edv-buchversand.de

Windows Server 2025

Das umfassende Handbuch

» Hier geht's direkt zum Buch

DIE LESEPROBE

Diese Leseprobe wird Ihnen von www.edv-buchversand.de zur Verfügung gestellt.

Kapitel 6
Active Directory

Das Active Directory (AD) ist der Anmelde- und Verzeichnisdienst von Microsoft und wird in den meisten größeren Firmen eingesetzt.

Wenn ein Unternehmen neue Mitarbeiter einstellt und diese sich an ihren Computern anmelden und auf Ressourcen zugreifen sollen, bedeutet das vorab viel Arbeit für das administrative Personal. Damit Sie nicht für Änderungen an jeden einzelnen Rechner laufen müssen, wird das *Active Directory (AD)* als Verzeichnisdienst genutzt. Mit diesem können Sie einen Benutzer schnell anlegen und ihm die notwendigen Ressourcen zuweisen, sodass ihm die Anmeldung an den Computern im Unternehmen ermöglicht wird. Außerdem lassen sich unternehmensweite Vorgaben schnell und strukturiert umsetzen. Beispielsweise können auf diesem Wege Kennwörter zurückgesetzt werden. Was das Active Directory genau ist und wie es funktioniert, erklären wir auf den folgenden Seiten. Wie es installiert wird, erläutern wir Ihnen ausführlich in Abschnitt 6.15.

Zunächst: Ein *Verzeichnis* ist eine Zusammenstellung von Informationen, ähnlich wie ein Telefonbuch. Das Active Directory stellt die Datenbank und die notwendigen Instrumente für die Verwaltung dieses Verzeichnisses zur Verfügung. Wie in jeder Datenbank hat jedes *Objekt* eine festgelegte Struktur, die *Attribute*. In einem Telefonbuch ist die Telefonnummer das Objekt (Klasse) und die Angaben wie Name, Vorname usw. sind die Attribute.

6.1 Die Geschichte von Active Directory

Der Verzeichnisdienst Active Directory wurde mit Windows Server 2000 eingeführt und bekam in den Nachfolgeversionen weitere Schlüsselfunktionen. Active Directory gehört damit zu den flexibelsten Verzeichnisstrukturen, die derzeit erhältlich sind. Durch die starke Integration von Anwendungen in das Verzeichnis können Unternehmen auch die schwierigsten Netzwerkumgebungen mithilfe von Active Directory verwalten. Ab der Version Windows Server 2008 wird der Dienst in fünf Rollen untergliedert. Im Kern stehen dabei die Active Directory-Domänendienste *(Active Directory Domain Services – AD DS)*.

Die Vorteile von Active Directory lassen sich leicht aufzählen:

- **Verwaltungsfähigkeit** – Das Active Directory basiert auf einem hierarchischen Verwaltungsmodell und kann durch die Administratoren flexibel angepasst werden.

- **Erweiterungsfähigkeit** – Das Schema, das die Struktur der Datenbank festlegt, kann individuell verändert und an die Anforderungen angepasst werden.
- **Skalierbarkeit** – Durch die Verwendung von AD-Standorten und die damit verbundene Verteilung der Domänencontroller auf die Standorte kann das AD beliebig angepasst werden. Auf diese Weise können Millionen Objekte verwaltet werden. Durch die Multimasterreplikation besteht ein hoher Schutz vor einem Ausfall, weil eine hohe Redundanz existiert.
- **zentrale Datenspeicherung** – Die Daten werden in einer Datenbank gespeichert und anschließend an andere Domänencontroller übertragen (repliziert). Dabei werden bandbreitenoptimierte Übertragungsmethoden verwendet.
- **flexible, sichere Authentifizierung und Autorisierung** – Im AD werden verschiedene Authentifizierungsmöglichkeiten unterstützt und domänenübergreifende Sicherheitsgruppen zur Verfügung gestellt.
- **Zusammenarbeit mit anderen Verzeichnisdiensten** – Das AD basiert auf Standardprotokollen wie DNS und LDAP und lässt sich somit mit vielen anderen Verzeichnisdiensten kombinieren.
- **Replikation von Informationen** – Das Active Directory repliziert die Informationen zwischen allen Domänencontrollern und schafft damit große Fehlertoleranz und hohe Verfügbarkeit. Durch diese Multimaster-Replikationstechnologie können Änderungen an unterschiedlichen Domänencontrollern durchgeführt werden, die dann an alle Domänencontroller repliziert werden. Selbst wenn ein Domänencontroller (DC) einmal ausfällt, erfolgt die Replikation, sobald der DC wieder verfügbar ist.

6.2 Was ist neu im Active Directory?

Da das Active Directory das Fundament der meisten Firmennetzwerke ist, wird mit Änderungen und neuen Features nur sehr vorsichtig umgegangen. Trotzdem bringt natürlich jede Version kleinere Änderungen mit sich. Wir gehen kurz auf die Neuerungen im Windows Server 2019 sowie im Windows Server 2025 ein, der sogar eine neue Funktionsebene mitbringt.

6.2.1 Neuerungen im Windows Server 2019

Auch wenn es auf den ersten Blick so aussieht, als wenn nichts angepasst worden wäre, so gibt es doch kleine Änderungen »unter der Haube«.

Sobald Sie den ersten Mitgliedsserver mit Windows Server 2019 zu einem Domänencontroller heraufstufen, wird das Schema auf die Version 88 hochgestuft. Durch das Schema-Update wird ein neues Attribut mit der Bezeichnung `msDS-preferredDataLocation` für die Klassen *Nutzer*, *Gruppen* und *Kontakte* eingefügt. Dieses Attribut kommt aus *Azure Entra ID* und wird von Office 365 für geografische Informationen genutzt.

Auch der *ESE Versions Store* (ESE: *Extensible Storage Engine*) wurde aktualisiert. In der Vergangenheit kam es wegen eines zu kleinen ESE-Versionsspeichers immer wieder zu Problemen im AD. Der neue Berechnungsalgorithmus wurde stark vereinfacht und an die 64-Bit-Technologie angepasst. Beim ersten Start von NTDS wird die Speichergröße der ESE-Version nun mit 10 % des physischen RAMs berechnet, wobei 400 MB das Minimum und 4 GB das Maximum sind. Mehr Informationen erhalten Sie unter folgendem Link:

https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/deep-dive-active-directory-ese-version-store-changes-in-server/ba-p/400510#:~:text=The%20algorithm%20is%20now%20greatly,physical%20machines%20and%20virtual%20machines.

Mit Windows Server 2019 wurde keine neue Funktionsebene im Active Directory eingeführt, wodurch es einfach gewesen ist, ältere Domänencontroller auf Windows Server 2019 heraufzustufen.

6.2.2 Die neue Funktionsebene in Windows Server 2025

In diesem Abschnitt beschreiben wir Ihnen die wichtigsten Neuerungen im Active Directory, wenn Sie Windows Server 2025 verwenden. Weitere Informationen finden Sie unter:

https://learn.microsoft.com/de-de/windows-server/get-started/whats-new-windows-server-2025

Folgende Neuerungen sind mit Windows Server 2025 im Active Directory implementiert worden:

- **Optionale Funktion »32-k-Datenbankseitengröße«**

  Mit Windows 2000 wurde die ESE-Datenbank *(Extensible Storage Engine)* eingeführt, die eine 8k-Datenbankseitengröße aufweist. Diese alte Architekturentscheidung hat zu Einschränkungen in AD geführt, die sich in der maximalen Skalierbarkeit von AD niederschlagen. Ein Beispiel für diese Einschränkung ist, dass ein AD-Objekt mit einem einzelnen Datensatz nicht größer als 8 Kilobyte sein darf. Die Umstellung auf ein 32k-Datenbankseitenformat bietet eine Verbesserung in Bereichen, wenn Sie von den alten Beschränkungen betroffen sind. So können mehrwertige Attribute jetzt bis zu ~3200 Werte enthalten, was einer Steigerung um den Faktor 2,6 entspricht.

  Neue Domänencontroller können mit einer 32k-Datenbankseite installiert werden, die 64-Bit-LIDs *(Long Value IDs)* verwenden und in einem 8k-Seitenmodus ausgeführt werden, um die Kompatibilität mit früheren Versionen zu gewährleisten. Ein aktualisierter Domänencontroller verwendet weiterhin sein aktuelles Datenbankformat und 8k-Seiten. Die Umstellung auf 32k-Datenbankseiten erfolgt für die Gesamtstruktur und setzt voraus, dass alle Domänencontroller in der Gesamtstruktur über eine 32k-Seiten-fähige Datenbank verfügen.

- **AD-Schema-Updates**

  Es werden drei neue LDFs *(Log Database Files)* eingeführt, die das AD-Schema erweitern: *sch89.ldf*, *sch90.ldf* und *sch91.ldf*. Die entsprechenden AD LDS-Schema-Updates befinden sich in der Datei *MS-ADAM-Upgrade3.ldf*.

- **Active Directory-Objektreparatur**

  In Active Directory ist es jetzt möglich, Objekte mit fehlenden Kernattributen `SamAccountType` und `ObjectCategory` zu reparieren. Das Attribut `LastLogonTimeStamp` kann für ein Objekt auf die aktuelle Uhrzeit zurückgesetzt werden. Die beiden genannten Vorgänge werden über ein neues `RootDSE`-Feature zur Vorgangsänderung vorgenommen, das als `fixupObjectState` bezeichnet wird.

- **Funktionsebene »Gesamtstruktur und Domäne«**

  Die neue Funktionsebene wird für den allgemeinen Support verwendet und ist für die neue Funktion der 32K Datenbankseitengröße erforderlich. Die neue Funktionsebene wird den Werten `DomainLevel 10` und `ForestLevel 10` für unbeaufsichtigte Installationen zugeordnet.

- **Verbesserte Sicherheit für Computerkonto-Standardkennwörter**

  Active Directory verwendet jetzt zufällig generierte Standardkennwörter für das Computerkonto. Windows Server 2025-Domänencontroller verhindern, dass für Computerkontokennwörter das Standardkennwort des Computerkontonamens verwendet werden kann.

- **Kerberos AES SHA256 und SHA384**

  Die Implementierung des Kerberos-Protokolls wurde aktualisiert, um stärkere Verschlüsselungs- und Signiermechanismen mit Unterstützung für RFC 8009 durch Hinzufügen von SHA-256 und SHA-384 zu unterstützen. Das veraltete RC4 wird außer Betrieb genommen und auf die Liste der Verschlüsselungsmethoden verschoben, die nicht mehr verwendet werden dürfen.

- **LDAP-Unterstützung für TLS 1.3**

  LDAP verwendet die neueste SCHANNEL-Implementierung und unterstützt TLS 1.3 für LDAP über TLS-Verbindungen. TLS 1.3 räumt mit veralteten Kryptografiealgorithmen auf, erhöht die Sicherheit gegenüber älteren Versionen und zielt darauf ab, einen möglichst großen Teil des Handshakes zu verschlüsseln.

Mit der neuen Funktionsebene in Windows Server 2025 wurden seit Langem mal wieder Anpassungen am Active Directory vorgenommen. Die Erweiterung der Datenbankseitengröße ist die wichtigste Änderung, von der Sie aber nur in sehr großen Umgebungen etwas spüren werden. Kleine Umgebungen werden von den Anpassungen nicht profitieren. Wenn Sie also nur eine Handvoll Server und eine überschaubare Anzahl User haben, werden Sie diese Änderungen nicht bemerken.

Mit Blick auf die IT-Sicherheit hat Microsoft das alte RC4-Protokoll entfernt und mit den zufälligen Computerkontokennwörtern die Sicherheit weiter erhöht.

Nachfolgend fassen wir kurz unsere Migrationsempfehlungen auf Windows Server 2025 zusammen:

- Wenn Sie in Ihrer Umgebung Windows Server 2016 einsetzen, dann empfehlen wir ein zeitnahes Upgrade auf Windows Server 2025, da der erweiterte Support von Windows Server 2016 bereits am 12.01.2027 ausläuft. Microsoft wird also nur noch bis dahin Sicherheitsupdates verteilen. Da wir alle wissen, dass eine Aktualisierung der AD-Umgebung einige Zeit in Anspruch nimmt, sollten Sie möglichst bald damit beginnen.
- Wenn Sie Windows Server 2019 einsetzen und Ihr AD keine sehr große Umgebung ist, dann können Sie sich mit dem Upgrade auf Windows Server 2025 noch etwas Zeit lassen. Zwar gibt es auch für Windows Server 2019 nur noch Sicherheitsupdates, diese stellt Microsoft aber noch bis zum 09.01.2029 bereit. Bis dahin müssen Sie die Migration aber auf jeden Fall planen und durchführen!
- Ist Ihre AD-Umgebung sehr groß, empfehlen wir ein zeitnahes Upgrade auf Windows Server 2025. Dadurch profitieren Sie nicht nur von der neuen Datenbankgröße, sondern Sie haben auch mehr Zeit für die Umstellung. Je früher Sie damit anfangen und eine Upgrade-Strategie entwickeln, desto besser.

Allerdings ist es (wie vor jedem größeren Upgrade) sehr wichtig, dass Sie Ihre gesamte Software auf die Kompatibilität mit Windows Server 2025 prüfen und die Systeme erst dann aktualisieren, wenn die Anwendungen durch den jeweiligen Hersteller für Windows Server 2025 freigegeben wurden. Falls Sie dies nicht beachten und es zu Problemen nach der Migration kommt, stehen Sie sehr wahrscheinlich ohne Support da.

6.3 Die Datenbank von Active Directory

Für die Speicherung der Informationen verwendet das Active Directory eine *Jet(Blue)-Datenbank*. Microsoft hat sich für diese Variante der Datenbank entschieden, weil sie keinen physischen Speicherplatz für leere Spalten verbraucht und relational sowie transaktionsorientiert arbeitet. Diese Datenbankvariante wird auch für Microsoft Exchange oder Access verwendet.

Die maximale Speichergröße beträgt 16 TB, und jeder Domänencontroller kann bis zu zwei Milliarden Objekte anlegen. Die Active Directory-Datenbank wird in der Datei *ntds.dit* im Verzeichnis *%Windir%\ntds* auf dem Domänencontroller gespeichert. Seit der Version Windows Server 2000 ist die Datenbank auf jedem Domänencontroller eine »Lese-/Schreibkopie« und wird innerhalb der Domäne repliziert, damit jeder Domänencontroller den gleichen Datenbankinhalt vorhält. Eine Besonderheit ist der Read-Only-Domänencontroller: Hier wird die Datenbank nur als Lesekopie gespeichert. Diese Domänencontrollervariante

wird verwendet, wenn der Domänencontroller an keinem sicheren Standort aufgebaut werden kann und Angriffen ausgesetzt sein könnte.

Die Datenbank wird in folgende Partitionen unterteilt (siehe auch Abbildung 6.1):

- In der *Konfigurationspartition* sind die Objekte enthalten, die die logische Struktur der Gesamtstruktur darstellen, einschließlich der Domänenstruktur und der Replikationstopologie. Gespeicherte Informationen sind die AD-Struktur inklusive der Domänen und Standorte sowie die Information, welche DCs existieren und welche Dienste verfügbar sind. Objekte dieser Partition müssen auf alle Domänencontroller der Gesamtstruktur repliziert werden. In der Konfigurationspartition werden zusätzlich die Informationen über die Exchange-, PKI- und DHCP-Server gespeichert.
- Die *Schemapartition* definiert die in der Gesamtstruktur erstellbaren Objekte (Klassen) sowie die Attribute, die diese Objekte haben können. Alle Objekte müssen sich an das vorgegebene Schema halten. Die Schemapartition muss auf alle Domänencontroller der Gesamtstruktur repliziert werden, und alle DCs verwenden dasselbe Schema, damit die Datenbankintegrität gewährleistet werden kann.
- Die *Domänenpartition* enthält alle in der Domäne gespeicherten Objekte und kann nur auf die Domänencontroller der Domäne repliziert werden. Alle Objekte in jeder Domänenpartition werden auch im globalen Katalog mit einer Teilmenge ihrer Attribute gespeichert.
- Die *Anwendungsverzeichnispartition* speichert Daten, die dynamisch und anwendungsspezifisch sind. Die Replikation wird von der Anwendung selbst gesteuert und verursacht keinen nennenswerten Netzwerkverkehr. Die Anwendungsverzeichnispartition kann beliebige Arten von Objekten enthalten. Ausgenommen hiervon sind Sicherheitsprinzipale wie Benutzer, Gruppen und Computer, die für die Vergabe von Zugriffberechtigungen verwendet werden können. Die Informationen der Anwendungsverzeichnispartition werden nicht im globalen Katalog gespeichert. Beispiele für Anwendungsverzeichnispartitionen sind die *ForestDNSZones* und die *DomainDNSZones*.

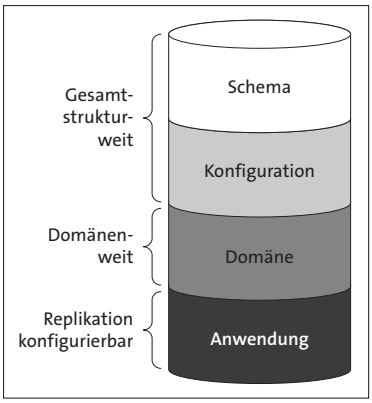

Abbildung 6.1 AD-Datenbank mit Replikationsbereichen

6.4 Die Komponenten von Active Directory

Im Active Directory stellen die *Organisationseinheiten (OUs)*, die Domänen oder die Gesamtstrukturen den logischen Aufbau einer Organisation dar. Die physische Struktur wird durch die Standorte, die Subnetze und die Domänencontroller abgebildet. Die logische und die physische Struktur werden im Active Directory vollständig voneinander getrennt.

6.4.1 Logischer Aufbau

Mithilfe der logischen Komponenten wird die logische Struktur des ADs aufgebaut (siehe Abbildung 6.2). Aufgrund der logischen Anordnung braucht der Nutzer sich keine Gedanken über den physischen Aufbau zu machen.

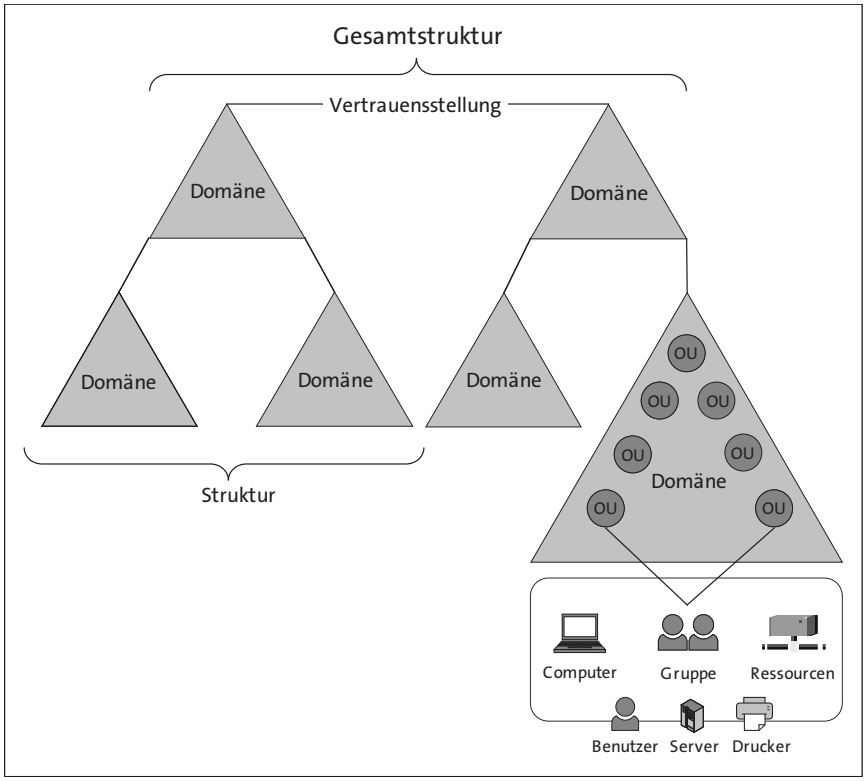

Abbildung 6.2 Darstellung einer logischen AD-Struktur

Struktur

Stellt eine Domäne eine untergeordnete Domäne einer anderen Domäne dar, so spricht man von einer *Struktur*. Wenn die Gesamtstruktur *intranet.rheinwerk-verlag.de* die beiden Domänen *europa.rheinwerk-verlag.de* und *asien.rheinwerk-verlag.de* umfasst (siehe Abbildung 6.3), so stellen diese Domänen einen zusammenhängenden Bereich im DNS-Namensraum und

damit einzelne Strukturen dar. Handelt es sich jedoch umgekehrt bei den beiden Domänen *intranet.rheinwerk-verlag.de* und *ichkanngarnix.de* nicht um einen zusammenhängenden Bereich im DNS-Namensraum (siehe Abbildung 6.4), so verfügt die Gesamtstruktur über zwei Strukturen.

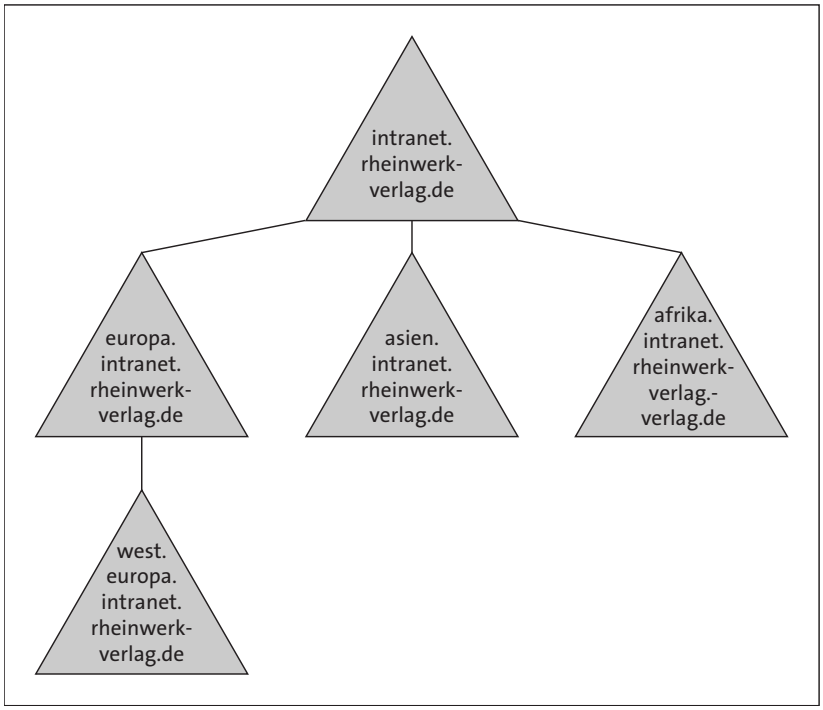

Abbildung 6.3 Darstellung einer Struktur

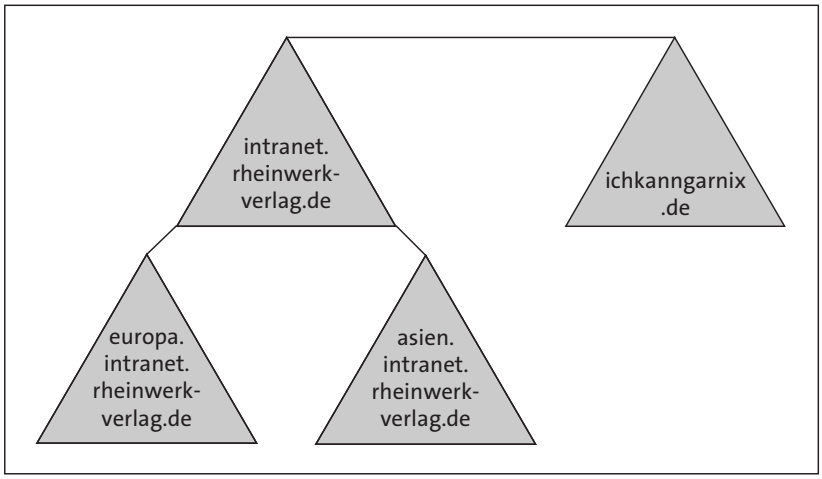

Abbildung 6.4 Darstellung einer Gesamtstruktur

Gesamtstruktur

Eine Gesamtstruktur ist eine Sammlung oder hierarchische Anordnung verschiedener Strukturen (AD-Domänen). Die erste in einer Gesamtstruktur installierte Domäne wird als *Gesamtstruktur* oder *Stammdomäne* bezeichnet und definiert den Pfad zur Schema- und Konfigurationspartition. Eine Gesamtstruktur ist eine einzelne Instanz des Verzeichnisses. Das heißt, Daten werden nicht außerhalb der Gesamtstrukturgrenzen repliziert. Die Gesamtstruktur stellt damit eine Sicherheitsgrenze dar.

Die Merkmale einer Gesamtstruktur sind:

- Die Strukturen in einer Gesamtstruktur haben entsprechend ihrer Domänen unterschiedliche Namensstrukturen.
- Alle Domänen arbeiten unabhängig, können jedoch über die Gesamtstruktur miteinander kommunizieren.
- Alle Domänen basieren auf dem gleichen gemeinsamen Schema.
- Für Microsoft ist eine Gesamtstruktur auch dann bereits gegeben, wenn nur eine Domäne vorhanden ist.
- Alle Domänen teilen sich die Informationen der Konfigurationspartition und sind damit gleich konfiguriert.

Domänen

Domänen sind im Active Directory die Grundlage der logischen Struktur und werden innerhalb einer Domäne in Organisationseinheiten unterteilt. Eine Domäne muss aus mindestens einem *Domänencontroller (DC)* bestehen, da die Domäne ohne ihn nicht arbeitsfähig ist. Aus Redundanzgründen sollten Sie in einem produktiven Umfeld mit mindestens zwei Mitgliedsservern *(Member Server)* als zukünftige DCs planen. Weitere Objekte einer Domäne sind z. B.:

- Mitgliedsserver (Member Server) – Das sind Server, die Dienste wie Exchange, SQL, Fileservices etc. bereitstellen und eben keine Domänencontroller sind.
- Computer
- Benutzer
- Benutzergruppen
- Organisationseinheiten

Organisationseinheiten (OU)

In einer OU *(Organizational Unit)* können sich z. B. Benutzer-, Computer- oder Gruppenobjekte befinden. Die OU stellt die kleinste administrative Einheit im AD dar. OUs werden z. B. genutzt, um Unternehmensstrukturen im AD abzubilden. Der Zugriff auf die OUs kann über ACLs (*Access Control Lists*, Zugriffskontrolllisten) gesteuert werden. OUs werden außerdem

für die Verknüpfung von Gruppenrichtlinien verwendet. Eine OU-Struktur sehen Sie in Abbildung 6.5.

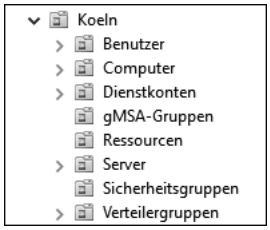

Abbildung 6.5 Darstellung einer OU-Struktur im Active Directory

6.4.2 Physischer Aufbau

Den physischen Aufbau des Active Directorys stellen die Domänencontroller und Standorte dar. Die Infrastruktur Ihres Unternehmens wird so im Active Directory abgebildet.

6.4.3 Globaler Katalog

Das AD erlaubt es Benutzern und Administratoren, Objekte innerhalb einer Domäne zu finden. Sollen Objekte außerhalb der eigenen Domäne, aber innerhalb der Gesamtstruktur ermittelt werden, ist eine andere Methode notwendig. Der *globale Katalog* ist der zentrale Speicher der Objektinformationen innerhalb einer Struktur oder Gesamtstruktur und wird standardmäßig auf dem ersten DC in der ersten Domäne der Gesamtstruktur erstellt. Jeder DC, der eine Kopie des globalen Katalogs speichert, wird *globaler Katalogserver* genannt. Der globale Katalog wird innerhalb der AD-Replikation mit repliziert.

Der globale Katalog speichert eine vollständige Sammlung aller Objektattribute seiner Hostdomäne und eine Teilmenge aller Objektattribute der in der Gesamtstruktur vorhandenen Domänen. Welche Objektattribute in den globalen Katalog aufgenommen werden, ist im *Schema* hinterlegt. Der globale Katalog ermöglicht damit die Benutzeranmeldung im Netzwerk und das Auffinden von Informationen im Verzeichnis, unabhängig davon, welche Domäne in der Gesamtstruktur die Daten tatsächlich enthält. Er kann Gruppenmitgliedschaften auf dem lokalen DC prüfen bzw. beantworten.

Somit muss die Anmeldung nicht immer über langsame WAN-Strecken erfolgen und der Netzwerkverkehr kann minimiert werden. Aus diesem Grund sollte auf jedem DC an einem AD-Standort eine Kopie des globalen Katalogs bereitgestellt werden.

Um einen DC nachträglich zum globalen Katalogserver zu machen, öffnen Sie die Eigenschaften des DCs in der Konsole *Active Directory-Standorte und -Dienste* und aktivieren die Option Globaler Katalog auf dem Reiter Allgemein der NTDS Settings (siehe Abbildung 6.6).

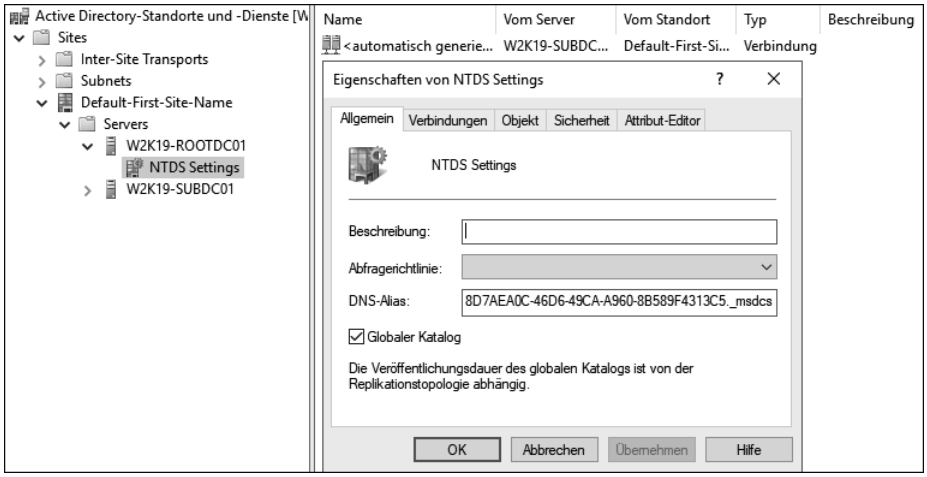

Abbildung 6.6 Die »NTDS Settings« des »W2k19-RootDC01« mit aktiviertem globalen Katalog

6.4.4 FSMO (Flexible Single Master Operations) bzw. Betriebsmaster

Das Active Directory wurde als Multimaster-Replikationssystem entwickelt. Dies bedeutet, dass alle Domänencontroller – mit Ausnahme der RODCs – Schreibzugriff auf die Active Directory-Datenbank haben müssen. Dieses System funktioniert problemlos für die meisten Aufgaben, aber für bestimmte Operationen gibt es genau einen Server, der diese Aufgabe durchführen darf. Der Domänencontroller, der diese spezifische Aufgabe durchführen kann, wird als *Betriebsmaster* oder *Operationsmaster* bezeichnet und besitzt eine der unten genannten Betriebsmaster-Rollen *(Flexible Single Master Operations (FSMO) Roles)*. Der Domänencontroller, der die Betriebsmasterrolle hat, darf diese speziellen Aufgaben durchführen, stellt die Konsistenz der Datenbank sicher und löst eventuelle Replikationskonflikte für seinen speziellen Bereich.

Infrastruktur-Master

Der Infrastruktur-Master ist dafür verantwortlich, die Berechtigungen von Benutzern aus unterschiedlichen Domänen zu steuern. Wenn das jeweilige Unternehmen Exchange einsetzt, wird die Rolle außerdem für die Auflösung von Verteilergruppen verwendet, da auch hier eine Gruppe Mitglieder aus unterschiedlichen Domänen haben kann. Pro Domäne kann es nur einen Infrastruktur-Master geben. Der globale Katalog kann auf dem DC, der die FSMO-Rolle *Infrastruktur-Master* hält, nur dann installiert werden, wenn auf jedem DC der globale Katalog installiert ist. Falls dem nicht so ist, darf auf dem DC mit der FSMO-Rolle *Infrastruktur-Master* der globale Katalog nicht vorhanden sein. Sobald das AD-Feature *AD-Papierkorb* aktiviert wurde, verhält sich jeder DC so, als wäre er der Infrastruktur-Master.

RID-Master

Der RID-Master verwaltet die *relativen IDs (RIDs)* und ist für die Zuweisung von RID-Pools an die Domänencontroller einer Domäne zuständig. Jeder Pool hat standardmäßig 500 IDs, und jeder Server fragt, wenn die Hälfte der IDs verbraucht ist, neue IDs beim RID-Master an. Den RID-Master kann es auch nur einmal pro Domäne geben. Funktioniert der RID-Master mal nicht und sind die IDs aufgebraucht, können keine Objekte (die eine relative ID besitzen, also z. B. Benutzer) mehr im AD angelegt werden. Mit dem Befehl `DCDIAG /test:ridmanager /v` können Sie sich die aktuellen Informationen Ihres RID-Masters in Ihrer Domäne anzeigen lassen. Hier sehen Sie einen Auszug der Ausgabe aus unserer Domäne:

```
Starting test: RidManager
  * Available RID Pool for the Domain is 2100 to 1073741823
  * PBON10SDCV00001.intranet.rheinwerk-verlag.de is the RID Master
  * DsBind with RID Master was successful
  * rIDAllocationPool is 1100 to 1599
  * rIDPreviousAllocationPool is 1100 to 1599
  * rIDNextRID: 1168
  ..................... PBON10SDCV00001 hat den Test RidManager bestanden.
```

Dem DC wurde der RID-Pool `1100` bis `1599` zugewiesen, und die nächste RID, die der DC verwenden würde, ist die `1169`.

Domain-Naming-Master

Der *Domain-Naming-Master* ist für die Namensgebung und das Hinzufügen und Entfernen von Domänen innerhalb der Gesamtstruktur verantwortlich. Den Domain-Naming-Master gibt es nur einmal pro Gesamtstruktur.

Schema-Master

Der *Schema-Master* steuert alle Veränderungen am Schema. Das Schema beschreibt alle Klassen und ihre Attribute. Den Schema-Master kann es nur einmal pro Gesamtstruktur geben. Um Änderungen durchzuführen, muss die administrative Kennung Mitglied der Gruppe *Schema-Administratoren* sein.

PDC-Emulator

Der *PDC-Emulator* ist das Benutzerkonto der primären Anmeldeserver für alle Prä-Windows-2000-Clients und dient für eventuell noch vorhandene Backup-Domain-Controller als primärer DC.

Der PDC verwaltet alle Kennwortänderungen, denn jeder DC meldet bei einer Kennwortänderung das Kennwort an den PDC. Kommt es zu einem Kennwortkonflikt innerhalb oder außerhalb der Domäne, wird der PDC befragt: Seine Antwort zählt. Der PDC-Emulator ver-

waltet zudem die GPOs, und jede Gruppenrichtlinienverwaltungskonsole verbindet sich standardmäßig mit dem PDC. Der PDC dient weiterhin als Zeitquelle für alle DCs innerhalb der Domäne. Und schließlich verwaltet der PDC die Kennwörter für die Vertrauensstellungen und übernimmt die Konsistenzprüfung für DFS. Den PDC-Emulator gibt es nur einmal je Domäne.

6.4.5 Standorte

Ein *AD-Standort* ist ein Subnetz oder eine Sammlung von Subnetzen. Ein AD-Standort stellt eine Standortgrenze dar und beinhaltet alle DCs an dem jeweiligen Standort. Im AD ist ein Standort kein Teil des Namensraums und bleibt deswegen für den Nutzer transparent. Ein AD-Standort beinhaltet nur Computer- und Verbindungsobjekte, die zur Konfiguration der Replikation zwischen den Standorten verwendet werden. Standardmäßig replizieren alle DCs an einem Standort direkt miteinander; das heißt, alle Änderungen werden sofort übertragen.

6.4.6 Distinguished Name

Der *Distinguished Name (DN)* ist der eindeutige Name des AD-Objekts. Zum Distinguished Name könnte man auch »LDAP-Pfad« sagen, aber eigentlich ist nur *DN* oder eben *Dinstinguished Name* gebräuchlich. Dieser Name identifiziert das AD-Objekt von der untersten Ebene, dem Objekt selbst, durch alle OUs/Container bis zur obersten Ebene, der Domäne. Der Wert kann aus dem gleichnamigen Attribut innerhalb des AD-Objekts ausgelesen werden. Die einzelnen Werte sind durch Kommas voneinander getrennt.

Eine administrative Kennung sieht so aus: `P1Karsten.Weigel`. Der vollständige Eintrag ist also:

```
CN=P1Karsten.Weigel,OU=Tier1,OU=Administration,DC=intranet,DC=rheinwerk-verlag,DC=de
```

6.4.7 Canonical Name

Der *Canonical Name* ist das Gleiche wie der Distinguished Name, jedoch wird das DNS-Domänennamenformat verwendet. Der DNS-Namensraum wird durch Punkte getrennt und die OUs bis zum Objekt selbst mit Slashes.

Die bereits bekannte administrativen Kennung sieht in dieser Schreibweise so aus:
`P1Karsten.Weigel`

```
intranet.rheinwerk-verlag.de/Administration/Tier1/P1Karsten.Weigel
```

6.4.8 Common Name

Der *Common Name (CN)* ist der allgemeine Name des AD-Objekts. Der Distinguished Name beginnt immer mit dem CN des AD-Objekts.

6.5 LDAP

Das *Lightweight Directory Access Protocol (LDAP)* ist ein Netzwerkprotokoll, das in den *RFCs 4510, 4511* und *4532* definiert wurde. LDAP ist kein Verzeichnis, sondern das Protokoll, das für Abfragen und Änderungen in einem verteilten Verzeichnisdienst genutzt wird.

Alle am Netzwerk angeschlossenen Systeme müssen für eine ungesicherte Übertragung den Port 389 nutzen und für eine mit TLS gesicherte Verbindung den Port 636. Diese Ports sind in den Firewalls des Netzwerks für den Datenaustausch zwischen den Systemen freizuschalten.

Die Entwicklung des LDAP begann in der Universität in Michigan, wo im Jahre 1993 ein RFC für eine vereinfachte Variante des *Directory Access Protocol (DAP)* verfasst wurde. Der Vorschlag beinhaltete ein Verzeichnis, das über unterschiedliche Server verteilt sein sollte und in dem innerhalb der Baumstruktur Abfragen möglich sein sollten.

LDAP folgt dem Ansatz der projektorientierten Programmierung, besteht also aus Klassen, Objekten und Attributen. Die Objekte im LDAP haben verschiedene Attribute, und in derselben Ebene kann es kein gleiches Objekt mit demselben Namen geben. Der *Distinguished Name* ist das *Pflichtattribut* jedes Objekts. Über ihn wird geprüft, ob das Objekt bereits im AD vorhanden ist. Durch die Verwendung von Organisationseinheiten besteht die Möglichkeit, das LDAP zu strukturieren.

Im *RFC 2253 UTF-8 String Representation of Distinguished Names* sind unter anderem folgende Attributtypen definiert:

- `CN: commonName`
- `O: organizationName`
- `OU: organizationalUnitName`
- `C: countryName`
- `STREET: streetAddress`
- `DC: domainComponent`
- `UID: userid`

Dies wirkt durch die vielen möglichen Attribute der unterschiedlichen Objekte erst mal sehr komplex, stellt sich später aber viel einfacher und übersichtlicher in einer Struktur dar.

Wenn Sie die Objekte und Attribute innerhalb eines Active Directorys betrachten und damit arbeiten, werden Sie die Zusammenhänge schnell verstehen.

6.6 Schema

Das *Schema* ist die Schablone für alle Active Directory-Einträge. Es definiert die Objekttypen, ihre Klassen, Attribute und ihre Syntax. Welche Objekttypen in Active Directory verfügbar sind, wird durch die Definition neuer Typen beeinflusst. Das Muster, das Sie dafür einhalten

müssen, ist eben das *Schema*, das die Objekte mit deren Attributen definiert. Nur Mitglieder der Gruppe der Schema-Administratoren können das Schema anpassen.

Damit Sie das Schema über die GUI anpassen können, müssen Sie die dafür notwendige Bibliothek *schmmgmt.dll* registrieren. Dies können Sie in einer administrativen Kommandozeile mit folgendem Befehl tun:

```
regsvr32.exe schmmgmt.dll
```

Danach fügen Sie einer leeren Verwaltungskonsole das Snap-In *Active Directory-Schema* hinzu. In ihr sind dann alle Klassen und deren Attribute sichtbar und können angepasst werden. Sie sollten aber immer nur dann Änderungen am Schema durchführen, wenn es zwingend notwendig ist! Notwendige Anpassungen, die von Anwendungen im AD benötigt werden, werden während der Installation der Anwendung automatisch vorgenommen.

6.7 Replikation

Die Replikation von Änderungen im Active Directory ist dann notwendig, wenn mehrere Domänencontroller in der Domäne betrieben werden. Jeder Domänencontroller repliziert bzw. synchronisiert den Inhalt seiner Active Directory-Datenbank mit den anderen Domänencontrollern in der Domänengesamtstruktur. Je größer die Umgebung ist, desto wichtiger ist die Replikation zwischen den DCs.

Die Active Directory-Datenbank ist in mehrere Verzeichnispartitionen eingeteilt, von denen jede für sich eine eigene Replikationsmethode besitzt:

- Die *Schemapartition* ist eine sogenannte *Organisationspartition* und wird innerhalb der Gesamtstruktur auf alle Domänencontroller repliziert.
- Die *Konfigurationspartition* wird ebenfalls als Organisationspartition auf alle Domänencontroller in der Gesamtstruktur repliziert.
- Die *Domänenpartition* wird nur auf die Domänencontroller der entsprechenden Domäne repliziert.

Während der Replikation werden immer nur die Deltas und nicht der komplette Dateninhalt übertragen.

6.7.1 Steuerung der AD-Replikation

Die AD-Replikation kann über die Konsole *Active Directory Standorte und -Dienste* ermittelt und verändert werden.

Die automatische Ermittlung der Replikationspartner am Standort und darüber hinaus übernimmt der Dienst *Knowledge Consistency Checker (KCC)*. Eine mögliche Replikation kann so wie in Abbildung 6.7 aussehen:

Kapitel 9
Dateiserver

In diesem Kapitel befassen wir uns mit dem Dateiserver. Wir vermitteln Ihnen einen Überblick über die möglichen Datenträger- und Dateiserver-Funktionen von Windows Server 2025.

Bei Dateiservern müssen Sie die Konfiguration gut planen, denn ein Dateiserver muss vielfältige Anforderungen bedienen. Diese reichen von der grundlegenden Bereitstellung von Funktionen für den Betrieb des Betriebssystems (weshalb ein Teil der *Dateiserver*-Rolle automatisch mit der Betriebssysteminstallation zur Verfügung steht) über die Dateiserver-Bereitstellung als zentrale Ablage von Dateien bis hin zur Bereitstellung von Speicher für Workloads, z. B. als zentraler *SMB*-Storage für *Hyper-V*.

9.1 Grundlagen des Dateisystems

Damit Sie verstehen, wie der Dateiserver angewendet werden kann, geben wir Ihnen hier zunächst einen Überblick über einige der grundlegenden Funktionen und Konfigurationsmöglichkeiten, um einen Dateiserver bereitzustellen.

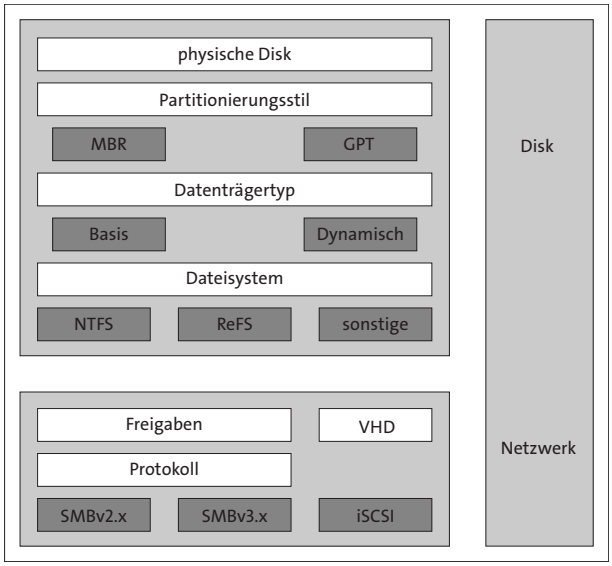

Abbildung 9.1 Dateisystem-Schichten

Der Dateiserver ist in Schichten aufgebaut. Auf der untersten Schicht befindet sich der physische (oder auch virtuelle) Datenträger. Auf der obersten Schicht liegen die letztendlich genutzten Protokolle. Den Aufbau dieser Schichten zeigt Abbildung 9.1.

Windows Storage Server

Der *Windows Storage Server* wurde von Microsoft mit der Windows Server-Version 2016 abgekündigt und erscheint seit Windows Server 2019 nicht mehr.

9.1.1 Datenträger und Volumes

Partitionierungsstil

Bei der Initialisierung neuer Datenträger müssen Sie sich für einen Partitionierungsstil des neu erkannten Datenträgers entscheiden. Hierbei haben Sie die Wahl zwischen MBR (Master Boot Record) und GPT (GUID-Partitionstabelle) (siehe Abbildung 9.2).

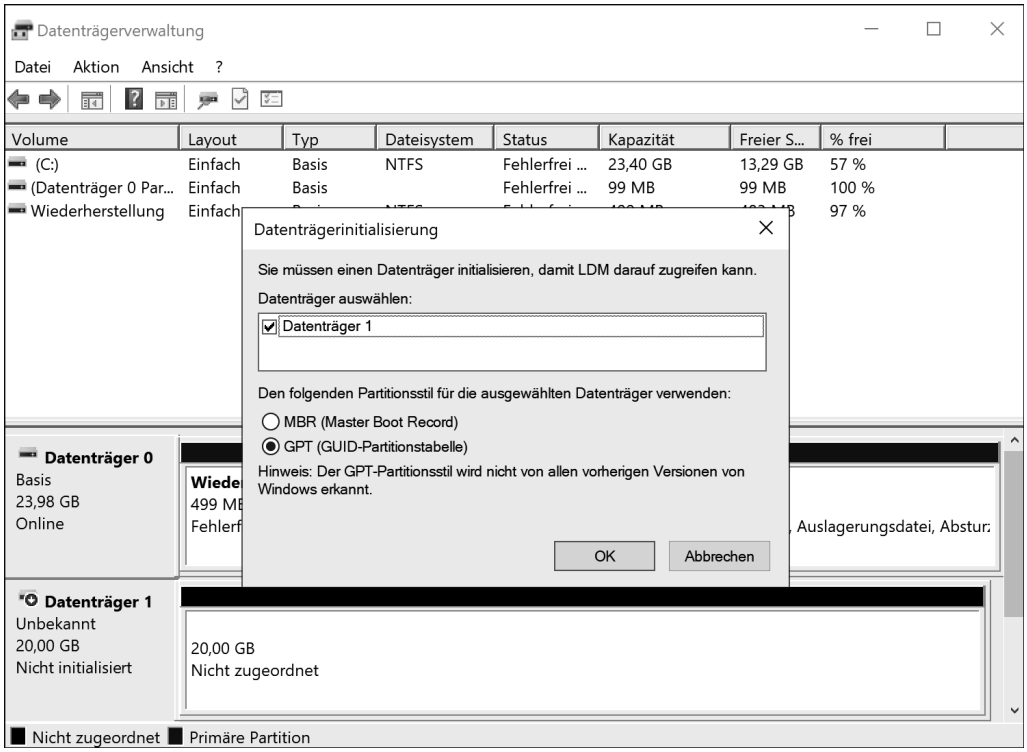

Abbildung 9.2 Auswahl des Partitionierungsstils

Der Partitionsstil übt maßgeblich Einfluss auf die Erstellung von Volumes aus. So stehen im Partitionsstil MBR lediglich vier Volumes mit insgesamt maximal 2 TB Speicherkapazität auf

dem gesamten Datenträger zur Verfügung, während durch GPT insgesamt bis zu 128 Volumes mit in Summe 18 EB (Exabyte) zur Verfügung stehen. Die wichtigsten Unterschiede listet Tabelle 9.1 auf.

	GPT	MBR
Volumes	128	4
Max. Partitionsgröße	18 EB	2 TB
Max. Harddisk-Größe	18 EB	2 TB
Datensicherheit	Sektoren für Prüfsummen und Backup	Ein Datensektor ohne Prüfsumme
Bezeichnung der Partitionen	GUID *(Global Unique ID)* mit 36 Zeichen Länge sowie Partitionsname	Gespeichert in der Partition

Tabelle 9.1 Auflistung der Partitionsschemas und ihrer Rahmendaten

Zusammenfassend kann festgehalten werden, dass es sich beim MBR um den älteren und nicht mehr zeitgemäßen Partitionierungsstil handelt. Daher empfehlen wir den Einsatz von GPT gerade in Hinblick auf die wachsenden Datenträgergrößen sowie auf die immense Datenflut.

Achten Sie jedoch darauf, dass das Boot-Volume in GPT nicht von älteren Systemen genutzt werden kann, die noch auf der 32-Bit-Architektur und einem Legacy-BIOS beruhen.

Bei bestehenden Datenträgern können Sie den zum Einsatz kommenden Partitionsstil in den Eigenschaften des Datenträgers einsehen. Gehen Sie hierzu wie folgt vor:

Drücken Sie die Tastenkombination [⊞]+[X], und wählen Sie die DATENTRÄGERVERWALTUNG aus. Alternativ können Sie auch mit [⊞]+[R] die Eingabeaufforderung öffnen und dort `diskmgmt.msc` eingeben.

In der DATENTRÄGERVERWALTUNG wählen Sie nun den Datenträger aus, dessen Partitionierungsstil Sie überprüfen wollen. Öffnen Sie hierfür mit einem Rechtsklick auf den Datenträger das Kontextmenü, und wählen Sie unter EIGENSCHAFTEN den Reiter VOLUMES (siehe Abbildung 9.3). Dort finden Sie die Zusammenfassung der Datenträgerinformationen. Unter dem Punkt PARTITIONSSTIL sehen Sie, welche Konfiguration auf dem Datenträger verwendet wird.

Auch die Konvertierung des verwendeten Partitionierungsstils von MBR in GPT (und umgekehrt) ist über die Datenträgerverwaltung möglich (siehe Abbildung 9.4). Beachten Sie jedoch, dass eine Konvertierung erst durchgeführt werden kann, nachdem Sie sämtliche Volumes des betroffenen Datenträgers entfernt haben. Sie sollten daher zunächst eine vollständige Sicherung durchführen, um die Inhalte der Volumes anschließend wiederherstellen zu können.

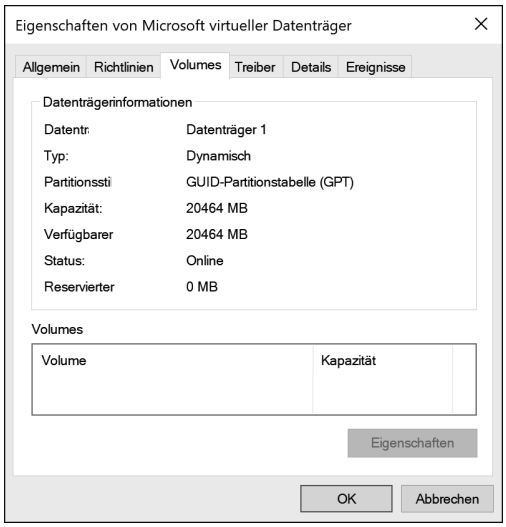

Abbildung 9.3 Volume-Eigenschaften von Datenträgern

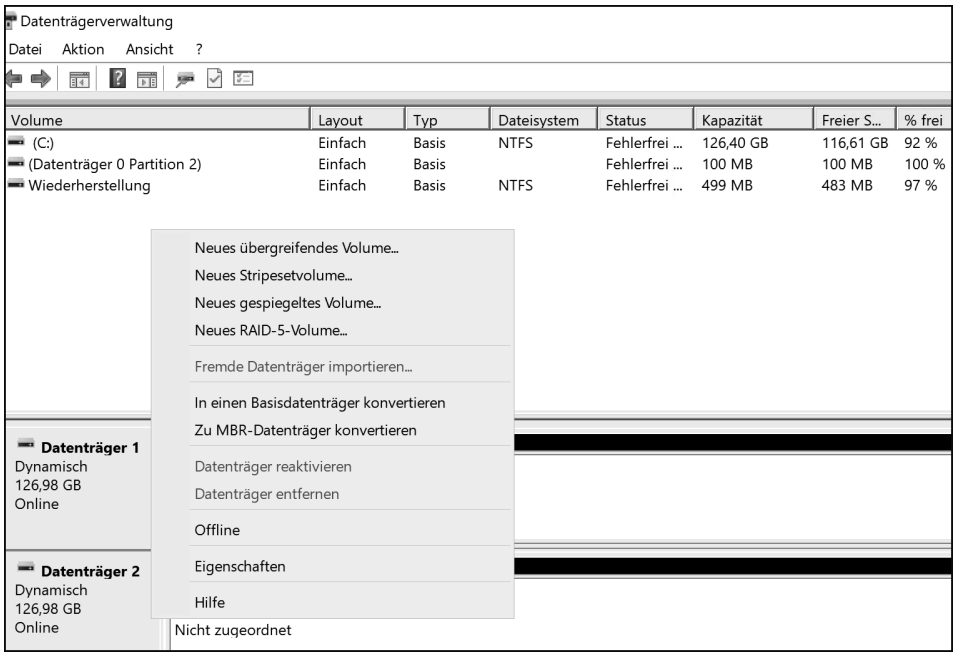

Abbildung 9.4 Konvertierung des Partitionierungsstils per »Datenträgerverwaltung«

Volume

Bei einem *Volume* handelt es sich um einen Speicherbereich, der auf einem Datenträger bereitgestellt wird und der mit einem Dateisystem formatiert ist. Hierbei kommen im Micro-

soft-Betriebssystem die *Dateisystemformate* FAT, FAT32, NTFS und ReFS zum Einsatz. Um die bereitgestellten Volumes (mit dem jeweils formatierten Dateisystem) verwenden zu können, wird diesen ein Laufwerksbuchstabe zugewiesen, der dann über das Betriebssystem referenziert werden kann. Alternativ besteht auch die Möglichkeit, das erstellte Volume per *Mountpoint* in eine bestehende Dateisystemstruktur einzubinden. Je nach verwendetem Partitionierungsstil können unterschiedlich viele und unterschiedlich große Volumes pro Datenträger angelegt werden.

Dynamische und nichtdynamische Datenträger

Der maßgebliche Unterschied zwischen dem *Basisdatenträger* (nichtdynamischer Datenträger) und dem *dynamischen Datenträger* besteht in den zusätzlichen Funktionen, die bei dynamischen Datenträgern zur Verfügung stehen. Diese ermöglichen es, die Volumes, die auf den logischen Laufwerken erzeugt werden, auf mehrere unterschiedliche dynamische Datenträger zu verteilen und dort zu spiegeln. Hierdurch erhöht sich die Ausfallsicherheit, jedoch benötigen Sie entsprechend zusätzliche physische Datenträger.

Standardmäßig werden neue Datenträger nach der Installation und Auswahl des Partitionierungsstils als Basisdatenträger angelegt. Diese können jedoch über die Datenträgerverwaltung in dynamische Datenträger konvertiert werden (siehe Abbildung 9.5).

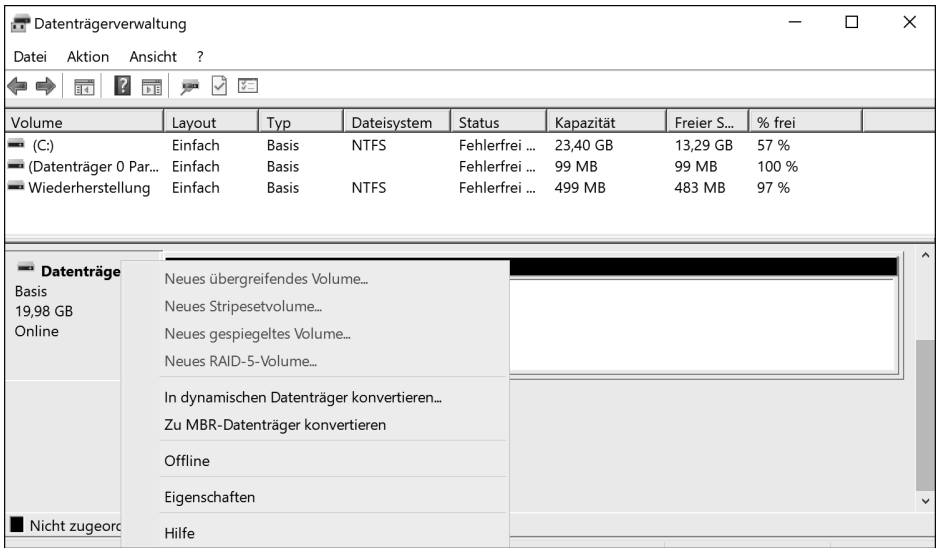

Abbildung 9.5 Einen Datenträger in einen dynamischen Datenträger konvertieren

Dynamische Datenträger können natürlich auch wieder in Basisdatenträger zurückkonvertiert werden (siehe Abbildung 9.6). Der entsprechende Menüpunkt erscheint im Kontextmenü des dynamischen Datenträgers.

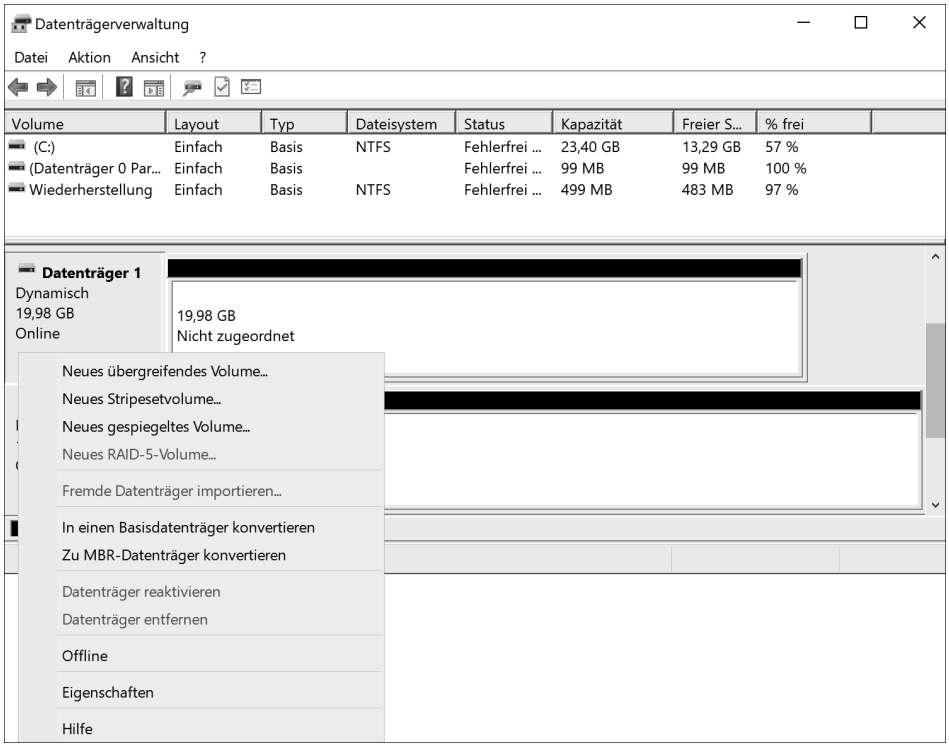

Abbildung 9.6 Erstellen von Volumes auf dynamischen Datenträgern

Beachten Sie hierbei, dass die Konvertierung in einen dynamischen Datenträger unterbrechungsfrei und ohne Datenverlust möglich ist. Allerdings müssen bei der Konvertierung eines dynamischen Datenträgers in einen Basisdatenträger die vorhandenen Volumes gelöscht werden. Sichern Sie daher wichtige Daten vorab.

Dateisystem

Wie bereits erwähnt, stehen Ihnen mehrere Dateisysteme zur Auswahl. Im Folgenden betrachten wir NTFS und ReFS genauer.

NTFS

Bei dem Dateisystem *NTFS* handelt es sich um das Standarddateisystem aller aktuellen Windows-Client- und -Serverbetriebssysteme. Das NTFS-Dateisystem wurde in den 80er-Jahren von Microsoft und IBM entwickelt und kontinuierlich erweitert, um immer neueren Anforderungen gerecht zu werden. So wurde es um die Dateisystemsicherheit (ACLs), Verschlüsselungen, Datenträgerkontingente, Selbstheilung, Transaction NTFS, Deduplizierung sowie Clusterfunktionalität und -kompatibilität erweitert. Als eine der wichtigsten Erweite-

rungen wurden auch die Grenzwerte für den maximalen Support von Volume-Größen auf nun 256 TB pro Volume erhöht, um den immer höheren Anforderungen an das Dateisystem gerecht werden zu können.

Blockgröße	Max. Volume-Größe	Max. Dateigröße
4 KB (Standardgröße)	16 TB	16 TB
8 KB	32 TB	32 TB
16 KB	64 TB	64 TB
32 KB	128 TB	128 TB
64 KB (max. unterstützt)	256 TB	256 TB

Tabelle 9.2 NTFS-Volume-Größenbegrenzungen basierend auf der Blockgröße

Achten Sie bei der Verwendung von nicht standardgemäßen Blockgrößen größer 4 KB darauf, dass Ihre Workloads, die den Datenträger oder Dateifreigaben für die Speicherung von Daten verwenden, damit kompatibel sind. Abweichende Blockgrößen können zu technischen Inkompatibilitäten oder Einschränkungen des jeweiligen Hersteller-Supports führen. Auch können bei falsch gewählten Blockgrößen Leistungseinschränkungen auftreten.

ReFS

Das Dateisystem ReFS *(Resilient File System*) wurde erstmals mit Windows Server 2012 als Alternative zum bestehenden und ein wenig in die Jahre gekommenen NTFS-Dateisystem bereitgestellt. ReFS war dabei, wie der Name bereits vermuten lässt, als widerstandsfähiges und leistungsfähiges Dateisystem für anspruchsvolle Workloads gedacht, z. B. für technische Lösungen wie *Storage Spaces Direct* oder *Hyper-V*. Jedoch gestaltete sich der Start des neuen Dateisystems mit Windows Server 2012 aufgrund fehlenden Supports für die verschiedenen Lösungen noch recht schwierig. Bis zur Einführung von Windows Server 2016 und der Aktualisierung des Dateisystems auf die Version 3.1 war es kaum von Belang.

Ein großer Vorteil von ReFS ist, dass es sich für das Bereitstellen besonders großer Volumes eignet. So können mittels ReFS Volumes in einem Umfang von bis zu 35 PB (Petabyte) angelegt werden. Dies entspricht einem Volumen von 35.000 TB und stellt somit gegenüber dem NTFS-Dateisystem mit dessen lediglich 256 TB je Volume einen erheblichen Puffer angesichts des bestehenden Datenwachstums dar.

Darüber hinaus ist das ReFS extrem robust gegenüber Fehlern und verfügt über Funktionen, die Probleme im Dateisystem wieder korrigieren können. Hierbei kommen Funktionen wie das optionale *Integrity Stream* zum Einsatz, was auf Basis einer Prüfsummenermittlung während der Datenspeicherung vor Fehlern schützt. Bitte beachten Sie, dass diese Funktion standardmäßig nicht aktiv ist, sondern manuell aktiviert werden muss.

Bei der Verwendung von Storage Spaces werden durch Spiegelungen sowie durch das Verwenden von *Parity Volumes* Fehler automatisch durch das Dateisystem korrigiert, ohne dass es notwendig ist, einzelne Volumes offline zu nehmen. Somit ist eine unterbrechungsfreie Datenbereitstellung für die verbundenen Services sichergestellt.

Durch die automatische und proaktive Fehlerkorrektur, die in regelmäßigen Abständen ausgeführt wird, werden die Volumes auf mögliche Fehler hin überprüft und gegebenenfalls durch die verfügbaren Schutzmaßnahmen korrigiert.

Auch unter Windows Server 2025 gilt weiter, dass die Verwendung von ReFS immer vom jeweiligen Einsatzzweck abhängig ist. So wird bei Hyper-V-Clustern mit SAN-Storage noch immer auf das NTFS-Dateisystem gesetzt, wobei die Einführung des Supports für die Deduplizierung von Hyper-V-Speicher das ReFS-Dateisystem attraktiver macht. Bei *SDS*-Lösungen *(Software-defined Storage)* mit lokalen nicht geteilten Storage-Kapazitäten führt zum Beispiel heute fast kein Weg mehr an ReFS vorbei.

Im Prinzip gilt aber weiterhin für den Einsatz des ReFS-Dateisystems die gleiche Empfehlung wie für alle Microsoft-Produkte: »It depends«. Sie müssen auf Basis der zur Verfügung stehenden Funktionen des ReFS-Dateisystems sowie auf Basis der zu betreibenden Workloads und deren Support-Empfehlungen entscheiden, ob der Einsatz von ReFS ratsam ist. Oder ist doch das bisher verwendete NTFS-Dateisystem die bessere Lösung? Vielleicht hilft Ihnen Tabelle 9.3 bei der Entscheidung.

Funktion	ReFS	NTFS
BitLocker-Verschlüsselung	✓	✓
Cluster-Shared-Volume-(CSV-)Support	✓	✓
Soft-Links	✓	✓
Failover-Cluster-Support	✓	✓
Access Control Lists (ACL)	✓	✓
USN-Journal	✓	✓
Change Notifications	✓	✓
Junction Points	✓	✓
Mount Points	✓	✓
Reparse Points	✓	✓
Volume Snapshots	✓	✓

Tabelle 9.3 Vergleich der Dateisysteme NTFS und ReFS auf Basis der verfügbaren Funktionen

Funktion	ReFS	NTFS
File-IDs	✓	✓
Oplocks	✓	✓
Sparse Files	✓	✓
Named Streams	✓	✓
Block Clone	✓	–
Sparse VDL	✓	–
Real-time-Tier-Optimierung*	✓	–
Dateisystemkomprimierung	✓	✓
Dateisystemverschlüsselung (transparente Verschlüsselung)	–	✓
Datendeduplizierung	✓	✓
Transaktionen	–	✓
Hard-Links	–	✓
Object-IDs	–	✓
Short Names	–	✓
Extended Attributes	–	✓
Disk-Quotas	–	✓
Bootable**	✓	✓
Support für Removable Media	–	✓
NTFS-Storage-Tiers	–	✓
* verfügbar unter Storage Spaces Direct ** verfügbar in Azure, Azure Stack sowie Azure Stack HCI		

Tabelle 9.3 Vergleich der Dateisysteme NTFS und ReFS auf Basis der verfügbaren Funktionen (Forts.)

9.1.2 iSCSI

iSCSI (*Internet Small Computer System Interface)* ist eine netzwerkbasierende Storage-Lösung, bei der das SCSI-Protokoll auf ein Netzwerkprotokoll übertragen wird. In vielen konvergenten Lösungen stellt iSCSI eine sehr verbreitete Lösung dar und ist somit zusammen mit dem

klassischen SAN-Fibre-Channel eine der am häufigsten implementierten Lösungen. Im Microsoft-Umfeld ist die Nutzung des iSCSI-Protokolls jedoch seit der Einführung von SMB 3 in modernen Lösungen immer weniger relevant.

Im iSCSI-Umfeld wird zwischen zwei Endpunkten unterschieden:

- serverseitige Bereitstellung von iSCSI-Speicher mittels sogenannter *iSCSI-Targets*
- Bereitstellung auf dem jeweiligen Client-System, dem *iSCSI-Initiator*

Die Einrichtung des iSCSI-Servers, also des iSCSI-Target-Servers, erfolgt über den Server-Manager, die PowerShell oder das Windows Admin Center. Sie finden die Funktion unter dem Punkt DATEI-/SPEICHERDIENSTE und dem Eintrag ISCSI-ZIELSERVER (siehe Abbildung 9.7). Beachten Sie, dass für das Installieren und Bereitstellen von iSCSI lokale Administratorrechte notwendig sind.

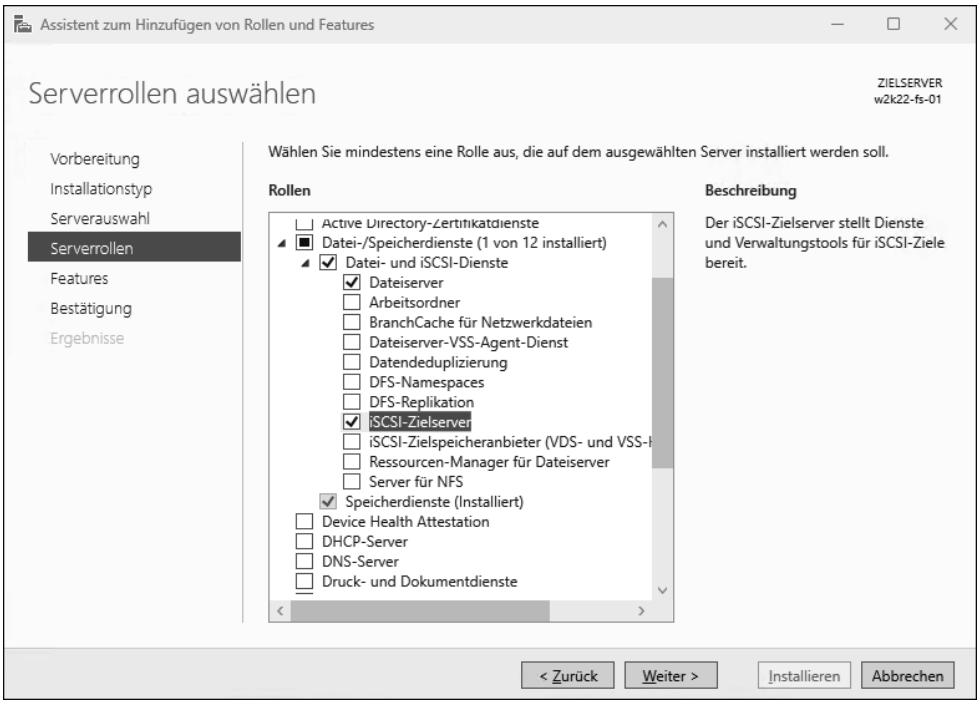

Abbildung 9.7 Installation des iSCSI-Target-Servers

Das Bereitstellen von iSCSI-Targets erfolgt nach der erfolgreichen Installation direkt über den Server-Manager. Nach der erfolgreichen Installation finden Sie im Server-Manager unter dem Dashboard die Auswahl DATEI-/SPEICHERDIENSTE und dort die Option ISCSI (siehe Abbildung 9.8).

Legen Sie nun im Konfigurationsassistenten den Speicherort der zu erzeugenden virtuellen Disk sowie deren Größe und Provisionierungsart fest. Da es sich um eine virtuelle Disk han-

delt, können Sie mehrere Optionen auswählen. Diese reichen von einer festen Diskgröße über eine dynamisch wachsende bis hin zu einer differenzierenden Disk.

Abbildung 9.8 Erstellen neuer oder Import bestehender iSCSI-Datenträger

Wenn noch kein iSCSI-Target vorhanden ist, erstellt der Bereitstellungsassistent ein neues iSCSI-Target. Hierzu können Sie einen Namen, den anzubindenden iSCSI-Initiator sowie das zu verwendende Authentifizierungsverfahren festlegen.

Beachten Sie bei der Auswahl des iSCSI-Initiators über die Abfrage des Active Directorys, dass für Microsoft Windows 7 und Windows Server 2008 R2 oder früher kein Support existiert. In diesem Fall müssen Sie den *IQN (iSCSI Qualified Name)* des iSCSI-Initiators verwenden.

Nachdem der Bereitstellungsassistent abgeschlossen ist, ist die virtuelle Disk im Dateisystem angelegt und das iSCSI-Target wird für die anzubindenden Clients zum Verbinden angeboten.

Um den iSCSI-Initiator nun anbinden zu können, öffnen Sie ihn in der Systemverwaltung des jeweiligen Clientsystems. Der iSCSI-Initiator wird Sie beim ersten Aufruf darüber informieren, dass der Microsoft iSCSI-Dienst gegenwärtig nicht läuft, und nachfragen, ob dieser gestartet werden soll. Dies bestätigen Sie mit JA (siehe Abbildung 9.9).

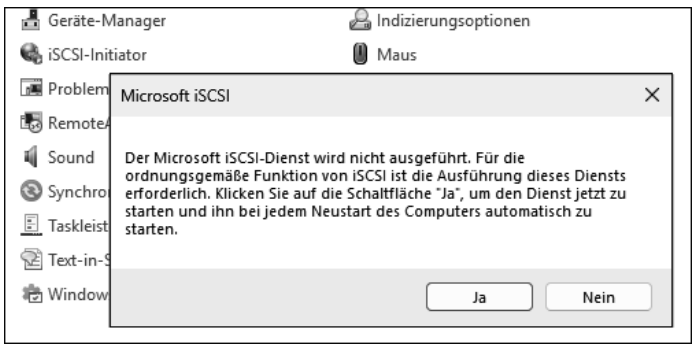

Abbildung 9.9 Verwenden des iSCSI-Initiators

Im iSCSI-Initiator hinterlegen Sie nun im Reiter ZIELSERVER den *FQDN* des iSCSI-Target-Servers und betätigen den Button SCHNELLE SUCHE. Die für dieses System angelegten iSCSI-Targets werden automatisch gefunden und in einer Auswahlliste zurückgeliefert. Wählen Sie nun die gewünschten iSCSI-Targets aus, und verwenden Sie die Option VERBINDEN. Die ausgewählten iSCSI-Targets werden daraufhin im Datenträger-Manager angezeigt und können partitioniert und formatiert werden.

Alternativ können Sie für die Anbindung von iSCSI-Targets einen *iSNS*-Server *(Internet Storage Name Service)* verwenden. Ähnlich wie auf einem DNS-Server lassen sich dort iSCSI-Targets zentral hinterlegen.

Port für iSCSI

Beachten Sie, dass zwischen dem iSCSI-Initiator und dem iSCSI-Target der Netzwerk-Port 3260 verfügbar sein muss, damit das Suchen und Anbinden des iSCSI-Targets möglich ist.

9.1.3 Schattenkopien

Die *Schattenkopien* (also der *Volume Shadow Copy Service*, VSS) sind seit Windows Server 2003 Bestandteil des Betriebssystems und können dem Administrator das Wiederherstellen von Daten aus nächtlichen Backups ersparen. Bei VSS werden, wie aus dem Namen dieser Funktion bereits hervorgeht, auf dem jeweiligen Volume, auf dem sie aktiviert wird, Kopien der darauf gespeicherten Daten vorgehalten. Diese Kopien können entweder auf demselben oder aber auch auf einem weiteren Datenträger abgelegt werden. Dies kann gerade bei Performance- oder Platzproblemen sehr hilfreich sein. Eine Änderung dieser Konfiguration kann jedoch nur dann vorgenommen werden, wenn keine Schattenkopien für das Volume vorhanden sind.

Keine Schattenkopien unter ReFS

Beachten Sie, dass Schattenkopien auf Volumes, die mit dem Dateisystem ReFS formatiert wurden, nicht zur Verfügung stehen.

Schattenkopien aktivieren Sie im EIGENSCHAFTEN-Dialog eines Volumes. Wählen Sie dort den Reiter SCHATTENKOPIEN, und klicken Sie auf JETZT ERSTELLEN (siehe Abbildung 9.10).

Über die Schaltfläche EINSTELLUNGEN gelangen Sie in den Konfigurationsdialog der Schattenkopien, der in Abbildung 9.11 zu sehen ist. Hier haben Sie die Möglichkeit, eine Größenbeschränkung für das Anlegen von Schattenkopien sowie deren Speicherort festzulegen.

Abbildung 9.10 Aktivieren und Erstellen von Schattenkopien

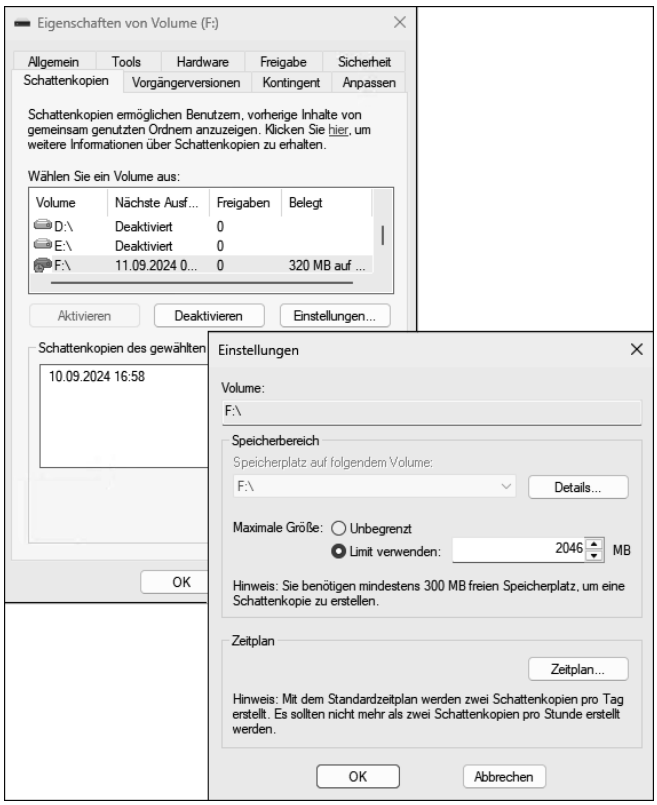

Abbildung 9.11 VSS-Konfiguration des Speicherpfades und des Speicherlimits

Sie haben die Möglichkeit, zu festgelegten Zeiten Schattenkopien zu erstellen, indem Sie detaillierte Zeitpläne hinterlegen (siehe Abbildung 9.12).

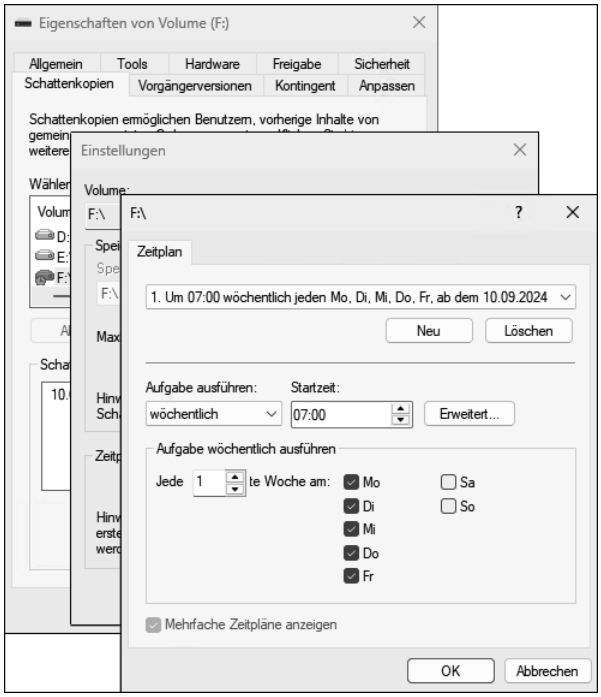

Abbildung 9.12 Hinterlegen von Zeitplänen für das Erstellen von Schattenkopien

Schattenkopien über den Tag verteilt anzulegen, ist sehr sinnvoll, um dem Fehlerteufel ein Schnippchen zu schlagen. So können Sie Dateien aus vorherigen Dateiversionen desselben Tages aus Schattenkopien wiederherstellen, die nur wenige Stunden alt sind (siehe Abbildung 9.13). Dies ist mit einem zentralen Backup normalerweise nicht möglich. Schattenkopien sind jedoch kein Ersatz für eine entsprechende Backup-Lösung, sondern sollen diese lediglich ergänzen.

Beachten Sie, dass die Anzahl an Schattenkopien durch den Speicherplatz beschränkt ist, der auf dem ausgewählten Datenträger zur Verfügung steht, bzw. durch das festgelegte Speicherlimit. Sobald nicht mehr ausreichend Speicher für die Erstellung einer neuen Schattenkopie zur Verfügung steht, werden die ältesten Schattenkopien schrittweise entfernt.

So wie Schattenkopien kein Ersatz für ein Backup darstellen, sind sie auch keine Dateiversionierung, sondern dienen lediglich zur schnellen Wiederherstellung von Dateien. Wenn Sie eine Dateiversionierung benötigen, sollten Sie über den Einsatz eines SharePoint-Servers nachdenken.

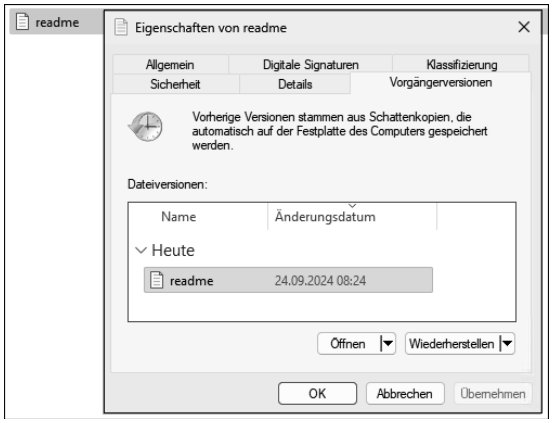

Abbildung 9.13 Wiederherstellen aus vorhandenen Schattenkopien

9.1.4 Freigaben

Mit der Netzwerkkomponente *Datei- und Druckerfreigabe für Microsoft-Netzwerke* des Betriebssystems können lokale Verzeichnisse per *UNC*-Pfad *(Universal Naming Convention)* über das Netzwerk zur Verfügung gestellt werden. Somit besteht für Benutzer die Möglichkeit, zentral Daten im Netzwerk auf einem Server abzulegen, wie Abbildung 9.14 zeigt.

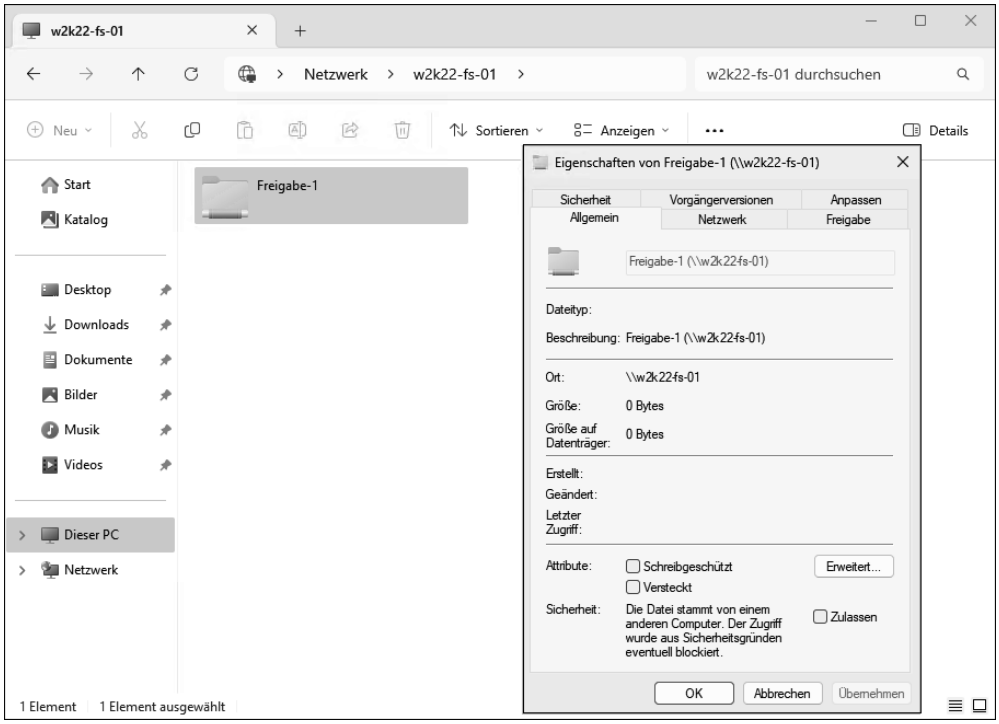

Abbildung 9.14 Zugriff auf eine Netzwerkfreigabe

Erstellen von Freigaben

Netzwerkfreigaben können Sie über den Datei-Explorer des jeweiligen Servers anlegen. Erstellen Sie hierzu an der gewünschten Stelle im Dateisystem einen Ordner, und öffnen Sie per Rechtsklick das Kontextmenü für diesen Ordner. Wählen Sie nun die Eigenschaften des Ordners aus, und wechseln Sie in den Reiter FREIGABE. Dort finden Sie nun zwei Optionen, um eine Freigabe zu erzeugen (siehe Abbildung 9.15). Verwenden Sie die ERWEITERTE FREIGABE, und setzen Sie in dem folgenden Menü ein Häkchen bei der Option DIESEN ORDNER FREIGEBEN.

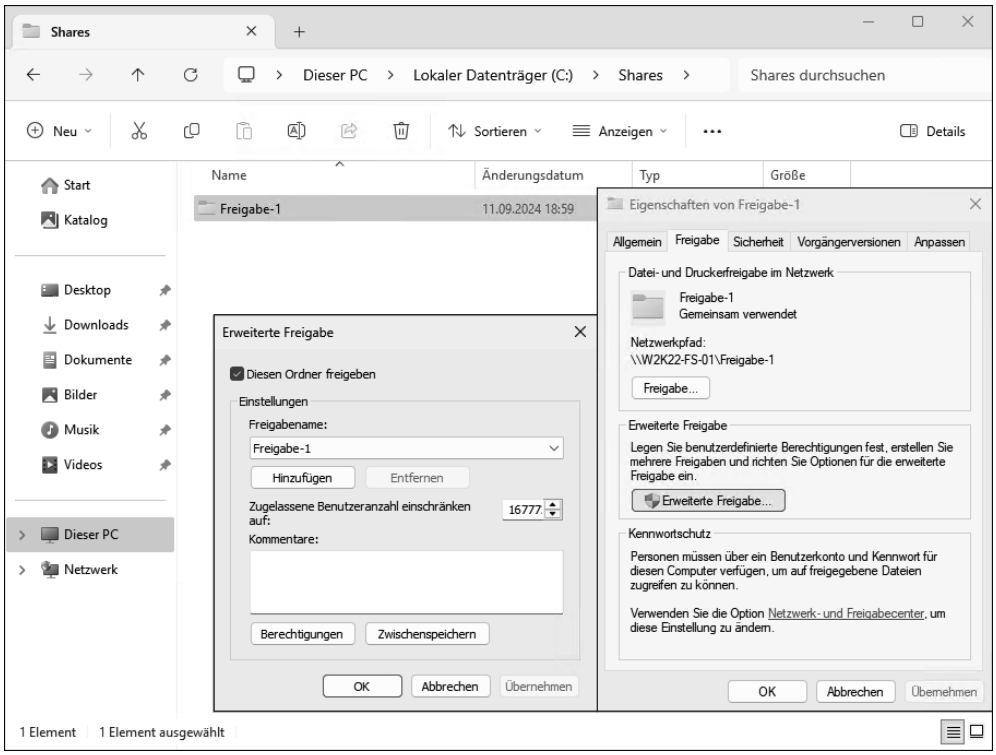

Abbildung 9.15 Erstellen einer Netzwerkfreigabe

Standardmäßig verwendet das Menü den Ordnernamen für die Freigabe. Sie können hier aber auch einen abweichenden Namen eintragen. Auf diese Weise lassen sich mehrere Freigaben für dasselbe Verzeichnis erstellen.

Beachten Sie, dass Sie unter der Option BERECHTIGUNGEN den Zugriff auf die Freigabe separat von der Berechtigung des Dateisystems vergeben können. Weitere Informationen dazu finden Sie in Abschnitt 9.1.5, »NTFS und Freigaben-Berechtigungen«.

Die Anbindung der Benutzer an diese Freigabe kann entweder per UNC-Pfad oder mit einer Netzlaufwerksverbindung erfolgen. In diesem Fall wird die Freigabe als virtuelles Laufwerk eingebunden.

Um *Netzlaufwerksverbindungen* anzubinden, verwenden Sie wahlweise den Kommandozeilenbefehl `net use`, eine Gruppenrichtlinie oder Sie erstellen die Verbindung mithilfe des Datei-Explorers. Wenn Sie die Verbindung herstellen, sollten Sie den FQDN des Dateiservers verwenden. So stellen Sie sicher, dass beim Verbindungsaufbau zum Dateiserver Kerberos für die Authentifizierung der Benutzer verwendet wird.

Um den Zugriff auf die von Ihnen erstellte Dateifreigabe zusätzlich zu den Berechtigungen der Freigabe sowie der NTFS-Berechtigung einschränken zu können, stehen Ihnen zwei Möglichkeiten zur Verfügung:

- Sie können beim Anlegen der Dateifreigabe hinter dem von Ihnen festgelegten Namen für die Dateifreigabe ein $-Zeichen anfügen. Dadurch wird die Dateifreigabe beim Aufruf des Dateiservers versteckt. Sie können die Dateifreigabe dennoch verwenden, indem Sie sie inklusive des $-Zeichens aufrufen.
- Sie können auch für einzelne Freigaben die ZUGRIFFSBASIERTE AUFZÄHLUNG *(Access-based Enumeration, ABE)* aktivieren, wie Sie in Abbildung 9.16 sehen. Dies führt dazu, dass der Dateiserver die Verzeichnisse und Dateien in der Freigabe für nicht berechtigte Benutzer ausblendet.

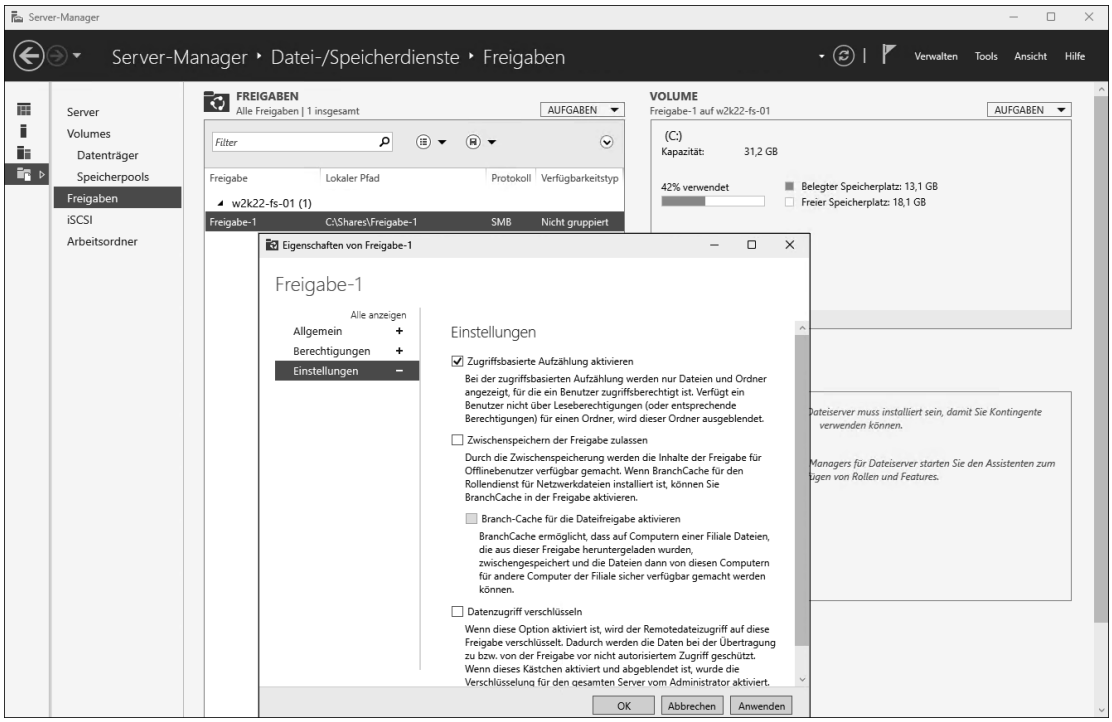

Abbildung 9.16 Aktivierung der ABE auf einer Dateifreigabe über den Server-Manager

Eingesetzte Protokolle

Beim Zugriff auf Netzwerkfreigaben kommt das Protokoll *SMB (Server Message Block*) zum Einsatz. Je nach verwendetem Betriebssystem und/oder Anwendung werden natürlich verschiedene Versionen des SMB-Protokolls genutzt. Die Entstehung dieses Protokolls geht auf Barry Feigenbaum (IBM) im Jahre 1983 zurück. Seitdem wurde SMB durch einige Unternehmen, darunter auch Microsoft, weiterentwickelt.

Das SMB-Protokoll wurde in den vergangenen Jahren unter verschiedenen Namen bekannt, so z. B. als *LAN-Manager-Protokoll* oder auch als *CIFS (Common Internet File System)*. Daher lesen Sie auch heute noch in vielen Artikeln, Blogs und einigen technischen Anleitungen den Begriff »CIFS-Protokoll«.

Das SMB-Protokoll stellt ein Netzwerkdateisystem bereit, das in seiner Funktion zum größten Teil vom Dateisystem des Betriebssystems unabhängig ist. Diese Bereitstellung erfolgte ursprünglich mittels *NetBIOS over TCP/IP (NBT)*, das die TCP/UDP-Ports im Bereich zwischen 137 und 139 sowie WINS bzw. Broadcasts zur Namensauflösung nutzte. In aktuellen Betriebssystemen ist dies nicht mehr der Fall: Hier wird im Rahmen der SMB-Kommunikation auf den TCP-Port 445 gesetzt, und die Auflösung der Namen erfolgt via *DNS* oder *LLMNR (Link-local Multicast Name Resolution*). Letzteres ist jedoch in größeren Infrastrukturen nicht relevant.

SMB 1.0

Die Notwendigkeit der beschriebenen NetBIOS-Auflösung entfiel mit Windows Server 2000. Die SMB-Kommunikation erfolgt daher direkt über Port 445.

SMB 1.0 ist inzwischen komplett veraltet, muss allerdings in vielen Umgebungen aus Gründen der Kompatibilität noch unterstützt werden. Dies ist (wahrscheinlich) auch der Hintergrund dafür, dass Microsoft es weiterhin als optionales Feature anbietet, obwohl eigentlich erwartet worden war, dass der Windows Server 2025 SMB 1.0 gar nicht mehr bereitstellen würde.

Vermeiden Sie es daher grundsätzlich, immer noch SMB in der Version 1.0 in einem produktiven Netz zu betreiben: Weil seine Sicherheitslücken nicht mehr geschlossen werden, ist SMB 1.0 eine Gefahr für Ihre Infrastruktur, denn es stellt ein erhebliches Risiko dar. So hat beispielsweise *WannaCry* (im Mai 2017) eine Sicherheitslücke innerhalb des Protokolls ausgenutzt, um Ransomware auf möglichst viele Systeme im lokalen Netzwerk zu verteilen. Für Betroffene war es besonders ärgerlich, da Microsoft noch rechtzeitig vor dem Auftreten dieses großflächigen Cyberangriffs ein entsprechendes Update veröffentlicht hatte, das allerdings nicht überall eingespielt wurde. Daher hat sich Microsoft entschieden, dieses Server-Feature mit der Veröffentlichung von Version 1709 im Oktober 2017 nicht mehr standardmäßig zu installieren (siehe Abbildung 9.17).

SMB 2.0

Im Rahmen der Bereitstellung des *SMB 2.0*-Protokolls wurde SMB grundlegend überarbeitet. Durch die Reduktion der verfügbaren SMB-Kommandos sowie durch weitere Anpassungen

wurde die Leistungsfähigkeit des Protokolls entscheidend verbessert, was vor allem die Übertragungsgeschwindigkeit in WAN-Netzwerken erhöht.

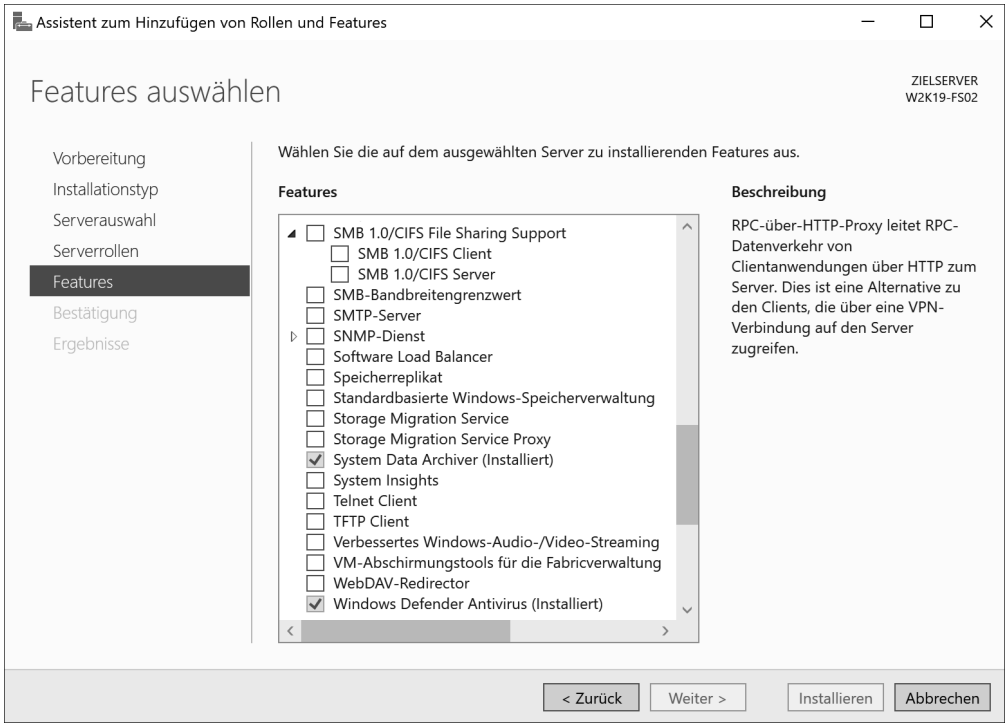

Abbildung 9.17 Das Windows-Feature »SMB 1.0/CIFS File Sharing Support« kann weiterhin installiert werden, wenn Sie es unbedingt brauchen.

SMB 3.0

In der SMB-Version 3.0 wurde das SMB-Protokoll um einige neue Features erweitert:

- **SMB-Direct** – Dieses Feature setzt die Verwendung von *RDMA*-Netzwerkkomponenten *(Remote Direct Memory Access)* voraus, was den direkten Zugriff auf den Arbeitsspeicher des jeweiligen Remotesystems ermöglicht.
- **Multichannel-SMB** – Hierdurch können mehrere Verbindungen zwischen dem SMB-Client und dem Zielserver aufgebaut werden, was durch redundante Netzwerkpfade den Durchsatz erheblich erhöhen kann.
- **Ende-zu-Ende-Verschlüsselung** – Dieses Feature ermöglicht die Verschlüsselung der versendeten Pakete über alle Transport-Hops hinweg, wodurch die Entschlüsselung der Inhalte nur den jeweiligen Kommunikationspartnern möglich ist.

Tabelle 9.4 fasst die Neuerungen in den einzelnen SMB-Versionen noch einmal kompakt zusammen.

SMB-Version	Betriebssystem	Neue Features
CIFS	Windows NT 4.0	
1.0	Windows 2000	SMB TCP/IP – keine Notwendigkeit von NetBIOS
2.0	Windows Vista bzw. Server 2008	Optimierung der Leistung durch Reduktion der Kommandos
2.1	Windows 7 bzw. Server 2008 R2	Weitere Optimierungen und Bereitstellung von Locking-Mechanismen
3.0	Windows 8 bzw. Server 2012	Erweiterungen für den Einsatz in virtuellen Infrastrukturen (SMB-Direct, Multichannel, Transparent Failover), Verschlüsselung
3.0.2	Windows 8.1 bzw. Server 2012 R2	
3.1.1	Windows 10/11 bzw. Server 2016/2019/2022/2025	Erweiterte Verschlüsselung (AES 128GCM/CCM) Integrationsüberprüfung (SHA-512)

Tabelle 9.4 Übersicht der einzelnen SMB-Versionen und -Funktionen

9.1.5 NTFS und Freigaben-Berechtigungen

Wie wir bereits in Abschnitt 9.1.4 beschrieben haben, können Sie die Berechtigungen des NTFS-Dateisystems und der von Ihnen erstellten Freigaben separat voneinander setzen. In der Vergangenheit haben die meisten Administratoren Berechtigungen ausschließlich auf dem NTFS-Dateisystem gesteuert und in der Freigabe für *Jeder* die Berechtigung *Vollzugriff* gewährt. Dies schützt Ihre Daten jedoch nur begrenzt und ermöglicht Ihnen nicht das Steuern von Zugriffen auf Dateisystempfade, die über mehrere Dateifreigaben zugänglich gemacht werden. Hier stellt das explizierte Vergeben von Berechtigungen auf der Dateifreigabe, zusätzlich zu der NTFS-Berechtigung des Dateisystems, eine gute Möglichkeit dar, diesen Zugriff granularer zu steuern.

NTFS

Mithilfe der NTFS-Berechtigungen können Sie festlegen, wer auf Dateien und Ordner zugreifen darf und wie weit der Zugriff für den jeweiligen Benutzer oder die jeweilige Gruppe reicht. Hierzu steht Ihnen im NTFS-Dateisystem (im Gegensatz zu der Dateifreigabe) eine Vielzahl von möglichen Berechtigungen zur Verfügung (siehe Abbildung 9.18):

- Vollzugriff – Durch den Vollzugriff sind Benutzer in der Lage, Dateien und Ordner zu lesen, zu schreiben, zu ändern und zu löschen. Außerdem können diese Benutzer die Berechtigungen für Dateien und Ordner ändern.

- ÄNDERN – Hierbei dürfen Benutzer Dateien und Ordner lesen, schreiben und auch löschen.
- LESEN, AUSFÜHREN – Dies ermöglicht es den Benutzern, Dateien (hierzu gehören auch Skripte und ausführbare Dateien) anzuzeigen und auszuführen.
- ORDNERINHALT ANZEIGEN – erlaubt es Benutzern, Dateien und Ordner aufzulisten sowie Dateien auszuführen.
- LESEN – Benutzer können mit dieser Berechtigung Inhalte von Ordnern auflisten.
- SCHREIBEN – Das Hinzufügen von Dateien und Ordnern sowie das Ändern von Dateien ist mit dieser Berechtigung möglich.

Abbildung 9.18 Zugriff auf die NTFS-Berechtigungen eines Ordners im Explorer

Um NTFS-Berechtigungen für Dateien und Ordner einsehen oder auch ändern zu können, können Sie mit dem Datei-Explorer die NTFS-Berechtigungen auflisten.

Gehen Sie hierzu wie folgt vor: Öffnen Sie den Datei-Explorer, und wechseln Sie in das Verzeichnis, in dem sich die Datei oder der Ordner befindet, dessen Berechtigung Sie einsehen bzw. ändern wollen.

Öffnen Sie die Eigenschaften der Datei oder des Ordners, und wählen Sie die Registerkarte SICHERHEIT (siehe Abbildung 9.18). Hier erhalten Sie eine Übersicht über die Berechtigungen der Benutzer und Gruppen. Mit BEARBEITEN können Sie die aufgelisteten Berechtigungen ändern.

Auf der Registerkarte SICHERHEIT können Sie über die Option ERWEITERT auf weitere Funktionen zugreifen (siehe Abbildung 9.19). Dazu zählen die Auflistung der vergebenen NTFS-Berechtigungen und der Dateifreigabe-Berechtigungen sowie die ÜBERWACHUNG und der EFFEKTIVE ZUGRIFF.

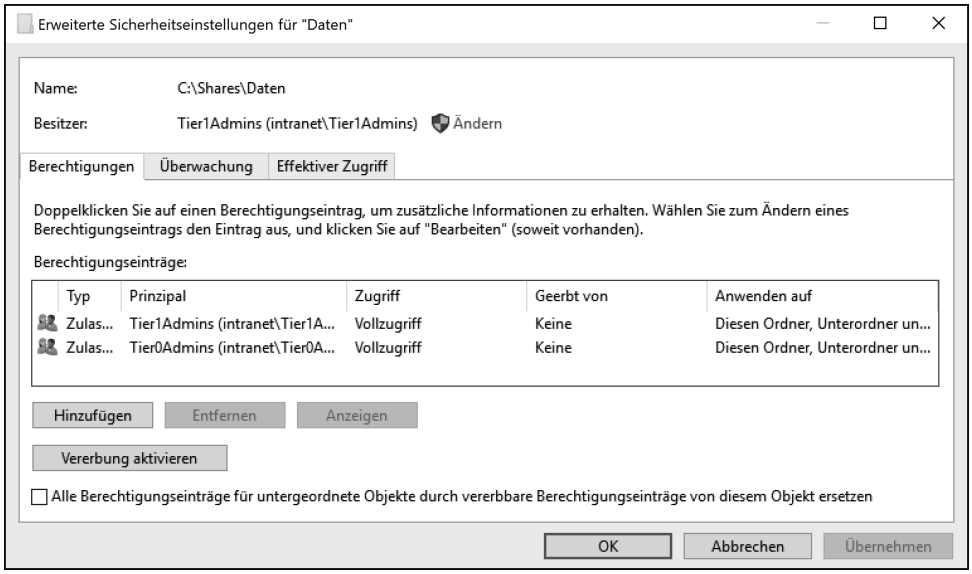

Abbildung 9.19 Erweiterte Sicherheitseinstellungen für Dateien und Ordner

Im Reiter BERECHTIGUNGEN können Sie zusätzlich zu den aufgelisteten Berechtigungen auch deren Anwendungsebene festlegen. Hier stehen Ihnen die Möglichkeiten zur Verfügung, die Berechtigungen nur für die ausgewählten Objekte anzuwenden oder sie auch an die darunter liegenden Strukturen und Dateien weiterzuvererben.

Auch das Vererben der Berechtigungen aus übergeordneten Strukturen kann hier aktiviert oder deaktiviert werden; außerdem ist es auch möglich, die gesetzten Berechtigungen an untergeordnete Strukturen zu vererben.

Über den Reiter FREIGABE (siehe Abbildung 9.18) erhalten Sie eine Auflistung der vergebenen Dateifreigabe-Berechtigungen und können diese dort weiter anpassen.

Der Reiter ÜBERWACHUNG (siehe Abbildung 9.19) bietet Ihnen die Möglichkeit, den Zugriff auf Dateien und Ordner für ausgewählte Benutzer und Gruppen zu überwachen. Hierbei werden die entsprechend konfigurierten Zugriffe im Eventlog des Dateiservers protokolliert.

Mit den Funktionen im Reiter EFFEKTIVER ZUGRIFF testen Sie, welche Auswirkungen die vergebenen NTFS-Berechtigungen haben. Sie können Benutzer, Gruppen oder Geräte auswählen und sehen sofort, wie sich der Zugriff auswirkt. Dies ist vor allem dann hilfreich, wenn Sie während der Fehlersuche festzustellen versuchen, warum ein Zugriff auf die Dateien und Ordner möglich oder auch nicht möglich ist (siehe Abbildung 9.20).

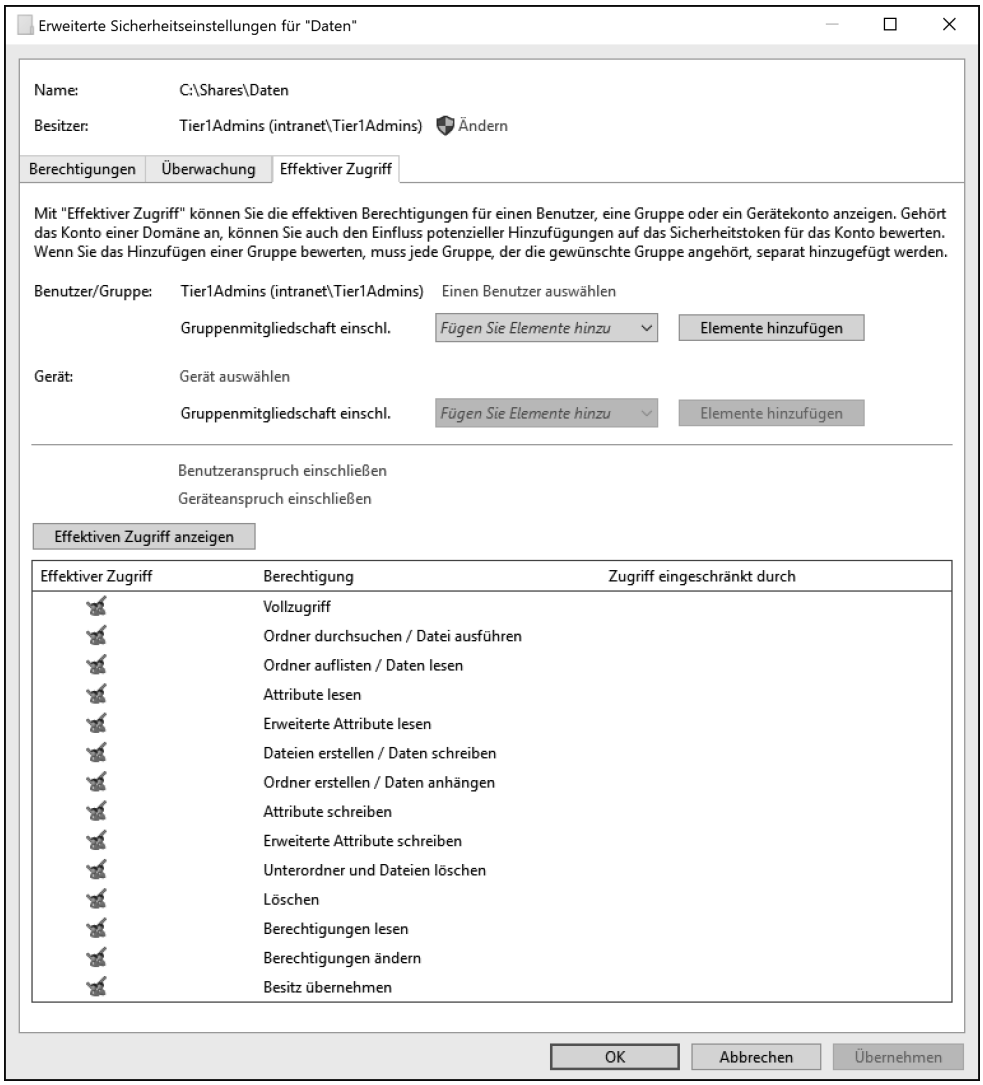

Abbildung 9.20 Überprüfung des effektiven Zugriffs für ausgewählte Benutzer, Gruppen oder Geräte

Zusätzlich zu Genehmigungsberechtigungen können Sie auch explizite Verweigerungsrechte vergeben. Der Vorteil hierbei ist, dass Verweigerungseinträge vorrangig behandelt werden: Wenn also ein Benutzer Mitglied in mehreren Gruppen ist, reicht das Verweigerungsrecht in irgendeiner Gruppenmitgliedschaft aus, um diesem Benutzer den Zugriff zu verwehren, selbst wenn ihm über eine der vorhandenen Gruppen Zugriff gewährt wird.

Um die Steuerung von Berechtigungen zu automatisieren, nutzen Sie die PowerShell. Verwenden Sie das Cmdlet `Get-ACL` zum Auslesen bestehender Berechtigungen und `Set-ACL`, um

Berechtigungen auf Dateien und/oder Ordnern zu setzen. Dies bietet sich zum Beispiel an, wenn Sie eine Berechtigungsrichtlinie für bestimmte Ordnerstrukturen festgelegt haben und diese automatisch in regelmäßigen Abständen erneut anwenden lassen.

Somit können Sie sicherstellen, dass die Berechtigungen, wenn diese manuell verändert wurden, in einem festgelegten Zeitfenster wieder der von Ihnen definierten Richtlinie entsprechen.

Dateifreigaben

Durch die Vergabe von Dateifreigabe-Berechtigungen können Sie festlegen, wie Benutzer über das Netzwerk auf die von Ihnen bereitgestellte Dateifreigabe zugreifen können und wie weitgehend deren Zugriff über das Netzwerk ist.

In der Dateifreigabe stehen Ihnen drei mögliche Berechtigungen zur Verfügung (siehe Abbildung 9.23):

- VOLLZUGRIFF – Benutzer, die über Vollzugriff verfügen, können in der Dateifreigabe lesen, ändern, Berechtigungen verändern und den Besitz von Dateien und Ordnern übernehmen.
- ÄNDERN – Hierdurch können Benutzer in den Dateifreigaben lesen, ausführen, schreiben und löschen.
- LESEN – Dies ermöglicht Benutzern das Auflisten von Inhalten in der Dateifreigabe.

Um Zugriff auf die Berechtigungen von Dateifreigaben zu erhalten, gehen Sie wie folgt vor: Öffnen Sie die Eigenschaften der Datei oder des Ordners, und wählen Sie die Registerkarte FREIGABE (siehe Abbildung 9.21).

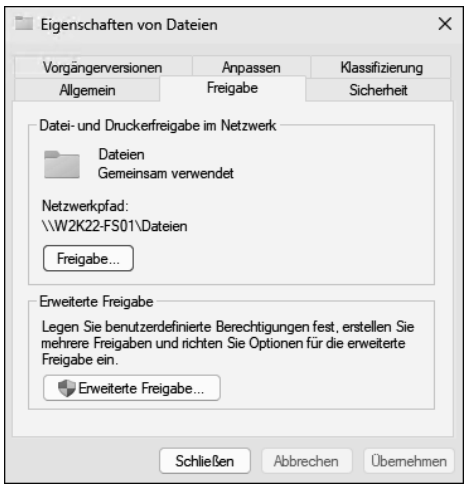

Abbildung 9.21 Freigabe-Eigenschaften einer Dateifreigabe im Explorer

Klicken Sie in der Registerkarte FREIGABE auf die Option ERWEITERTE FREIGABE.

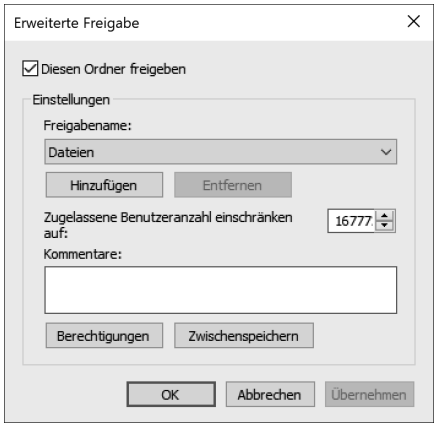

Abbildung 9.22 »Erweiterte Freigabe«-Eigenschaften der Dateifreigabe im Explorer

In der ERWEITERTEN FREIGABE aus Abbildung 9.22 können Sie nun über die Option BERECHTIGUNGEN die Berechtigungen der Dateifreigabe einsehen und gegebenenfalls anpassen (siehe Abbildung 9.23).

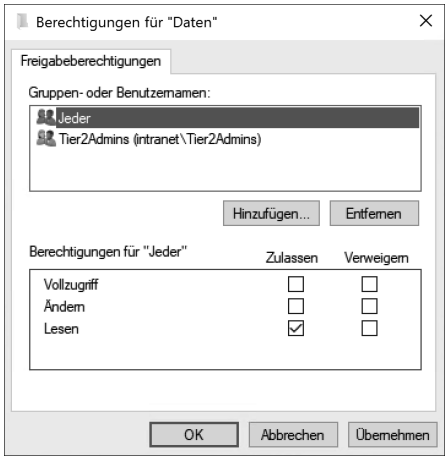

Abbildung 9.23 Zugriff auf die Dateifreigabe-Berechtigungen im Explorer

Kombination von Dateifreigabe- und NTFS-Berechtigungen

Wenn Sie eine Dateifreigabe auf einem Ordner einrichten, auf dem eine NTFS-Berechtigung vergeben wurde, wird bei einem Zugriff über das Netzwerk auf die Dateifreigabe und das darunter liegende Dateisystem die restriktivste Berechtigung angewendet.

Wenn das NTFS-Dateisystem einem Benutzer also Vollzugriff gewährt, in der Dateifreigabe jedoch nur eine Leseberechtigung eingerichtet ist, dann kann der Nutzer nur lesend auf die Dateien zugreifen. Eine schematische Darstellung dieser Zugriffsberechtigung sehen Sie in Abbildung 9.24.

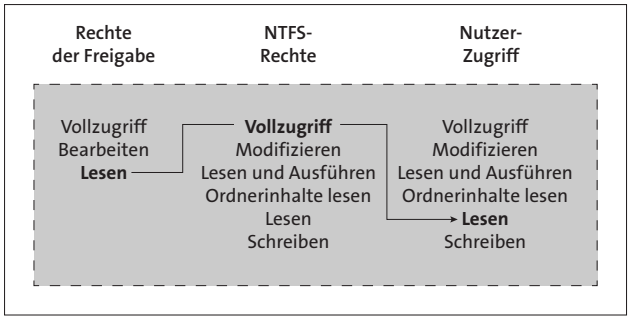

Abbildung 9.24 Sechematische Darstellung einer lesenden Dateifreigabe-Berechtigung

Im Umkehrschluss bedeutet dies, dass selbst dann, wenn die Freigabe den Vollzugriff erlaubt, für den Nutzer nur eine Leseberechtiung besteht, falls das NTFS-Dateisystem nicht mehr erlaubt. Es wird ja, wie bereits beschrieben, immer die restriktivste Berechtigung angewendet. In Abbildung 9.25 finden Sie eine Darstellung der beschriebenen Berechtigung.

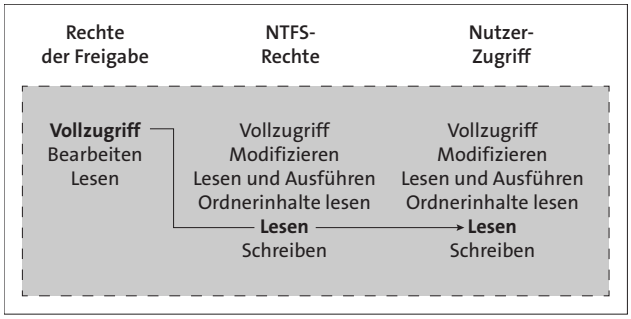

Abbildung 9.25 Schematische Darstellung einer Vollzugriff-Dateifreigabe-Berechtigung

Sicherheitsgruppen

Wenn ein Benutzer Mitglied in mehreren Sicherheitsgruppen ist, die für den Zugriff auf die Dateifreigabe konfiguriert wurden, wirken die Berechtigungen kumuliert.

Wenn ein Benutzer also durch eine Sicherheitsgruppe lesende Berechtigungen für die Dateifreigabe bekommt und durch eine zweite Sicherheitsgruppe schreibende Berechtigungen für dieselbe Dateifreigabe, resultiert daraus die effektiv kumulierte Berechtigung *lesender und schreibender Zugriff*. Dies verhält sich auf Ebene der Dateifreigabe ebenso wie auf der Ebene der NTFS-Berechtigungen.

9.1.6 Offlinedateien

Offlinedateien sind eine Funktion zum Synchronisieren von Dateien zwischen einem Windows-Clientbetriebssystem und einer bereitgestellten Netzwerkfreigabe. Hierbei wer-

den in zeitlich festgelegten Abständen die Daten mit dem Dateiserver abgeglichen. Die Speicherung erfolgt also auch im Online-Modus (d. h., wenn eine Verbindung zum Dateiserver besteht) immer erst in die lokale Replik und wird dann synchronisiert.

Ob es diese Funktion weiterhin geben wird, ist unklar, da Microsoft aktuell immer mehr das Cloud-Geschäft in den Fokus stellt und die damit verbundenen Produkte fördert. Die Offlinedateien stehen mit der Cloud-basierenden Lösung *OneDrive* bzw. *OneDrive for Business* in Konkurrenz.

Das Einrichten der Offlinedateien kann über die lokale Konfiguration im Clientbetriebssystem erfolgen oder für das flächendeckende Konfigurieren in Unternehmen per GPO ausgerollt werden. Hierbei ist jedoch darauf zu achten, dass nicht alle Konfigurationen zwischen den einzelnen Windows-Clientbetriebssystemversionen kompatibel sind.

Bei den Offlinedateien wird zwischen den Betriebsmodi *Online*, *Langsame Verbindung*, *automatisch Offline* sowie *manuell Offline* unterschieden. Hierbei wird die Verbindungsgeschwindigkeit zwischen dem Client und dem Server durch die Übertragung eines Pakets mit der Standardpaketgröße überprüft, um festzustellen, wie groß die Gesamtlaufzeit der Übertragung ist. Sobald eine Gesamtlaufzeit kleiner als 80 ms festgestellt wird, wird die Verbindung als lokales Netzwerk bzw. als stabile Remoteverbindung betrachtet und somit in den Online-Modus gewechselt. Zeiten über 80 ms werden demnach als *Langsame Verbindung* eingestuft und es wird standardmäßig in den Offline-Modus gewechselt.

Die Erstsynchronisation wird nach dem erfolgreichen Einrichten im Hintergrund ausgeführt und nach erfolgreicher Beendigung mit dem Offlinedateien-Synchronisations-Icon (SYNCHRONISIERUNGSCENTER) in der Taskleiste bestätigt (siehe Abbildung 9.26). Jede weitere Synchronisation erfolgt in einem Standardzeitfenster von 5 Minuten.

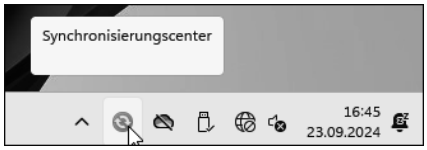

Abbildung 9.26 Offline-Synchronisation in der Taskleiste

Serverseitig ist keine besondere Konfiguration für die Verwendung der Offlinedateien erforderlich. Standardmäßig hat der Benutzer die Möglichkeit, während der Erstellung von Freigaben Offlinedateien für diese einzurichten. Wir raten Ihnen jedoch dringend davon ab, diese Funktion für Freigaben mit mehr als einem Benutzer zu verwenden: Abgesehen von dem hohen Replikationsaufkommen besteht hier das Risiko, dass eine Vielzahl nicht auflösbarer Konflikte im Rahmen der Replikation entstehen. Ausnahmen sind Verzeichnisse, wie beispielsweise Dateivorlagen, auf die ausschließlich lesend zugegriffen wird.

In den OFFLINEEINSTELLUNGEN finden Sie die folgenden drei Optionen aus Abbildung 9.27:

- Nur von Benutzern angegebene Dateien und Programme sind offline verfügbar – Hierdurch kann der Benutzer Dateien und Ordner für die Offline-Synchronisation explizit auswählen. Außerdem besteht die Möglichkeit, BranchCache zu aktivieren. Dabei handelt es sich um einen weiteren Dienst der Windows Server-Rolle *Datei-/Speicherdienste*. Mit BranchCache können Server, die z. B. in Außenstellen stehen, einmal abgerufene Dateiinhalte in dem jeweiligen Standort zwischenspeichern. Dies soll das erneute Herunterladen von einem anderen Standort verhindern. Wenn kein Server am Standort vorhanden ist, werden durch *BranchCache* die vor Ort vorhandenen Clients zum Zwischenspeichern verwendet. Die Auswahl dieser Option steht erst zur Verfügung, nachdem BranchCache auf dem Dateiserver installiert wurde.
- Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen – Hierdurch wird die Funktion unterbunden, Offlinedateien für die jeweilige Dateifreigabe zu verwenden.

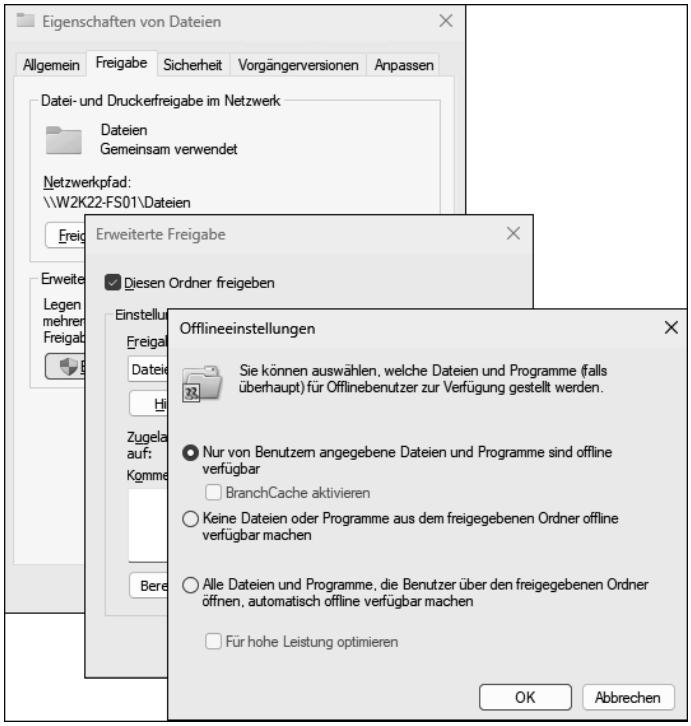

Abbildung 9.27 Freigabe zur Nutzung der Offlinedateien bereitstellen

- Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen – Die Einstellung erstellt automatisch Offlinedateien von Dateien und Programmen, die durch den Benutzer aufgerufen werden. Dabei reicht schon das einmalige Öffnen der Dateien oder Programme aus, damit Offlinedateien angelegt werden. Durch die Option Für hohe Leistung optimieren wird das

Synchronisationsverhalten für ausführbare Programme verbessert. Es wird dann nur die Programmversion der ausführbaren Datei geprüft; erst wenn sich diese ändert, wird eine erneute Synchronisation dieser Datei ausgelöst.

Wenn die maximale Cachegröße erreicht wurde, wird das System automatisch mit der Datenbereinigung beginnen. Dabei werden Dateien aus dem Cache entfernt, die bereits seit Längerem nicht mehr verwendet wurden und nicht explizit zur Offline-Speicherung durch den Benutzer markiert wurden. Solange die Bereinigung nicht durchgeführt wurde und somit kein weiterer Speicher für den Cache zur Verfügung steht, werden keine weiteren Dateien offline bereitgestellt.

Auch die Protokollierung der Synchronisation, die im *Sync Center* zu finden ist, kann Hinweise zur Behebung von Problemen liefern.

Manchmal kann es erforderlich sein, den Offlinedateien-Cache zu leeren, um Fehlerbilder zu beseitigen, beispielsweise Dateien, die sich nicht mehr synchronisieren lassen. Hierzu muss die Option `FormatDatabase` im Registry-Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CSC\Parameters* auf den Wert `1` gesetzt und das System neu gestartet werden.

Alle nicht synchronisierten Daten werden hierdurch unwiederbringlich gelöscht!

Laut Microsoft sind die Netzwerkports aus Tabelle 9.5 für die Kommunikation mit Offlinedateien notwendig.

Anwendungsprotokoll	Zielsystem	Protokoll	Port
SMB	Dateiserver	TCP	445
Global Catalog	Domänencontroller	TCP	3269
Global Catalog	Domänencontroller	TCP	3268
LDAP Server	Domänencontroller	TCP/UDP	389
LDAP SSL	Domänencontroller	TCP	636

Tabelle 9.5 Auflistung der notwendigen Netzwerkports

9.1.7 Datendeduplizierung

Das stetig wachsende Datenaufkommen führt zu der Frage, wie man redundante Daten erkennt und löscht. Hierfür hat Microsoft mit Windows Server 2012 die Datendeduplizierung eingeführt und bis heute stetig ausgebaut.

Die *Deduplizierung* prüft ein Volume blockweise auf identische Blöcke und setzt für gefundene Duplikate Adress-Pointer, die auf ihre Dublette verweisen. Im Ergebnis sind doppelte Datenblöcke nur noch einmal pro Volume vorhanden. Das Einsparpotenzial ist hierbei

enorm. In Abhängigkeit von den vorhandenen Daten lassen sich Speicherkapazitäten von bis zu 90 % einsparen – zum Beispiel bei virtuellen Datenträgern (*VHD/X*-Dateien) von Gastbetriebssystemen, die sich auf demselben Volume befinden.

Die Grenzen der Deduplizierung

Beachten Sie, dass die Deduplizierung nur auf Ebene eines Volumes konfiguriert werden kann und nicht auf Ordnerebene. Daten lassen sich auch nicht über die Grenzen des ausgewählten Volumes hinweg deduplizieren.

Die Standardkonfiguration der Deduplizierung basiert auf vordefinierten Kategorien für Dateiserver, *VDI*-Server *(Virtual Desktop Infrastructure)* und virtualisierte Backupserver. Darüber hinaus gibt es jedoch weitere Szenarien, die von den jeweiligen Lösungen unterstützt werden: Hierzu gehören z. B. Bereitstellungsfreigaben von SCCM *(System Center Configuration Manager)* und SCVMM (*System Center Virtual Machine Manager*, die Library-Freigaben) sowie Sicherungsvolumes von SQL- und Exchange-Servern.

Mit der Installation der Rolle *Datendeduplizierung* können Sie im Server-Manager die Deduplizierung für ausgewählte Volumes aktivieren (siehe Abbildung 9.28).

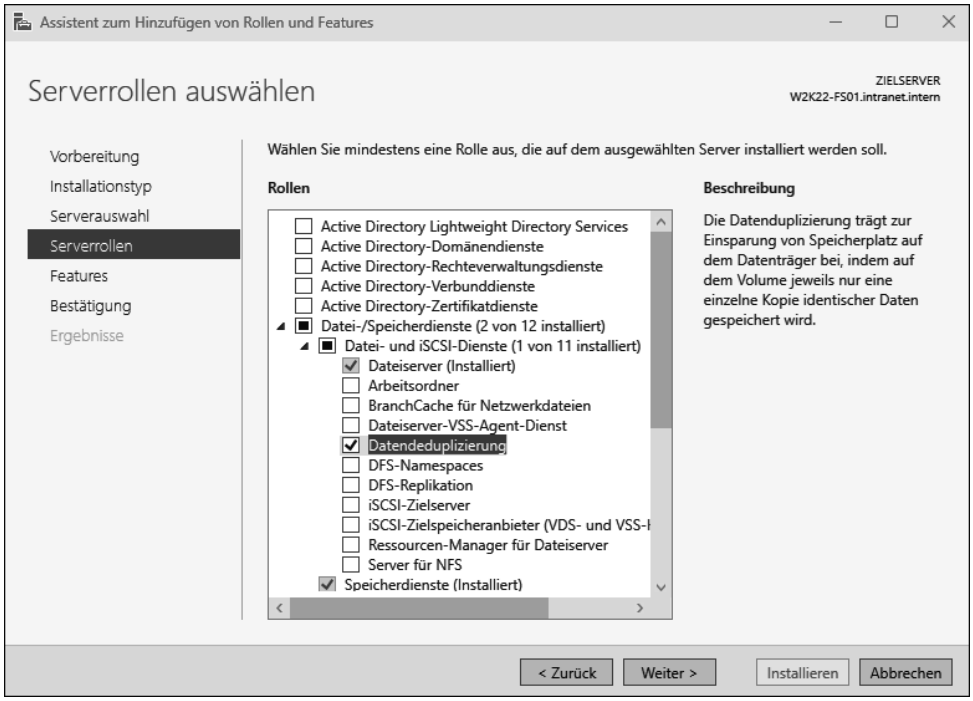

Abbildung 9.28 Installation der Dateiserver-Deduplizierung

Die Konfiguration der Deduplizierung erfolgt über einen Assistenten (siehe Abbildung 9.29) und ermöglicht es Ihnen, eine Kategorie für die Deduplizierung zu hinterlegen. Sie können zudem bestimmen, ab welchem Alter eine Datei dedupliziert werden soll und welche Dateierweiterungen davon ausgenommen werden sollen.

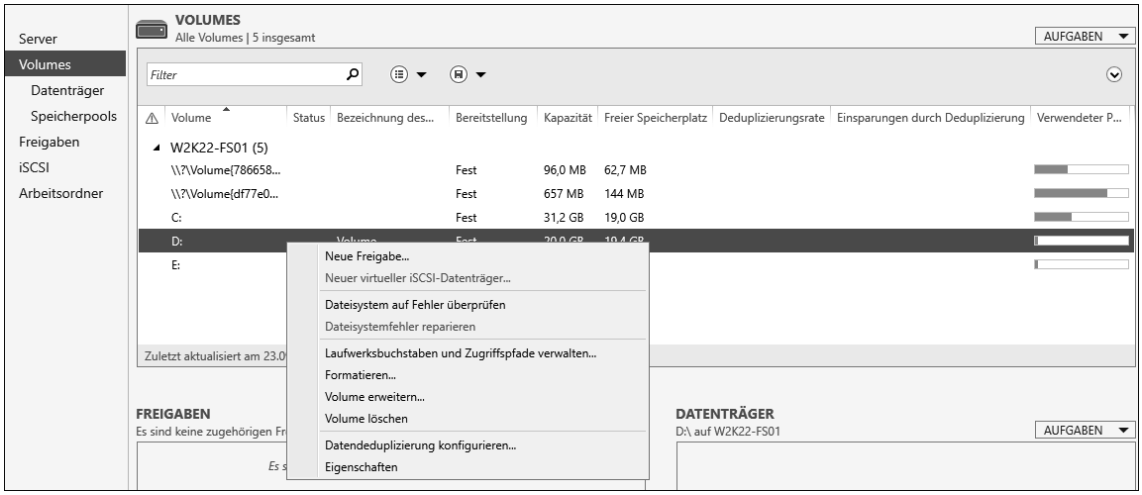

Abbildung 9.29 Einrichten der Deduplizierung für ein Volume

Auch bei der Deduplizierung lässt sich ein Zeitplan anlegen. Das Aktivieren der Hintergrundoptimierung bietet sich hierbei an, wenn es auf dem Server lastfreie bzw. lastarme Zeiten gibt, die für die Deduplizierung der Daten genutzt werden können. Wir empfehlen jedoch, einen eigenen Zeitplan zu hinterlegen, der außerhalb von Servicezeiten und Backup-Fenstern liegt. Somit kann die Deduplizierung ungestört durchgeführt werden, ohne sich als Störfaktor auf angeschlossene Dienste auszuwirken.

Nach dem erfolgreichen Einrichten der Deduplizierung und ihrem ersten Lauf können Sie sie per PowerShell abfragen, um festzustellen, wie effektiv die Deduplizierung auf dem ausgewählten Volume durchgeführt wurde. Nutzen Sie dazu das Cmdlet `Get-DedupStatus`:

```
PS C:\> Get-DedupStatus -Volume "E:"
FreeSpace    SavedSpace   OptimizedFiles     InPolicyFiles      Volume
---------    ----------   --------------     -------------      ------
125.04 GB    2.52 GB      9666               9666               E:
```

9.2 Neues mit Server Windows 2025

Microsoft hat mit Windows Server 2025 eine Reihe von Verbesserungen für das SMB-Protokoll eingeführt, die SMB-Shares sicherer machen sollen.

9.2.1 SMB über QUIC

Um die sichere Übertragung von Daten mittels des SMB-Protokolls an entfernte Systeme über eine unzuverlässige Verbindung (z. B. VPN) zu ermöglichen, hat Microsoft bereits in der *Windows Server 2022 Azure Edition* QUIC über SMB eingeführt. Nun findet dieses Feature auch seinen Weg in den Windows Server 2025.

Die Verbindung wird über UDP (Port 445) mittels TLS 1.3 authentifiziert und ermöglicht das Bündeln der zu übertragenden Daten aus verschiedenen Datenquellen in parallele Datenströme. Das QUIC-Protokoll sorgt für eine Staukontrolle und die Wiederherstellung von verlorenen Paketen während der Übertragung.

Sie steuern diese Funktion entweder über eine Gruppenrichtlinie und per PowerShell. Die Einstellung Enable SMB over QUIC finden Sie im Gruppenrichtlinien-Editor unter den folgenden Pfaden:

Computerkonfiguration\Administrative Vorlagen\Netzwerk\Lanman-Arbeitsstation

Computerkonfiguration\Administrative Vorlagen\Netzwerk\Lanman-Server

Per PowerShell aktivieren Sie das Feature so:

```
Set-SmbClientConfiguration -EnableSMBQUIC $true
```

Als weitere Absicherung können Sie *Client Access Control für SMB über QUIC* konfigurieren. Hierbei stellen Sie für die Clients, die Sie anbinden wollen, Zertifikate einer vertrauenswürdigen Zertifizierungsstelle aus. Die Hashwerte der Client-Zertifikate können Sie dann auf dem Zielsystem in einer Zugangsliste zusammenfassen. Nun vergleicht Ihr Server bei einer eingehenden SMB-über-QUIC-Verbindung das vom Client verwendete Zertifikat mit den Hashwerten aus der hinterlegten Zugangsliste und gibt die Verbindung nur dann frei, wenn der Hashwert des Zertifikats auf der Zugangsliste steht.

9.2.2 Verbesserte Verwaltung der SMB-Dialektkontrolle

Durch die verbesserte Kontrolle der SMB-Dialekte können Sie in Windows Server 2025 einzelne SMB-Protokollversionen blockieren. Dies hat erhebliche Auswirkungen auf die Kompatibilität Ihres Dateiservers mit angebundenen Betriebssystemen. Andererseits können Sie so die Performance Ihres Dateiservers verbessern und durch das Deaktivieren älterer und ungenutzter SMB-Versionen die Sicherheit Ihres Netzwerks verbessern.

Auf dem Server aktivieren Sie diese Funktion per PowerShell so:

```
Set-SmbServerConfiguration -Smb2DialectMax SMB311 -Smb2DialectMin SMB300
```

Auf der Client-Seite erfolgt die Konfiguration wie folgt:

```
Set-SmbClientConfiguration -Smb2DialectMax SMB311 -Smb2DialectMin SMB311
```

Zur Auswahl stehen folgende SMB-Protokolle:

- None
- SMB202
- SMB210
- SMB300
- SMB302
- SMB311

Alternativ können Sie dies auch per Gruppenrichtline konfigurieren. Die notwendigen Einstellungen für Maximale Version von SMB vorgeben sowie Mindestversion von SMB vorgeben finden Sie im Gruppenrichtlinien-Editor unter folgenden Pfaden:

Computerkonfiguration\Administrative Vorlagen\Netzwerk\Lanman-Server

Computerkonfiguration\Administrative Vorlagen\Netzwerk\Lanman-Arbeitsstation

9.2.3 NTLM für SMB deaktivieren

Kaum etwas verbessert die Sicherheit Ihrer Dateiserver so sehr wie das Abschalten alter Autorisierungsprotokolle. Im Windows Server 2025 können Sie nun auch NTLM über das SMB-Protokoll abschalten – falls keine Anwendung in Ihrem Netzwerk diese Option braucht.

Die Deaktivierung erfolgt einfach über die PowerShell:

```
Set-SmbClientConfiguration -DisableNTLM $true
```

Auch per Gruppenrichtlinie können Sie diese Einstellung verteilen. Die Einstellung NTLM blockieren (LM, NTLM, NTLMv2) finden Sie unter folgendem Pfad im Gruppenrichtlinien-Editor:

Computerkonfiguration\Administrative Vorlagen\Netzwerk\Lanman-Arbeitsstation

Sollten Sie Systeme haben, die Sie von dieser Einstellung ausnehmen wollen, können Sie eine Ausnahmeliste per Gruppenrichtlinie pflegen. Die Einstellung finden Sie im selben Pfad wie die Deaktivierung unter der Option NTLM-Serverausnahmeliste blockieren. Hinterlegen Sie die Systeme, die Sie ausnehmen wollen, Zeile für Zeile in der Ausnahmeliste. Geben Sie zu den Systemen auch ihren DNS-Namen, ihre IP-Adresse oder ihren NetBIOS-Namen an.

9.2.4 SMB-Authentifizierungsraten begrenzen

Mit dem SMB-Authentifizierungsratenbegrenzer hat Microsoft in Windows Server 2025 einen Mechanismus eingeführt, um unterschiedliche Brute-Force-, Credential-Stuffing- und Rainbow-Table-Angriffe einzuschränken. Bei solchen Angriffen werden Server im Sekunden-

takt mit unzähligen Benutzernamen und Passwortversuchen bombardiert, was zu erheblichen Performance-Einbrüchen und im schlimmsten Fall zur Kompromittierung eines Benutzerkontos führt.

Um solche Angriffe zu unterbinden, wird bei jedem fehlerhaften Versuch, der per NTLM oder PKU2U *(Public Key Cryptography Based User-to-User)* erfolgt, eine Verzögerung von 2 Sekunden zwischen jedem Anmeldeversuch erzwungen. Wenn ein Angreifer zwei Minuten lang 150 fehlschlagende Anmeldeversuche pro Sekunde durchführt, könnte er in dieser kurzen Zeit 18.000 Kombinationen ausprobieren. Durch die Anmeldeverzögerung wird für die gleiche Anzahl an Anmeldeversuchen ein Zeitraum von mehr als 10 Stunden benötigt – was für den Angreifer deutlich weniger attraktiv ist.

Diese Anmeldeverzögerung können Sie nach eigenen Bedürfnissen anpassen und eine individuelle Verzögerung konfigurieren:

```
Set-SmbServerConfiguration -InvalidAuthenticationDelayTimeInMs XX
```

Wenn Sie lieber per Gruppenrichtlinie arbeiten, schauen Sie sich die Option Begrenzer für Authentifizierungsrate aktivieren im Pfad *Computerkonfiguration\Verwaltungsvorlagen\Netzwerk\Lanman-Server* an.

Beachten Sie aber, dass per Gruppenrichtlinie lediglich diese Funktion ein- bzw. ausgeschaltet werden kann. Um das Intervall zu verändern, brauchen Sie die PowerShell.

9.2.5 SMB-Signierung als Standardeinstellung aktivieren

Microsoft empfiehlt schon seit geraumer Zeit, die SMB-Signierung zu aktivieren, um Relay-Angriffe zu vermeiden. Hierbei wird jede SMB-Nachricht mit einem Sitzungsschlüssel signiert, um Manipulationen zu verhindern. In Windows Server 2025 ist diese Option nun standardmäßig aktiviert. Dies gilt für alle Windows Server 2025- sowie Windows 11-Versionen außer den Home-Editionen.

9.2.6 Härtung der SMB-Firewall-Regeln

Windows Server 2025 verfügt standardmäßig über gehärtete SMB-Firewall-Regeln. Sie konfigurieren die Härtung über die PowerShell:

```
New-NetFirewallRule -DisplayName "SMB-Out" -Direction Outbound -Protocol TCP `
  -LocalPort 445 -Action Allow -Profile Domain
```

Für eingehende Verbindungen verwenden Sie das folgende PowerShell-Kommando:

```
New-NetFirewallRule -DisplayName "SMB-In" -Direction Inbound -Protocol TCP `
  -LocalPort 445 -Action Allow -Profile Domain
```

Für das flächendeckende Konfigurieren der SMB-Firewall-Regeln per Gruppenrichtlinie können Sie mithilfe des Gruppenrichtlinien-Editors unter den folgenden Pfaden die eingehenden und ausgehenden Regeln für die SMB-Härtung einstellen und an Ihre Anforderungen anpassen.

Die Firewall-Regeln finden Sie im Gruppenrichtlinien-Editor unter:

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit

9.3 Distributed File System (DFS)

Das *Distributed File System* (verteilte Dateisystem) kann bei der Bereitstellung zentraler sowie dezentraler Dateiserver eine erhebliche Erleichterung in Sachen Transparenz, Konfiguration und Hochverfügbarkeit bieten. Wir erläutern im Folgenden die beiden Verfahren *DFS-N (Distributed File System Namespace*) und *DFS-R (Distributed File System Replication)*.

9.3.1 DFS-N (Distributed File System Namespace)

Grundsätzlich wird bei *DFS-N* zwischen zwei Bereitstellungmodellen unterschieden: dem *domänenbasierten* und dem *eigenständigen DFS*. Im Grunde werden bei beiden Bereitstellungen die eingesetzten Dateiserver durch einen festgelegten Namespace maskiert. Der Benutzer sieht dadurch seine freigegebenen Ordner, braucht aber nicht zu wissen, auf welchem Server sie tatsächlich liegen. Dies bietet viele Vorteile:

- **persistente Pfade** – Die Freigabepfade sind für den Benutzer transparent und führen ihn immer auf den nächsten Server, der über die jeweilige Dateifreigabe verfügt. Dies ist unabhängig davon, welche und wie viele Dateiserver sich hinter dem gewählten Namespace verbergen. Der Pfad für den Benutzer bleibt immer identisch, was auch im Falle des Austauschs einzelner Server recht einfach kompensiert werden kann, ohne dass dies Auswirkungen auf die Verfügbarkeit der verwendeten Freigaben hat.
- **Teilen von Inhalten** – Durch das Speichern auf einer per DFS-N bereitgestellten Freigabe kann auf mehrere Server ohne räumliche Beschränkungen zugegriffen werden, wenn diese repliziert wurden. Somit können alle Benutzer über denselben *UNC*-Pfad *(Universal Naming Convention)* auf den jeweils nächsten Server zugreifen.
- **vereinfachte Konsolidierung** – Das Herauslösen alter Dateiserver stellt immer ein Problem dar. Denn meistens ist nicht bekannt, wer diesen Dateiserver verwendet und wer darüber informiert werden muss, dass sich der Name des Servers verändert hat bzw. verändern wird. Gerade in größeren Unternehmen ist dies häufig ein nicht zu bewältigendes Problem. Wenn diese Dateiserver jedoch im DFS-N eingebunden sind, ist der Austausch problemlos möglich, da die verwendeten UNC-Pfade sich im DFS-N nicht ändern.

Kapitel 17
Patchmanagement für Windows Server

Das Patchmanagement ist vergleichbar mit der Durchführung von Kleinreparaturen, wie dem Reparieren von klemmenden Fenstern oder Türen, die wegen einer Temperaturänderung immer wieder aufspringen: eigentlich alles kein großer Aufwand, aber die Menge macht das Patchen zu einer umfangreichen Aufgabe.

Patching – also das Beheben bekannter Sicherheitslücken und Bugs in der Software – stellt einen fundamentalen Bestandteil einer Sicherheitsstrategie dar. Denn nachweislich wurden bei etlichen Angriffen ältere Softwarelücken ausgenutzt, um ein System zu übernehmen. Inzwischen wird das Patching häufig auch verwendet, um zusätzliche Funktionen bereitzustellen.

17.1 Einführung

Der *Windows Server Update Service (WSUS)* bietet die Möglichkeit, die Microsoft-eigene Umgebung zu patchen. Im Folgenden geht es um die Planung, Konfiguration und den Betrieb einer auf der WSUS basierenden Patchmanagement-Lösung. Diese erfordert keine Ausgaben für Cloud-Dienste. Zum Abschluss wird noch die Update-Steuerung über Azure Update Manager eingeführt – als moderne Lösung für Systeme, die über Azure Arc verbunden sind.

17.1.1 Patching in der Windows-Welt

Spätestens der »I love you«-Virus aus dem Jahr 2000 und der Wurm »Code Red« von 2001 führten bei Microsoft zu der sicherlich frustrierenden Erkenntnis, dass die weite Verbreitung der eigenen Software auch das Schließen der in Software kaum vermeidbaren Sicherheitslücken erfordert. 2002 strebte Bill Gates an, die gesamte Industrie mit einer Selbstverpflichtung zum *Trustworthy Computing* (dt. »verlässliche IT-Nutzung«) anzuführen.

Bereits in Windows 98 gab es die Möglichkeit, die Microsoft-Update-Komponente zu installieren und auf der Clientseite nach verfügbaren Updates (Security und andere) für Windows, aber auch für Office und weitere Microsoft-Programme (wie Visual Studio und SQL) zu suchen.

Mit der Einführung des *Patch Tuesday* (Patch-Dienstags) erfolgte 2005 die nächste wichtige Änderung, die maßgeblich auf die Effizienz und Beherrschbarkeit im Unternehmensumfeld abzielte. Seither stellt Microsoft alle angefallenen und zur Veröffentlichung anstehenden Sicherheitsupdates an jedem zweiten Dienstag eines Monats gesammelt zur Verfügung. Der Patch Tuesday wird auch als »B«-Release bezeichnet. Am dritten und vierten Dienstag gibt es zusätzliche Vorschau-Funktionen im C- bzw. D-Release.

17.1.2 Die Geschichte von WSUS

WSUS geht auf den sogenannten *Server Update Service (SUS)* zurück, der Administratoren die Option gab, Updates auf Serversysteme auszurollen. Mit der Veröffentlichung von Windows Server 2003 R2 im Jahr 2005 wurde WSUS 2.0 zum Systembestandteil und löste somit SUS ab, der jedoch bis 2007 weiterhin unterstützt wurde.

Bereits in der ersten WSUS-Version gab es die Möglichkeit, den Update-Status von Computern sichtbar zu machen und auf Maschinenebene den Patchstand abzufragen. Seitdem arbeiten alle WSUS-Versionen mit einem Microsoft-Repository, das für jeden Patch einen Status hinterlegt, der pro Computergruppe unterschiedlich sein kann.

Jede Windows Server-Version erhielt auch eine neue WSUS-Version. Mit Windows Server 2016 kam die Version 5.0 heraus. Gemäß der Angabe in der WSUS-Administrationsoberfläche und der Versionsinformation in der Registrierung ist es bei Windows Server 2019 und den nachfolgenden Versionen jedoch Version 10.0. Von der Funktionalität und dem Erscheinungsbild her hat sich seit Windows Server 2012 R2 an WSUS nichts wesentlich verändert. Seit jeher besteht WSUS aus einer Datenbank, einem Repository und einer Steuerungsoberfläche.

17.1.3 Patch Tuesday

Der eben angesprochene *Patch Tuesday* ist traditionell der zweite Dienstag eines Monats. Diese Gesetzmäßigkeit wurde jedoch von Microsoft 2016 durch die Einführung des sogenannten *Servicing-Modells* und durch die konsequente Einführung von *kumulativen Rollups* aufgeweicht.

Es bleibt aber (mit wenigen Ausnahmen) bei der Veröffentlichung an einem Dienstag. Dieser Dienstag kann jedoch der zweite (B-Veröffentlichung), dritte (C-Veröffentlichung) oder vierte Dienstag (D-Veröffentlichung) eines Monats sein. Sowohl die C- als auch die D-Veröffentlichungen enthalten allerdings keine sicherheitsrelevanten Updates, sondern lediglich Vorschau-Updates für den funktionalen Anteil des nächsten B-Updates.

Für den Systemadministrator gibt es also folgende Phasen:

Woche	Geplante Veröffentlichung
A (ab 1. Dienstag)	Nur für schwerwiegende Zero-Day-Lücken
B (ab 2. Dienstag)	Reguläres Rollup (Sicherheit und Funktion)
C (ab 3. Dienstag)	Vorschau auf Funktionsupdates
D (ab 4. Dienstag)	Vorschau auf Funktionsupdates (optional)

Tabelle 17.1 Phasen der Microsoft-Updates

Diese Update-Steuerung gilt für das Basisbetriebssystem, also für alle unterstützten Betriebssysteme seit Windows 7 SP1 und Windows Server 2008 R2 SP1, sowie für das .NET Framework. Andere Produkte werden nur noch mittels einzelner Patches bedient. Das heißt, es gibt für diese keine kumulativen Patch-Pakete mehr.

Zunächst waren die Vorschau-Updates lediglich für Woche C geplant, inzwischen erscheinen sie allerdings auch in Woche D. Wobei dies nicht für jeden Monat gilt. In diesen Wochen können Unternehmen Updates zur Prüfung von kritischen Anwendungen ausrollen und in Pilotgruppen testen.

Im monatlichen Patch-Paket sind also die aktuellen Sicherheitsupdates und die in der Vorschau getesteten Funktionsupdates des Vormonats enthalten.

In nicht mehr unterstützten Windows-Versionen gab es noch leicht abweichende Patch-Regeln: Hier gab es bis zum Ende des Lebenszyklus die Option, auf funktionale Updates zu verzichten und sogenannte *Security-Only-Updates* zu installieren. Dies ist für Windows Server 2025 und die anderen unterstützten Server-Systeme nicht mehr möglich.

17.1.4 Best Practices für das Patching

Zwei grundlegende Faktoren sind in Bezug auf die Best Practices zum Thema Patching zu nennen und praktisch umzusetzen: *Geschwindigkeit* und *Stabilität*.

Geschwindigkeit

Sobald ein Patch veröffentlicht wird, lässt sich die Schwachstelle leicht erkunden. Auf Basis der Beschreibung, aber vor allem durch die Veränderungen an Systemdateien lassen sich Lücken und Probleme nachvollziehen. Daher wird die Schwachstelle kurz nach der Veröffentlichung des Patchs in der Regel in Schadsoftware eingebaut, um nicht gepatchte Systeme möglichst effektiv anzugreifen. Einige Studien zeigen, dass nicht gepatchte Systeme eines der häufigsten Einfallstore für gezielte Angriffe sind. Das gilt natürlich nicht nur für Windows-

bzw. Microsoft-Patches, sondern auch für Patches aller auf dem System eingesetzten Anwendungen. Daher sollten Sie alle Patches so schnell wie möglich direkt installieren.

Während funktionale Updates aus der Woche C oder D für alle Kunden bereitstehen, werden Security-Updates nur einem kleinen Kundenkreis vorab zur Verfügung gestellt, um die Kenntnis von Schwachstellen nicht unnötig zu verbreiten.

Im sogenannten *Security Update Validation Program (SUVP)* werden ausgewählten Kunden (ihre genaue Anzahl ist nicht bekannt) die Security-Updates des folgenden Patch Tuesdays bereitgestellt, um diese ca. drei Wochen vor dem Release in realen Umgebungen zu testen. Die Teilnahme am SUVP erfolgt nur nach ausführlicher Prüfung, der Unterzeichnung verschiedener Verträge und der Freigabe durch Microsoft. Die genauen Auswahlkriterien sind ebenso wie die Namen der teilnehmenden Unternehmen nicht öffentlich.

Vorgesehen ist auch hier keine flächendeckende Installation, sondern die Installation in Qualitätssicherungsumgebungen oder Testumgebungen. Die Updates wurden in der Vergangenheit für WSUS bereitgestellt.

In der Realität muss geprüft werden, wie schnell Updates in einem Windows-Netzwerk überhaupt verteilt werden können. Dafür gibt es organisatorische und technische Grenzen: Beispielsweise sind in Unternehmen, in denen viele Außendienstmitarbeiter nur eine schlechte Verbindung zum Firmennetz haben, andere Mechanismen notwendig als in Unternehmen, in denen alle Mitarbeiter ihre Arbeit an einem zentralen Standort durchführen. Zunehmend ist das Konnektivitätsproblem jedoch keine echte Herausforderung mehr; allerdings gibt es weiterhin Länder mit eingeschränkter und begrenzter mobiler Konnektivität. Außerdem müssen die Bearbeitung von Updates und der Umgang mit möglichen Ausfällen oder Störungen eingeplant werden.

Wir empfehlen Ihnen, die Microsoft-E-Mails zur Veröffentlichung von Updates auf der Microsoft-Website des *Microsoft Security Response Center* zu abonnieren:

https://www.microsoft.com/en-us/msrc/technical-security-notifications

Dadurch stellen Sie sicher, alle Informationen, Updates und neuen Versionen (Revisionen) von Updates zu erhalten. Das ist besonders hilfreich für außerplanmäßige Updates, die sich nicht an die Veröffentlichungsfrequenz halten.

Wir empfehlen Ihnen zudem, klare Update-Ziele und Kennzahlen zu definieren. Diese können beispielsweise darin bestehen, 99 % der Systeme innerhalb von zwei Wochen auf 100 % Patch-Installation zu bekommen. Anhand dieser Ziele sollten Sie die Abläufe planen und technische Vorkehrungen treffen.

Ein Ablauf könnte folgendermaßen aussehen (siehe auch Tabelle 17.2): Tag 1 bezeichnet den Tag der Veröffentlichung von Updates (zweiter Dienstag im Monat). Alle anderen Update-Veröffentlichungen sind für Testzwecke, also nicht für eine vollständige Installation vorgesehen. Es sei denn, es existieren Probleme, die mit einem dieser Preview-Updates behoben werden.

Sie sollten für Ihre Umgebung einen vergleichbaren Plan aufstellen. Versuchen Sie, möglichst alle Faktoren zu bedenken:

- Wie wichtig ist das zeitnahe Einspielen der Updates?
- Wie schnell können Sie reagieren?
- Wie ausführlich müssen Updates geplant werden?

Zeitpunkt	Status vonseiten Microsofts	Administrator-Tätigkeit
Tag 1	Eine Update-Benachrichtigung wird verschickt.	Sichtung der Unterlagen
Tag 1	Die Updates werden veröffentlicht (in der Regel am späten Dienstagabend).	Verifizierung der Verfügbarkeit von Updates
Tag 2	Die Updates stehen zur Installation bereit.	Vorbereitung des Deployments, Test auf ausgewählten Systemen
Tag 3	Die Updates stehen zur Installation bereit.	Ausweitung der Tests und Freigabe für die übrigen Systeme
Tag 4–14	Die Updates stehen zur Installation bereit.	Installation auf allen Systemen in verschiedenen Phasen (Redundanzen beachten!)
Tag 15	Die Updates stehen zur Installation bereit.	Installationsstatus prüfen, Fehler in Update-Vorgängen beheben und letzte Systeme updaten
Tag 16	Die Updates stehen zur Installation bereit.	Report erstellen, eventuell vorhandene Dokumentation aktualisieren

Tabelle 17.2 Beispielhafter Ablauf eines Patchmanagements

Der Ablauf aus Tabelle 17.2 ermöglicht es Ihnen, in gut zwei Wochen alle Systeme auf den aktuellen Stand zu bringen und dies zu dokumentieren. WSUS erleichtert diesen Kraftakt, indem es dafür sorgt, dass Administratoren ein solches System mit beherrschbarem Aufwand umsetzen können.

Stabilität

Der zweite angesprochene Punkt ist die *Stabilität*. Es hat sich immer wieder gezeigt, dass Updates auch negative Effekte auf die Stabilität haben können. Idealerweise prüfen Sie das Update zunächst in einer gesonderten Testumgebung und spielen den Patch erst aus, wenn Sie sich sicher sind, dass er keine Probleme macht. In der Realität ist dies allerdings kaum

praktikabel. Sie brauchen daher einen Notfallplan, falls ein Update wirklich einmal Ärger bereitet. Daher benötigen Sie neben dem Standardplan auch einen Plan für die eventuelle Rücknahme eines Patchs.

17.1.5 Begriffe im Microsoft Update-Umfeld

Um die folgenden Abschnitte verständlich zu gestalten, führen wir an dieser Stelle die für WSUS und die Microsoft Update-Welt spezifischen Begriffe ein und erläutern diese.

Definitionen

Die offizielle Microsoft-Dokumentation zu diesen Begriffen finden Sie unter:

- *https://support.microsoft.com/en-us/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro*
- *https://docs.microsoft.com/de-de/sccm/sum/get-started/configure-classifications-and-products*

Unterschiede zwischen Microsoft Update, Windows Update und WSUS

Microsoft Update bezeichnet die Online-Update-Funktionalität von Microsoft, die vom Windows Update-Client in den jeweiligen Betriebssystemen angesprochen werden kann. Microsoft Update wird als Online-Dienst bereitgestellt und kann von jedem mit dem Internet verbundenen und aktivierten Windows-Computer uneingeschränkt verwendet werden.

Über *Windows Update* lassen sich Produkte von Microsoft und anderen Herstellern (beispielsweise Adobe Flash Player) aktualisieren, deren Updates über Microsoft Update bereitgestellt werden.

Der *Windows Server Update Service (WSUS)* hingegen ist eine Rolle auf Servern, die seit Windows Server 2003 R2 regelmäßig erneuert wird und im Basisbetriebssystem ohne zusätzliche Lizenzkosten verwendet werden kann. Mit WSUS werden Updates heruntergeladen, gesteuert und zur zentralen Verteilung in einem Unternehmensnetzwerk bereitgestellt. WSUS unterstützt hierbei standardmäßig ausschließlich Microsoft-Produkte. Der Client verwendet beim Download der Updates vom WSUS-Server das Windows Update.

Der *Azure Update Manager* (siehe Abschnitt 17.6) ist die aktuelle Azure-basierte Update-Orchestrierungslösung, die für Microsoft-basierte Betriebssysteme und weitere Betriebssysteme genutzt werden kann. Sie erfordert eine Integration der Server-Systeme in Azure Arc.

Produkte

Als *Produkte* werden im WSUS-Umfeld die verschiedenen Software-Angebote von Microsoft bezeichnet. Durch die Option lässt sich steuern, welche Updates im Netzwerk angeboten werden. Ein Produkt ist beispielsweise eine Windows-Version wie Windows Server 2019, aber

auch eine Programmversion von Microsoft SQL oder Microsoft Office. Mittels WSUS können Sie ebenso die über Windows Update angebotenen Treiber (z. B. Windows Server-Treiber) und Zusatzprodukte (z. B. Windows Defender) installieren.

Klassifizierungen

Klassifizierungen beschreiben die verschiedenen Typen von Aktualisierungspaketen, die für ein Produkt bereitstehen. Sie folgen einer bestimmten Nomenklatur (die Reihenfolge der Auflistung entspricht dem Auftreten in der WSUS-Konfigurationsoberfläche):

- **Definitionsupdates** – Definitionsupdates sind freigegebene Aktualisierungen für eine Definitionsdatenbank eines Produkts. Bekannt sind sie z. B. von Virenscannern, die mit diesen Definitionen schadhafte Codebestandteile oder andere Attribute erkennen können.
- **Feature Packs** – Neue Produktfunktionalitäten werden zunächst als Feature Pack, später als Teil eines vollständigen Produkt-Releases veröffentlicht oder ergänzen ein bestehendes Produkt.
- **Schnellinstallationsdateien** – Schnellinstallationsdateien sind *Delta-Updates*. Kumulative Updates enthalten häufig Inhalte, die bereits in einem vorangegangenen Update enthalten waren und deswegen auf Clientseite möglicherweise schon vorhanden sind. Mit Schnellinstallationsdateien werden mehr Daten auf dem WSUS-Server generiert (für jede Möglichkeit), allerdings wird der Download-Traffic für den Client stark reduziert. Im Azure Update Manager steht dies nicht zur Verfügung.
- **Service Packs** – Ein getestetes, kumulatives Update-Paket, das aus Hotfixes, Sicherheitsupdates, kritischen Updates und Updates besteht, wurde bislang als *Service Pack* bezeichnet. In der Regel wurden mit diesem auch Designveränderungen und weitere Änderungen durchgeführt. Neue Windows-Versionen erhalten keine Service Packs mehr.
- **Sicherheitsupdates** – Ein Sicherheitsupdate ist ein allgemein veröffentlichtes Update, um eine produktspezifische sicherheitsrelevante Verwundbarkeit zu beheben oder einzuschränken. Sicherheitsupdates werden nach der Kritikalität eingestuft.
- **Tools** – Mit Tools sind kleine Hilfsprogramme gemeint, mit denen sich administrative Aufgaben leicht erledigen lassen. Bisher wurden Tools zum Entfernen schädlicher Programmteile verteilt.
- **Treiber** – Ein Treiber ist Software, die das Verhalten eines Geräts kontrolliert. Im Azure Update Manager steht diese Option nicht zur Verfügung.
- **Treibersätze** – Treibersätze oder *Treiberpakete* enthalten gesammelt mehrere Treiberaktualisierungen in einem Update, etwa für ein Microsoft Surface. Im Azure Update Manager steht diese Option nicht zur Verfügung.
- **Update-Rollups** – Ein Update-Rollup ist eine getestete, kumulative Sammlung von Hotfixes, Sicherheitsupdates, kritischen Updates und Updates, die zur einfachen Verteilung in einem Paket gebündelt wurden.

- **Updates** – Ein Update ändert ein einzelnes Feature oder Verhalten, um ein Problem zu beheben.
- **Upgrades** – Upgrades ist eine Kategorie für Windows 10-Features und -Funktionalitäten. Damit sind Pakete gemeint, die es Ihnen ermöglichen, von einer Windows 10-Version auf die nächste zu kommen. Dies existiert seit WSUS-Version 4.0 mit Hotfix 3095113. Im Azure Update Manager steht dies Option nicht zur Verfügung.
- **Wichtige Updates** – Dies sind kritische, getestete Updates, mit denen ein oder mehrere wichtige, nicht sicherheitsrelevante Fehler behoben werden.

17.2 Eine WSUS-Installation planen

Bevor Sie eine WSUS-Installation in Ihrer Infrastruktur beginnen, sollten Sie sich Gedanken über die Planung machen.

17.2.1 Systemvoraussetzungen

Ein WSUS-Server ist vor allem mit der Steuerung und der Auslieferung von Updates beschäftigt. Er hat daher einen hohen Bedarf an Bandbreite und muss große Speicherreserven für die Updates vorhalten, die er zur Verfügung stellt. Dies gilt jedoch nur, wenn die Updates zentral vom WSUS-Server ausgeliefert werden.

Die offizielle Dokumentation von Microsoft spricht auch heutzutage noch von 40 GB Speicher. Die allgemeinen Systemvoraussetzungen von Microsoft (unabhängig von der Rolle, die der WSUS-Server einnimmt) finden Sie im Kasten.

Systemvoraussetzungen

Hardware (virtuell oder physisch):

- 1,4-GHz-CPU (Eine 2-GHz-CPU oder schneller wird empfohlen.)
- 2 + 2 GB RAM (2 GB für Windows Server 2019 mit Desktop Experience und 2 GB für WSUS)
- Netzwerkadapter mit 100 Mbit/s
- 40 GB Speicher für WSUS

Software:

- Microsoft Report Viewer Runtime 2012
- SQL SYS CLR-Types für SQL Server 2012
- .NET Framework

Berechtigungen:

- lokale Administrationsrechte auf dem für WSUS vorgesehenen Computer

- Sie müssen zum Erstellen bzw. Ändern einer GPO berechtigt sein, falls Sie Updates zentral steuern wollen.
- Alternativ müssen Sie lokale Policys auf Systemen erstellen können, die Updates von WSUS erhalten sollen. Dies ist jedoch nicht empfohlen bzw. nur für Umkreisnetzwerk-Systeme empfohlen, die nicht Teil der Domäne sind.

Die oben genannten Mindestanforderungen an die Hardware sind jedoch in keiner Weise realistisch: Bei einem Single-CPU-Deployment mit diesem Arbeitsspeicher kommt es zu starken Performance-Einbußen und Timeouts der Services aufgrund von verlängerten Antwortzeiten der Datenbank. Eine Netzwerkbereitstellung mit 100 Mbit/s ist ebenfalls nicht empfehlenswert, da dies zu einer verzögerten Übertragung an die Clients führen wird. Außerdem ist die geplante Festplattengröße zu gering: Bereits Updates, die innerhalb von zwei Monaten erscheinen und nur für eine Windows Server-Version sowie .NET gelten, bewegen sich in der Größenordnung von 1 bis 2 GB (ohne Schnellinstallationsdateien). Je nach ausgewählten Produkten und Sprachen sowie Typen von Updates können auch mehrere Hundert Gigabyte anfallen. Rechnen Sie also bei allen Microsoft-Vorgaben deutlich großzügiger, und planen Sie besonders beim Festplattenplatz mit deutlich mehr Bedarf.

17.2.2 Bereitstellungsoptionen

Mit WSUS können Sie verschiedene Anforderungen erfüllen. Während wir uns im weiteren Verlauf des Kapitels vor allem mit den Konfigurationen eines einzelnen WSUS-Servers beschäftigen, sind die verschiedenen Bereitstellungsoptionen die Chance für einen weiteren Ausbau. Prüfen Sie, was für Ihre Umgebung am sinnvollsten ist: eine WSUS-Konfiguration als Einzelserver, ein hierarchischer Aufbau oder ein WSUS-Server, der vom Netzwerk getrennt ist.

WSUS-Deployment als Einzelserver

In einem WSUS-Deployment als Einzelserver wird der WSUS-Server über das Internet mit Microsoft Update verbunden, und alle Clients (dies können Server oder Windows-Clients sein) verbinden sich mit dem WSUS-Server (siehe Abbildung 17.1).

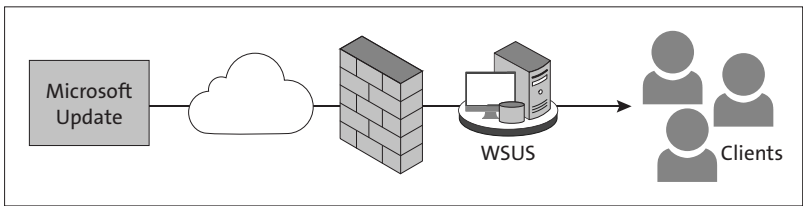

Abbildung 17.1 Einzelbereitstellung

Um den WSUS-Server mit dem Internet zu verbinden, sind einige URLs notwendig, die wir im folgenden Kasten gesammelt haben. Sie müssen dafür sorgen, dass sie erreichbar sind und nicht durch Ihre Firewalls geblockt werden.

Notwendige URLs für Windows Update

- *http://windowsupdate.microsoft.com*
- *http://*.windowsupdate.microsoft.com*
- *https://*.windowsupdate.microsoft.com*
- *http://*.update.microsoft.com*
- *https://*.update.microsoft.com*
- *http://*.windowsupdate.com*
- *http://download.windowsupdate.com*
- *http://download.microsoft.com*
- *http://*.download.windowsupdate.com*
- *http://test.stats.update.microsoft.com*
- *http://ntservicepack.microsoft.com*

Ein einzelner WSUS-Server kann verschiedene Computergruppen steuern. Um unterschiedliche Computer unterschiedlich zu behandeln, sind also nicht mehrere WSUS-Server notwendig (siehe Abbildung 17.2).

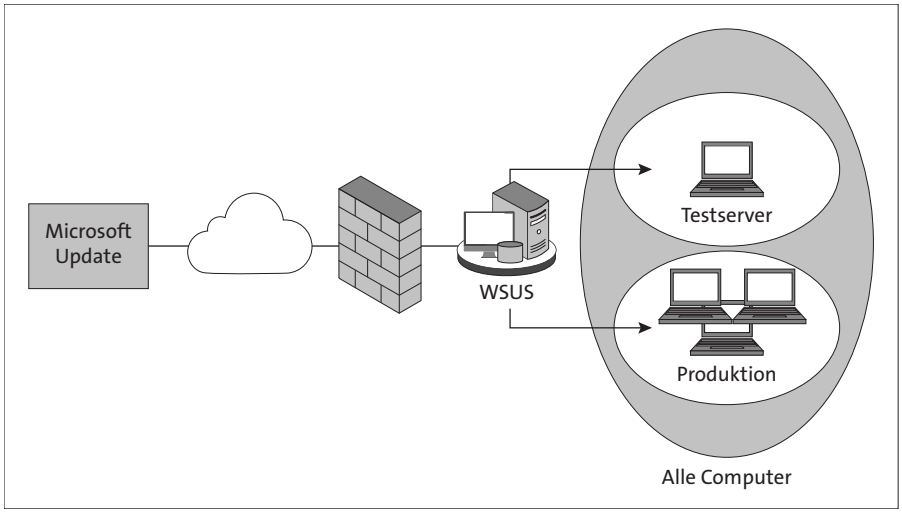

Abbildung 17.2 Single-WSUS-Server mit verschiedenen Computergruppen

Alle Clients, die für den WSUS-Server vorgesehen sind, bilden zusammen die Gruppe *Alle Computer*. Darunter können verschiedene Gruppen auf mehreren Ebenen angelegt werden.

Vom Netzwerk getrennter WSUS-Server

Der vom Netzwerk getrennte WSUS-Server unterstützt Szenarien, in denen keine Internetverbindung besteht. Dies ist für einige Umgebungen der Fall, in denen aufgrund von Sicherheitsanforderungen oder wegen Auflagen einer Regulierungsbehörde der Internetzugang vollständig unterbleiben muss oder schlicht nicht möglich ist.

Für diese Art von WSUS-Aufbau sind mindestens zwei WSUS-Server notwendig. Dabei fungiert einer als Download- und Export-Server, der andere als Import- und echter Update-Server.

Aufgaben des Download- und Export-Servers	Aufgaben des Import-Servers
▸ Verbindung zum Internet herstellen ▸ Download der Updates ▸ Bereitstellung der Updates ▸ Bereitstellung der Meta-Daten	▸ Import der Updates ▸ Import der Meta-Daten ▸ Reporting

Die operative Umsetzung des Exports und Imports erläutern wir im Verlauf dieses Kapitels.

WSUS-Server-Hierarchie

WSUS-Server können in einer Hierarchie angeordnet werden. Dadurch wird ein mehrfacher Download von Microsoft Updates verhindert. Dies ist vor allem in Umgebungen mit einer schmalbandigen Internetanbindung eine sinnvolle Konfiguration.

Die Idee dahinter ist, dass der Downstreamserver sehr nah an den zu versorgenden Clientcomputern steht, um einen mehrfachen Download von Updates über eine langsame WAN-Leitung zu vermeiden. Außerdem können Downstreamserver so eingerichtet werden, dass sie unterschiedliche Spracheinstellungen unterstützen.

Unterstützt werden Hierarchien mit bis zu drei Stufen (siehe Abbildung 17.3).

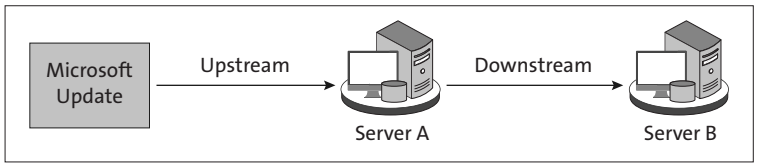

Abbildung 17.3 Upstream- und Downstreamserver

In einer WSUS-Hierarchie können die Server in zwei verschiedenen Betriebsmodellen benutzt werden. Einer sorgt für eine zentrale Administration *(Replikatserver)*, der andere für eine verteilte Administration *(autonomer Downstreamserver)*.

Der größte Unterschied ist der Anteil an Informationen, der von einem WSUS-Server mit dem anderen geteilt wird.

17.2.3 Installationsoptionen

Ein WSUS-Server kann auf unterschiedliche Weise und mit unterschiedlichen Optionen installiert werden.

Sie müssen die grundlegende Entscheidung treffen, ob Sie mit der internen Datenbank (*Windows Internal Database*, *WID*, seit Windows Server 2012) oder mit einer (separat zu lizenzierenden) SQL-Datenbank arbeiten möchten. Für den Beginn empfiehlt es sich zu testen, ob die Performance und die Benutzerfreundlichkeit der WID für Sie ausreichen, denn eine Migration auf eine SQL-Datenbank ist später ohne Probleme möglich. Die Datenbank enthält ausschließlich Meta-Informationen:

- WSUS-Server-Konfigurationsinformationen
- Meta-Daten zu jedem Update
- Informationen über Clientcomputer, Updates und Interaktionen (z. B. über den Updatestatus)

Die interne Windows-Datenbank (WID)

- WSUS erzeugt bei der Installation eine SQL-Instanz mit dem Namen `MSSQL$MICROSOFT##WID`.
- Der zuständige Dienst ist nicht *SQL Server*, sondern *WID*.
- Die Datenbank wird unter *%windir%\wid\data* gespeichert. In den meisten Fällen ist das *C:\Windows\wid\data*.
- Die Datenbankdatei heißt *SUSDB.mdf*.
- Wenn Sie nicht die *Windows Server-Sicherung* benutzen, dann müssen Sie im Rahmen von Backups darauf achten, dass eine Sicherungsvariante genutzt wird, die mit der Datenbank kompatibel ist.

Weitere Informationen zur Planung einer WSUS-Installation finden Sie unter:

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-deployment#BKMK_1.1

17.3 Installation und Konfiguration von WSUS-Server

In diesem Abschnitt beschäftigen wir uns mit der Installation und der Konfiguration der Rolle *WSUS-Server*. Dabei gehen wir davon aus, dass ein Server existiert, der Mitglied der Domäne ist und die in Abschnitt 17.2.1 beschriebenen Systemvoraussetzungen erfüllt. Ein WSUS-Server kann auch als Server einer Workgroup betrieben werden.

19.6 Absichern des Zugriffs auf Netzwerkgeräte über das RADIUS-Protokoll

Außer zum Zugriff auf das Netzwerk selbst kann ein NPS auch dazu verwendet werden, um die Authentifizierungen an den Netzwerkkomponenten, z. B. Switches und Routern, zentral zu steuern und dadurch einfach zu protokollieren. Für den normalen Betrieb und die Administration werden keine lokalen Konten auf den Netzwerkkomponenten benötigt, sondern es werden Benutzer (Administratorkonten) aus dem Active Directory verwendet.

Wir möchten dieses Vorgehen und die Konfiguration anhand eines *Cisco 3560*-Switchs beschreiben. Die Konfiguration und die Funktion können bei anderen Modellen abweichen. Prüfen Sie hierzu die Dokumentation des Geräts. Andere Hersteller bieten allerdings gleiche oder zumindest sehr ähnliche Optionen, um die Administration der Geräte abzusichern.

Der Hauptvorteil einer Authentifizierung über einen NPS (RADIUS) besteht darin, dass auf den Geräten keine zusätzlichen Benutzer angelegt werden müssen, wodurch die Kennwortpflege dieser Konten deutlich vereinfacht wird.

Genau wie bei der Konfiguration der Switches für 802.1x sollten Sie auch hier die Konfiguration Schritt für Schritt erstellen und jeden einzelnen Schritt prüfen, um mögliche Fehler schnell erkennen zu können.

19.6.1 RADIUS-Server für die Authentifizierung konfigurieren

Im ersten Schritt muss der Switch so konfiguriert werden, dass er bei Verbindungen über Telnet oder SSH einen RADIUS-Server für die Authentifizierung verwendet.

In Listing 19.6 finden Sie den relevanten Auszug aus der Konfiguration (`sh run`):

```
!
username cisco privilege 15 password 0 cisco
aaa new-model
!
aaa group server radius NPS
 server 192.168.1.84 auth-port 1812 acct-port 1813
!
aaa authentication login userAuthentication local group NPS
aaa authorization exec userAuthorization local group NPS if-authenticated
aaa authorization network userAuthorization local group NPS
aaa accounting exec default start-stop group NPS
aaa accounting system default start-stop group NPS
!
aaa session-id common
```

Listing 19.6 Konfiguration des lokalen »Notfallkontos« und Festlegen der AAA-Konfiguration

Listing 19.6 beschreibt die Konfiguration eines lokalen Kontos mit `privilege 15`-Rechten (also höchsten Rechten). Dadurch ist es möglich, auf das System zuzugreifen, sollte eine zentrale Anmeldung nicht möglich sein. Hier sollte natürlich ein komplexes Kennwort hinterlegt werden, das verschlüsselt gespeichert werden muss.

Nun wird eine Servergruppe mit dem Namen `NPS` unterhalb von `aaa` *(Authentication/Authorization/Accounting)* angelegt und dort ein Server mit der IP-Adresse 192.168.1.84 hinterlegt, was der IP-Adresse des NPS-Servers entspricht. Die verwendeten Ports können bei Bedarf angepasst werden. Windows-Systeme verwenden standardmäßig Port 1812 (Authentication) und 1813 (Accounting). Die Standard-Cisco-Ports sind 1645 und 1646.

```
ip radius source-interface FastEthernet0/23
!
radius-server host 192.168.1.84 key secret12key
radius-server host 192.168.1.84 auth-port 1812 acct-port 1813 key secret12key
!
line con 0
line vty 0 4
 authorization exec userAuthorization
 login authentication userAuthentication
 transport input telnet ssh
line vty 5 15
 authorization exec userAuthorization
 login authentication userAuthentication
 transport input telnet ssh
```

Listing 19.7 Konfiguration der unterschiedlichen Schnittstellen für die Verwaltung

`line con 0` ist der Konsolenanschluss des Switchs. Dieser ist in unserem Beispiel ohne zusätzliche Authentifizierung zugänglich. `line vty 0 4` ist für den Zugriff über Telnet oder SSH aktiviert und ist für die Privilege-Level 0 bis 4 vorgesehen. Dieser Zugang soll für die Benutzer vorgesehen sein, die nicht die vollen administrativen Rechte auf dem System besitzen. Hier wird definiert, dass dieser Zugang über eine Authentifizierung und Autorisierung erfolgen muss. `line vty 5 15` ist der Telnet- bzw. SSH-Zugang mit den höheren Rechten.

Die konkrete Steuerung, wer welchen Level an Privilegien bekommt, kann später auf dem NPS-Server über Windows-Gruppen erfolgen. Zusätzlich wird in diesem Abschnitt noch definiert, welche Schnittstelle des Switchs für die Kommunikation mit dem NPS verwendet wird.

Separate Netzwerke möglich

Sie können für die Kommunikation des Switchs mit dem NPS-Server separate Netzwerkverbindungen verwenden, um den Datenverkehr der Netzwerkwerkgeräte vom normalen Netzwerkverkehr zu trennen. Dazu können Sie dem NPS-Server eine zweite Netzwerkschnittstelle zuweisen, die dann für den Authentifizierungsverkehr verwendet wird.

Nachdem die Konfiguration abgeschlossen ist, können Sie einen Zugriff auf den Switch – z. B. per PuTTY – versuchen (siehe Abbildung 19.109).

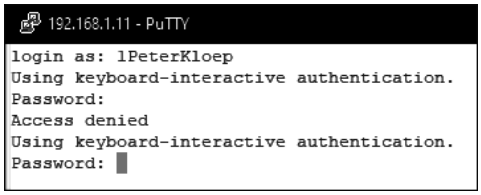

Abbildung 19.109 Fehlgeschlagene Authentifizierung bei der Verwendung des NPS-Servers über PuTTY

Verbindet sich nun ein Administrator – in diesem Fall der Benutzer *1PeterKloep* aus der Domäne des NPS-Servers (`intranet.rheinwerk-verlag.de`) –, wird die Authentifizierung nicht erfolgreich sein. PuTTY wird immer wieder nach dem (richtigen) Kennwort fragen, bevor nach einigen Versuchen die Verbindung getrennt wird.

Wenn Sie nun auf den NPS wechseln, werden Sie in der Ereignisanzeige unter Benutzerdefinierte Ansichten • Serverrollen • Netzwerkrichtlinien- und Zugriffsdienste die Protokolle finden. Hier wird ein Ereignis mit der ID 13 und der Quelle NPS registriert (siehe Abbildung 19.110).

Der Eintrag besagt, dass ein nicht bekannter RADIUS-Client (Switch) eine RADIUS-Meldung an den NPS-Server gesendet hat. Damit ist belegt, dass der Switch die Authentifizierungsanforderung an den NPS-Server weitergeleitet hat. Eine Kommunikation zwischen Switch und Server besteht also, und keine Firewall-Regel stört die Kommunikation. Sollte der Eintrag nicht erstellt werden, müssen Sie die Verbindung zwischen dem Switch und dem NPS-Server prüfen.

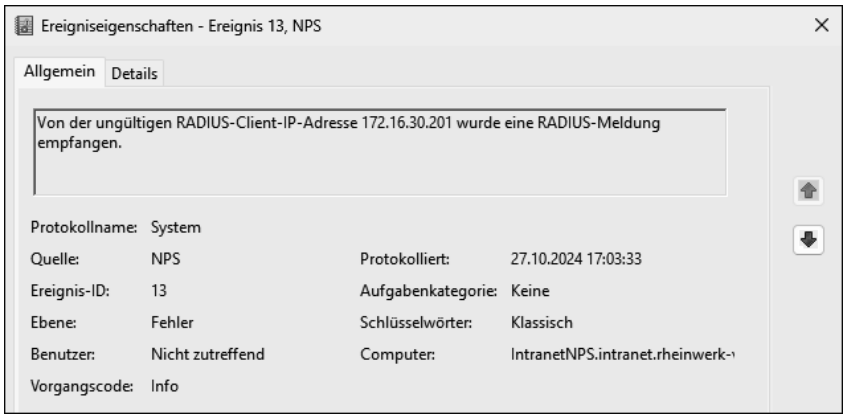

Abbildung 19.110 Ereignisprotokoll-Eintrag zu dem unbekannten RADIUS-Client

19.6.2 Definition des RADIUS-Clients

Der nächste Schritt der Konfiguration ist die Definition des RADIUS-Clients. Wechseln Sie dazu in der NPS-Verwaltungskonsole des NPS-Servers zum Knotenpunkt NPS (LOKAL) • RADIUS-CLIENTS, und erstellen Sie einen neuen Eintrag. Klicken Sie dazu mit der rechten Maustaste auf RADIUS-CLIENTS, und wählen Sie die Option NEU.

In dem Fenster, das sich nun öffnet, definieren Sie folgende Werte:

- ANZEIGENAME – Hier sollte ein »sprechender« Name verwendet werden. Dieser kann später beim Erstellen der Regeln als Abfragewert benutzt werden.
- ADRESSE (IP ODER DNS) – Hier legen Sie entweder die IP-Adresse oder den DNS-Namen des RADIUS-Clients fest.
- GEMEINSAMER GEHEIMER SCHLÜSSEL – Tragen Sie hier das Kennwort aus Listing 19.7 ein.

Wechseln Sie im Anschluss auf die Registerkarte ERWEITERT, und wählen Sie als Herstellername CISCO aus (siehe Abbildung 19.111). Bestätigen Sie die Einstellungen mit OK.

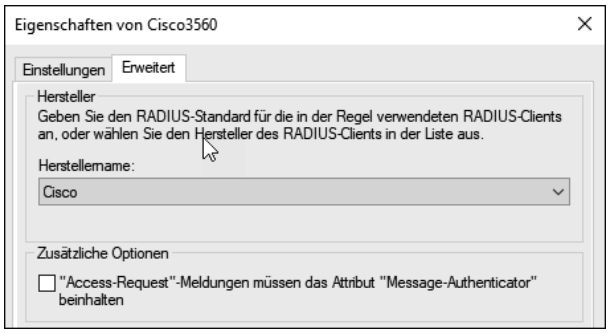

Abbildung 19.111 Den Herstellernamen des RADIUS-Clients festlegen

Durch die Definition des Herstellernamens werden Zusatzfunktionen des jeweiligen Herstellers aktiviert und ausgewertet. Sie können die Einstellungen nachträglich prüfen und anpassen (siehe Abbildung 19.112).

Nachdem nun der RADIUS-Client definiert wurde, versuchen Sie erneut, über PuTTY eine Verbindung zum Switch herzustellen. Dieser Verbindungsversuch wird mit der gleichen Meldung fehlschlagen. Auch dieser Fehler ist zu diesem Zeitpunkt zu erwarten.

Wenn Sie nun die Ereignisanzeige des NPS-Servers prüfen, werden Sie einen Ereignisprotokolleintrag mit der ID 6273 und der Quelle MICROSOFT WINDOWS SECURITY finden. Beachten Sie, dass dieser Eintrag als INFORMATION klassifiziert ist und nicht als Warnung oder Fehler (siehe Abbildung 19.113).

Abbildung 19.112 Konfiguration des RADIUS-Clients

Abbildung 19.113 Ereignisanzeige-Eintrag über eine abgelehnte Authentifizierung

Listing 19.8 zeigt einen Auszug der einzelnen Abschnitte des Ereignisses, in denen die relevanten Informationen protokolliert werden. Dadurch kann der Grund der verweigerten Anmeldung schnell ermittelt werden:

```
Der Netzwerkrichtlinienserver hat einem Benutzer den Zugriff verweigert.

Wenden Sie sich an den Administrator des Netzwerkrichtlinienservers, um weitere
Informationen zu erhalten.

Benutzer:
    Sicherheits-ID:    intranet\1PeterKloep
    Kontoname:         1PeterKloep
    Kontodomäne:       INTRANET
    Vollqualifizierter Kontoname:    intranet.rheinwerk-verlag.de/Netzwerk/
                                     Administratoren/1PeterKloep
```

Listing 19.8 Ergebnis der Authentifizierung und Beschreibung des Kontos

Bei der Verwendung von PuTTY muss der Domänenname nicht mit angegeben werden. Dieser wird beim NPS automatisch angefügt. Neben dem Anmeldenamen (`NetBIOS-Name der Domäne\SAMAccoutName des Kontos`) wird auch der vollqualifizierte Domänenname (FQDN, *Fully Qualified Domain Name*) des Benutzers angegeben. Hier können Sie sehr einfach feststellen, in welcher Organisationseinheit oder welchem Container sich das Objekt befindet.

```
NAS:
    NAS-IPv4-Adresse:        192.168.1.11
    NAS-IPv6-Adresse:        -
    NAS-ID:                  -
    NAS-Porttyp:             Virtuell
    NAS-Port:                1

RADIUS-Client:
    Clientanzeigename:       Cisco3560
    Client-IP-Adresse:       192.168.1.11
```

Listing 19.9 Informationen zum RADIUS-Client

Der nächste Abschnitt des Eintrags (siehe Listing 19.9) liefert Informationen zum RADIUS-Client, also zu dem Switch, an dem sich der Benutzer authentifizieren wollte. Neben der IP-Adresse wird auch – wenn vorhanden – der NAS-Port angegeben. Der `Clientanzeigename` ist der Name, mit dem der Switch als RADIUS-Client im NPS konfiguriert wurde.

```
Authentifizierungsdetails:
    Name der Verbindungsanforderungsrichtlinie:   Windows-Authentifizierung
                                                  für alle Benutzer verwenden
```

```
Netzwerkrichtliniienname:     Verbindungen mit anderen Zugriffsservern
Authentifizierungsanbieter:   Windows
Authentifizierungsserver:     PNHN11SSEP00001.intranet.rheinwerk-verlag.de
Authentifizierungstyp:        PAP
EAP-Typ:                      -
Kontositzungs-ID:             -
```

Listing 19.10 In den Authentifizierungsdetails werden die angewendeten Regeln und der Authentifizierungstyp beschrieben.

Im nächsten Abschnitt (siehe Listing 19.10) finden Sie die Authentifizierungsdetails. Hier können Sie erkennen, welche RADIUS-Proxy-Regel (`Name der Verbindungsanforderungsrichtlinie`) und welche RADIUS-Regel (`Netzwerkrichtlinienname`) angewendet wurden. Hier sehen Sie auch, dass die Netzwerkrichtlinie mit dem Namen `Verbindungen mit anderen Zugriffsservern` angewendet wurde. Diese Regel ist eine der Standard-Verweigern-Regeln. Damit ist erwiesen, dass bei keiner Netzwerkrichtlinie die Bedingungen zutreffend waren, weswegen keine erfolgreiche Authentifizierung durchgeführt werden konnte.

```
Protokollierungsergebnisse:  Die Kontoinformationen wurden in
                             die lokale Protokolldatei geschrieben.
Ursachencode:                65
Ursache:                     Die Einstellung "Netzwerkzugriffsberechtigung"
                             in den Einwähleinstellungen des Benutzerkontos
                             in Active Directory ist so festgelegt, dass
                             dem Benutzer der Zugriff verweigert wird. Zum
                             Ändern der Einstellung "Netzwerkzugriffs-
                             berechtigung" in "Zugriff zulassen" oder
                             "Zugriff über NPS-Netzwerkrichtlinien steuern"
                             fordern Sie die Eigenschaften des Benutzer-
                             kontos in Active Directory-Benutzer und
                             -Computer an, klicken Sie auf die Register-
                             karte "Einwählen", und ändern Sie "Netzwerk-
                             zugriffsberechtigung".
```

Listing 19.11 Ergebnis des Authentifizierungsversuchs

Im `Ergebnis`-Abschnitt des Eintrags (siehe Listing 19.11) wird neben einem Ursachencode auch ein beschreibender Text zur Ursache ausgegeben. Damit ist eine mögliche Fehlersuche einfacher.

Da in unserem Beispiel noch keine Netzwerkrichtlinie erstellt wurde, war die fehlgeschlagene Authentifizierung zu erwarten. Damit haben wir getestet, dass der RADIUS-Client die Authentifizierungsversuche an den NPS-Server weitergeleitet hat.

19.6.3 Sicherheitsgruppen erstellen

Für den nächsten Schritt erstellen wir nun zwei Windows-Gruppen. Wir erstellen eine globale Sicherheitsgruppe mit dem Namen *P1SG-NetzwerkSwitchAdmins* und eine Gruppe mit dem Namen *P1SG-NetzwerkSwitchOperator*. Die *Admins*-Gruppe ist für die Netzwerkadministratoren vorgesehen und beinhaltet den Benutzer *1PeterKloep*, der mit administrativen Rechten (`Privilege: 15`) für die Administration des Switchs zuständig ist. In der *Operator*-Gruppe wird der Benutzer *PeterKloep* (kein Administratorkonto) Mitglied. Diese Gruppe soll nur ein Lese-Recht auf dem Switch bekommen (`Privilege: 1`).

Wechseln Sie in der NPS-Konsole zum Punkt NPS (LOKAL) • RICHTLINIEN • NETZWERKRICHTLINIEN, klicken Sie mit der rechten Maustaste auf NETZWERKRICHTLINIEN, und wählen Sie NEU.

Erstellen Sie als Erstes die Richtlinie für die Admins so, wie in Abbildung 19.114 gezeigt.

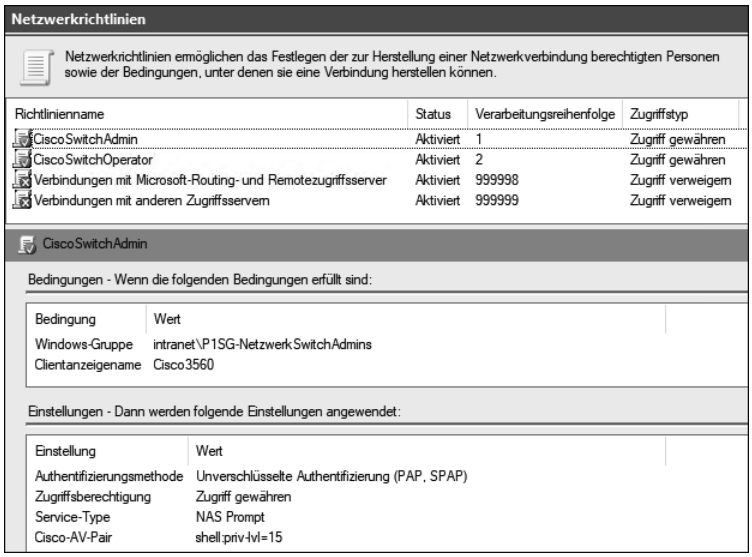

Abbildung 19.114 Anzeige der Richtlinie für die Switch-Admins

Wählen Sie die folgenden Einstellungen. Zwischen den einzelnen Seiten können Sie im Assistenten mit WEITER wechseln. Für alle nicht beschriebenen Werte übernehmen Sie die Standardeinstellungen.

- RICHTLINIENNAME – `CiscoSwitchAdmin`
- BEDINGUNG – `Windows-Gruppe intranet\P1SG-NetzwerkSwitchAdmins`
- BEDINGUNG – Clientanzeigename: `Cisco3560`
- AUTHENTIFIZIERUNGSMETHODE – nur unverschlüsselte Authentifizierung (PAP, SPAP)
- EINSTELLUNGEN KONFIGURIEREN – Service-Type: NAS-Prompt (zu finden unter ANDERE)
- EINSTELLUNGEN KONFIGURIEREN – Herstellerspezifisch: Cisco-AV-Pair: `shell:priv-lvl=15`

Eine zusätzliche Regel wird für die Switch-Operatoren angelegt:

- RICHTLINIENNAME – `CiscoSwitchOperator`
- BEDINGUNG – `Windows-Gruppe intranet\P1SG- NetzwerkSwitchOperator`
- BEDINGUNG – Clientanzeigename: `Cisco3560`
- AUTHENTIFIZIERUNGSMETHODE – nur unverschlüsselte Authentifizierung (PAP, SPAP)
- EINSTELLUNGEN KONFIGURIEREN – Service-Type: NAS-Prompt (zu finden unter ANDERE)
- EINSTELLUNGEN KONFIGURIEREN – Herstellerspezifisch: Cisco-AV-Pair: `shell:priv-lvl=1`

Die Zusammenfassung sieht dann so wie in Abbildung 19.115 aus.

Einstellungen - Dann werden folgende Einstellungen angewendet:

Einstellung	Wert
Authentifizierungsmethode	Unverschlüsselte Authentifizierung (PAP, SPAP)
Zugriffsberechtigung	Zugriff gewähren
Service-Type	NAS Prompt
Cisco-AV-Pair	shell:priv-lvl=1

Abbildung 19.115 Anzeige der Berechtigungseinstellungen für die Operatoren

Bedenken Sie, dass Sie sicherstellen müssen, dass kein Konto in beiden verwendeten Sicherheitsgruppen Mitglied ist: Die erste Regel, bei der die Bedingung zutrifft, wird angewendet und die Abarbeitung der Regeln wird beendet.

Über das Attribut CLIENTANZEIGENAME können Sie zusätzlich noch einschränken, auf welchen Geräten ein Benutzer berechtigt wird. Alternativ können Sie unterschiedliche Windows-Gruppen erstellen.

Verbindet sich nun ein Konto mit administrativen Rechten auf dem Switch mit dem Gerät, wechselt der Switch automatisch in den Enable-Modus (siehe Abbildung 19.116).

```
192.168.1.11 - PuTTY
login as: 1PeterKloep
Using keyboard-interactive authentication.
Password:

Switch#
```

Abbildung 19.116 Erfolgreiche Anmeldung am Switch mit automatisch aktiviertem Enable-Modus

Diese erfolgreiche Authentifizierung am Switch wird – wie erwartet – auf dem NPS-Server in der Ereignisanzeige protokolliert. Zusätzlich kann über den NPS neben der lokalen Protokollierung (Kontoführung) auch eine zentrale Speicherung in einem SQL-Server erfolgen.

Das Ereignis in der Ereignisanzeige hat die ID 6272 und kommt von der Quelle `Microsoft Windows security auditing`.

Genau wie bei der vorher beschriebenen fehlerhaften Anmeldung werden in dem Ereignis die gleichen Informationen dokumentiert (siehe Abbildung 19.117).

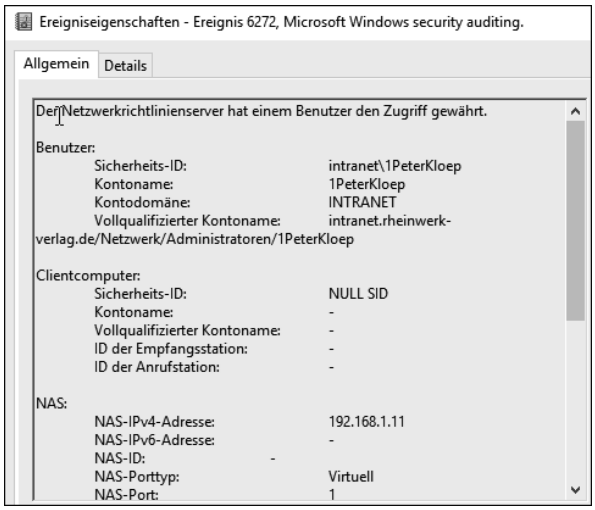

Abbildung 19.117 Erfolgreiche Anmeldung eines Administrators

In der Ereignisanzeige wird jedoch nicht protokolliert, welche Parameter an den Switch übertragen wurden. Damit Sie feststellen können, ob es ein Operator- oder Administratorzugriff war, sollten Sie den Netzwerkrichtlinien aussagekräftige Namen geben, sodass Sie anhand des Namens die Art und Weise des Zugriffs bestimmen können.

Die Kommunikation zwischen dem Switch und dem NPS-Server kann mit einem Netzwerksniffer (hier Wireshark) mitgeschnitten werden. In Abbildung 19.118 können Sie die beiden Authentifizierungspakete (80 und 81) und die beiden Kontoführungspakete (82 und 83) sehen. Sie finden ebenfalls die verwendete Benutzerkennung (`1PeterKloep`) sowie das verschlüsselte Kennwort, das für die Authentifizierung verwendet wurde.

Abbildung 19.118 Mitschnitt einer Authentifizierung

Führt ein Operator eine Anmeldung durch (siehe Abbildung 19.119), kann der Benutzer keinen Enable-Modus aktivieren. In der Abbildung können Sie erkennen, dass der Benutzer `PeterKloep` (nicht administrativ) eine Authentifizierung am Switch durchgeführt hat und der Standardmodus (`Switch>`) aktiviert wurde. Der Versuch, den Modus per `enable` zu wechseln, schlägt fehl.

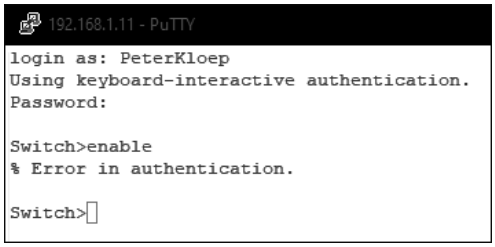

Abbildung 19.119 Verweigern des Enable-Modus für einen Operator

Eine Anmeldung als Operator kann über die Ereignisanzeige nachvollzogen werden. Listing 19.12 zeigt einen Auszug aus den Daten des Ereignisanzeigeeintrags:

```
Der Netzwerkrichtlinienserver hat einem Benutzer den Zugriff gewährt.

Benutzer:
    Sicherheits-ID:       intranet\PeterKloep
    Kontoname:            PeterKloep
    Kontodomäne:          INTRANET
    Vollqualifizierter Kontoname:  intranet.rheinwerk-
                                   verlag.de/Users/PeterKloep

Authentifizierungsdetails:
    Name der Verbindungsanforderungsrichtlinie:  Windows-Authentifizierung
                                                 für alle Benutzer verwenden
    Netzwerkrichtlinienname:                     CiscoSwitchOperator
    Authentifizierungsanbieter:                  Windows
    Authentifizierungsserver:    PNHN11SSEP00001.intranet.rheinwerk-verlag.de
    Authentifizierungstyp:       PAP
    EAP-Typ:                     -
    Kontositzungs-ID:            -
    Protokollierungsergebnisse:  Die Kontoinformationen wurden in die lokale
                                 Protokolldatei geschrieben.
```

Listing 19.12 Authentifizierung eines Switch-Operators

Andere Anbieter von Netzwerkkomponenten bieten unter Umständen ähnliche Authentifizierungsmethoden für die sichere Administration an.

Leider verträgt sich die Authentifizierung an den Netzwerkkomponenten nicht mit anderen Sicherheitsfunktionen. Ist eines der Konten, die sich am Switch anmelden sollen, Mitglied der Gruppe *Protected Users*, ist eine Authentifizierung aufgrund von Protokollbeschränkungen nicht möglich. Versucht ein Benutzer eine Authentifizierung, schlägt diese fehl und es wird ein Eintrag im Ereignisprotokoll erstellt (siehe Abbildung 19.120).

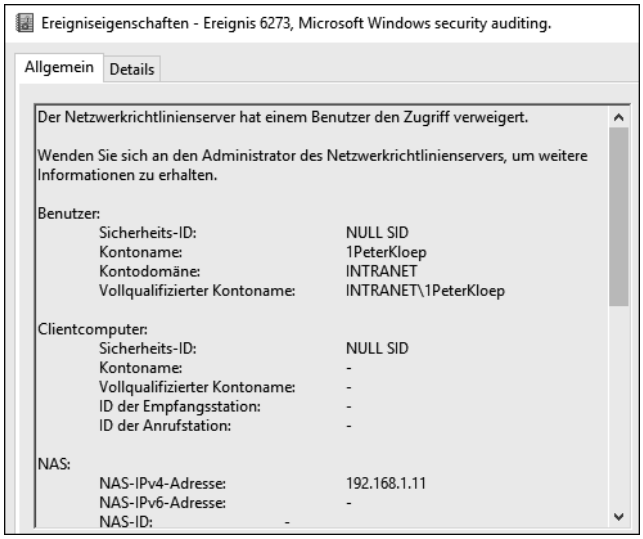

Abbildung 19.120 Ereignisprotokoll einer Authentifizierung, die aufgrund der »Protected Users«-Gruppe fehlschlug

In den Details des Eintrags findet sich der Grund für den verweigerten Zugriff (Listing 19.13 zeigt einen Auszug):

```
Der Netzwerkrichtlinienserver hat einem Benutzer den Zugriff verweigert.

Authentifizierungsdetails:
    Name der Verbindungsanforderungsrichtlinie:  Windows-Authentifizierung
                                                 für alle Benutzer verwenden
    Netzwerkrichtlinienname:                     -
    Authentifizierungsanbieter:                  Windows
    Authentifizierungsserver:                    PNHN11SSEP00001.intranet.
                                                 rheinwerk-verlag.de
    Authentifizierungstyp:                       PAP
    EAP-Typ:                                     -
    Kontositzungs-ID:                            -
    Protokollierungsergebnisse:                  Die Kontoinformationen
                                                 wurden in die lokale
                                                 Protokolldatei geschrieben.
    Ursachencode:                                38
```

```
Ursache:                Authentifizierungsfehler aufgrund einer
                        Benutzerkontoeinschränkung oder einer nicht
                        befolgten Anforderung. Dies kann beispielsweise
                        dann der Fall sein, wenn die Benutzer-
                        kontoeinstellungen die Verwendung eines Kennworts
                        erfordern, der Benutzer sich jedoch mit einem
                        leeren Kennwort anmelden wollte.
```

Listing 19.13 Auszug aus den Informationen zur fehlgeschlagenen Authentifizierung

In Listing 19.13 können Sie erkennen, dass keine Netzwerkrichtlinie angewendet wurde. Der Grund dafür ist, dass bei den *Protected Users* nur eine Kerberos-Authentifizierung möglich ist.

Wenn Sie beide Funktionen nutzen möchten, müssen Sie ein separates administratives Konto erstellen, das dann für die Administration bzw. die Authentifizierung an den Netzwerkkomponenten verwendet wird.