Kapitel 1

Windows Server 2012-Administration im Überblick

In diesem Kapitel:

Microsoft Windows 2012 ist ein leistungsfähiges, vielseitiges und umfangreich ausgestattetes Serverbetriebssystem, das auf den Verbesserungen aufbaut, die Microsoft in Windows Server 2008 Release 2 entwickelt hat. Windows Server 2012 und Windows 8 haben eine Reihe Features gemeinsam, weil sie aus demselben Entwicklungsprojekt hervorgegangen sind. Diese gemeinsamen Features haben dieselbe Codebasis und erstrecken sich über viele Bereiche der beiden Betriebssysteme, zum Beispiel Verwaltung, Sicherheit, Netzwerk und Speicherung. Daher können Sie vieles von dem, was Sie bereits über Windows 8 wissen, auch auf Windows Server 2012 anwenden.

Dieses Kapitel beschreibt den Einstieg in Windows Server 2012 und in welcher Weise sich die Änderungen an der Architektur auf die Nutzung und Administration von Windows Server 2012 auswirken. In diesem wie auch in allen folgenden Kapiteln finden Sie außerdem detaillierte Beschreibungen der umfassenden Features und Verbesserungen im Bereich der Sicherheit. Diese Beschreibungen stellen Techniken vor, mit denen alle Aspekte der Computersicherheit verbessert wurden, also Hardware-, Daten- und Netzwerksicherheit. Auch wenn sich dieses Buch auf die Windows Server 2012-Administration konzentriert, können die hier vorgestellten Tipps und Techniken allen helfen, die mit dem Betriebssystem Windows Server 2012 in Support, Entwicklung oder der täglichen Benutzung zu tun haben.

Windows Server 2012 und Windows 8

Bevor Sie Windows Server 2012 bereitstellen, sollten Sie die Serverarchitektur sorgfältig planen. Im Rahmen Ihrer Implementierungsplanung müssen Sie die benötigte Softwarekonfiguration genau analysieren und die Hardwarekonfiguration individuell für jeden Server anpassen, um die Anforderungen zu erfüllen. Sie sind bei der Serverbereitstellung sehr flexibel, weil Sie die Wahl zwischen drei Installationstypen haben:

- **Server mit GUI** Eine Installationsoption, die den vollständigen Funktionsumfang bietet. Wird auch als *vollständige Serverinstallation* bezeichnet. Sie können einen Server so konfigurieren, dass er eine beliebige erlaubte Kombination aus Rollen, Rollendiensten und Features anbietet und eine vollständige Benutzeroberfläche zum Verwalten des Servers bereitstellt. Diese Installationsoption ist eine universelle Lösung, sie wird für Bereitstellungen von Windows Server 2012 empfohlen, bei der sich die Serverrolle im Lauf der Zeit womöglich ändert.
- **Server Core** Eine minimale Installation, die einen bestimmten Satz von Rollen zur Verfügung stellt, aber ohne grafische Servershell, Microsoft Management Console und Desktopdarstellung auskommt. Sie können eine Server Core-Installation mit einem beschränkten Satz von Rollen konfigurieren. Zum Verwalten des Servers steht eine eingeschränkte Benutzeroberfläche zur Verfügung, die meisten Verwaltungsaufgaben werden lokal in einer Eingabeaufforderung oder im Remotezugriff mit Verwaltungstools erledigt. Diese Installationsoption eignet sich perfekt für Situationen, in denen Sie Server für eine bestimmte Serverrolle oder eine bestimmte Kombination von Rollen nutzen. Weil keine weiteren Funktionen installiert werden, laufen keine anderen Dienste, sodass mehr Ressourcen für die tatsächlich benötigten Rollen zur Verfügung stehen.
- **Server mit minimaler Oberfläche** Eine Installationsoption, bei der Sie eine vollständige Serverinstallation durchführen und dann die grafische Shell für Server deinstallieren. Somit bleiben eine minimale Benutzeroberfläche, Microsoft Management Console, Server-Manager und ein Teil der Systemsteuerung für die lokale Verwaltung übrig. Diese Installationsoption eignet sich am besten, wenn Sie zwar im Detail festlegen wollen, welche Aufgaben auf einem Server durchgeführt werden dürfen und welche Rollen und Features installiert sind, aber trotzdem eine bequeme grafische Benutzeroberfläche haben wollen.

Sie wählen den Installationstyp während der Installation des Betriebssystems. Im Gegensatz zu älteren Versionen von Windows Server haben Sie nun die Möglichkeit, den Installationstyp auch noch nach der Installation eines Servers zu ändern. Ein wesentlicher Unterschied besteht bei den Installationstypen darin, ob die grafischen Verwaltungstools und die grafische Shell vorhanden sind. Eine Server Core-Installation hat keine von beiden, eine vollständige Serverinstallation beide und eine Installation mit minimaler Oberfläche nur die grafischen Verwaltungstools.

WEITERE INFORMATIONEN Es gibt einige Serverfeatures und -rollen, die eine grafische Shell voraussetzen. Das sind unter anderem Faxserver, Remotedesktop-Sitzungshost, Windows-Bereitstellungsdienste und die Benutzeroberfläche zum Internetdrucken. Außerdem benötigen die Detailansicht in der Ereignisanzeige sowie die grafische Benutzeroberfläche der Windows-Firewall die grafische Shell.

Wie Windows 8 stellt Windows Server 2012 die folgenden Features bereit:

- **Modularisierung für Sprachunabhängigkeit und Datenträgerabbilder für Hardwareunabhängigkeit** Jede Komponente des Betriebssystems ist als unabhängiges Modul entworfen, das Sie ganz einfach hinzufügen oder entfernen können. Dieses Feature bildet die Basis für die Konfigurationsarchitektur von Windows Server 2012. Microsoft liefert Windows Server 2012 auf Medien im WIM-Datenträgerabbildformat (Windows Imaging Format) aus, das die Größe der Abbilddateien mithilfe von Komprimierung und Speicherungsoptimierung deutlich verringert.
- **Vorinstallations- und Vorstartumgebungen** Windows Preinstallation Environment 4.0 (Windows PE 4.0) ersetzt MS-DOS als Vorinstallationsumgebung und bietet eine startfähige Umgebung für Installation, Bereitstellung, Wiederherstellung und Problembehandlung. Die Windows-Vorstartumgebung stellt eine Systemstartumgebung mit einem Startmanager zur Verfügung, in der Sie auswählen können, welche Startanwendung ausgeführt werden soll, um das Betriebssystem zu laden. Auf Systemen mit mehreren Betriebssystemen können Sie auf ältere Betriebssysteme zugreifen, indem Sie den entsprechenden Eintrag in der Startumgebung auswählen.
- **Benutzerkontensteuerung und Privilegienanhebung** Die Benutzerkontensteuerung (User Account Control, UAC) verbessert die Computersicherheit, indem sie Standardbenutzer- und Administratorbenutzerkonten konsequent voneinander trennt. Dank der UAC laufen alle Anwendungen entweder mit Standardbenutzer- oder mit Administratorbenutzerprivilegien, und Sie erhalten in der Standardeinstellung eine Sicherheitseingabeaufforderung, sobald Sie versuchen, eine Anwendung auszuführen, die Administratorprivilegien erfordert. Auf welche Weise die Sicherheitseingabeaufforderung arbeitet, wird über Gruppenrichtlinieneinstellungen gesteuert. Falls Sie sich mit dem eingebauten Administratorkonto anmelden, erhalten Sie normalerweise keine Anhebungsaufforderungen.

Alle Features, die auf der gemeinsamen Codebasis von Windows 8 und Windows Server 2012 aufbauen, haben dieselben Verwaltungsoberflächen. Praktisch alle Systemsteuerungsprogramme, die in Windows Server 2012 zur Verfügung stehen, gibt es in identischer oder zumindest sehr ähnlicher Form auch in Windows 8. Natürlich gibt es einige Ausnahmen bei den Standardeinstellungen. Da Windows Server 2012 keine Leistungsbewertungen verwendet, gibt es für Windows-Server keinen Windows-Leistungsindex. Weil Windows Server 2012 nicht mit dem Energiesparmodus oder ähnlichen Modi arbeitet, stehen für Windows-Server keine Optionen für Energiesparmodus, Ruhezustand oder Aufwecken des Computers zur Verfügung. Weil die erweiterten Energieverwaltungsoptionen auf Windows-Servern normalerweise gar nicht benutzt werden, stellt Windows Server 2012 nur einen begrenzten Satz von Energieoptionen zur Verfügung.

Auch die Windows Aero-Erweiterungen, Windows-Sidebar, Windows-Minianwendungen oder andere Verbesserungen der grafischen Oberfläche stehen in Windows Server 2012 nicht zur Verfügung. Windows

Server 2012 wurde mit dem Ziel entwickelt, optimale Leistung für Serveraufgaben zur Verfügung zu stellen, nicht um das Aussehen des Desktops möglichst flexibel anpassen zu können. Bei Bedarf können Sie in einer vollständigen Serverinstallation trotzdem das Feature *Desktopdarstellung* hinzufügen und einige Windows 8-Features auf Ihrem Server aktivieren.

Die Desktopdarstellung stellt auf dem Server die Funktionen des Windows-Desktops zur Verfügung. Zu den verfügbaren Windows-Funktionen gehören der Windows Media Player, Desktopdesigns, Video für Windows (AVI-Unterstützung), Windows-Defender, Datenträgerbereinigung, Synchronisierungscenter, Audiorecorder, Zeichentabelle und Snipping Tool. Dank dieser Features können Sie einen Server zwar wie einen Desktopcomputer nutzen, sie verschlechtern aber unter Umständen die Leistung des Servers.

Weil sich die gemeinsamen Features von Windows 8 und Windows Server 2012 so stark ähneln, verzichte ich darauf, die Veränderungen der Benutzeroberfläche gegenüber älteren Betriebssystemversionen zu beschreiben, zu erklären, wie die Benutzerkontensteuerung funktioniert und dergleichen. Diese Themen werden in *Microsoft Windows 8 – Ratgeber für Administratoren* (Microsoft Press, 2012) ausführlich behandelt, daher empfehle ich, diesen Ratgeber mit diesem Buch zu kombinieren. Neben allgemeinen Verwaltungsaufgaben beschäftigt sich der Ratgeber für Windows 8 mit der Anpassung von Betriebssystem und Windows-Umgebung, Konfiguration von Hardware- und Netzwerkgeräten, Verwaltung des Benutzerzugriffs und globaler Einstellungen, Konfiguration von Notebooks und mobiler Netzwerknutzung, Arbeit mit Remoteverwaltung und Remoteunterstützung, Problembehandlung von Systemproblemen und vielen weiteren Themen. Dieser Ratgeber für Windows Server 2012 konzentriert sich dagegen auf Verzeichnisdienst-, Daten- und Netzwerkadministration.

Der Einstieg in Windows Server 2012

Die Familie der Windows Server 2012-Betriebssysteme umfasst mehrere unterschiedliche Editionen. Alle Editionen von Windows Server 2012 unterstützen mehrere Prozessorkerne. Selbst wenn eine Edition nur einen Prozessorsockel (also einen *physischen Prozessor*) unterstützt, kann dieser Prozessor bis zu 8 Prozessorkerne enthalten (die *logischen Prozessoren*).

Windows Server 2012 steht nur in einer 64-Bit-Version zur Verfügung. In diesem Buch bezeichne ich 64-Bit-Computer, die auf Basis der x64-Architektur entworfen wurden, als *64-Bit-Systeme*. Die verschiedenen Editionen unterstützen dieselben Hauptfeatures und Verwaltungstools. Daher können Sie die in diesem Buch erläuterten Verfahren unabhängig von der verwendeten Windows Server 2012-Edition einsetzen.

Wenn Sie ein Windows Server 2012-System installieren, konfigurieren Sie das System entsprechend seiner Funktion im Netzwerk. Dafür gelten die folgenden Richtlinien:

- Server werden im Allgemeinen einer Arbeitsgruppe oder einer Domäne zugewiesen.
- Arbeitsgruppen sind lockere Zusammenschlüsse von Computern, in denen jeder Computer einzeln verwaltet wird.
- Domänen sind Zusammenstellungen von Computern, die mithilfe von Domänencontrollern gemeinsam verwaltet werden können. Domänencontroller sind Windows Server 2012-Systeme, die den Zugriff auf das Netzwerk, die Verzeichnisdatenbank und freigegebene Ressourcen verwalten.

HINWEIS In diesem Buch bezeichnen die Begriffe »Windows Server 2012« und »Windows Server 2012-Familie« alle Editionen von Windows Server 2012. Die verschiedenen Editionen unterstützen die gleichen Hauptfeatures und Verwaltungstools.

Im Unterschied zu Windows Server 2008 verwendet Windows Server 2012 eine Startseite. *Start* ist ein Fenster, kein Menü. Programme können Kacheln auf der Startseite haben. Wenn Sie eine Kachel antippen oder anklicken, wird das Programm ausgeführt. Wenn Sie mit der rechten Maustaste auf ein Programm klicken oder es gedrückt halten, wird normalerweise eine Optionsleiste angezeigt. Die Charms-Leiste ist eine Optionsleiste für Start, Desktop und Einstellungen. Mit einer Touchoberfläche zeigen Sie die Charms an, indem Sie von der rechten Seite des Bildschirms her streifen. Mit Maus und Tastatur zeigen Sie die Charms an, indem Sie den Mauszeiger auf die versteckte Schaltfläche in der rechten oberen oder rechten unteren Ecke des Start-, Desktop- oder Einstellungen-Bildschirms bewegen oder die Tastenkombination WINDOWS+C drücken.

Tippen oder klicken Sie auf das Suchen-Charm, um die Suchleiste anzuzeigen. Jeder Text, den Sie auf der Startseite eintippen, wird in das Suchfeld der Suchleiste eingegeben. Das Suchfeld kann sich auf Apps, Einstellungen oder Dateien beziehen. Wenn Sie *Apps* auswählen, können Sie mit dem Suchfeld schnell die installierten Programme finden. Wenn Sie *Einstellungen* auswählen, können Sie mit dem Suchfeld schnell die benötigten Einstellungen und Optionen in der Systemsteuerung finden. Und wenn Sie *Dateien* auswählen, können Sie nach Dateien suchen.

Sie können ein Programm schnell öffnen, indem Sie die WINDOWS-Taste drücken, den Dateinamen des Programms eingeben und dann die EINGABETASTE drücken. Das funktioniert, solange die Suchkategorie *Apps* ausgewählt ist (was normalerweise die Standardeinstellung ist).

Mit einem Druck auf die WINDOWS-Taste schalten Sie zwischen Startseite und Desktop um (oder, wenn Sie mit PC-Einstellungen arbeiten, zwischen Start und Einstellungen). In Start gibt es eine Desktopkachel, die Sie antippen oder anklicken können, um den Desktop anzuzeigen. Sie können den Desktop auch anzeigen, indem Sie die Tastenkombination WINDOWS+D drücken. Und solange Sie die Tastenkombination WINDOWS+, gedrückt halten, wird der Desktop ebenfalls angezeigt. Auf der Startseite erhalten Sie Zugriff auf die Systemsteuerung, indem Sie die entsprechende Kachel antippen oder anklicken. Auf dem Desktop öffnen Sie die Systemsteuerung, indem Sie die Charms öffnen, auf *Einstellungen* tippen oder klicken und dann auf *Systemsteuerung* tippen oder klicken. Weil der Datei-Explorer standardmäßig auf der Desktop-Taskleiste angeordnet ist, können Sie die Systemsteuerung auf dem Desktop normalerweise so öffnen:

1. Öffnen Sie den Datei-Explorer, indem Sie das entsprechende Taskleistensymbol antippen oder anklicken.
2. Tippen oder klicken Sie auf die Optionsschaltfläche (Pfeilsymbol) ganz links in der Adressleiste.
3. Tippen oder klicken Sie auf *Systemsteuerung*.

Startseite und Desktop verfügen über ein praktisches Menü, das Sie anzeigen, indem Sie mit der rechten Maustaste in die linke untere Ecke der Startseite oder des Desktops klicken beziehungsweise diese Stelle gedrückt halten. Nützliche Befehle in diesem Menü sind *Eingabeaufforderung*, *Eingabeaufforderung (Administrator)*, *Geräte-Manager*, *Ereignisanzeige*, *System* und *Task-Manager*. Auf der Startseite zeigt die versteckte Schaltfläche in der linken unteren Ecke ein Vorschaubild des Desktops, wenn sie aktiviert wird. Durch Antippen oder Anklicken dieses Vorschaubilds öffnen Sie den Desktop. Auf dem Desktop zeigt die versteckte Schaltfläche in der linken unteren Ecke ein Vorschaubild der Startseite, wenn sie aktiviert wird. Durch Antippen oder Anklicken des Vorschaubilds öffnen Sie die Startseite. Wenn Sie das Vorschaubild mit der rechten Maustaste anklicken oder es gedrückt halten, wird das Kontextmenü angezeigt.

Herunterfahren und Neustarten sind nun Befehl der Energieoptionen. Daher gehen Sie folgendermaßen vor, um einen Server herunterzufahren oder neu zu starten:

1. Zeigen Sie die Startoptionen an, indem Sie von der rechten Bildschirmseite nach innen streifen oder den Mauszeiger in die untere oder obere rechte Ecke des Bildschirms bewegen.
2. Tippen oder klicken Sie auf *Einstellungen* und dann auf *Ein/Aus*.
3. Tippen oder klicken Sie auf *Herunterfahren* oder *Neu starten*.

Stattdessen können Sie auch den Hauptschalter des Computers drücken. Daraufhin wird er ordnungsgemäß heruntergefahren, wobei Sie abgemeldet werden und der Computer dann ausgeschaltet wird. Wenn Sie ein System der Desktopklasse einsetzen und der Computer eine Energiespartaste hat, ist sie standardmäßig deaktiviert. Dasselbe gilt für Optionen beim Zuklappen eines Notebooks. Server sind außerdem so konfiguriert, dass sie den Bildschirm nach 10 Minuten ohne Benutzeraktivität abschalten.

Windows 8 und Windows Server 2012 unterstützen ACPI 5.0 (Advanced Configuration and Power Interface). Windows nutzt ACPI, um die Energiestatusübergänge von System und Geräten zu steuern und um Geräte zwischen den Modi »Eingeschaltet«, »Standby« und »Ausgeschaltet« umzuschalten und so den Energieverbrauch zu senken.

Die Energieeinstellungen für einen Computer werden vom aktiven Energiesparplan festgelegt. Sie greifen in der Systemsteuerung auf die Energiesparpläne zu, indem Sie auf *System und Sicherheit* und dann auf *Energieoptionen* tippen oder klicken. Windows Server 2012 stellt auch das Dienstprogramm *Powercfg.exe* bereit, mit dem Sie die Energieoptionen in einer Befehlszeile verwalten können. Wenn Sie in einer Eingabeaufforderung den Befehl **powercfg /l** ausführen, bekommen Sie die konfigurierten Energiesparpläne angezeigt. Der aktive Energiesparplan ist dabei mit einem Stern markiert.

Der standardmäßig aktive Energiesparplan in Windows Server 2012 heißt *Ausbalanciert*. Dieser Plan nimmt folgende Einstellungen vor:

- Festplatten werden nie ausgeschaltet. Sie können stattdessen auch so konfiguriert werden, dass sie nach einer festgelegten Leerlaufdauer angehalten werden.
- Zeitgeberereignisse wecken den Computer nicht auf, wenn er sich in einem Energiesparmodus befindet.
- Der selektive Energiesparmodus von USB-Geräten ist aktiviert. Dabei schaltet Windows den gesamten Computer sofort in den Energiesparmodus, ohne zu warten, bis alle angeschlossenen USB-Geräte auf die Anweisung reagiert haben, in den Energiesparmodus zu schalten.
- Für PCI Express-Verbindungen, die sich im Leerlauf befinden, werden mittlere Energiesparmodi verwendet. Stattdessen können auch maximale oder minimale Energiesparmodi eingestellt werden.
- Das System wird aktiv gekühlt, indem erst die Ventilatorgeschwindigkeit erhöht wird, bevor die Prozessoren gedrosselt werden. Bei der passiven Systemkühlung werden dagegen die Prozessoren gedrosselt, bevor die Ventilatoren beschleunigt werden.
- Es werden Prozessormodi für minimale und maximale Leistung genutzt, sofern sie zur Verfügung stehen. Stattdessen können Sie auch konfigurieren, dass nur ein fest eingestellter Modus genutzt wird.

HINWEIS Der Energieverbrauch ist ein wichtiges Thema, besonders für Organisationen, die sich für den Umweltschutz engagieren. Durch sinkenden Stromverbrauch spart Ihre Organisation unter Umständen auch Geld und kann, sofern bestimmte Voraussetzungen erfüllt sind, mehr Server in ihren Datencentern installieren. Wenn Sie Windows Server 2012 auf einem Notebook installieren (etwa zum Testen oder als Desktopsystem), werden Sie etwas andere Energieeinstellungen bekommen. In diesem Fall stehen auch Einstellungen zur Verfügung, die festlegen, wie sich das System verhält, wenn es mit dem Akku betrieben wird.

Energieverwaltungsoptionen

Wenn Sie mit der Energieverwaltung arbeiten, sind vor allem die folgenden Einstellungen wichtig:

- Kühlungsmodi
- Gerätezustände
- Prozessorzustände

ACPI definiert aktive und passive Kühlungsmodi. Diese Kühlungsmodi wenden unterschiedliche Taktiken an:

- Die passive Kühlung verringert die Systemleistung, macht den Computer aber leiser, weil die Ventilatoren langsamer laufen. Bei der passiven Kühlung verringert Windows den Energieverbrauch, um die Temperatur des Computers zu verringern. Das geht allerdings auf Kosten der Systemleistung. Windows drosselt dabei erst einmal die Prozessorgeschwindigkeit, um zu versuchen, den Computer abzukühlen. Erst danach beschleunigt es die Ventilatoren, weil das den Energieverbrauch erhöht.
- Die aktive Kühlung bietet höchstmögliche Systemleistung. Bei der aktiven Kühlung erhöht Windows den Energieverbrauch, um die Temperatur des Computers zu senken. Dabei beschleunigt Windows die Ventilatoren, wenn es versucht, den Computer abzukühlen. Erst wenn diese Möglichkeit ausgeschöpft ist, drosselt es die Prozessorgeschwindigkeit.

Die Energierichtlinie legt Ober- und Untergrenzen für den Prozessorzustand fest, die als *Maximaler Leistungszustand des Prozessors* beziehungsweise *Minimaler Leistungszustand des Prozessors* bezeichnet werden. Diese Zustände werden mithilfe eines Features implementiert, das seit ACPI 3.0 zur Verfügung steht, der sogenannten Prozessordrosselung. Die Zustände legen fest, welchen Bereich momentan verfügbarer Prozessorleistungszustände Windows nutzen darf. Indem Sie die Maximal- und Minimalwerte festlegen, definieren Sie die Grenzen für die erlaubten Leistungszustände. Stattdessen können Sie auch für beide Einstellungen denselben Wert eintragen, dann zwingen Sie das System dauerhaft in diesen Leistungszustand. Windows senkt den Energieverbrauch, indem es die Prozessorgeschwindigkeit drosselt. Liegt beispielsweise die obere Grenze bei 100 Prozent und die untere bei 5 Prozent, kann Windows den Prozessor innerhalb dieses Bereichs drosseln und den Energieverbrauch senken, sofern nicht die volle Last benötigt wird. In einem Computer mit einem 3-GHz-Prozessor regelt Windows die Taktfrequenz des Prozessors dann zwischen 0,15 GHz und 3,0 GHz.

Prozessordrosselung und die zugehörigen Leistungszustände wurden bereits in Windows XP eingeführt, sie sind kein neues Feature. Die älteren Implementierungen wurden aber für Computer entwickelt, deren Prozessor nur einen einzigen Kern hat, nicht für die heutigen Mehrkernprozessoren. Daher senken sie den Energieverbrauch von Computern mit mehreren logischen Prozessoren nicht so effektiv. Seit der Version Windows 7 senkt Windows den Energieverbrauch in Computern mit Mehrkernprozessoren, indem es ein Feature von ACPI 4.0 nutzt, das *Stilllegen von logischen Prozessoren* (logical processor idling), und indem es die Funktionen zur Prozessordrosselung so erweitert, dass es mit einzelnen Prozessorkernen arbeitet.

Das Stilllegen von logischen Prozessoren soll sicherstellen, dass Windows möglichst wenige Prozessorkerne nutzt. Dazu fasst Windows die Arbeitslast auf möglichst wenigen Kernen zusammen und legt die inaktiven Prozessorkerne still. Wird mehr Rechenleistung benötigt, aktiviert Windows die inaktiven Prozessorkerne wieder. Diese Stilllegungsfunktion arbeitet mit der Verwaltung der Prozessorleistungszustände im Systemkern zusammen.

ACPI definiert Prozessorleistungszustände, die sogenannten P-States, sowie Prozessorleerlaufzustände, die C-States. Prozessorleistungszustände sind P0 (der Prozessor beziehungsweise Kern läuft mit höchster Leistung und verbraucht am meisten Strom), P1 (Prozessor/Kern ist auf eine Leistung beschränkt, die

unter der Höchstleistung liegt, und verbraucht weniger Strom als bei voller Geschwindigkeit) und P*n* (wobei der Wert *n* vom Prozessor abhängt, der Prozessor/Kern läuft dabei auf dem niedrigsten Niveau, das noch im aktiven Zustand möglich ist, und verbraucht am wenigsten Strom).

Prozessorleerlaufzustände sind C0 (der Prozessor/Kern kann Anweisungen ausführen), C1 (der Prozessor/Kern hat die geringste Latenz, während er sich in einem Zustand befindet, in dem keine Anweisungen ausgeführt werden), C2 (der Prozessor/Kern hat eine höhere Latenz, verbraucht aber weniger Strom als im Zustand C1) und C3 (der Prozessor/Kern hat die höchste Latenz, verbraucht aber weniger Strom als in den Zuständen C1 und C2).

WEITERE INFORMATIONEN Die Spezifikation ACPI 4.0 wurde im Juni 2009 fertiggestellt, ACPI 5.0 im Dezember 2011. Computer, die vor diesem Zeitpunkt hergestellt wurden, bieten wahrscheinlich keine Firmware, die vollständig zu dieser Version kompatibel ist. Unter Umständen müssen Sie die Firmware aktualisieren, sobald eine neuere Version verfügbar wird. In manchen Fällen, insbesondere bei älterer Hardware, ist es überhaupt nicht möglich, die Firmware eines Computers so zu aktualisieren, dass sie vollständige Kompatibilität zu ACPI 4.0 oder ACPI 5.0 bietet. Wenn Sie beim Konfigurieren der Energieoptionen feststellen, dass die Optionen *Maximaler Leistungszustand des Prozessors* und *Minimaler Leistungszustand des Prozessors* nicht zur Verfügung stehen, ist die Firmware des Computers nicht vollständig kompatibel zu ACPI 3.0; in diesem Fall bietet sie wahrscheinlich auch keine vollständige Unterstützung für ACPI 4.0. Prüfen Sie aber auf jeden Fall auf der Website des Hardwareherstellers, ob er Firmwareupdates anbietet.

Windows kann Prozessoren/Kerne annähernd verzögerungsfrei (binnen Bruchteilen von Millisekunden) zwischen den verschiedenen P-States sowie vom Zustand C1 in den Zustand C0 umschalten. Die anderen Leerlaufzustände vermeidet Windows im Allgemeinen, sodass Sie keine Leistungseinbrüche durch das Drosseln oder Aufwecken von Prozessoren/Kernen befürchten müssen. Die Prozessoren/Kerne stehen jederzeit zur Verfügung, sobald sie gebraucht werden. Wollen Sie die Auswirkungen der Prozessorenergieverwaltung dennoch vermeiden, können Sie den minimalen und den maximalen Leistungszustand des Prozessors auf jeweils 100 Prozent setzen.

Die Stilllegung von logischen Prozessoren wird genutzt, um den Energieverbrauch zu senken. Dabei wird ein logischer Prozessor aus der Liste entfernt, mit der das Betriebssystem Aufgaben verteilt, die nicht an einen bestimmten Prozessor gebunden sind. Sind Aufgaben an bestimmte Prozessoren gebunden (die sogenannte Prozessoraffinität oder Prozessorzugehörigkeit), beschränkt das die Wirksamkeit dieses Features. Daher sollten Sie einen Plan ausarbeiten, wenn Sie die Prozessoraffinität für Anwendungen konfigurieren. Im Ressourcenmonitor von Windows können Sie die Prozessorressourcen mithilfe von Prozentwerten der Prozessorauslastung und Regeln für die Prozessoraffinität verteilen. Beide Techniken wirken sich negativ auf die Effektivität der Stilllegung von logischen Prozessoren aus.

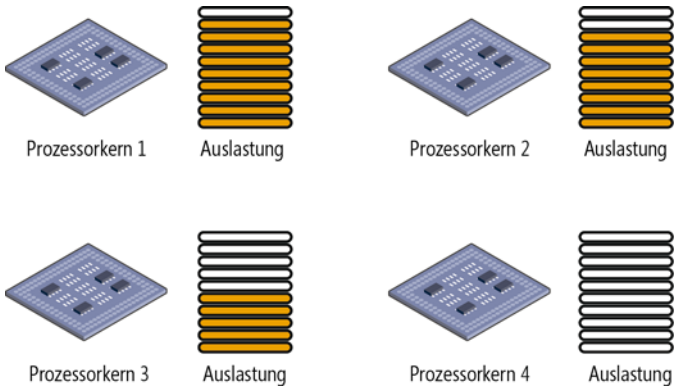

Abbildung 1.1 Prozessorzustände

Windows spart Strom, indem es Prozessorkerne in geeignete P- und C-Zustände schaltet. Nehmen wir an, bei einem Computer mit vier logischen Prozessoren stehen Windows die P-Zustände 0 bis 5 zur Verfügung, wobei P0 100 Prozent Leistung bietet, P1 90 Prozent, P2 80 Prozent, P3 70 Prozent, P4 60 Prozent und P5 50 Prozent. Ist der Computer aktiv, läuft der logische Prozessor 0 wahrscheinlich im P-Zustand 0 bis 5 und die anderen Prozessoren entweder in einem geeigneten P-Zustand oder einem Leerlaufzustand. Abbildung 1.1 zeigt ein Beispiel. Hier läuft der logische Prozessor 1 mit 90 Prozent, der logische Prozessor 2 mit 80 Prozent, der logische Prozessor 3 mit 50 Prozent, und der logische Prozessor 4 befindet sich im Energiesparmodus.

PRAXISTIPP ACPI 4.0 und ACPI 5.0 definieren vier globale Energiezustände. Der Zustand G0 ist der Arbeitszustand, in dem Software ausgeführt wird. Hier ist der Energieverbrauch am höchsten und die Latenz ist am geringsten. G1 ist der Energiesparmodus, in dem keine Software ausgeführt wird. Die Latenz hängt vom konkreten Modus ab, und der Energieverbrauch ist kleiner als im Zustand G0. G2 (auch als S5-Energiesparmodus bezeichnet) ist der Standbymodus, in dem das Betriebssystem nicht mehr läuft. Die Latenz ist hoch und der Energieverbrauch beträgt fast 0. Im Zustand G3 ist der Computer vollständig ausgeschaltet. Das Betriebssystem läuft nicht, die Latenz ist hoch und der Energieverbrauch ist 0. Außerdem gibt es einen speziellen globalen Zustand (S4 nonvolatile sleep), in dem das Betriebssystem seinen gesamten Systemkontext in eine Datei auf einem nichtflüchtigen Speichermedium schreibt, sodass der Systemkontext gesichert und wiederhergestellt werden kann.

Der globale Energiesparmodus G1 umfasst mehrere Variationen. S1 ist ein Energiesparmodus, in dem der gesamte Systemkontext erhalten bleibt. S2 ähnelt dem Energiesparmodus S1, allerdings gehen CPU- und Systemcachekontext verloren und das System läuft nach einem Reset weiter. S3 ist ein Energiesparmodus, in dem alle CPU-, Cache- und Chipsatzkontexte verloren gehen und die Hardware nur den Arbeitsspeicherkontext beibehält und einen Teil des CPU- und L2-Cache-Konfigurationskontextes wiederherstellt. S4 ist ein Energiesparmodus, in dem davon ausgegangen wird, dass die Hardware alle Geräte ausschaltet, um den Energieverbrauch möglichst weit zu senken; dabei wird nur der Plattformkontext beibehalten. S5 schließlich ist ein Energiesparmodus, in dem die Hardware vorübergehend ausgeschaltet ist, sodass kein Kontext erhalten bleibt; um das System aufzuwecken, muss es in diesem Fall vollständig hochgefahren werden.

Auch einzelne Geräte haben Energiezustände. D0 bedeutet, dass das Gerät vollständig eingeschaltet ist und am meisten Strom verbraucht. D1 und D2 sind Zwischenzustände, die nur von wenigen Geräten genutzt werden. D3hot ist ein Energiesparzustand, in dem das Gerät von der Software erkannt wird und optional den Gerätekontext beibehält. D3 ist der ausgeschaltete Zustand, in dem der Gerätekontext verloren geht und das Betriebssystem das Gerät neu initialisieren muss, um es wieder einzuschalten.

Netzwerktools und -protokolle

Windows Server 2012 verfügt über eine Familie von Netzwerktools. Dazu gehören Netzwerk-Explorer, Netzwerk- und Freigabecenter und Netzwerkdiagnose. Abbildung 1.2 zeigt das Netzwerk- und Freigabecenter.

Grundlagen der Netzwerkoptionen

Die Konfigurationsoptionen für Freigabe und Netzwerkerkennung im Netzwerk- und Freigabecenter steuern die grundlegenden Netzwerkeinstellungen. Wenn die Netzwerkerkennung eingeschaltet ist und ein Server mit einem Netzwerk verbunden ist, kann der Server andere Netzwerkcomputer und -geräte sehen, und er ist selbst im Netzwerk sichtbar. Wenn die Freigabeeinstellungen ein- beziehungsweise ausgeschaltet sind, sind die entsprechenden Freigabefunktionen erlaubt beziehungsweise verboten. Wie in Kapitel 12, »Datenfreigabe, Sicherheit und Überwachung«, beschrieben, stehen im Rahmen der Frei-

gabe Optionen für Dateifreigabe, Freigabe des öffentlichen Ordners, Druckerfreigabe und kennwortgeschützte Freigabe zur Verfügung.

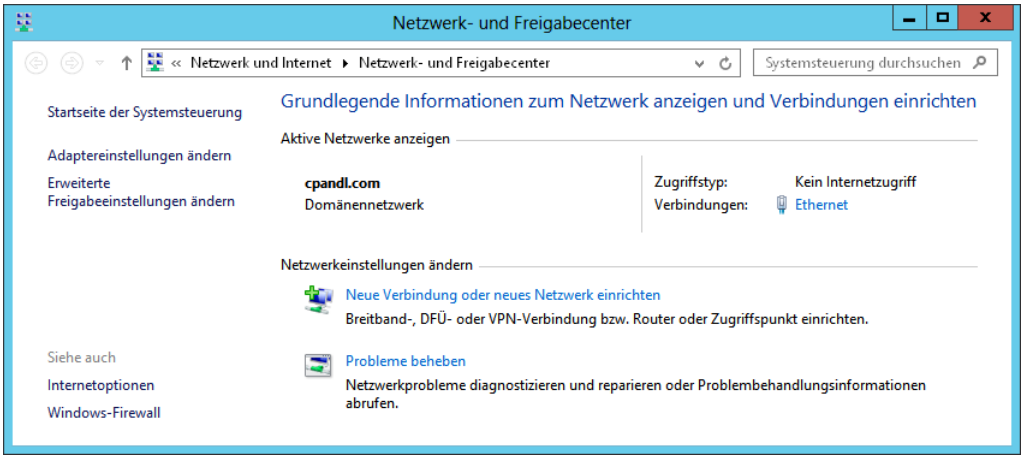

Abbildung 1.2 Das Netzwerk- und Freigabecenter bietet schnellen Zugriff auf Optionen für Freigabe, Erkennung und Netzwerkfunktionen

In Windows 8 und Windows Server 2012 werden Netzwerke in einen der folgenden Netzwerktypen eingeordnet:

- **Domäne** Ein Netzwerk, in dem die Computer an die Unternehmensdomäne angeschlossen sind, bei der sie Mitglieder sind.
- **Arbeitsplatz** Ein privates Netzwerk, in dem die Computer als Mitglieder einer Arbeitsgruppe konfiguriert und nicht direkt mit dem öffentlichen Internet verbunden sind.
- **Privat** Ein privates Netzwerk, in dem die Computer als Mitglieder einer Heimnetzgruppe konfiguriert und nicht direkt mit dem öffentlichen Internet verbunden sind.
- **Öffentlich** Ein öffentliches Netzwerk, in dem die Computer mit einem Netzwerk verbunden sind, das nicht rein privat ist, sondern einen öffentlich zugänglichen Ort abdeckt, zum Beispiel ein Internetcafé oder einen Flughafen.

Diese Netzwerktypen sind in drei Kategorien untergliedert: privat oder Arbeitsplatz, Domäne sowie öffentlich. Zu jeder Netzwerkkategorie gibt es ein eigenes Netzwerkprofil. Weil ein Computer die Freigabe- und Firewalleinstellungen für jede Netzwerkkategorie getrennt speichert, können Sie für jede Netzwerkkategorie andere Einstellungen wählen. Wenn Sie eine Verbindung zu einem neuen Netzwerk herstellen, öffnet sich ein Dialogfeld, in dem Sie die Netzwerkkategorie einstellen. Falls Sie die Kategorie *Privat* auswählen und der Computer feststellt, dass er mit der Unternehmensdomäne verbunden ist, bei der dieser Computer Mitglied ist, wird als Netzwerkkategorie ein Domänennetzwerk eingestellt.

Abhängig von der Netzwerkkategorie konfiguriert Windows Server die Einstellungen so, dass die Netzwerkerkennung ein- oder ausgeschaltet wird. Die Einstellung *Ein* (aktiviert) bedeutet, dass der Computer andere Computer und Geräte im Netzwerk erkennt, und dass umgekehrt die anderen Computer im Netzwerk diesen Computer erkennen. Die Einstellung *Aus* (deaktiviert) bedeutet, dass der Computer keine anderen Computer und Geräte im Netzwerk erkennt und dass andere Computer im Netzwerk diesen Computer nicht erkennen.

In den Fenstern *Netzwerk* oder *Erweiterte Freigabeeinstellungen* des Netzwerk- und Freigabecenters aktivieren Sie die Erkennung und Dateifreigabe. In einem öffentlichen Netzwerk sind Erkennung und Dateifreigabe standardmäßig blockiert. Das erhöht die Sicherheit, weil verhindert wird, dass Computer im öffentlichen Netzwerk andere Computer und Geräte erkennen, die ebenfalls an dieses Netzwerk angeschlossen sind. Wenn Erkennung und Dateifreigabe deaktiviert sind, können Sie nicht auf Dateien und Drucker zugreifen, die Sie auf einem anderen Computer im Netzwerk freigegeben haben. Auch einige Programme sind dann unter Umständen nicht in der Lage, auf das Netzwerk zuzugreifen.

Arbeiten mit Netzwerkprotokollen

Damit ein Server Zugriff auf ein Netzwerk erhält, müssen Sie TCP/IP und eine Netzwerkkarte installieren. Windows Server 2012 nutzt TCP/IP als Standardprotokoll für WAN (Wide Area Network). Normalerweise werden die Netzwerkfunktionen während der Installation des Betriebssystems installiert. Sie können TCP/IP auch über das Eigenschaftendialogfeld einer LAN-Verbindung installieren.

Die Protokolle TCP und IP ermöglichen es Computern, mithilfe von Netzwerkkarten über verschiedene Netzwerke und das Internet zu kommunizieren. Seit der Version Windows 7 besitzt Windows eine zweiteilige IP-Schichtarchitektur, in der IPv4 (Internet Protocol Version 4) sowie IPv6 (Internet Protocol Version 6) implementiert sind und die Transport- und Netzwerkschicht gemeinsam nutzen. IPv4 arbeitet mit 32-Bit-Adressen; es ist in den meisten Netzwerken die primäre IP-Version, auch im Internet. IPv6 verwendet dagegen 128-Bit-Adressen, es ist die kommende IP-Generation.

HINWEIS DirectAccess-Clients senden nur IPv6-Verkehr über die DirectAccess-Verbindung an den DirectAccess-Server. Dank der NAT64/DNS64-Unterstützung auf einem Windows Server 2012-DirectAccess-Server können DirectAccess-Clients nun auch mit reinen IPv4-Hosts im Unternehmensintranet kommunizieren. NAT64/DNS64 arbeiten zusammen, um eingehenden Verkehr von einem IPv6-Knoten in IPv4-Verkehr umzusetzen. NAT64 übersetzt den eingehenden IPv6-Verkehr in IPv4-Verkehr und führt beim Antwortverkehr die umgekehrte Wandlung durch, und DNS64 löst den Namen eines reinen IPv4-Hosts in eine übersetzte IPv6-Adresse auf.

PRAXISTIPP Das Feature der TCP-Chimney-Abladung wurde in Windows Vista und Windows Server 2008 eingeführt. Es ermöglicht dem Netzwerksubsystem, die Verarbeitung einer TCP/IP-Verbindung von den Prozessoren des Computers auf die Netzwerkkarte auszulagern, sofern die Netzwerkkarte die TCP/IP-Abladung unterstützt. Sowohl TCP/IPv4- als auch TCP/IPv6-Verbindungen können ausgelagert werden. Seit Windows 7 werden TCP-Verbindungen standardmäßig auf 10-GBit/s-Netzwerkkarten ausgelagert, aber nicht auf 1-GBit/s-Netzwerkkarten. Wollen Sie TCP-Verbindungen auf eine 1-GBit/s- oder 10-GBit/s-Netzwerkkarte auslagern, müssen Sie die TCP-Abladung aktivieren, indem Sie in einer Administratoreingabeaufforderung den folgenden Befehl ausführen: **netsh int tcp set global chimney=enabled**. Den Status der TCP-Abladung erfahren Sie, indem Sie **netsh int tcp show global** eingeben. Die TCP-Abladung funktioniert zwar in Kombination mit der Windows-Firewall, wird aber nicht von den Diensten für IPsec, Windows-Virtualisierung (Hyper-V), Netzwerklastenausgleich oder NAT (Network Address Translation) genutzt. Ob die TCP-Abladung funktioniert, stellen Sie fest, indem Sie **netstat –t** eingeben und den Wert unter *Abladungsstatus* prüfen. Der Status wird als *Abgeladen* oder *InHost* angezeigt.

Windows nutzt außerdem die empfangsseitige Skalierung (Receive-Side Scaling, RSS) und den direkten Cachezugriff (Network Direct Memory Access, NetDMA). Sie aktivieren oder deaktivieren RSS, indem Sie **netsh int tcp set global rss=enabled** beziehungsweise **netsh int tcp set global rss=disabled** eingeben. Den Status von RSS liefert der Befehl **netsh int tcp show global**. NetDMA aktivieren oder deaktivieren Sie, indem Sie unter dem Registrierungseintrag *EnableTCPA* den DWord-Wert 1 beziehungsweise 0 eintragen. Sie finden diesen Registrierungseintrag unter *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters*.

Die 32-Bit-Adressen von IPv4 werden üblicherweise in Form von vier getrennten Dezimalzahlen geschrieben, zum Beispiel 127.0.0.1 oder 192.168.10.52. Die vier Dezimalzahlen werden als Oktette bezeichnet, weil sie für jeweils 8 Bits der 32-Bit-Zahl stehen. Bei Standard-Unicast-IPv4-Adressen gibt ein Teil der IP-Adresse die Netzwerk-ID an und der andere Teil der IP-Adresse die Host-ID. Die Länge der beiden Teile ist variabel. Zwischen der IPv4-Adresse eines Hosts und der internen MAC-Adresse der Netzwerkkarte besteht keine direkte Beziehung.

Die 128-Bit-Adressen von IPv6 werden in acht 16-Bit-Blöcke unterteilt, die durch Doppelpunkte voneinander getrennt sind. Jeder 16-Bit-Block wird im Hexadezimalformat geschrieben, zum Beispiel FEC0:0:0:02BC:FF:BECB:FE4F:961D. Bei Standard-Unicast-IPv6-Adressen stehen die vorderen 64 Bits für die Netzwerk-ID, die hinteren 64 Bits für die Netzwerkschnittstelle. Weil viele IPv6-Adressblöcke den Wert 0 haben, kann ein fortlaufender Satz solcher Nullblöcke als »::« abgekürzt werden. Diese Notation wird als *Doppel-Doppelpunkt-Notation* bezeichnet. Mithilfe dieser Notation lassen sich die beiden 0-Blöcke im obigen Beispiel als FEC0::02BC:FF:BECB:FE4F:961D abkürzen. Drei oder mehr 0-Blöcke werden auf dieselbe Art zusammengefasst, zum Beispiel wird FFE8:0:0:0:0:0:0:1 zu FFE8::1.

Wenn während der Installation des Betriebssystems Netzwerkhardware erkannt wird, sind standardmäßig sowohl IPv4 als auch IPv6 aktiviert. Sie brauchen keine separate Komponente zu installieren, um Unterstützung für IPv6 nachzurüsten. Die seit Windows 7 veränderte IP-Architektur trägt den Namen »Next Generation TCP/IP Stack«. Sie umfasst viele Verbesserungen, die IPv4 und IPv6 leistungsfähiger machen.

Domänencontroller, Mitgliedserver und Domänendienste

Wenn Sie Windows Server 2012 auf einem neuen System installieren, können Sie den Server als Mitgliedserver, Domänencontroller oder eigenständigen Server konfigurieren. Diese Unterscheidung ist äußerst wichtig. Mitgliedserver sind Teil einer Domäne, speichern jedoch keine Verzeichnisinformationen. Domänencontroller unterscheiden sich von Mitgliedservern dadurch, dass sie Verzeichnisinformationen speichern und Authentifizierungs- und Verzeichnisdienste für die Domäne bereitstellen. Eigenständige Server sind nicht Teil einer Domäne und besitzen eine eigene Benutzerdatenbank. Deshalb authentifizieren sie Anmeldeanforderungen allein.

Arbeiten mit Active Directory

Windows Server 2012 unterstützt ein Multimaster-Replikationsmodell. Darin kann jeder Domänencontroller Verzeichnisänderungen verarbeiten und diese anschließend automatisch auf andere Domänencontroller replizieren. Windows Server verteilt ein ganzes Verzeichnis an Informationen, das als *Datenspeicher* (data store) bezeichnet wird. Im Datenspeicher befinden sich Gruppen von Objekten, die Benutzer-, Gruppen- und Computerkonten sowie freigegebene Ressourcen beschreiben, zum Beispiel Server, Dateien und Drucker.

Domänen, die Active Directory-Dienste nutzen, werden als *Active Directory-Domänen* bezeichnet. Zwar funktionieren Active Directory-Domänen auch mit einem einzigen Domänencontroller, es können und sollten aber mehrere Domänencontroller in der Domäne konfiguriert werden. Auf diese Weise können bei Ausfall eines Domänencontrollers die anderen die Authentifizierung und andere wichtige Aufgaben übernehmen.

Bereits in Windows Server 2008 hat Microsoft Active Directory in etlichen Aspekten grundlegend geändert. Dabei wurden die Verzeichnisfunktionen neu strukturiert und eine Gruppe zusammengehöriger Dienste entwickelt. Wichtige Dienste sind:

- **Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS)** AD CS stellt Funktionen zum Ausstellen und Widerrufen digitaler Zertifikate für Benutzer, Clientcomputer und Server zur Verfügung. AD CS greift auf die Zertifizierungsstellen (Certificate Authorities, CAs) zu, deren Verantwortung es ist, die Identität von Benutzern und Computern zu überprüfen, und stellt dann Zertifikate aus, um diese Identitäten zu bestätigen. Domänen haben eine Stammzertifizierungsstelle des Unternehmens, das heißt Zertifikatserver, die den Stamm der Zertifikathierarchien für Domänen und die Zertifikatserver mit der höchsten Vertrauenswürdigkeit im Unternehmen bilden, sowie untergeordnete Zertifizierungsstellen, die Mitglieder einer bestimmten Unternehmenszertifikathierarchie sind. Arbeitsgruppen haben eigenständige Stammzertifizierungsstellen, das heißt Zertifikatserver im Stamm einer separaten Zertifikathierarchie, sowie eigenständige untergeordnete Zertifizierungsstellen, die Mitglieder einer bestimmten separaten Zertifikathierarchie sind.
- **Active Directory-Domänendienste (Active Directory Domain Services, AD DS)** AD DS stellt die grundlegenden Verzeichnisdienste zur Verfügung, die zum Betreiben einer Domäne erforderlich sind. Dazu gehören die Datenspeicher, in denen Informationen über Objekte im Netzwerk abgelegt sind. Diese Informationen stellt AD DS den Benutzern zur Verfügung. AD DS nutzt Domänencontroller, um den Zugriff auf Netzwerkressourcen zu verwalten. Sobald sich ein Benutzer bei der Anmeldung an einer Domäne authentifiziert hat, können die dabei gespeicherten Anmeldeinformationen verwendet werden, um auf Ressourcen im Netzwerk zuzugreifen. Weil AD DS den Kern von Active Directory bildet und die Voraussetzung für verzeichnisfähige Anwendungen und Technologien ist, bezeichne ich diesen Dienst meist einfach als »Active Directory« statt als »Active Directory-Domänendienste« oder »AD DS«.
- **Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)** AD FS ergänzt die Authentifizierungs- und Zugriffsverwaltungsfunktionen von AD DS, indem es sie auf das World Wide Web ausweitet. AD FS nutzt Webagents, um Benutzern Zugriff auf intern betriebene Webanwendungen zu ermöglichen. Der Clientzugriff wird mithilfe von Proxys verwaltet. Wenn AD FS konfiguriert ist, können Benutzer sich anhand ihrer digitalen Identitäten über das Web authentifizieren und mit einem Webbrowser wie dem Internet Explorer auf intern betriebene Webanwendungen zugreifen.
- **Active Directory Lightweight Directory Services (AD LDS)** AD LDS stellt einen Datenspeicher für verzeichnisfähige Anwendungen zur Verfügung, die AD DS nicht benötigen und nicht auf Domänencontrollern bereitgestellt werden müssen. AD LDS läuft nicht als Betriebssystemdienst und kann sowohl in Domänen- als auch Arbeitsgruppenumgebungen verwendet werden. Jede Anwendung, die auf einem Server läuft, kann ihre eigenen Datenspeicher über AD LDS implementieren.
- **Active Directory-Rechteverwaltungsdienste (Active Directory Rights Management Services, AD RMS)** AD RMS bietet einen Schutzwall für die Informationen einer Organisation, der über das eigene Unternehmen hinausreicht. Damit können unter anderem E-Mail-Nachrichten, Dokumente und Intranetwebseiten vor nichtautorisiertem Zugriff geschützt werden. AD RMS greift auf einen Zertifikatdienst zurück, um Rechtekontozertifikate (Rights Account Certificates, RACs) auszustellen, die vertrauenswürdige Benutzer, Gruppen und Dienste identifizieren. Ein Lizenzierungsdienst gewährt autorisierten Benutzern, Gruppen und Diensten Zugriff auf geschützte Informationen, und ein Protokollierungsdienst überwacht die Rechteverwaltungsdienste. Sobald die Vertrauenswürdigkeit eines Benutzers bestätigt wurde, können Benutzer, die über ein Rechtekontozertifikat verfügen, Rechte für Informationen vergeben. Diese Rechte steuern, welche Benutzer auf die Informationen Zugriff

erhalten und was sie damit anstellen dürfen. Benutzer mit Rechtekontozertifikaten können auch auf geschützte Inhalte zugreifen, für die ihnen Zugriff gewährt wurde. Verschlüsselung stellt sicher, dass der Zugriff auf geschützte Informationen sowohl innerhalb als auch außerhalb des Unternehmens eingeschränkt bleibt.

In Windows Server 2012 führt Microsoft weitere Änderungen ein. Das sind unter anderem eine neue Domänenfunktionsebene und eine neue Gesamtstrukturfunktionsebene, die jeweils *Windows Server 2012* heißen. Die vielen weiteren Änderungen werden in Kapitel 6, »Arbeiten mit Active Directory«, beschrieben.

Schreibgeschützte Domänencontroller

Windows Server unterstützt seit der Version Windows Server 2008 schreibgeschützte Domänencontroller, und Active Directory-Domänendienste können bei Bedarf automatisch neu gestartet werden. Ein schreibgeschützter Domänencontroller (Read-Only Domain Controller, RODC) ist ein zusätzlicher Domänencontroller, der eine schreibgeschützte Kopie des Active Directory-Datenspeichers einer Domäne verwaltet. RODCs eignen sich perfekt für Zweigstellen, in denen die physische Sicherheit eines Domänencontrollers nicht garantiert werden kann. Abgesehen von Kennwörtern speichern RODCs dieselben Objekte und Attribute wie beschreibbare Domänencontroller. Diese Objekte und Attribute werden mithilfe unidirektionaler Replikation von einem beschreibbaren Domänencontroller, der als Replikationspartner agiert, auf die RODCs repliziert.

Weil RODCs in der Standardeinstellung abgesehen von ihrem eigenen Computerkonto und dem Kerberos-Target-Konto (*Krbtgt*) keine Kennwörter oder Anmeldeinformationen speichern, rufen sie die Anmeldeinformationen für Benutzer und Computer von einem beschreibbaren Domänencontroller ab, der unter Windows Server 2008 oder neuer läuft. Falls es die Kennwortreplikationsrichtlinie auf dem beschreibbaren Domänencontroller erlaubt, ruft ein RODC die Anmeldeinformationen bei Bedarf ab und speichert sie lokal so lange, bis sich die Anmeldeinformationen verändern. Da nur ein Teil der Anmeldeinformationen auf einem RODC gespeichert ist, bleibt die Zahl der betroffenen Anmeldeinformationen begrenzt, selbst wenn der Server kompromittiert wird.

TIPP Jeder Domänenbenutzer kann zum lokalen Administrator eines RODCs gemacht werden, ohne dass ihm dafür irgendwelche anderen Rechte in der Domäne gewährt werden müssen. Ein RODC kann als globaler Katalog agieren, aber nicht die Funktion eines Betriebsmasters übernehmen. RODCs können zwar Informationen von Domänencontrollern abrufen, die unter Windows Server 2003 laufen, aber Updates der Domänenpartition können RODCs nur von einem beschreibbaren Domänencontroller in derselben Domäne abrufen, der unter Windows Server 2008 oder neuer läuft.

Neustartfähige Active Directory-Domänendienste

Neustartfähige Active Directory-Domänendienste bedeuten, dass ein Administrator AD DS starten und beenden kann. In der Konsole *Dienste* von Domänencontrollern wird der Eintrag *Active Directory-Domänendienste* aufgeführt, mit dem Sie AD DS problemlos beenden und neu starten können, genauso wie jeden anderen Dienst, der lokal auf dem Server läuft. Während AD DS nicht läuft, können Sie Wartungsaufgaben durchführen, für die Sie andernfalls den gesamten Server neu starten müssten. Zum Beispiel können Sie eine Offlinedefragmentierung der Active Directory-Datenbank durchführen, Updates für das Betriebssystem einspielen oder eine autorisierende Wiederherstellung einleiten. Während AD DS auf einem Server angehalten wurde, können andere Domänencontroller Authentifizierungs- und Anmeldeaufgaben übernehmen. Zwischengespeicherte Anmeldeinformationen, Smartcards und biometrische Anmeldemethoden werden weiterhin unterstützt. Falls kein anderer Domänencontroller verfügbar ist

und keine dieser Anmeldemethoden genutzt wird, können Sie sich trotzdem noch mithilfe des Verzeichnisdienstwiederherstellungskontos und des zugehörigen Kennworts am Server anmelden.

Alle Domänencontroller, die unter Windows Server 2008 oder neuer laufen, unterstützen neustartfähige Active Directory-Domänendienste – sogar RODCs. Als Administrator können Sie AD DS über den Eintrag *Domänencontroller* in der Konsole *Dienste* starten oder beenden. Weil Active Directory neustartfähig ist, können sich Domänencontroller, die unter Windows Server 2008 oder neuer laufen, in einem der drei folgenden Zustände befinden:

- **Active Directory gestartet** In diesem Zustand wurde Active Directory gestartet, und der Domänencontroller befindet sich im selben Betriebszustand wie ein Domänencontroller, der unter Windows 2000 Server oder Windows Server 2003 läuft. Der Domänencontroller kann Authentifizierungs- und Anmeldedienste für eine Domäne erledigen.
- **Active Directory beendet** In diesem Zustand wurde Active Directory beendet. Der Domänencontroller kann keine Authentifizierungs- und Anmeldedienste für eine Domäne erledigen. Dieser Modus weist zum einen Merkmale eines Mitgliedservers auf, zum anderen Merkmale eines Domänencontrollers während der Verzeichnisdienstwiederherstellung. Wie bei einem Mitgliedserver gehört der Server zu einer Domäne. Benutzer können sich interaktiv mithilfe zwischengespeicherter Anmeldeinformationen, Smartcards und biometrischer Anmeldemethoden anmelden. Auch über das Netzwerk können sich Benutzer anmelden, indem sie einen anderen Domänencontroller für die Domänenanmeldung einsetzen. Wie bei der Verzeichnisdienstwiederherstellung (Directory Services Restore Mode, DSRM) ist die Active Directory-Datenbank (*Ntds.dit*) des lokalen Domänencontrollers offline. Das bedeutet, dass Sie AD DS-Offlineoperationen durchführen können, zum Beispiel die Datenbank defragmentieren oder Sicherheitsupdates einspielen, ohne den Domänencontroller neu starten zu müssen.
- **Verzeichnisdienstwiederherstellung** In diesem Zustand befindet sich Active Directory im Wiederherstellungsmodus. Der Domänencontroller arbeitet im selben Wiederherstellungszustand wie ein Domänencontroller, der unter Windows Server 2003 läuft. In diesem Modus können Sie eine autorisierende oder nichtautorisierende Wiederherstellung der Active Directory-Datenbank vornehmen.

Während Sie AD DS beenden, werden auch die abhängigen Dienste beendet. Das bedeutet, dass auch Dateireplikationsdienst, Kerberos-Schlüsselverteilungscenter (Key Distribution Center, KDC) und Standortübergreifender Messagingdienst beendet werden, bevor Active Directory beendet wird. Selbst falls diese Dienste laufen, werden sie neu gestartet, sobald Active Directory neu gestartet wird. Außerdem gilt: Sie können zwar einen Domänencontroller so neu starten, dass er sich in der Verzeichnisdienstwiederherstellung befindet, aber nicht so, dass er im Zustand »Active Directory beendet« läuft. Den Zustand »Active Directory beendet« erreichen Sie nur, wenn Sie den Domänencontroller erst einmal normal starten und dann AD DS beenden.

Namensauflösungsdienste

Windows-Betriebssysteme greifen auf die Namensauflösung (name resolution) zurück, damit es einfacher ist, mit anderen Computern in einem Netzwerk zu kommunizieren. Die Namensauflösung verknüpft Computernamen mit den numerischen IP-Adressen, die für die Netzwerkkommunikation genutzt werden. Statt also eine lange Ziffernfolge eingeben zu müssen, können die Benutzer auf einen Computer im Netzwerk zugreifen, indem sie seinen Anzeigename verwenden.

Aktuelle Windows-Betriebssysteme unterstützen nativ drei Namensauflösungssysteme:

- DNS (Domain Name System)
- WINS (Windows Internet Name Service)
- LLMNR (Link-Local Multicast Name Resolution)

Die folgenden Abschnitte beschreiben diese Dienste.

DNS

DNS ist ein Namensauflösungsdienst, der Computernamen in IP-Adressen auflöst. Mit DNS kann zum Beispiel der vollqualifizierte Hostname *computer84.cpandl.com* in eine IP-Adresse aufgelöst werden, die es den Computern erlaubt, sich gegenseitig im Netzwerk zu finden. DNS arbeitet über den TCP/IP-Protokollstapel und kann mit WINS, DHCP (Dynamic Host Configuration Protocol) und Active Directory-Domänendiensten integriert werden. Wie in Kapitel 15, »Betreiben von DHCP-Clients und -Servern«, beschrieben, ermöglicht DHCP die dynamische IP-Adresszuweisung und TCP/IP-Konfiguration.

DNS teilt Gruppen von Computern in Domänen ein. Diese Domänen sind in Form einer hierarchischen Struktur organisiert, die für öffentliche Netzwerke internetweit oder für private Netzwerke (auch als Intranets und Extranets bezeichnet) unternehmensweit aufgebaut sein kann. Die verschiedenen Ebenen innerhalb der Hierarchie identifizieren einzelne Computer, Organisationsdomänen und Topleveldomänen. Im vollqualifizierten Hostnamen *computer84.cpandl.com* sind *computer84* der Hostname eines bestimmten Computers, *cpandl* der Name der Organisationsdomäne und *com* die Topleveldomäne.

Topleveldomänen liegen im Stamm der DNS-Hierarchie, sie werden daher als *Stammdomänen* (root domain) bezeichnet. Diese Domänen werden nach Staaten, Organisationstypen und Aufgabe untergliedert. Normale Domänen, zum Beispiel *cpandl.com*, werden auch als *übergeordnete Domänen* (parent domain) bezeichnet, weil sie übergeordnete Elemente innerhalb einer Organisationsstruktur bilden. Übergeordnete Domänen können in untergeordnete Domänen (subdomain, manchmal auch child domain) untergliedert werden, zum Beispiel für Gruppen oder Abteilungen innerhalb einer Organisation.

Nehmen wir einmal an, der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) eines Computers lautet *jacob.hr.cpandl.com*. In diesem Fall ist *jacob* der Hostname, *hr* die untergeordnete Domäne und *cpandl.com* die übergeordnete Domäne.

Active Directory-Domänen verwenden DNS, um ihre Namensstruktur und -hierarchie zu implementieren. Active Directory und DNS sind so eng miteinander verknüpft, dass Sie DNS im Netzwerk installieren müssen, bevor Sie Domänencontroller für Active Directory installieren können. Während der Installation des ersten Domänencontrollers in einem Active Directory-Netzwerk bekommen Sie angeboten, DNS automatisch zu installieren, falls kein DNS-Server im Netzwerk gefunden wurde. Sie können dabei auch angeben, ob DNS und Active Directory vollständig integriert werden sollen. In den meisten Fällen sollten Sie diese beiden Möglichkeiten nutzen. Bei vollständiger Integration werden die DNS-Informationen direkt in Active Directory gespeichert, sodass Sie die Fähigkeiten von Active Directory nutzen können. Der Unterschied zwischen teilweiser und vollständiger Integration ist sehr wichtig.

- **Teilweise Integration** Bei der teilweisen Integration verwendet die Domäne eine Standarddateispeicherung. Die DNS-Informationen werden in Textdateien mit der Erweiterung *.dns* gespeichert, die standardmäßig unter *%SystemRoot%\System32\Dns* abgelegt sind. DNS-Aktualisierungen werden von einem einzigen autorisierenden DNS-Server verarbeitet. Dieser Server wird als primärer DNS-Server für die jeweilige Domäne oder einen bestimmten Bereich innerhalb einer Domäne festgelegt, die sogenannte *Zone*. Clients, die DHCP mit dynamischen DNS-Aktualisierungen kombinieren, müssen so konfiguriert werden, dass sie den primären DNS-Server in der Zone benutzen, sonst wer-

den ihre DNS-Informationen nicht aktualisiert. Und natürlich können keine dynamischen Aktualisierungen über DHCP vorgenommen werden, falls der primäre DNS-Server offline ist.

- **Vollständige Integration** Bei vollständiger Integration arbeitet die Domäne mit verzeichnisintegrierter Speicherung. Die DNS-Informationen werden direkt in Active Directory gespeichert und stehen über den Container für das Objekt *dnsZone* zur Verfügung. Weil die Informationen Teil von Active Directory sind, können alle Domänencontroller auf die Daten zugreifen. Dynamische Aktualisierungen über DHCP können mithilfe eines Multimasterverfahrens implementiert werden. So kann jeder Domänencontroller, auf dem der DNS-Serverdienst läuft, dynamische Aktualisierungen verarbeiten. Außerdem können Clients, die dynamische DNS-Aktualisierungen über DHCP vornehmen, dafür jeden beliebigen DNS-Server innerhalb der Zone verwenden. Ein weiterer Vorteil der Verzeichnisintegration ist die Fähigkeit, mithilfe der Verzeichnissicherheit den Zugriff auf DNS-Informationen zu steuern.

Wenn Sie sich ansehen, wie DNS-Informationen über das Netzwerk repliziert werden, werden noch mehr Vorteile der vollständigen Integration mit Active Directory deutlich. Bei einer teilweisen Integration werden DNS-Informationen getrennt von Active Directory gespeichert und repliziert. Wenn Sie zwei separate Strukturen verwenden, verringern Sie die Leistung von DNS wie auch Active Directory und machen die Administration komplizierter. Weil DNS weniger effizient ist als Active Directory, wenn es um die Replikation von Änderungen geht, erhöhen Sie möglicherweise den Netzwerkverkehr, und es dauert länger, DNS-Änderungen im gesamten Netzwerk zu verteilen.

Um DNS im Netzwerk aktivieren zu können, müssen Sie DNS-Clients und -Server konfigurieren. Wenn Sie DNS-Clients konfigurieren, teilen Sie den Clients die IP-Adressen der DNS-Server im Netzwerk mit. Mithilfe dieser Adressen können Clients mit DNS-Servern kommunizieren, die sich irgendwo im Netzwerk befinden. Die Server können sich dabei sogar in anderen Subnetzen befinden.

Wenn das Netzwerk DHCP nutzt, sollten Sie DHCP so konfigurieren, dass es mit DNS zusammenarbeitet. Dazu müssen Sie die DHCP-Bereiche 006 (DNS-Server) und 015 (DNS-Domänenname) einstellen, wie in »Festlegen von Bereichsoptionen« auf Seite 617 beschrieben. Falls Computer im Netzwerk von anderen Active Directory-Domänen aus erreichbar sein sollen, müssen Sie außerdem Datensätze für diesen Computer in DNS eintragen. DNS-Datensätze sind in Form von Zonen organisiert. Eine Zone ist einfach ein Bereich innerhalb einer Domäne. Wie Sie einen DNS-Server konfigurieren, ist in »Konfigurieren eines primären DNS-Servers« auf Seite 643 erklärt.

Wenn Sie den DNS-Serverdienst auf einem RODC installieren, kann der RODC eine schreibgeschützte Kopie aller Anwendungsverzeichnispartitionen abrufen, die von DNS benutzt werden, inklusive *ForestDNSZones* und *DomainDNSZones*. Clients können dann Abfragen für eine Namensauflösung an den RODC schicken. Das funktioniert genauso, als würden sie Abfragen an irgendeinen anderen DNS-Server senden. Wie bei Verzeichnisaktualisierungen unterstützt der DNS-Server auf einem RODC allerdings keine direkten Aktualisierungen. Das bedeutet, dass der RODC keine Namenserver-Ressourceneinträge (NS) für Active Directory-integrierte Zonen registriert, die er hostet. Wenn ein Client versucht, seine DNS-Datensätze in einem RODC zu aktualisieren, gibt der Server einen Verweis auf einen DNS-Server zurück, bei dem der Client seine Aktualisierung registrieren kann. Der DNS-Server auf dem RODC müsste den aktualisierten Datensatz von dem DNS-Server, der die Aktualisierungsdaten entgegengenommen hat, in Form einer speziellen, als Hintergrundprozess laufenden Anforderung zur Replikation eines einzelnen Objekts bekommen.

Seit der Version Windows 7 bringt Windows Unterstützung für DNSSEC (DNS Security Extensions) mit. Der DNS-Client, der auf diesen Betriebssystemen läuft, kann Abfragen senden, die angeben, dass DNSSEC unterstützt wird, entsprechende Einträge verarbeiten und feststellen, ob ein DNS-Server die in seinem Auftrag vorgenommenen Einträge verifiziert hat. Auf Windows-Servern können Ihre DNS-Server

Zonen sicher signieren und DNSSEC-signierte Zonen hosten. Außerdem sind DNS-Server in der Lage, entsprechende Einträge zu verarbeiten und sowohl Überprüfung als auch Authentifizierung durchzuführen.

WINS (Windows Internet Name Service)

WINS ist ein Namensauflösungsdienst, der Computernamen in IP-Adressen auflöst. Mit WINS wird ein Computername wie etwa *COMPUTER84* in eine IP-Adresse aufgelöst, die es Computern in einem Microsoft-Netzwerk ermöglicht, sich gegenseitig zu finden und Informationen auszutauschen. WINS ist erforderlich, wenn Prä-Windows 2000-Systeme und ältere Anwendungen unterstützt werden sollen, die mit NetBIOS über TCP/IP arbeiten, zum Beispiel die *NET*-Befehlszeilenprogramme. Sofern Sie keine Prä-Windows 2000-Systeme oder alte Anwendungen im Netzwerk haben, brauchen Sie WINS nicht.

WINS funktioniert am besten in Client/Server-Umgebungen, wo WINS-Clients Single-Label-Namensabfragen nach einer Hostnamensauflösung an WINS-Server senden und WINS-Server diese Abfragen auflösen und eine Antwort zurückschicken. Wenn all Ihre DNS-Server unter Windows Server 2008 oder neuer laufen und Sie eine globale Namenszone bereitstellen, werden statische, globale Einträge mit Kurznamen erstellt, die nicht auf WINS aufbauen. So können Benutzer mithilfe von Kurznamen auf Hosts zugreifen und brauchen keine FQDNs zu verwenden; WINS ist dafür nicht mehr notwendig. Um WINS-Abfragen und andere Informationen zu versenden, benutzen die Computer NetBIOS. NetBIOS stellt eine Programmierschnittstelle (Application Programming Interface, API) zur Verfügung, die es Computern erlaubt, in einem Netzwerk zu kommunizieren. NetBIOS-Anwendungen greifen auf WINS oder die lokale Datei *LMHOSTS* zurück, um Computernamen in IP-Adressen aufzulösen. In Prä-Windows 2000-Netzwerken ist WINS der primäre Namensauflösungsdienst. In Netzwerken ab Windows 2000 ist dagegen DNS der primäre Namensauflösungsdienst und WINS übernimmt eine andere Funktion. In diesem Fall erlaubt WINS es nämlich Prä-Windows 2000-Systemen, Listen der Ressourcen im Netzwerk zu durchsuchen, damit Systeme, die mit Windows 2000 oder neuer arbeiten, NetBIOS-Ressourcen finden können.

Um die WINS-Namensauflösung in einem Netzwerk aktivieren zu können, müssen Sie WINS-Clients und -Server konfigurieren. Wenn Sie WINS-Clients konfigurieren, teilen Sie den Clients die IP-Adressen der WINS-Server im Netzwerk mit. Anhand der IP-Adresse können Clients mit WINS-Servern kommunizieren, die sich an beliebiger Stelle im Netzwerk befinden, sogar in anderen Subnetzen. WINS-Clients können auch über eine Broadcastmethode kommunizieren, bei der die Clients ihre Nachrichten an alle anderen Computer im lokalen Netzwerksegment senden und deren IP-Adressen anfordern. Weil die Nachrichten im Broadcastverfahren gesendet werden, wird kein WINS-Server benutzt. Alle Clients, die nicht mit WINS arbeiten, aber diese Art von Broadcastnachricht unterstützen, können über diese Methode ebenfalls Computernamen in IP-Adressen konvertieren.

Wenn Clients mit WINS-Servern kommunizieren, richten sie Sitzungen ein, die aus drei Kernelementen bestehen:

- **Namensregistrierung** Während der Namensregistrierung teilt der Client dem Server seinen Computernamen und seine IP-Adresse mit und fordert den Server auf, ihn zur WINS-Datenbank hinzuzufügen. Falls der angegebene Computername und die IP-Adresse noch nicht innerhalb des Netzwerks verwendet werden, akzeptiert der WINS-Server die Anforderung und registriert den Client in der WINS-Datenbank.
- **Namenserneuerung** Die Namensregistrierung ist nicht dauerhaft. Der Client bekommt den Namen nur für einen bestimmten Zeitraum. Dieser Zeitraum wird als Lease bezeichnet. Der Client bekommt auch mitgeteilt, nach welcher Zeitdauer die Lease erneuert werden muss. Dies ist das Erneuerungsintervall. Der Client muss sich während des Erneuerungsintervalls erneut beim WINS-Server registrieren.

- **Namensfreigabe** Falls der Client die Lease nicht erneuert, wird die Namensregistrierung freigegeben, sodass ein anderes System im Netzwerk den Computernamen, die IP-Adresse oder beide benutzen kann. Die Namen werden auch dann freigegeben, wenn Sie einen WINS-Client herunterfahren.

Sobald ein Client eine Sitzung mit einem WINS-Server aufgebaut hat, kann er Namensauflösungsdienste anfordern. Welche Methode benutzt wird, um Computernamen in IP-Adressen aufzulösen, hängt von der Netzwerkkonfiguration ab. Es stehen die folgenden vier Namensauflösungsmethoden zur Verfügung:

- **B-Knoten (Broadcast)** Die Computernamen werden mithilfe von Broadcastnachrichten in IP-Adressen aufgelöst. Computer, die einen Namen auflösen wollen, senden an alle Hosts im lokalen Netzwerk eine Broadcastnachricht, mit der die IP-Adresse für einen Computernamen angefordert wird. In einem großen Netzwerk mit Hunderten oder Tausenden von Computern können diese Broadcastnachrichten wertvolle Netzwerkbandbreite verbrauchen.
- **P-Knoten (Peer-to-Peer)** Die Computernamen werden mithilfe von WINS-Servern in IP-Adressen aufgelöst. Wie weiter oben erklärt, umfassen Clientsitzungen drei Teile: Namensregistrierung, Namenserneuerung und Namensfreigabe. Wenn ein Client in diesem Modus einen Computernamen in eine IP-Adresse auflösen will, sendet er eine Abfragenachricht an den Server, und der Server schickt eine Antwort.
- **M-Knoten (gemischt)** Kombiniert B- und P-Knoten. Bei M-Knoten versucht ein WINS-Client zuerst, eine Namensauflösung über B-Knoten durchzuführen. Falls dieser Versuch fehlschlägt, verwendet der Client anschließend P-Knoten. Weil zuerst B-Knoten probiert werden, weist diese Methode dieselben Probleme bezüglich der Netzwerkbandbreitenbelastung auf wie B-Knoten.
- **H-Knoten (hybrid)** Kombiniert ebenfalls B-Knoten und P-Knoten. Bei H-Knoten versucht ein WINS-Client zuerst, eine Peer-to-Peer-Namensauflösung über P-Knoten durchzuführen. Falls dieser Versuch fehlschlägt, verwendet der Client Broadcastnachrichten mit B-Knoten. Weil Peer-to-Peer als primäre Methode eingesetzt wird, bieten H-Knoten in den meisten Netzwerken die beste Leistung. H-Knoten sind die Standardmethode für die WINS-Namensauflösung.

Falls WINS-Server im Netzwerk zur Verfügung stehen, verwenden Windows-Clients für die Namensauflösung die Methode mit P-Knoten. Sind dagegen keine WINS-Server im Netzwerk vorhanden, erledigen Windows-Clients die Namensauflösung mit B-Knoten. Windows-Computer können auch DNS und die lokalen Dateien *LMHOSTS* und *HOSTS* benutzen, um Netzwerknamen aufzulösen. Die Benutzung von DNS wird in Kapitel 16, »Optimieren von DNS«, genauer beschrieben.

Wenn Sie IP-Adressen mithilfe von DHCP dynamisch zuweisen, sollten Sie die Namensauflösungsmethode für die DHCP-Clients festlegen. Dazu müssen Sie in den DHCP-Optionen den Bereich 046 (WINS/NBT-Knotentyp) konfigurieren, wie in »Festlegen von Bereichsoptionen« auf Seite 617 beschrieben. Die beste Methode sind H-Knoten. Sie erhalten damit die optimale Leistung, und der Verkehr im Netzwerk verringert sich.

LLMNR (Link-Local Multicast Name Resolution)

LLMNR füllt eine Lücke bezüglich Peer-to-Peer-Namensauflösungsdiensten für Geräte, die Adressen im Format IPv4, IPv6 oder beide haben. Mit LLMNR können IPv4- und IPv6-Geräte im selben Subnetz arbeiten, ohne dass ein WINS- oder DNS-Server die Namen der jeweils anderen Geräteklasse auflösen muss. Einen solchen Dienst können weder WINS noch DNS vollständig zur Verfügung stellen. WINS kann zwar sowohl Client/Server- als auch Peer-to-Peer-Namensauflösungsdienste für IPv4 bereitstellen, bietet aber keine Unterstützung für IPv6-Adressen. DNS unterstützt dagegen zwar sowohl IPv4- als auch IPv6-Adressen, für die Namensauflösungsdienste werden aber Server benötigt.

Seit der Version Windows 7 bietet Windows Unterstützung für LLMNR. LLMNR kann IPv4- wie auch IPv6-Clients bedienen, wenn keine anderen Namensauflösungssysteme zur Verfügung stehen. Einige Einsatzbereiche sind zum Beispiel:

- Heim- oder kleine Büronetzwerke
- Ad-hoc-Netzwerke
- Unternehmensnetzwerke, in denen keine DNS-Dienste verfügbar sind

LLMNR soll DNS ergänzen, indem es eine Namensauflösung in Situationen anbietet, in denen keine herkömmliche DNS-Namensauflösung möglich ist. LLMNR kann zwar WINS ersetzen, sofern NetBIOS nicht mehr erforderlich ist, aber LLMNR ist kein Ersatz für DNS, weil es nur im lokalen Subnetz arbeitet. Da LLMNR-Verkehr nicht über Routergrenzen weitergeleitet wird, ist sichergestellt, dass er nicht versehentlich das Netzwerk flutet.

Wie WINS dient auch LLMNR dazu, einen Hostnamen, zum Beispiel *COMPUTER84*, in eine IP-Adresse umzuwandeln. In der Standardeinstellung ist LLMNR auf allen Computern aktiviert, die unter Windows 7 oder neuer laufen. Diese Computer verwenden LLMNR nur, wenn alle anderen Versuche, einen Hostnamen über DNS aufzulösen, fehlgeschlagen sind. Daher läuft die Namensauflösung seit Windows 7 folgendermaßen ab:

1. Ein Hostcomputer sendet eine Abfrage an seinen primären DNS-Server. Falls der Hostcomputer keine Antwort oder einen Fehler empfängt, versucht er es nacheinander bei allen alternativen DNS-Servern. Falls der Host keine DNS-Server konfiguriert hat oder keine fehlerfreie Verbindung zu einem DNS-Server herstellen kann, wird die Namensauflösung an LLMNR weitergereicht.
2. Der Hostcomputer sendet über UDP (User Datagram Protocol) eine Multicastabfrage, in der die IP-Adresse für den gesuchten Namen angefordert wird. Diese Abfrage ist auf das lokale Subnetz beschränkt (die »lokale Verbindung« aus dem Namen »Link-Local Multicast Name Resolution«).
3. Jeder Computer in der lokalen Verbindung, der LLMNR unterstützt und so konfiguriert ist, dass er auf eingehende Abfragen antwortet, empfängt die Abfrage und vergleicht den Namen mit seinem eigenen Hostnamen. Falls der Hostname nicht übereinstimmt, verwirft der Computer die Abfrage. Falls der Hostname übereinstimmt, sendet der Computer eine Unicastnachricht mit seiner IP-Adresse an den ursprünglichen Host.

Sie können mit LLMNR auch eine IP-Adresse in einen Hostnamen konvertieren (das sogenannte »reverse mapping«). Dabei sendet ein Computer eine Unicastabfrage an eine bestimmte IP-Adresse und fordert den Hostnamen des Zielcomputers an. Wenn ein LLMNR-fähiger Computer diese Anforderung empfängt, sendet er eine Unicastantwort, die seinen Hostnamen enthält, als Antwort an den ursprünglichen Host.

Computer müssen LLMNR-fähig sein, um sicherzustellen, dass ihre Namen innerhalb des lokalen Subnetzes einmalig sind. In den meisten Fällen prüft ein Computer in folgenden Fällen, ob sein Name eindeutig ist: beim Start, wenn er aus einem Ruhezustand aufgeweckt wird und wenn Sie die Einstellungen seiner Netzwerkschnittstelle ändern. Falls ein Computer noch nicht sichergestellt hat, dass sein Name einmalig ist, muss er auf diesen Umstand hinweisen, wenn er auf eine Namensabfrage antwortet.

PRAXISTIPP In der Standardeinstellung wird LLMNR auf Computern, die unter Windows 7 oder neuer laufen, automatisch aktiviert. Sie können LLMNR über Registrierungseinstellungen deaktivieren.

Um LLMNR für alle Netzwerkschnittstellen zu deaktivieren, können Sie den folgenden Registrierungswert anlegen und auf den Wert 0 (null) setzen: *HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast*. Um LLMNR für eine bestimmte Netzwerkschnittstelle zu deaktivieren, können Sie den folgenden Registrierungswert

anlegen und auf den Wert 0 (null) setzen: *HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/<Adapter-GUID>/EnableMulticast*, wobei *<Adapter-GUID>* für die GUID (Globally Unique Identifier) des Netzwerkadapters steht, bei dem Sie LLMNR deaktivieren wollen. Sie können LLMNR jederzeit wieder aktivieren, indem Sie diese Registrierungswerte auf den Wert 1 setzen. Sie können LLMNR auch über Gruppenrichtlinien verwalten.

Häufig benutzte Tools

Für die Verwaltung von Windows Server 2012-Systemen stehen zahlreiche Dienstprogramme zur Verfügung. Die folgenden Tools werden am häufigsten verwendet:

- **Systemsteuerung** Eine Sammlung von Tools zum Verwalten der Systemkonfiguration. Sie können die Systemsteuerung auf unterschiedliche Arten strukturieren; dafür stehen mehrere Ansichten zur Verfügung. Eine Ansicht dient als einfache Möglichkeit, Optionen zu organisieren und aufzulisten. Sie wählen die verwendete Ansicht unter *Anzeige* aus. Die nach Kategorien organisierte Systemsteuerungsansicht ist die Standardansicht, sie bietet Zugriff auf die Tools anhand von Kategorie, Tool und wichtigen Aufgaben. Die Ansichten mit großen und kleinen Symbolen listen alle Tools anhand ihrer Namen auf.
- **Grafische Verwaltungsprogramme** Die wichtigsten Tools zum Verwalten von Netzwerkcomputern und deren Ressourcen. Sie greifen auf diese Tools zu, indem Sie sie einzeln in der Programmgruppe *Verwaltung* auswählen.
- **Verwaltungsassistenten** Tools, die für die Automatisierung wichtiger Verwaltungsarbeiten entwickelt wurden. Viele Verwaltungsassistenten können Sie im Server-Manager starten, der zentralen Administrationskonsole in Windows Server 2012.
- **Befehlszeilendienstprogramme** Die meisten Verwaltungsprogramme lassen sich über die Befehlszeile starten. Zusätzlich zu diesen Dienstprogrammen bietet Windows Server 2012 noch weitere Tools, die für die Arbeit mit Windows Server 2012-Systemen nützlich sind.

  Wie *NET*-Befehlszeilentools arbeiten, finden Sie heraus, indem Sie in einer Eingabeaufforderung **NET HELP** eingeben, gefolgt vom Befehlsnamen, zum Beispiel **NET HELP SHARE**. Windows Server 2012 zeigt dann einen Überblick an, wie der Befehl verwendet wird.

Windows PowerShell 3.0

Um Ihren Befehlszeilenskripts mehr Flexibilität zu verleihen, können Sie Windows PowerShell 3.0 benutzen. PowerShell 3.0 ist eine umfassende Befehlsshell, die eingebaute Befehle (die sogenannten *Cmdlets*), eingebaute Programmierungsfeatures und Standardbefehlszeilenprogramme nutzen kann. Es stehen eine Befehlskonsole und eine grafische Umgebung zur Verfügung.

Zwar werden die Windows PowerShell-Konsole sowie die grafische Skriptumgebung in der Standardeinstellung installiert, es fehlen aber einige andere PowerShell-Features. Das sind unter anderem das Windows PowerShell 2.0-Modul, das Abwärtskompatibilität zu vorhandenen PowerShell-Hostanwendungen sicherstellt, und Windows PowerShell Web Access, mit dem ein Server als Webgateway agiert, damit er über PowerShell und einen Webclient im Remotezugriff verwaltet werden kann.

PRAXISTIPP Sie können diese zusätzlichen Windows PowerShell-Features mit dem Assistenten zum Hinzufügen von Rollen und Features installieren. Auf dem Desktop tippen oder klicken Sie dazu in der Taskleiste auf die Schaltfläche *Server-Manager*. Tippen oder klicken Sie dann im Server-Manager auf *Verwalten* und dann auf *Rollen und Features hinzufügen*. Daraufhin wird der Assistent zum Hinzufügen von Rollen und Features gestartet, in dem Sie die gewünschten Features

auswählen können. Beachten Sie aber, dass Sie in Windows Server 2012 nicht nur eine Rolle oder ein Feature deaktivieren, sondern auch die Binärdateien der jeweiligen Rolle oder des Features entfernen können. Binärdateien, die für die Installation von Rollen und Features nötig sind, werden als *Nutzlast* (payload) bezeichnet.

Die Windows PowerShell-Konsole (*Powershell.exe*) ist eine 32-Bit- oder 64-Bit-Umgebung, die Sie nutzen, um in einer Befehlszeile mit Windows PowerShell zu arbeiten. In 32-Bit-Versionen von Windows finden Sie die ausführbare 32-Bit-Datei im Verzeichnis *%SystemRoot%\System32\WindowsPowerShell\v1.0*. In 64-Bit-Versionen von Windows befindet sich die ausführbare 32-Bit-Datei im Verzeichnis *%SystemRoot%\SysWow64\WindowsPowerShell\v1.0* und die ausführbare 64-Bit-Datei in *%SystemRoot%\System32\WindowsPowerShell\v1.0*.

Auf dem Desktop öffnen Sie die Windows PowerShell-Konsole, indem Sie die Schaltfläche *Windows PowerShell* auf der Taskleiste antippen oder anklicken. Auf 64-Bit-Systemen wird standardmäßig die 64-Bit-Version von PowerShell gestartet. Wollen Sie auf einem solchen System die 32-Bit-PowerShell-Konsole verwenden, müssen Sie den Befehl *Windows PowerShell (x86)* wählen.

Aus einer Windows-Eingabeaufforderung (*Cmd.exe*) starten Sie Windows PowerShell, indem Sie folgenden Befehl ausführen:

```
powershell
```

HINWEIS Der Verzeichnispfad von Windows PowerShell müsste standardmäßig in Ihren Befehlspfad eingetragen sein. So ist sichergestellt, dass Sie Windows PowerShell von einer Eingabeaufforderung starten können, ohne erst in das entsprechende Verzeichnis wechseln zu müssen.

Wenn Sie Windows PowerShell gestartet haben, können Sie in der Eingabeaufforderung den Namen eines Cmdlets eingeben. Es wird dann genauso ausgeführt wie bei der Eingabe als Befehlszeilenkommando. Sie können Cmdlets auch aus einem Skript heraus ausführen. Die Namen von Cmdlets werden aus Verb-Substantiv-Paaren gebildet. Das Verb verrät, was das Cmdlet prinzipiell tut. Das Substantiv gibt an, mit welchem Objekt das Cmdlet arbeitet. Zum Beispiel ruft das Cmdlet *Get-Variable* entweder alle Windows PowerShell-Umgebungsvariablen ab und gibt ihre Werte zurück, oder sie ruft eine bestimmte Umgebungsvariable anhand ihres Namens ab und gibt ihren Wert zurück. Die folgenden Verben werden häufig für Cmdlets benutzt:

- ***Get-*** Fragt ein bestimmtes Objekt oder eine Untermenge von Objekttypen ab, zum Beispiel einen bestimmten oder alle Leistungsindikatoren.
- ***Set-*** Verändert bestimmte Einstellungen eines Objekts.
- ***Enable-*** Aktiviert eine Option oder ein Feature.
- ***Disable-*** Deaktiviert eine Option oder ein Feature.
- ***New-*** Erstellt eine neue Instanz eines Elements, zum Beispiel ein neues Ereignis oder einen Dienst.
- ***Remove-*** Entfernt eine Instanz eines Elements, zum Beispiel ein Ereignis oder ein Ereignisprotokoll.

Sie können sich in der Windows PowerShell-Eingabeaufforderung eine vollständige Liste aller verfügbaren Cmdlets anzeigen lassen, indem Sie **get-help** *-* eingeben. Die Hilfedokumentation zu einem bestimmten Cmdlet zeigen Sie an, indem Sie **get-help** gefolgt vom Namen des Cmdlets eingeben, zum Beispiel **get-help get-variable**.

Für alle Cmdlets gibt es auch konfigurierbare Aliasnamen, die Sie als Abkürzung zum Ausführen des entsprechenden Cmdlets verwenden können. Sie können sich alle verfügbaren Aliasnamen anzeigen lassen, indem Sie in der Windows PowerShell-Eingabeaufforderung den Befehl **get-item –path alias:** eingeben. Mit der folgenden Syntax definieren Sie ein Alias, das einen beliebigen Befehl aufruft:

```
new-item -path alias:Aliasname -value:VollständigerBefehlspfad
```

Dabei stehen *AliasName* für den Aliasnamen, der definiert werden soll, und *VollständigerBefehlspfad* für den vollständigen Pfad des Befehls, der ausgeführt werden soll. Ein Beispiel:

```
new-item -path alias:sm -value:c:\windows\system32\compmgmtlauncher.exe
```

Dieses Beispiel definiert den Aliasnamen *sm*, um den Server-Manager zu starten. Sie können diesen Aliasnamen in Windows PowerShell verwenden, indem Sie einfach **sm** eingeben und dann die EINGABETASTE drücken.

PRAXISTIPP Praktisch alles, was Sie in einer Eingabeaufforderung eingeben, können Sie auch in der PowerShell-Eingabeaufforderung verwenden. Das ist möglich, weil PowerShell im Rahmen seiner normalen Verarbeitung nach externen Befehlen und Dienstprogrammen sucht. Solange der externe Befehl oder das Dienstprogramm in einem Verzeichnis liegt, das in der Umgebungsvariable *PATH* enthalten ist, wird der Befehl oder das Dienstprogramm ausgeführt. Denken Sie aber daran, dass die Ausführungsreihenfolge von PowerShell Einfluss darauf hat, ob ein Befehl wie erwartet läuft. In PowerShell ist die Ausführungsreihenfolge folgendermaßen festgelegt:

1. integrierte oder im Profil definierte Aliasnamen,
2. integrierte oder im Profil definierte Funktionen,
3. Cmdlets oder Sprachschlüsselwörter,
4. Skripts mit der Erweiterung *.ps1* und
5. externe Befehle, Dienstprogramme und Dateien.

Trägt also irgendein Element aus den Punkten 1 bis 4 der Ausführungsreihenfolge denselben Namen wie ein Befehl, wird statt des erwarteten Befehls dieses Element ausgeführt.

Windows-Remoteverwaltung

Die Remotefeatures von Windows PowerShell bauen auf dem Protokoll WS-Verwaltung (WS-Management) und dem Dienst *Windows-Remoteverwaltung* (WinRM) auf, der WS-Verwaltung in Windows implementiert. Computer, die unter Windows 7 oder neuer laufen, enthalten WinRM 2.0 oder eine neuere Version. Wenn Sie einen Windows Server 2012-Computer von einer Arbeitsstation aus verwalten wollen, müssen Sie sicherstellen, dass WinRM 2.0 und Windows PowerShell 3.0 installiert sind und auf dem Server ein WinRM-Listener aktiviert ist. Mithilfe einer IIS-Erweiterung, die als Windows-Feature namens *WinRM-IIS-Erweiterung* installiert wird, können Sie einen Server als Webgateway einrichten, um ihn im Remotezugriff mit WinRM und einem Webclient zu verwalten.

Aktivieren und Verwenden von WinRM

Gehen Sie folgendermaßen vor, um die Verfügbarkeit von WinRM 2.0 zu überprüfen und Windows PowerShell für den Remotezugriff zu konfigurieren:

1. Tippen oder klicken Sie auf *Start* und dann auf *Windows PowerShell*. Starten Sie Windows PowerShell als Administrator, indem Sie die Verknüpfung *Windows PowerShell* mit der rechten Maustaste anklicken oder gedrückt halten und *Als Admin ausführen* wählen.
2. Der WinRM-Dienst ist standardmäßig mit dem Starttyp *Manuell* konfiguriert. Sie müssen den Starttyp auf jedem Computer, den Sie verwalten wollen, auf *Automatisch* ändern und den Dienst starten.

In der Windows PowerShell-Eingabeaufforderung können Sie mit dem folgenden Befehl überprüfen, ob der WinRM-Dienst läuft:

```
get-service winrm
```

Wie im folgenden Beispiel zu sehen, sollte in der Ausgabe unter *Status* der Wert *Running* angezeigt werden:

```
Status   Name               DisplayName
------   ----               -----------
Running  winrm              Windows-Remoteverwaltung (WS-Verwaltung)
```

Läuft der Dienst nicht, können Sie den folgenden Befehl eingeben, um ihn zu starten und so zu konfigurieren, dass er künftig automatisch gestartet wird:

```
set-service -name winrm -startuptype automatic -status running
```

3. Führen Sie folgenden Befehl aus, um Windows PowerShell für die Remoteverwaltung zu konfigurieren:

   ```
   Enable-PSRemoting -force
   ```

   Sie können die Remoteverwaltung nur aktivieren, wenn Ihr Computer mit einem Domänen- oder privaten Netzwerk verbunden ist. Ist Ihr Computer dagegen an ein öffentliches Netzwerk angeschlossen, müssen Sie diese Verbindung trennen, den Computer an ein Domänen- oder privates Netzwerk anschließen und diesen Schritt wiederholen. Falls mindestens eine Verbindung Ihres Computers den Netzwerkverbindungstyp *Öffentlich* hat, Sie aber momentan mit einem Domänen- oder privaten Netzwerk verbunden sind, müssen Sie den Netzwerkverbindungstyp im Netzwerk- und Freigabecenter umstellen und diesen Schritt wiederholen.

In vielen Fällen können Sie mit Remotecomputern arbeiten, die sich in anderen Domänen befinden. Liegt der Remotecomputer allerdings nicht in einer vertrauenswürdigen Domäne, kann er Ihre Anmeldeinformationen möglicherweise nicht authentifizieren. Damit die Authentifizierung funktioniert, müssen Sie den Remotecomputer in WinRM unter Umständen zur Liste der vertrauenswürdigen Hosts für den lokalen Computer hinzufügen. Geben Sie dazu den folgenden Befehl ein:

```
winrm set winrm/config/client '@{TrustedHosts"RemoteComputer"}'
```

Dabei ist *RemoteComputer* der Name des Remotecomputers. Ein Beispiel:

```
winrm set winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

Wenn Sie mit Computern in Arbeitsgruppen oder Heimnetzgruppen arbeiten, müssen Sie HTTPS als Transport verwenden oder den Remotecomputer zu den TrustedHosts-Konfigurationseinstellungen hinzufügen. Gelingt es Ihnen nicht, eine Verbindung zu einem Remotehost herzustellen, sollten Sie prüfen, ob der Dienst auf dem Remotehost läuft und Anforderungen entgegennimmt. Führen Sie dazu auf dem Remotehost diesen Befehl aus:

```
winrm quickconfig
```

Dieser Befehl analysiert und konfiguriert den WinRM-Dienst. Ist der WinRM-Dienst richtig konfiguriert, müsste die Ausgabe etwa so aussehen:

```
WinRM ist bereits zum Empfangen von Anforderungen auf diesem Computer konfiguriert.
WinRM ist bereits für die Remoteverwaltung auf diesem Computer eingerichtet
```

Falls der WinRM-Dienst nicht richtig eingerichtet ist, erhalten Sie Fehlermeldungen. Anschließend müssen Sie mehrere Eingabeaufforderungen bestätigen, damit die Remoteverwaltung automatisch konfiguriert wird. Sobald dieser Vorgang abgeschlossen ist, müsste WinRM richtig konfiguriert sein.

Wenn Sie die Remoteverwaltungsfeatures von Windows PowerShell nutzen wollen, müssen Sie Windows PowerShell grundsätzlich als Administrator starten, indem Sie *Windows PowerShell* mit der rechten Maus-

taste anklicken oder gedrückt halten und *Als Admin ausführen* wählen. Wenn Sie Windows PowerShell aus einem anderen Programm heraus starten, etwa in der Eingabeaufforderung, müssen Sie dieses Programm als Administrator ausführen.

Konfigurieren von WinRM

Wenn Sie mit einer Administratoreingabeaufforderung arbeiten, können Sie das WinRM-Befehlszeilenprogramm verwenden, um die Remoteverwaltungskonfiguration anzuzeigen und zu ändern. Geben Sie **winrm get winrm/config** ein, um sich ausführliche Informationen über die Remoteverwaltungskonfiguration anzeigen zu lassen.

Wenn Sie die Ausgabe dieses Befehls betrachten, stellen Sie fest, dass die Daten hierarchisch untergliedert sind. Der Stamm der Hierarchie, die Ebene *Config*, wird über den Pfad *winrm/config* angesprochen. Darunter befinden sich Ebenen für Client, Dienst und WinRS, die über *winrm/config/client*, *winrm/config/service* beziehungsweise *winrm/config/winrs* aufgerufen werden. Sie können die Werte der meisten Konfigurationsparameter mit folgendem Befehl ändern:

```
winrm set ConfigPath @{Parametername="Wert"}
```

Dabei ist *ConfigPath* der Konfigurationspfad, *Parametername* der Name des Parameters, den Sie ändern wollen, und *Wert* der neue Wert des Parameters. Hier ein Beispiel:

```
winrm set winrm/config/winrs @{MaxShellsPerUser="10"}
```

Hier legen Sie den Wert des Parameters *MaxShellsPerUser* unter *winrm/config/winrs* fest. Er steuert, wie viele Verbindungen zu einem Remotecomputer pro Benutzer höchstens aktiv sein dürfen. (In der Standardeinstellung kann jeder Benutzer höchstens fünf aktive Verbindungen haben.) Denken Sie daran, dass manche Parameter schreibgeschützt sind und nicht auf diese Weise geändert werden können.

WinRM benötigt mindestens einen Listener, der festlegt, über welche Transporte und IP-Adressen die Verwaltungsanforderungen entgegengenommen werden. Der Transport kann HTTP, HTTPS oder beides sein. Bei HTTP können Nachrichten mit NTLM- oder Kerberos-Verschlüsselung verschlüsselt werden. Bei HTTPS wird SSL (Secure Sockets Layer) für die Verschlüsselung eingesetzt. Sie können sich den konfigurierten Listener ansehen, indem Sie **winrm enumerate winrm/config/listener** eingeben. Wie das folgende Listing zeigt, gibt dieser Befehl die Konfigurationsdetails für die konfigurierten Listener aus.

```
Listener
    Address = *
    Transport = HTTP
    Port = 80
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.1.225
```

In der Standardeinstellung ist Ihr Computer wahrscheinlich so konfiguriert, dass er auf allen IP-Adressen antwortet. In diesem Fall ist die Ausgabe leer. Soll WinRM auf bestimmte IP-Adressen eingeschränkt werden, können die lokale Loopbackadresse des Computers (127.0.0.1) und die zugewiesenen IPv4- und IPv6-Adressen explizit als überwachte Adressen konfiguriert werden. Mit dem folgenden Befehl konfigurieren Sie einen Computer so, dass er Anforderungen auf allen konfigurierten IP-Adressen über HTTP entgegennimmt:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
```

Der nächste Befehl konfiguriert den Computer so, dass er Anforderungen über HTTPS auf allen IP-Adressen entgegennimmt:

```
winrm create winrm/config/listener?Address=*+Transport=HTTPS
```

Der Stern (*) steht in diesem Fall für alle konfigurierten IP-Adressen. Beachten Sie, dass die Eigenschaft *CertificateThumbprint* leer sein muss, wenn die SSL-Konfiguration mit einem anderen Dienst gemeinsam genutzt werden soll.

Sie aktivieren oder deaktivieren einen Listener für eine bestimmte IP-Adresse, indem Sie folgenden Befehl ausführen:

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=HTTP@{Enabled="true"}
```

oder

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=HTTP@{Enabled="false"}
```

Sie aktivieren oder deaktivieren die Standardauthentifizierung auf dem Client mit

```
winrm set winrm/config/client/auth @{Basic="true"}
```

oder

```
winrm set winrm/config/client/auth @{Basic="false"}
```

Die Windows-Authentifizierung mit NTLM oder Kerberos (abhängig von der Konfiguration) aktivieren oder deaktivieren Sie mit dem Befehl

```
winrm set winrm/config/client @{TrustedHosts="<local>"}
```

oder

```
winrm set winrm/config/client @{TrustedHosts=""}
```

Sie können WinRM nicht nur in der Befehlszeile verwalten, sondern auch mithilfe von Gruppenrichtlinien. Daher kann es sein, dass Gruppenrichtlinieneinstellungen die von Ihnen eingegebenen Einstellungen überschreiben.