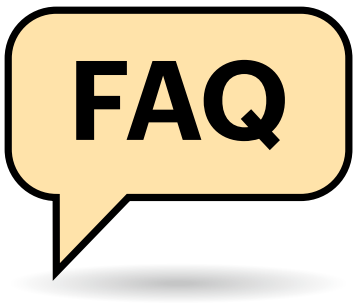


Dateien bequem und sicher teilen

Der Austausch von Dateien über Netze oder das Internet birgt immer wieder Überraschungen und wirft Fragen auf. Wir bereiten Sie darauf vor und liefern Antworten.

Von Peter Siering

Netzwerkverbindung testen

Wie kann ich testen, ob meine Netzwerkverbindung für den Dateiaustausch geeignet ist?

Solange keine Firewall zwischen den Netzwerken der beteiligten Systeme sitzt, sollte ein Dateiaustausch über die gängigen Protokolle stets möglich sein. Mit Unix-Systemen lässt sich der Befehl `nc` (Netcat) zum Testen verwenden. Sie brauchen außer diesem Programm auf beiden Seiten noch Informationen über das zum Austausch verwendete Protokoll. SMB braucht heutzutage beispielsweise nur noch den Port 445 und als Protokoll TCP. Auf dem Server starten Sie Netcat mit `netcat -l 445` und auf dem Client mit `netcat <IP> 445`. Auf dem Server müssen Sie gegebenenfalls `sudo` voranstellen, weil der Port kleiner als 1024 ist (die darf nur der Nutzer root verwenden). Sie können, wenn eine Verbindung zustande gekommen ist, auf beiden Seiten Text eingeben, der jeweils auf der anderen Seite ausgegeben wird. Wenn das klappt, sollte auch eine SMB-Verbindung funktionieren. Andernfalls müssen Sie sich nach einer anderen Methode für den Datenaustausch umsehen.

SMB-Freigaben im VPN weg

Mein Notebook läuft mal im heimischen Netz und mal im Firmennetz. Nur in letzterem komme ich an die Freigaben heran. Geht das nicht per VPN?

Das kommt darauf an. Oft führen Unterschiede in der Namensauflösung zu solchen Problemen. Am einfachsten ist es, wenn Sie die IP-Adresse des Servers statt seines Namens angeben, zum Beispiel „//192.168.278.10/dateien“. Wenn das nicht klappt, sprechen Sie mit den Zuständigen für das Netzwerk, an das Sie sich per VPN einbuchen. Wenn es klappt, könnte ein Namensbestandteil das Problem sein: Hängen Sie dann versuchsweise mal den Domainnamen an den Namen des Servers an, etwa „//nas.<IhreDomain>/dateien“.

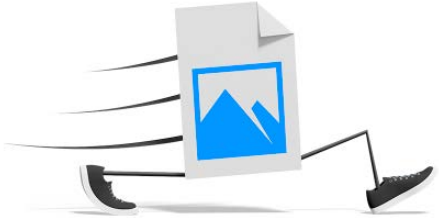
SMB-Freigabe als Verzeichnis

Ich möchte eine Freigabe unter Windows nicht als Laufwerk sichtbar machen, sondern unterhalb von C: als Verzeichnis einbinden. Geht das?

Dafür lassen sich die NTFS-eigenen Soft Links hernehmen, die Sie mit dem Befehl `mklink` in der Eingabeaufforderung erstellen können. Statt eines lokalen Link-Zieles geben Sie dabei einfach den Pfad der Freigabe an, zum Beispiel so:

```
mklink /d C:\video \\nas\video
```

Den `mklink`-Befehl müssen Sie als Administrator ausführen. Damit Windows die Verbindung zur Freigabe beim Betreten des Verzeichnisses durch einen Nutzer herstellen kann, muss er hinreichend Rechte dort haben und über gültige Anmeldedaten verfügen. Gegebenenfalls können Sie die dauerhaft in den Anmeldeinformationen speichern.



Dateien über wackelige Netze übertragen

Ich muss große Dateimengen übers Netz kopieren, aber manchmal reißt die Verbindung ab. Wie kann ich einen solchen Prozess zuverlässig so anlegen, dass er sauber zum Ende kommt?

Wenn das Reparieren der Netzwerkverbindung keine Option ist, helfen Programme wie robocopy für Windows und rsync für Windows und Linux. Sie können Kopiervorgänge fortsetzen (Obacht: sie synchronisieren eher und löschen deswegen auch Dateien, die an der Quelle nicht mehr da sind). Das Überprüfen der Dateien am Ziel mittels Prüfsummen beherrscht allerdings nur rsync. Wer robocopy verwendet, muss dafür Extra-Software bemühen. In Windows-Kreisen wird dafür oft der „File Checksum Integrity Verifier“ empfohlen.

File Checksum Integrity Verifier:
ct.de/yhpq

Kopieren mit Rechten

Ich möchte Dateien übers Netzwerk von einem auf einen anderen PC kopieren, sodass die vergebenen Rechte und Eigentümer erhalten bleiben. Wie geht das?

Wie das erfolgreich klappt, hängt von zwei wesentlichen Faktoren ab. Der erste ist der wichtigste: Rechte und Eigentumsinformationen hängen bei gängigen Dateisystemen und Netzwerktechniken nicht an Benutzernamen, sondern an einer Nummer, die den Nutzer lokal repräsentiert. Unter Unix sind das meist einfache User-IDs wie zum Beispiel 1001; mit der

Eingabe von `id` in einer Terminalsitzung kann man sie ausgeben. Windows verwendet eine komplexere ID, die sich von einem Security Identifier ableitet, den das Betriebssystem bei der Installation erzeugt. Der macht Windows-Konten laut Microsoft weltweit und dauerhaft einmalig. Die System-SID wird in diese SID für den Benutzer eingebaut. Wenn Sie diese mal sehen möchten, geben Sie in einer Eingabeaufforderung `whoami /user` ein.

Um nun Dateien verschiedener Benutzer von einem auf ein anderes System zu kopieren, ist es nötig, dass die Benutzer-ID auf beiden Systemen identisch ist. Für ein Unix-System kann man das von Hand herbeiführen, indem alle relevanten Nutzer auf beiden Systemen identische User-IDs erhalten – eine Notlösung. Empfehlenswert wäre es eher, beide Systeme eine externe Benutzerdatenbank verwenden zu lassen. Und das ist genau der Weg, den man bei Windows gehen muss: In einer Windows-Domäne trauen alle zu Mitgliedern erklärten Systeme einer Benutzerdatenbank. Dateien, die Nutzer auf verschiedenen Systemen anlegen, gehören dadurch derselben SID. Ein Kopieren von Dateien innerhalb der Domäne kann deshalb auch die Besitzverhältnisse sinnvoll erhalten.

Der zweite wichtige Faktor ist die Art und Weise, wie kopiert wird beziehungsweise wer es tut: Ein Benutzer kann üblicherweise nur die Dateien kopieren, die ihm gehören und die mit ihm geteilt wurden. Auch kann er nur dort Dateien ablegen, wo er Rechte dazu hat. Es gibt eine Ausnahme davon, die für Backups vorgesehen ist: Mit speziellen Rechten und Funktionen können Benutzer dann Dateien kopieren, die sie nicht einmal lesen dürfen. Das ist aber nur in Ausnahmefällen hilfreich. In der Regel wird ein Nutzer mit administrativen Rechten die Dateien anderer Nutzer von einem Ort zu einem anderen kopieren. Er hat üblicherweise hinreichend Rechte, um alles zu lesen und die Dateien am Ziel wieder mit den Besitzverhältnissen und Rechten auszustatten, die sie an der Quelle hatten. Das gilt zum Beispiel für robocopy und rsync (siehe auch „Dateien über wackelige Netze übertragen“). Wobei: rsync kennt Optionen, mit denen man Unix-Nutzer auch ohne ID-Gleichstand kopieren kann.

Admin-Freigaben: IPC$, ADMIN$ und C$

Wenn ich mir ansehe, welche Freigaben auf meinem Windows-PC aktiv sind, dann finde ich dort solche mit einem $-Zeichen am Ende des Namens. Ich habe die nicht eingerichtet. Was ist das?

Das sind die sogenannten administrativen Freigaben, die Microsoft unter anderem für die Verwaltung von Windows in größeren Netzen heranzieht. Eine Verbindung dorthin kann nur aufbauen, wer direkt in einer Gruppe mit administrativen Rechten geführt ist. Andere Konten können darauf nicht zugreifen. Was Sie durchaus sehen könnten: an die Freigabe IPC$ verbundene Nutzer – das dient der Kommunikation im Netzwerk und ist per se nicht bedenklich.

Aktive SMB-Nutzer anzeigen

Wie kann man herausfinden, ob noch Nutzer mit einem SMB-Server verbunden sind?

Auf einem Linux-System oder einem NAS mit SSH-Zugang leistet das der `smbstatus`-Befehl, der auch viele weitere Details ausgibt, etwa zur Protokollversion, mit der ein Client verbunden ist, ob das Signieren der Paket aktiv ist und sogar welche Dateien ein Client in welchem Modus geöffnet hat. Unter Windows hilft in einer Eingabeaufforderung mit Admin-Rechten `net session` und in der grafischen Bedienoberfläche die Management-Console für „Freigegebene Ordner“. Diese starten Sie am einfachsten, indem Sie Windows+R drücken, `fsmgmt.msc` eingeben und Enter drücken.

SMB im Internet

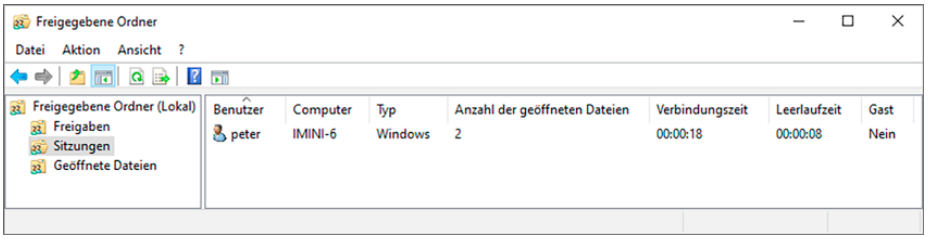
SMB hieß doch auch Common Internet File System. Kann ich es gefahrlos ins Internet hängen?

Bloß nicht: Ein per SMB erreichbarer Computer verrät mehr über sich, als Sie die Welt wissen lassen wollen. Ein Versehen beim Einrichten von Freigaben genügt und schon können Dritte auf Ihre Daten zugreifen – dafür gibt es inzwischen viele Beispiele mit prominenten Bezügen, etwa Autovermieter und Arztpraxen [1, 2]. Hinzu kommen eventuelle Sicherheitslücken in den Protokollen, die im Fall vom veralteten und glücklicherweise meist abgestellten SMB1 eine Einladung für Skriptkiddies waren. Wenn es partout sein muss: Filtern Sie per Firewall, wer auf den SMB-Port 445 überhaupt zugreifen darf, indem Sie nur einzelne IP-Adressen zulassen.

Netzwerk unerträglich lahm

Beim Kopieren von Dateien über einen PC in meinem kabelgebundenen Netzwerk geht ein PC besonders träge zu Werke. Er braucht glatt die dreifache Zeit für eine Videodatei, wenn es gut geht. Ich habe schon alle Einstellungen in Windows überprüft. Was kann ich noch tun?

Oft gibt es ganz einfache Ursachen, die man vorschnell dem Betriebssystem anlastet: Tauschen Sie unbedingt mal die Patch-Kabel und den Netzwerkport, an dem der PC hängt. Schon oft endete



Eine Management-Console verrät sogar in der Home-Edition, wer übers Netz mit dem PC verbunden ist.

eine langatmige Fehlersuche mit der Diagnose: Kabelbruch. Ein Tipp dazu: Schneiden Sie ein defektes Kabel gleich durch, dann landet es nicht in der Restekiste und ärgert Sie ein weiteres Mal. Wer genauer hinsieht, erkennt solche Probleme auch anders: Pendeln die Eigenschaften, die Netzwerkswitch und angeschlossenes Gerät automatisch aushandeln, unregelmäßig zwischen Fast- und Gigabit-Ethernet oder Voll- und Halbduplex, sind üblicherweise Kabel oder Port fritte.

S3-Speicher für den Austausch

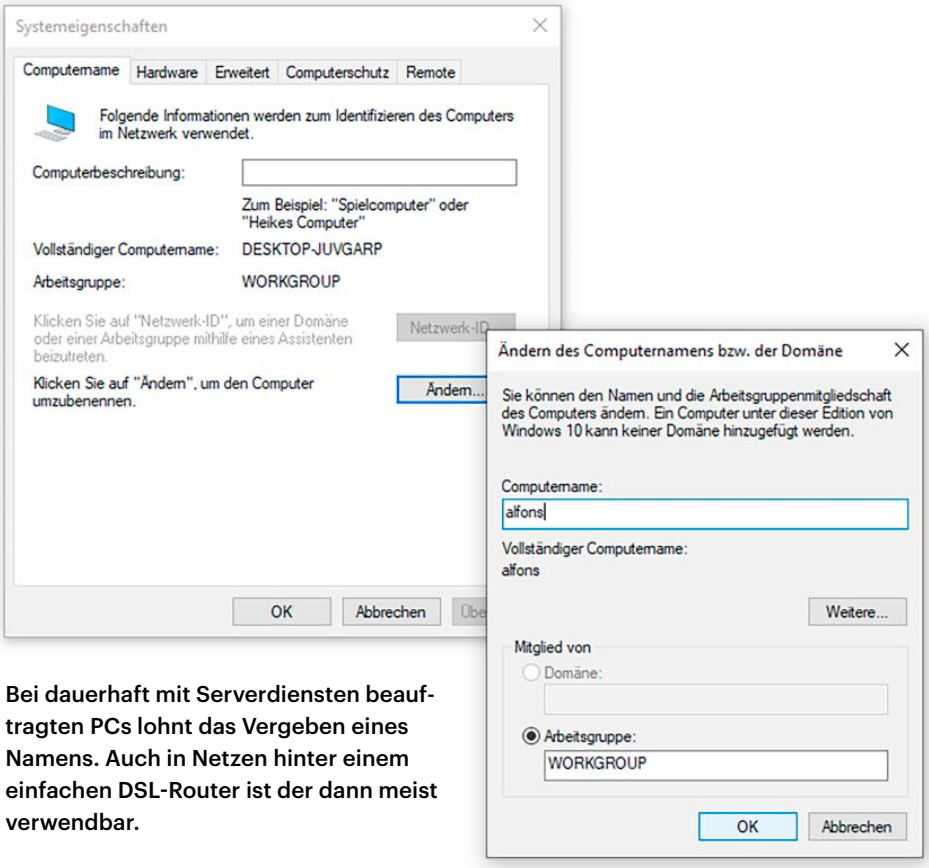
Man liest immer wieder von sogenanntem S3-Speicher, den zum Beispiel Amazon in der Cloud vermietet, den man mit Software via „minio“ aber auch lokal bereitstellen kann. Eignet sich diese Art von Speicher zum Dateiaustausch?

Theoretisch ja, praktisch nicht ohne weitere Hilfe: Was Amazon als Simple Storage Service (S3) in die Welt gesetzt hat, ist ein sehr spezieller Datenspeicher: Der Zugriff auf dort abgelegte Daten erfolgt per HTTP/HTTPS. Im Vergleich zu gängigen Dateisystemen bietet S3 ein anderes Ordnungskonzept in Form von Buckets und Objekten. Dadurch ist es nicht für die direkte Nutzung vorgesehen, sondern dient eher als Backend für Dienste zum Dateiaustausch.

Windows-PC-Namen ändern

Windows vergibt so kryptische Rechnernamen. Wie kann ich die Namensvergabe beeinflussen?

Über einen Rechtsklick auf das Symbol „Dieser PC“ im Explorer und den Aufruf von „Eigenschaften“ nehmen Sie eine Abkürzung in die zuständige Abteilung der Systemsteuerung (alternativ: Windows+Pause drücken). Klicken Sie auf den Link „Einstellungen für Computernamen, Domäne und Arbeitsgruppe“ und dann auf „Ändern“. Der neue Name sollte nach einem Neustart und einer gewissen Weile auch dem Netzwerk bekannt sein – Router wie eine Fritzbox lösen als lokaler Nameserver solche Namen auf.



Bei dauerhaft mit Serverdiensten beauftragten PCs lohnt das Vergeben eines Namens. Auch in Netzen hinter einem einfachen DSL-Router ist der dann meist verwendbar.

SMB-Version ermitteln

Wie finde ich heraus, welche SMB-Version ein Server oder Client spricht?

Auf einem Linux-Server oder einem NAS mit SSH-Zugang liefert `smbstatus` für jede bestehende Verbindung zu Samba diese Information. Auf Windows-Clients finden Sie mit der Powershell heraus, ob auf dem Server noch SMB1 aktiv ist: `Get-SmbServerConfiguration` heißt der Befehl und das Feld „EnableSMB1Protocol“ ist entscheidend. Ob ein Windows-Client SMB1 spricht, kriegen Sie mit `sc qc lanmanworkstation` heraus. Unter „DEPENDENCIES“ steht dann „MRxSmb10“. Das sollte dort eigentlich nicht stehen, sondern lediglich „MRxSmb20“, was sowohl SMB2 und 3 aktiviert. Ein längerer Beitrag von Microsoft nennt diverse weitere Details.

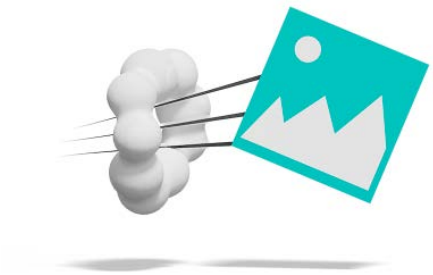
Auf dem Mac liefert `smbutil statshares -a` Informationen zu den Fähigkeiten und Versionen des Servers. Eine Funktion, die Fähigkeit des macOS-Clients in Erfahrung zu bringen, kennen wir nicht. In der Datei /etc/nsmb.conf kann man mit:

```
[default]
smb_neg=smb2_only
```

macOS anweisen, keine Verbindung mit SMB1 herzustellen. Die aktuelle Fassung Catalina tut das von sich aus nicht mehr.

(ps@ct.de)

Microsoft zur SMB-Versionserkennung: ***ct.de/yhpq***



Literatur

[1] Ronald Eikenberg, Hartmut Gieselmann, Joerg Heidrich und Christian Wölbert , Daten-GAU bei Buchbinder, Persönliche Informationen von 3 Millionen Kunden der Autovermietung Buchbinder offen im Netz, c't 4/2020, S. 12

[2] Ronald Eikenberg, Dr. Datenleck, Warum eine komplette Arztpraxis offen im Netz stand, c't 25/2019, S. 16