Neuerungen in Windows Server 2008 R2

Christian Zahler

1 Active Directory

1.1 Domänen-Funktionsebenen

Neue Domänenfunktionsebene:

- Windows Server 2008 R2: nur Windows Server 2008 R2 DCs

Verfügbare Funktionalität ab Domänenfunktionsebene „Windows Server 2008 R2"

Die auf der Domänenfunktionsebene von Windows Server 2008 R2 verfügbaren Features umfassen neben den auf der Domänenfunktionsebene von Windows Server 2008 verfügbaren Features zusätzlich folgendes Feature:

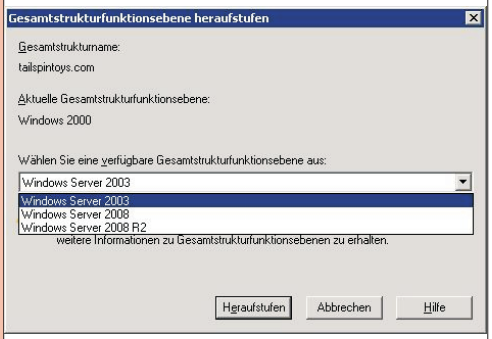
- Authentifizierungszusicherung, mit der anhand des Kerberos-Tokens eines Benutzers bestimmt werden kann, welche Anmeldemethode von diesem Benutzer verwendet wurde.

1.2 Gesamtstruktur-Funktionsebenen

Neue Gesamtstrukturfunktionsebene:

- Windows Server 2008 R2

Verfügbare Features ab Gesamtstruktur-Funktionsebene „Windows Server 2008 R2"



- Papierkorb: Bietet (sofern aktiviert) die Möglichkeit zum Wiederherstellen gelöschter Objektein ihrer Gesamtheit, während die Active Directory-Domänendienste ausgeführt werden.

Alle in der Gesamtstruktur erstellten neuen Domänen werden standardmäßig auf der Domänenfunktionsebene von Windows Server 2008 R2 ausgeführt.

1.3 Active Directory Module for Windows PowerShell

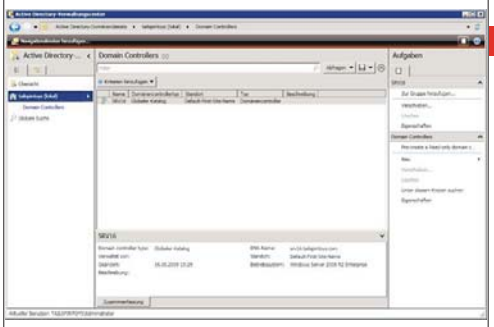
Neu ab Windows Server 2008 R2. Dieses Modul stellt eine Kommandozeilenschnittstelle dar, mit der Administratoren alle ADDS- und ADLDS-Instanzen verwalten und überwachen können. Dieses Feature besteht aus einer Reihe von PowerShell-CmdLets und einem AD-Provider, mit dem durch das AD in hierarchischer Art und Weise (ähnlich wie das NTFS-Dateisystem) navigiert werden kann.

Es ist möglich, sich mit allen vorhandenen ADDS- und ADLDS-Instanzen sowie zu AD-Snapshots zu verbinden.

Mit diesen Powershell-Cmdlets ist es auch möglich, Gruppenrichtlinien zu verwalten.

1.4 Active Directory-Verwaltungscenter

Dieses Tool ist neu in Windows Server 2008 R2 und basiert auf PowerShell 2.0.



Mit diesem Tool können auf Basis einer grafischen Oberfläche Routineaufgaben vereinfacht ausgeführt werden.

1.5 Offline Domain Join

Mit entsprechender Vorbereitung ist es möglich, Arbeitsstationen ohne Verbindung zum firmeninternen Netzwerk an die Domäne anzubinden.

Führen Sie auf dem DC zunächst folgende Anweisung aus:

```
DJOIN /Provision /Domain domain_name /Machine
pc23 /SaveFile pc23.Djoin
```

Damit wird ein Computerkonto in AD erstellt, außerdem wird eine verschlüsselte "Beitrittsdatei" erzeugt, mit deren Hilfe der Domänenbeitritt erledigt werden kann. Kopieren Sie diese Datei auf einen USB-Stick und führen Sie auf der Offline-Windows-Maschine folgende Anweisung aus:

```
DJOIN /Requestodj /LoadFile pc23.DJoin
/WindowsPath \Mount\Windows
```

Damit wird `pc23` zur Domäne hinzugefügt.

1.6 Reanimierung von gelöschten ADDS-Objekten mit dem Papierkorb

1.6.1 Active Directory Recycle Bin

Wenn Sie die Domäne in der Domänenfunktionsebene Windows Server 2008 R2 betreiben, so steht Ihnen für die Reanimierung von Objekten der erweiterte *"Recycle Bin"* (Papierkorb) zur Verfügung. Dieses Feature ist standardmäßig deaktiviert; es muss über die AD-Powershell wie folgt aktiviert werden:

```
Enable-ADOptionalFeature 'Recycle Bin Feature'
-Scope ForestOrConfigurationSet
  -Target 'fabrikam.com' –server dc01
```

Grob zusammengefasst, wird bei aktiviertem Papierkorb die Erstellung von Tombstones geändert: Es werden alle Attribute (Linked-Value und Nicht-Linked-Value-Attribute) im Tombstone beibehalten und können dadurch auch wiederhergestellt werden. Der Wiederherstellungsvorgang selbst ändert sich dadurch aber nicht.

1.6.2 Reanimierung über PowerShell

Auf einem Windows Server 2008 R2-DC im Gesamtstruktur-Funktionsebene „Windows Server 2008 R2" kann der AD Recycle Bin aktiviert werden. Im Falle des aktivierten „Papierkorbs" kann mit dem AD-Modul für Powershell wie folgt ein versehentlich gelöschtes Benutzerobjekt „Mary" wiederhergestellt werden:

```
Get-ADObject -Filter {displayName -eq "Mary"}
-IncludeDeletedObjects | Restore-ADObject
```

2 VPN Reconnect (auch Windows 7)

Hiermit wird eine VPN-Verbindung automatisch wieder hergestellt, sobald die Internetverbindung wieder verfügbar ist. So müssen die Benutzer nicht erneut ihre Anmeldeinformationen eingeben und die VPN-Verbindung wieder herstellen.

Bei der VPN-Verbindungswiederherstellung handelt es sich um ein neues Feature der Routing- und RAS-Dienste, das eine nahtlose und einheitliche VPN-Verbindung für die Benutzer bereitstellt und eine VPN-Verbindung automatisch wieder herstellt, wenn die Internetverbindung eines Benutzers vorübergehend getrennt wird. Für Benutzer, die eine Verbindung über drahtloses mobiles Breitband herstellen, stellt diese Funktion den größten Vorteil dar. Mit der VPN-Verbindungswiederherstellung stellt Windows 7 aktive VPN-Verbindungen automatisch wieder her, wenn die Internetverbindung wiederhergestellt wird. Auch wenn das erneute Herstellen der Verbindung einige Sekunden dauern kann, ist dies transparent für die Benutzer.

Bei der VPN-Verbindungswiederherstellung wird der IPsec-Tunnelmodus mit Internetschlüsselaustausch Version 2 *(Internet Key Exchange 2, IKEv2)* verwendet (in RFC 4306 beschrieben) verwendet. Dabei wird insbesondere das in RFC 4555 beschriebene IKEv2-MOBIKE *(Mobility and Multihoming Extension)* verwendet.

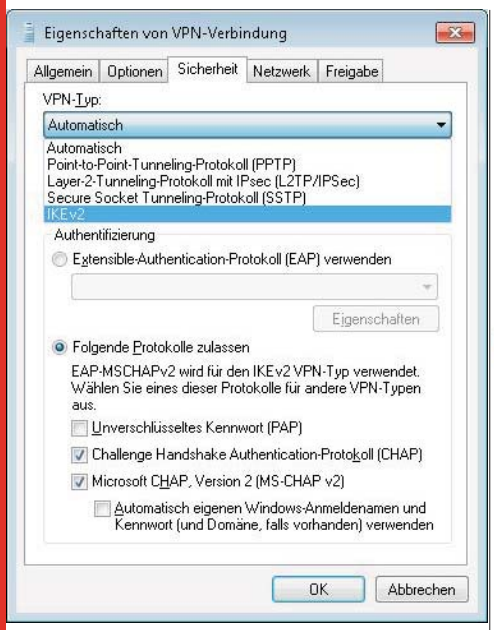
Die VPN-Verbindungswiederherstellung wird im RRAS-Rollendienst der NPAS-Rolle (*Network Policy and Access Services*, Netzwerkrichtlinien- und Zugriffsdienste) eines Computers unter Windows Server 2008 R2 implementiert. Die Überlegungen zur Infrastruktur entsprechen den Überlegungen für NPAS und RRAS. Auf den Clientcomputern muss Windows 7 ausgeführt werden, damit die VPN-Verbindungswiederherstellung optimal genutzt werden kann.

Firewall-Ausnahmeregeln (müssen sowohl am VPN-Server als auch am VPN-Client erstellt werden):

- UDP ports 500 and 4500 (IKE)
- IP Protocol ID 50 *(Encapsulating Security Protocol, ESP)*

Die benötigten Regeln werden bei der Installation von Routing und Remote Access auf dem Server automatisch erstellt. Auf Clients ist nach außen gehender Datenverkehr, der vom Client selbst initiiert wird, automatisch erlaubt. Standardmäßig sollte die Firewall also alle benötigten Protokolle durchlassen.

Die Reconnection-Fähigkeit wird aktiviert, wenn man in den Eigenschaften der Client-VPN-Verbindung als VPN-Typ IKEv2 wählt.



3 DirectAccess (auch Windows 7)

DirectAccess ist eine Technologie, mit der es möglich ist, als berechtigter DirectAccess-Benutzer von einem Remote-PC ohne VPN auf ein Firmennetzwerk zuzugreifen. Dabei wird eine bidirektionale Verbindung aufgebaut, über die auch Software-Updates und Gruppenrichtlinien bezogen werden können.

DirectAccess soll eine Alternative zu VPN darstellen, da VPN-Verbindungen folgende Nachteile aufweisen:

- Aufbau einer VPN-Verbindung benötigt mehrere Schritte
- Bei Organisationen, die den Client überprüfen, bevor eine VPN-Verbindung zugelassen wird, kann der VPN-Aufbau mehrere Minuten dauern.
- Immer, wenn die Internet-Verbindung auf der Client-Seite abbricht, muss die VPN-Verbindung wiederhergestellt werden.
- Internet-Performance leidet unter VPN-Datenverkehr

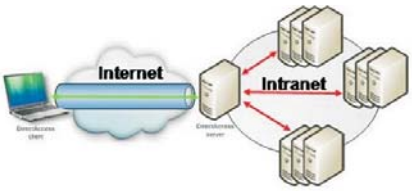
Voraussetzungen

- Domänencontroller mit Windows Server 2008; wenn Zwei-Faktor-Authentifizierung verwendet werden soll (SmartCard-Unterstützung), Windows Server 2008 R2
- DirectAccess Server mit Windows Server 2008 R2, zwei Netzwerkkarten (eine mit Verbindung zum Corporate Network, eine zweite mit Verbindung ins Internet); dieser Server sollte Domänenmitglied sein
- PKI
- IPv6 auf allen Computern aktiviert
- Client-Computer mit Windows 7 Enterprise oder Ultimate Edition, muss Domänenmitglied sein!

Die Authentifizierung in DirectAccess beruht auf IPSec. DirectAccess verwendet für die Authentifizierung zwischen DA-Client und DA-Server den IPSec-Transportmodus und den Tunnelmodus.

Wenn ein Remote-DA-Client Daten zum Firmennetzwerk sendet, so wird der Datenverkehr in einem verschlüsselten IPSec-Tunnel verkapselt:

End-to-Edge-Zugriffsmodell: Die Clients stellen eine IPSec-Sitzung zu einem IPSec-Gateway-Server her (kann derselbe Server wie der DirectAccess-Server sein); der Tunnel endet beim IPSec-Gateway. Der IPSec-Server leitet dann unverschlüsselten IP-Verkehr an die Firmenserver weiter. Diese Architektur benötigt kein IPSec im Intranet und funktioniert mit allen Anwendungsservern, die IPv6 unterstützen.



End-to-End-Zugriffsmodell: Die Clients stellen IPSec-Sitzungen her, die bei den internen Anwendungsservern enden. Diese Architektur stellt die höchstmögliche Sicherheit zur Verfügung, setzt aber Anwendungsserver voraus, die sowohl IPv6 als auch IPSec unterstützen.

Client-IP-Konfiguration	Verbindungsmethode
Global routbare IPv6-Adresse	Global routbare IPv6-Adresse
Public IPv4-Adresse	6to4
Private (NAT) IPv4-Adresse	Teredo
Wenn der Client sich nicht mit einer der vorher genannten Methoden verbinden kann	IP-HTTPS

Teredo, 6to4 und das *Intra Site Automatic Tunnel Addressing Protocol* (ISATAP) sind Beispiele für Übergangstechnologien von IPv4 und IPv6. Diese Technologien erlauben es Ihnen, IPv6 zu nutzen, bevor die gesamte Netzwerkinfrastruktur IPv6 unterstützt. IP-HTTPS ist ein neues Protokoll für Windows 7, das Hosts hinter einem Proxy oder einer Firewall erlaubt, eine Verbindung über einen IP-Tunnel innerhalb eines HTTPS-Tunnels aufzubauen. HTTPS wird statt HTTP verwendet, damit Proxy-Server nicht versuchen, in die Pakete des Datenstroms hineinzuschauen und die Verbindung zu beenden, wenn der Datenverkehr "abnormal" aussieht. HTTPS stellt dabei aber keinen Sicherheitsmechanismus bereits; Sicherheit wird einzig und allein durch IPSec bereitgestellt.

Namensauflösung: DirectAccess unterstützt DNSSEC, falls der DNS-Serverdienst auf Windows Server 2008 R2 installiert ist.

Die NRPT *(Name Resolution Policy Table)* speichert eine Liste von Namespaces und Konfigurationseinstellungen, die das Verhalten des DNS-Clients in Bezug auf diesen Namespace festlegen.

Namensauflösungsanfragen werden mit den Namespaces verglichen, die in der NRPT gespeichert sind, und entsprechend der Konfiguration verarbeitet.

So wird in DirectAccess festgelegt, ob eine Anfrage verschlüsselt wird oder nicht und zu welchem DNS-Server sie gesendet werden.

Wenn eine Anfrage nicht mit einem in der NPRT gespeicherten Namespace übereinstimmt, dann wird sie unverschlüsselt zu dem DNS-Server gesendet, der in den TCP/IP-Einstellungen festgelegt ist (Standardverhalten). Im Fall eines Remote-Clients wird das häufig der DNS-Server des Internet Service Providers sein.

Wenn für den Aufruf einer Intranet-Seite ein einteiliger Name wie zum Beispiel `http://intranet` abgefragt wird, so wird der Client alle jene DNS-Suffixe anhängen, die er konfiguriert hat, bevor er in der NRPT-Tabelle nachschaut. Sollten keine DNS-Suffixe konfiguriert sein bzw. der eingegebene Name keinem anderen in der NPRT gespeicherten Hostnamen entsprechen, so wird die Anfrage wieder an den in der TCP/IP-Einstellungen angegebenen DNS-Server weitergeleitet.

Die NPRT-Tabelle wird folgendermaßen befüllt:

- Angabe des Namensraums (`beispielsweise.corp.contoso.com`)
- Name oder IP-Adresse des/der DNS-Server(s), der/die Anfragen für diesen Namensraum beantworten soll(en)

Bei Angabe einer IP-Adresse für den DNS-Server werden alle DNS-Anfragen über den verschlüsselten IPSec-Tunnel direkt zu diesem DNS-Server gesendet. Für diese Konfiguriation sind keine weiteren Sicherheitsmaßnahmen erforderlich.

Wenn allerdings in der NPRT ein FQDN für den DNS-Server eingegeben wird (etwa `dns.contoso.com`), dann muss dieser Name öffentlich (im Internet) auflösbar sein, wenn der Client seinen in den TCP/IP-Einstellungen konfigurierten DNS-Server abfragt. Es könnte in diesem Fall ein Angreifer versuchen, diese externe Namensabfrage zu "kapern" und eine gefälschte DNS-Antwort zurückschicken. Daher ist für dieses Szenarion IPSec-Verschlüsselung zu empfehlen.

Firewallkonfiguration

Firewall	Port bzw. Protokollnummer	Richtung und Ziel
Äußerer	IPv6	eingehend und ausgehend
Äußerer	IP Protocol 50 (ESP)	eingehend und ausgehend
Äußerer	UDP 3544 (Teredo)	eingehend
Äußerer	IP Protocol 41	eingehend und ausgehend
Äußerer	TCP 443 (SSL)	eingehend
Innerer	UDP 500 (AuthIP)	eingehend und ausgehend
Innerer	IP Protocol 50 (ESP)	eingehend und ausgehend

http://www.microsoft.com/germany/windowsserver2008r2/

3.1 Ablauf des DirectAccess-Verbindungsaufbaus

DirectAccess-Clients verwenden den folgenden Prozess, um eine Verbindung zu Intranetressourcen herzustellen:

1. Der DirectAccess-Windows 7-Clientcomputer stellt fest, dass eine Verbindung zu einem Netzwerk hergestellt ist.
2. Der DirectAccess-Clientcomputer versucht, eine Verbindung zu einer vom Administrator während der DirectAccess-Konfiguration festgelegten Intranet-Website herzustellen. Wenn die Website erreichbar ist, dann stellt der DirectAccess-Client fest, dass er bereits mit dem Intranet verbunden ist, und der Verbindungsvorgang wird beendet. Ist diese Website nicht erreichbar, dann stellt der DirectAccess-Client fest, dass er mit dem Internet verbunden ist – in diesem Fall wird der Verbindungsvorgang fortgesetzt.
3. Der DirectAccess-Clientcomputer stellt eine Verbindung zum DirectAccess-Server mit IPv6 und Ipsec her. Sollte ein natives IPv6-Netzwerk nicht zur Verfügung stehen (was derzeit sehr wahrscheinlich ist, wenn der Benutzer mit dem Internet verbunden ist!), dann versucht der Client den Verbindungsaufbau mit einem IPv6-over-IPv4-Tunnel unter Verwendung der Protokolle 6to4 oder Teredo. Der Benutzer muss sich nicht angemeldet haben, damit dieser Schritt beendet werden kann.
4. Sollte eine Firewall oder ein Proxyserver verhindern, dass ein Client eine 6to4 oder Teredo-Verbindung zum DirectAccess-Server aufbaut, so versucht der Client automatisch, eine Verbinduing mit dem IP-HTTPS-Protokoll aufzubauen. IP-HTTPS verwendet eine Secure Sockets Layer (SSL)-Verbindung.
5. Als Teil des IPSec-Verbindungsaufbaus erfolgt zwischen DirectAccess-Client und –Server eine gegenseitige Authentifizierung durch Computerzertifikate.
6. Schließlich wird durch Überprüfung der Zugehörigkeit zu den Active Directory-Gruppen festgestellt, ob Computer und Benutzer autorisiert sind, über DirectAccess eine Verbindung aufzubauen.

   Hinweis: Um das Risiko einer Denial of Service (DoS) Attacke zu minimieren, IPsec on the DirectAccess server de-prioritizes key negotiation traffic using Differentiated Services Code Points (DSCPs).
7. Wenn Network Access Protection (NAP) aktiviert ist und auch die Integritätsüberprüfung konfiguriert ist, dann bezieht der DirectAccess-Client ein Integritätszertifikat (engl. health certificate) von der Health Registration Authority (HRA) im Intranet, bevor eine Verbindung zum DirectAccess-Server hergestellt wird. Die HRA sendet den Integritätsstatus des DirectAccess-Clients weiter zum NAP-Richtlinienserver. Die NAP-Integritätskontrolle verarbeitet die im Network Policy Server (NPS)-Server definierten Richtlinien und stellt fest, ob der Client "compliant" mit den Regeln der Integritätsrichtlinie ist. Wenn das der Fall ist, dann bezieht die HRA ein Integritätszertifikat für den DirectAccess-Client. Wenn sich dann der DirectAccess-Client zum DirectAccess-Server verbindet, so sendet er ihm sein Integritätszertifkat für die Authentifizierung.
8. Der DirectAccess-Server beginnt, den Datenverkehr vom DirectAccess-Client zu den Intranet-Ressourcen weiterzuleiten, für die der Benutzer Zugriffsberechtigungen hat.

Standardmäßig implementiert DirectAccess eine Richtlinie, die zwei verschlüsselte IPSec-Tunnel aufbaut:

1. Der erste Tunnel verwendet IPsec/ESP mit einem Client-Computerzertifikat für die Authentifizierung des Computers. Dieser Tunnel stellt eine sicheren Verbindungskanal zwischen einem DA-Client und den Ressourcen des Unternehmens her, bevor sich der User am DA-Clientcomputer anmeldet. Das ist unbedingte Voraussetzung dafür, dass sich der Benutzer an den Domänencontrollern des Unternehmens anmelden kann.
2. Der zweite Tunnel verwendet IPsec/ESP mit einem Client-Computerzertifikat und Kerberos-Benutzeranmeldeinformationen. Dieser zweite Tunnel wird benötigt, um Zugriff auf alle anderen Unternehmensressourcen zu erhalten, wenn der Benutzer bereits an der Domäne angemeldet ist.

3.2 Vorbereitende Tätigkeiten

Für den reibungslosen Betrieb sind etliche vorbereitende Maßnahmen nötig:

- Stellen Sie den reibungslosen Betrieb der PKI sicher; alle Computer müssen automatisch Computerzertifikate beziehen, auch die CRL muss korrekt veröffentlicht worden sein.
- Legen Sie im Active Directory eine Sicherheitsgruppe *DirectAccessComputers* an. Alle Computer, die DirectAccess nutzen sollen, müssen Mitglied dieser Sicherheitsgruppe werden.
- Entfernen Sie ISATAP aus der standardmäßigen globalen DNS-Sperrliste:

```
dnscmd /config /globalqueryblocklist wpad
```

- Treten Sie mit dem DirectAccess-Clientcomputer der Domäne bei.
- Fügen Sie das Computerkonto des DirectAccess-Clientcomputers zur Sicherheitsgruppe *DirectAccessComputers* hinzu.

3.3 Installation des DirectAccess-Servers

Bereiten Sie den DirectAccess-Server wie folgt vor:

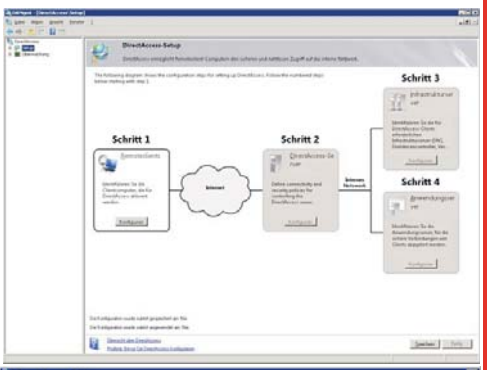
- Konfigurieren Sie die beiden Netzwerkkarten mit statischen IP-Adressen. Achten Sie darauf, dass IPv6 unterstützt wird.
- Konfigurieren Sie die öffentliche Netzwerkkarte mit zwei aufeinanderfolgenden öffentlichen statischen IP-Adressen.
- Treten Sie der Firmendomäne bei.
- Firewall-Regelsätze: bei der externen Netzwerkkarte *"Öffentlich"*, bei der internen Netzwerkkarte *"Domäne"*.
- Installieren Sie die Webserver-Rolle.

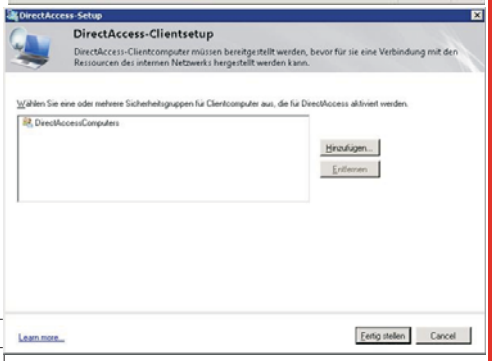
Fügen Sie über den Server-Manager das Feature *"DirectAccess Verwaltungskonsole"* hinzu.

Das Feature *„Gruppenrichtlinienverwaltung“* ist Voraussetzung für die DirectAccess-Verwaltungskonsole und wird gegebenenfalls nachinstalliert.

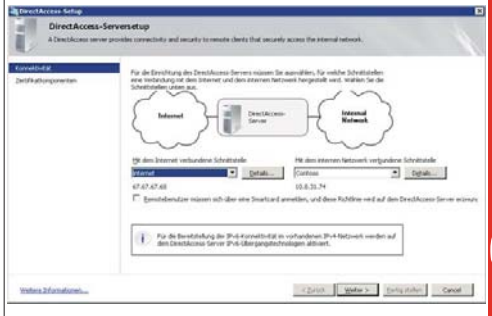
Im Verwaltungsmenü wird das Snap-In *DirectAccess* hinzugefügt.

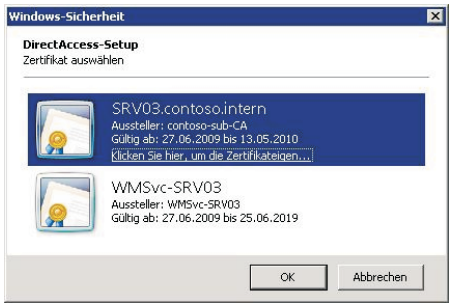
Folgen Sie dem Setup-Assistenten und legen die die Sicherheitsgruppe der DirectAccess-Clientcomputer, die verwendeten IPv6-Technologien sowie das SSL-Zertifikat, das der Client bei IP-HTTPS verwenden soll, fest.

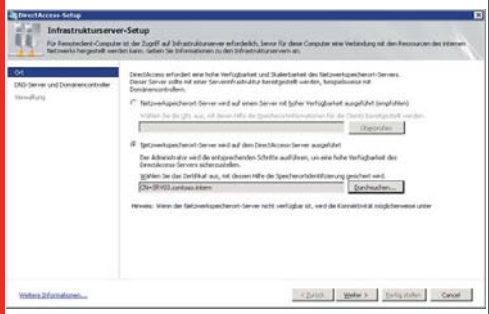


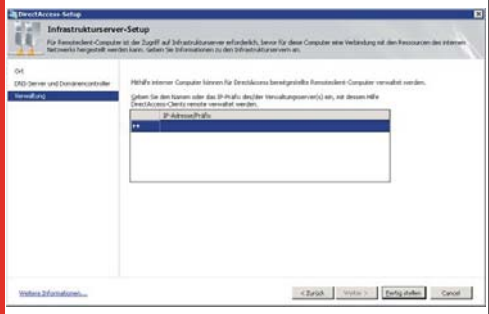


Beachten Sie, dass die interne Netzwerkschnittstelle mit einem verbindungsspezifischen DNS-Suffix konfiguriert sein muss.









Führen Sie folgenden Befehl auf dem Domänencontroller, Webserver und allen DirectAccess-Clients aus, damit sie sich selbst als ISATAP-Host konfigurieren:

```
sc control iphlpsvc paramchange
```

Testen Sie die Konnektivität zu einer Intranet-Seite und zu einem freigegebenen Ordner im firmeninternen Netz.

4 BranchCache (Windows Server 2008 R2/Windows 7)

Wenn BranchCache aktiviert ist, so wird eine Kopie allen Daten, die von Intranet-Webservern und Fileservern in eine Zweigstelle heruntergeladen werden, in der Zweigstelle lokal gecacht. Wenn ein zweiter Client im selben Zweigstellennetz dieselbe Datei herunterladen möchte, so wird sie vom lokalen Cache und nicht übers WAN geladen.

BranchCache speichert nur Leseanforderungen zwischen, er greift nicht in Speichervorgänge eines Benutzers ein.

BranchCache kann in zwei Betriebsmodi arbeiten:

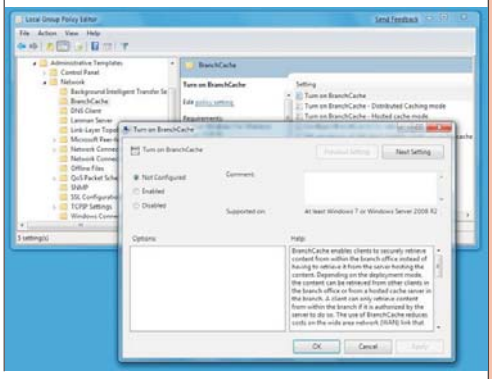
- **Distributed Cache:** Verwendet eine Peer-to-Peer-Architektur. Hier wird der gecachte Inhalt auf einem Windows 7-Clientcomputer in der Zweigstelle zwischengespeichert. Ein Windows Server 2008 R2-Server ist nur in der Zentrale nötig.
- **Hosted Cache:** Hier wird der Inhalt auf einem Windows Server 2008 R2-Server (Core oder Vollinstallation möglich) in der Zweigstelle zwischengespeichert.

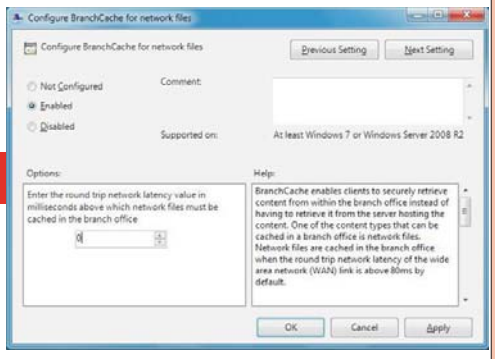
Zunächst muss auf dem betroffenen Web- oder BITS-Server das Feature BranchCache installiert werden.

Um auf einem Client BranchCache zu aktivieren, sind folgende Arbeitsschritte durchzuführen:

- BranchCache einschalten
- Cache-Modus wählen: Distributed Cache oder Hosted Cache
- Hostname des Hosted-Cache-Servers festlegen
- Client-Cache-Größe als Prozentanteil der Festplattengröße oder Bytes angeben
- Cache-Speicherort auf der Festplatte festlegen
- Firewall-Ausnahmeregeln konfigurieren
- Inhaltserkennung: UDP 3702 (WS-Discovery protocol)
- Inhaltsdownload: TCP 80 (HTTP protocol)

Um BranchCache auf Client-Computern zu aktivieren, sind einige Gruppenrichtlinien einzurichten.





Im Gruppenrichtlinieneditor finden Sie die folgenden BranchCache-Richtlinien unter *Administrative Vorlagen – Netzwerk – BranchCache*:

Richtlinie

Funktion

Turn on BranchCache

Legt fest, ob *BranchCache* eingeschaltet werden soll. Verwenden Sie diese Richtlinie in Zweigstellen mit geringer Bandbreite und hoher Latenz zur Zentrale. Es ist nicht nötig, diese Richtlinie in gut angebundenen Zweigstellen zu setzen.

Aktiviert: BranchCache ist eingeschaltet

Deaktiviert oder nicht konfiguriert: BranchCache ist ausgeschaltet.

Turn on BranchCache – Distributed Caching mode

Legt fest, ob der *BranchCache Distributed Cache*-Modus aktiviert werden soll. Verwenden Sie diese Richtlinie in Zweigstellen mit geringer Bandbreite und hoher Latenz zur Zentrale. Es ist nicht nötig, diese Richtlinie in gut angebundenen Zweigstellen zu setzen.

Aktiviert: Distributed Cache-Modus ist eingeschaltet

Deaktiviert oder nicht konfiguriert: Distributed Cache-Modus ist ausgeschaltet.

Turn on BranchCache – Hosted Caching mode

Hier wird der Name des Hosted Cache-Servers festgelegt. Diese Einstellung muss getroffen werden, wenn ein Hosted Cache in der Zweigstelle eingerichtet wird. Wichtig: Der hier eingetragene Servername muss mit dem im SSL-Zertifikat verwendeten Namen exakt übereinstimmen. Es wird empfohlen, den FQDN des Servers zu verwenden.Clients verwenden SSL, um mit dem Hosted Cache zu kommunizieren. Beachten Sie, dass das Computerkonto des Clients-PCs dem Zertifikat der Stammzertifizierungsstelle vertrauen muss.

Aktiviert: Manuelle Eingabe des Hosted Cache-Servers nötig.

Deaktiviert oder nicht konfiguriert: Hosted Cache wird in der Zweigstelle nicht verwendet.

Set percentage of disk space used for client computer cache

Hier können Sie den Prozentanteil des gesamten verfügbaren Festplattenspeicherplatzes festlegen, der für BranchCache verwendet werden soll.

Aktiviert: Manuelle Eingabe des Prozentsatzes erforderlich.

Deaktiviert oder nicht konfiguriert: In diesem Fall wird der Prozentsatz auf 5 % des gesamten Festplattenspeicherplatzes am Clientcomputer festgelegt.

BranchCache for network files

Legt fest, ob BranchCache auch SMB-Dateien bzw. SMB-Downloads cachen soll.

Aktiviert: Hier können Sie die minimale Latenz festlegen, unterhalb derer BranchCache nicht für SMB-Verkehr verwendet werden soll.

Deaktiviert oder nicht konfiguriert: BranchCache optimiert SMB-Verkehr nicht.

5 Weitere Neuerungen in der Netzwerkinfrastruktur von Windows Server 2008 R2

5.1 Mobiles Breitband

Windows 7 stellt Plug & Play-Zugriff und eine einheitliche Benutzeroberfläche für mobile Breitbandverbindungen bereit, unabhängig davon, ob der Benutzer die Verbindung über eine integrierte oder externe Datenkarte für drahtloses Breitband herstellt. Mit dem mobilen Breitband wird in Windows 7 keine zusätzliche Software mehr benötigt, um eine Verbindung mit mobilen Breitbandnetzwerken herzustellen.

5.2 URL-basierter QoS

In Windows 7 und Windows Server 2008 R2 können IT-Administratoren mit Gruppenrichtlinieneinstellungen Webdatenverkehr auf Grundlage der URL priorisieren. Mit URL-basiertem QoS (Quality of Service, Dienstqualität) können IT-Administratoren sicherstellen, dass kritischer Webdatenverkehr die richtige Priorität erhält. So wird die Leistung in Netzwerken mit hoher Auslastung gesteigert.

5.3 DNS-Sicherheitserweiterungen

Durch die Unterstützung von DNSSEC können Windows 7- und Windows Server 2008 R2-Computer DNS-Server authentifizieren. Hierdurch können Man-in-the-Middle-Angriffe abgewehrt werden. Bei einem *Man-in-the-Middle*-Angriff werden Clients zu einem böswilligen Server umgeleitet, sodass Angreifer Kennwörter oder vertrauliche Daten abfangen können.

6 Anwendungsplattform

Im folgenden ein kleiner Ausschnitt an neues Features in der Anwendungsplattform von Windows Server 2008 R2:

6.1 Remote Desktop Services

Die *"Terminal Services"* wurden in *"Remote Desktop Services"* umbenannt.

Außerdem wurde eine Vielzahl von Features überarbeitet:

- Verbesserung des Gesamteindrucks beim Endbenutzer durch Aero Glass-Unterstützung, Audiorecorder, Unterstützung mehrerer Bildschirme usw.
- Unterstütung von Nicht-Microsoft-Betriebssystemen (Apple MacOS)
- Virtual Desktop Integration (VDI): Programme, die von Remote Desktop Services zur Verfügung gestellt werden (RemoteApp), erscheinen im Startmenü und werden dadurch nahtlos in die Benutzeroberfläche des Endbenutzers integriert.

6.2 Hyper-V 2.0

Zusätzliche Features:

- Live Migration (Voraussetzung: Windows Failover Cluster)
- Cluster Shared Volumes

6.3 Internet Information Services 7.5

Neue Features:

- FTP 7 bereits integriert
- Neuer *"Configuration Editor"* im MMC-Snap-In *"Internet Informationsdienste-Manager"*
- Einige Erweiterungen sind bereits vorinstalliert (WebDAV) und müssen nicht mehr separat installiert werdenalliert werden

Wichtiger Nachtrag

Nach einer Standardinstallation eines Windows Server 2008 R2-DNS-Servers besteht das Problem, dass manche Seiten nicht aufgelöst werden, zum Beispiel `www.microsoft.com`, `www.bing.com`, `www.windowsupdate.com` usw.

Die Ursache dafür ist, dass der DNS-Server-Dienst von Windows Server 2008 R2 bei seinen DNS-Abfragen eine leicht modifizierte Version von EDNS0, einer relativ neuen DNS-Erweiterung, verwendet. Diese Änderung führt aber bei den Akamai-DNS-Servern, die für die DNS-Auflösung der oben angeführten Seiten zuständig sind, zu Problemen („falsches Format").

Um diese Probleme zu beseitigen, ist es empfehlenswert, EDNS wie folgt auszuschalten (wie gesagt, nur am DNS-Server nötig):

```
dnscmd /config /EnableEDNSProbes 0
```

Und dann funktioniert wieder alles.

Links zu Windows Server 2008

Produktinformationen

Produkthomepage

`http://www.microsoft.com/Germany/windowsserver2008/default.mspx`

Produkthomepage R2

`http://www.microsoft.com/germany/windowsserver2008r2/default.mspx`

Windows Server 2008 bei Technet

`http://technet.microsoft.com/de-de/windowsserver/default.aspx`

Windows Server 2008 bei Wikipedia

`http://de.wikipedia.org/wiki/Microsoft_Windows_Server_2008`

Gelesen bei Christian Haberls "Kraut und Rüben Blog"

Windows 7 und Windows Server 2008 R2 Readiness – Demo Videos

`http://blog.this.at/post/2009/06/16/Windows-7-und-Windows-Server-2008-R2-Readiness-e28093-Demo-Videos.aspx`

Softlinks und Hardlinks in Windows Vista und Windows Server 2008

`http://blog.this.at/post/2007/11/22/Softlinks-und-Hardlinks-in-Windows-Vista-und-Windows-Server-2008.aspx`

Windows Server 2008 Webcasts

`http://blog.this.at/post/2008/03/22/Windows-Server-2008-Webcasts.aspx`

Massive Probleme beim Network Monitoring mittels WMI unter Windows Vista und Windows Server 2008 erst mit Windows 7 RC behoben

`http://blog.this.at/post/2009/07/14/Massive-Probleme-beim-Network-Monitoring-mittels-WMI-unter-Windows-Vista-und-Windows-Server-2008-erst-mit-Windows-7-RC-behoben.aspx`

`http://www.microsoft.com/germany/windowsserver2008r2/`