich Ressourcen aus Berlin und *uk.fabrikam.com* hauptsächlich solche aus London. Der Domänenname *Fabrikam.com* wird auch für die öffentliche Website des Unternehmens verwendet.

Die Server im Netzwerk führen teilweise Windows Server 2008 R2 und teilweise Windows Server 2012 aus, auf den Clients werden die Betriebssysteme Windows 7 und Windows 8 verwendet.

Zusammen mit der IT-Abteilung planen Sie die Bereitstellung von DirectAcces. Zurzeit erfolgt die Remoteverbindung der Benutzer mit dem Unternehmensnetzwerk über ein VPN, wobei die VPN-Server in beiden Büros Windows Server 2008 R2 aufweisen.

1. Die Büros in Berlin und London weisen jeweils zwei Ressourcen in der Domäne *Fabrikam.com* auf, auf die einige Remotebenutzer über eine DirectAccess-Verbindung zugreifen müssen. Sie möchten dafür sorgen, dass DirectAccess-Clients, die Verbindung mit Ressourcen in der Domäne *Fabrikam.com* aufnehmen, ein DNS-Lookup dafür durchführen, indem Sie sich an die internen DNS-Server wenden. Für die Verbindungsaufnahme mit der öffentlichen Website *www.fabrikam.com* dagegen sollen sich die DirectAccess-Clients an öffentliche DNS-Server wenden. Wie können Sie dafür sorgen, dass die DirectAccess-Clients jeweils die richtigen DNS-Server verwenden, wenn Sie auf Ressourcen mit dem Domänensuffix *fabrikam.com* zugreifen?
2. Remotebenutzer sollen automatisch über DirectAccess mit dem nächstliegenden Eintrittspunkt zum Unternehmensnetzwerk verbunden werden, sei es nun London oder Berlin. Wie können Sie dies erreichen, und welche Voraussetzungen müssen dazu erfüllt sein?
3. Wenn Remotebenutzer im Berliner Büro über eine DirectAccess-Verbindung eine Adresse wie *http://app1* eingeben, soll in DNS zunächst die Adresse *app1.de.fabrikam.com* und danach *app1.uk.fabrikam.com* abgefragt werden. Wie können Sie dies erreichen.
4. Für bestimmte Benutzer, die eine Remoteverbindung zu vertraulichen Ressourcen benötigen, möchten Sie eine zweistufige Authentifizierung einrichten. Allerdings scheuen Sie die Kosten und den Verwaltungsaufwand für herkömmliche Smartcards. Welche beiden Alternativen können Sie in Ihrer Umgebung für die zweistufige Authentifizierung nutzen?

Antworten

Dieser Abschnitt enthält die Antworten auf die Fragen der Lernzielkontrolle und die Lösung des Gedankenexperiments in diesem Kapitel.

Lernziel 6.1: Lernzielkontrolle

1. **Richtige Antwort: C**
   a. **Falsch:** In Windows Server 2012 und Windows 8 kann Kerberos anstelle von Computerzertifikaten verwendet werden.
   b. **Falsch:** Für eine DirectAccess-Verbindung ist kein Benutzerzertifikat erforderlich.
   c. **Richtig:** DirectAccess-Verbindungen stützen sich auf IPv6-Kommunikation. Wenn der DirectAccess-Client keine globale IPv6-Adresse aus seiner Umgebung beziehen kann, muss er dies über eine IPv6-Übergangstechnologie tun.
   d. **Falsch:** Für DirectAccess ist keine IPv4-Kommunikation erforderlich.
2. **Richtige Antwort: B**
   a. **Falsch:** Wenn nur Desktopcomputer und VMs Probleme mit der Verbindungsaufnahme über DirectAccess haben, ist diese Einstellung höchstwahrscheinlich bereits aktiviert.
   b. **Richtig:** Dieser Befehl deaktiviert die Einstellung, die die DirectAccess-Anbindung auf mobile Computer beschränkt.
   c. **Falsch:** Diese Einstellung leitet den gesamten Datenverkehr vom Client zwangsweise über eine DirectAccess-Verbindung. Das hilft Desktopcomputern und VMs nicht dabei, eine DirectAccess-Verbindung herzustellen.
   d. **Falsch:** Diese Einstellung sorgt dafür, dass nicht mehr der gesamte Datenverkehr von den Clients über eine DirectAccess-Verbindung geleitet werden muss. Das hilft Desktopcomputern und VMs nicht dabei, eine DirectAccess-Verbindung herzustellen.
3. **Richtige Antwort: A**
   a. **Richtig:** Mit diesem Befehl wird DirectAccess ausschließlich für die Remoteverwaltung bereitgestellt.
   b. **Falsch:** Mit diesem Befehl wird DirectAccess vollständig, also sowohl für die Remoteverwaltung als auch für den Clientzugriff, bereitgestellt.
   c. **Falsch:** Mit diesem Befehl werden NAP-Integritätsprüfungen für DirectAccess-Clients gefordert. Dadurch wird DirectAccess nicht ausschließlich für die Verwaltung eingerichtet.
   d. **Falsch:** Mit diesem Befehl werden NAP-Integritätsprüfungen für DirectAccess-Clients deaktiviert. Dadurch wird DirectAccess nicht ausschließlich für die Verwaltung eingerichtet.

Gedankenexperiment

1. Sie können die vier internen Ressourcen von *Fabrikam.com* in der Tabelle für Netzwerkauflösungsrichtlinien (NRPT) mit internen DNS-Servern verknüpfen.
2. Sie können eine Bereitstellung für mehrere Standorte einrichten. Dazu müssen die DirectAccess-Server Windows Server 2012 und die Clients Windows 8 ausführen. Außerdem muss das Unternehmen eine PKI bereitgestellt haben.
3. Richten Sie beim Infrastrukturserver-Setup der DirectAccess-Bereitstellung eine Suchliste für DNS-Suffixe für die Domäne *de.fabrikam.com* ein.
4. Sie können virtuelle Smartcards und OTPs verwenden.