Server 2012 - NTFS Rechte und ABE

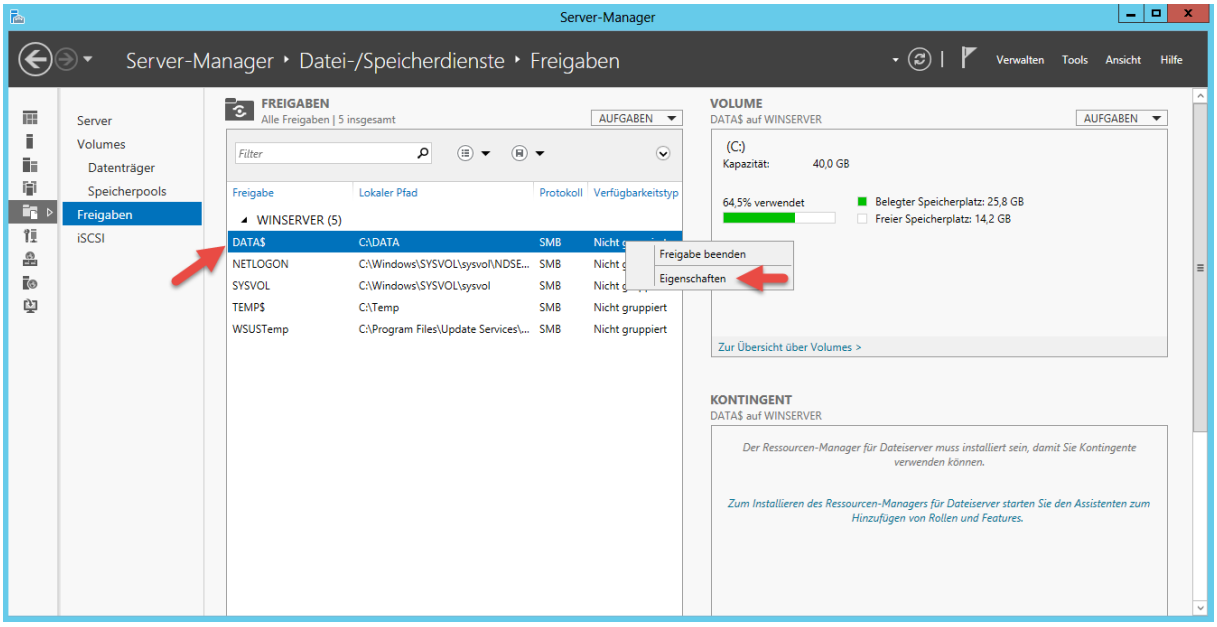
Access Based Enumeration (Zugriffsbasierte Aufzählung) ist eine Funktion die uns dabei hilft Ordner und Dateien auf denen wir keine Berechtigung besitzen auszublenden.

ABE kann somit als ein Sicherheitsfeature betrachtet werden und erhöht gleichzeitig den Komfort bei der Verwaltung/Übersicht von Daten auf denen man expliziten Zugriff hat. Wir sehen nur noch das worauf wir auch berechtigt sind.

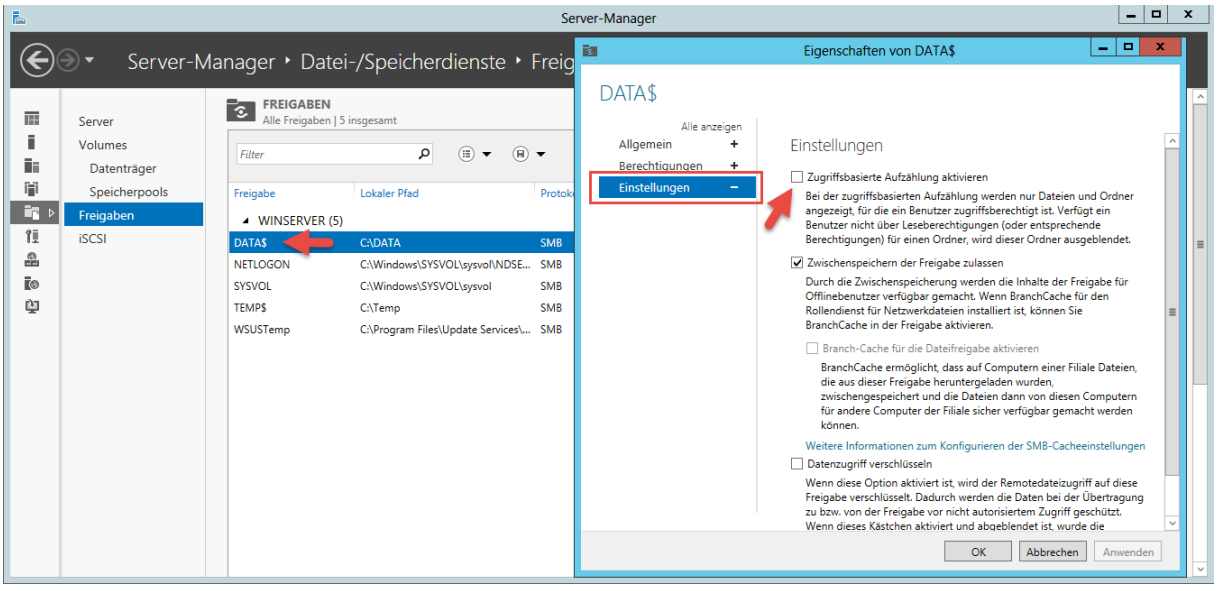
Zur Demonstration habe ich unter C:\ einen Ordner namens DATA angelegt und freigegeben.

Über den **Servermanager > Datei-/Speicherdienste > Freigaben** administrieren wir zentral unsere Freigaben und Berechtigungen.

Über einen Rechtsklick auf die Freigabe DATA$ öffnet sich ein Menü und lassen uns die Eigenschaften anzeigen.



Unter dem Menüpunkt „Einstellungen" finden wir die „Zugriffsbasierte Aufzählung" die sogenannte ABE.



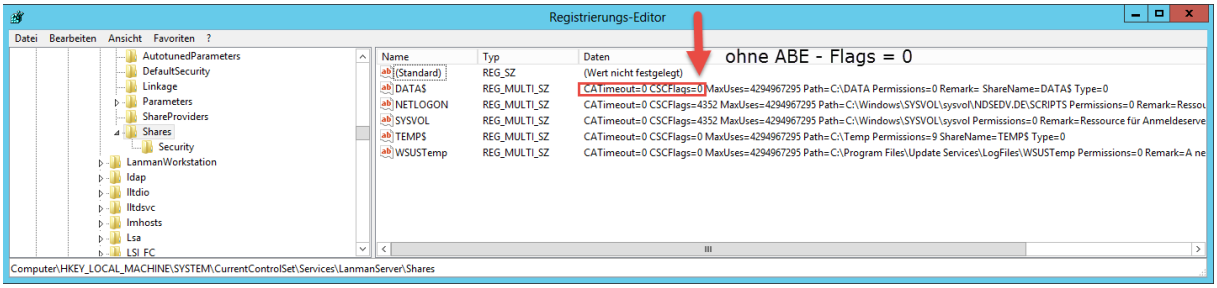
Diese Funktion aktivieren wir nun.

Server 2012 - NTFS Rechte und ABE

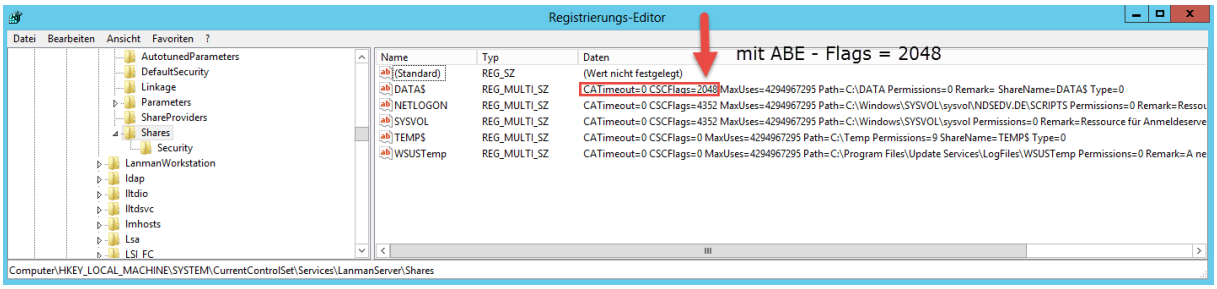
Das Aktivieren dieser Funktion hat nichts mit dem NTFS Attribut versteckt (hidden) zu tun auch die Freigabeberechtigung spielt hier keine Rolle.

Sobald die Zugriffsbasierte Aufzählung auf eine Freigabe aktiviert wurde, setzt Windows in der Registry ein Flag.

Vorher ohne ABE:



Nachher mit ABE:

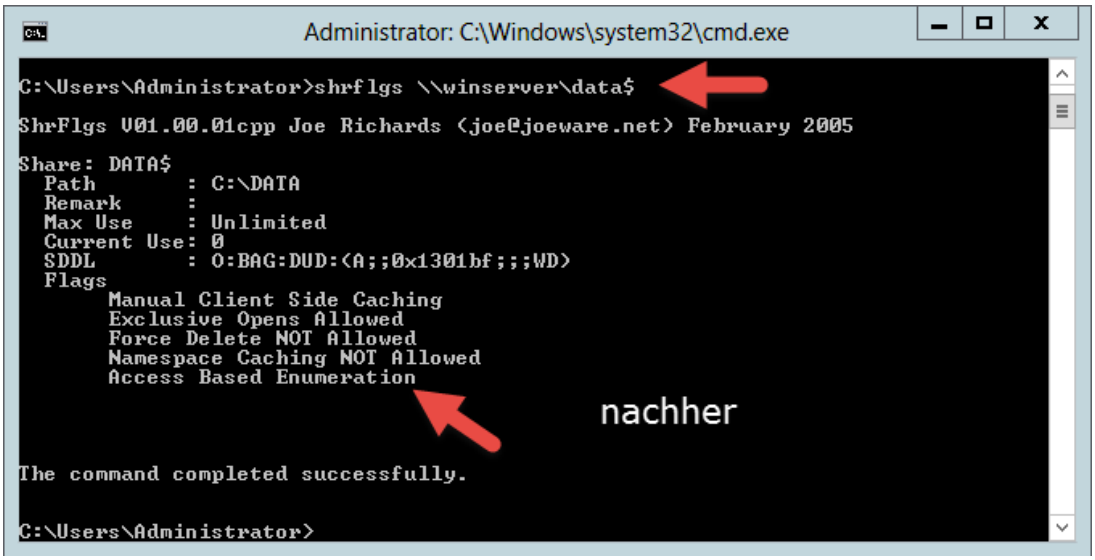


Das Flag 2048 steht für die aktive ABE Funktion.

Mit einem Tool lassen sich die gesetzten Flags auch per Commandline abfragen.

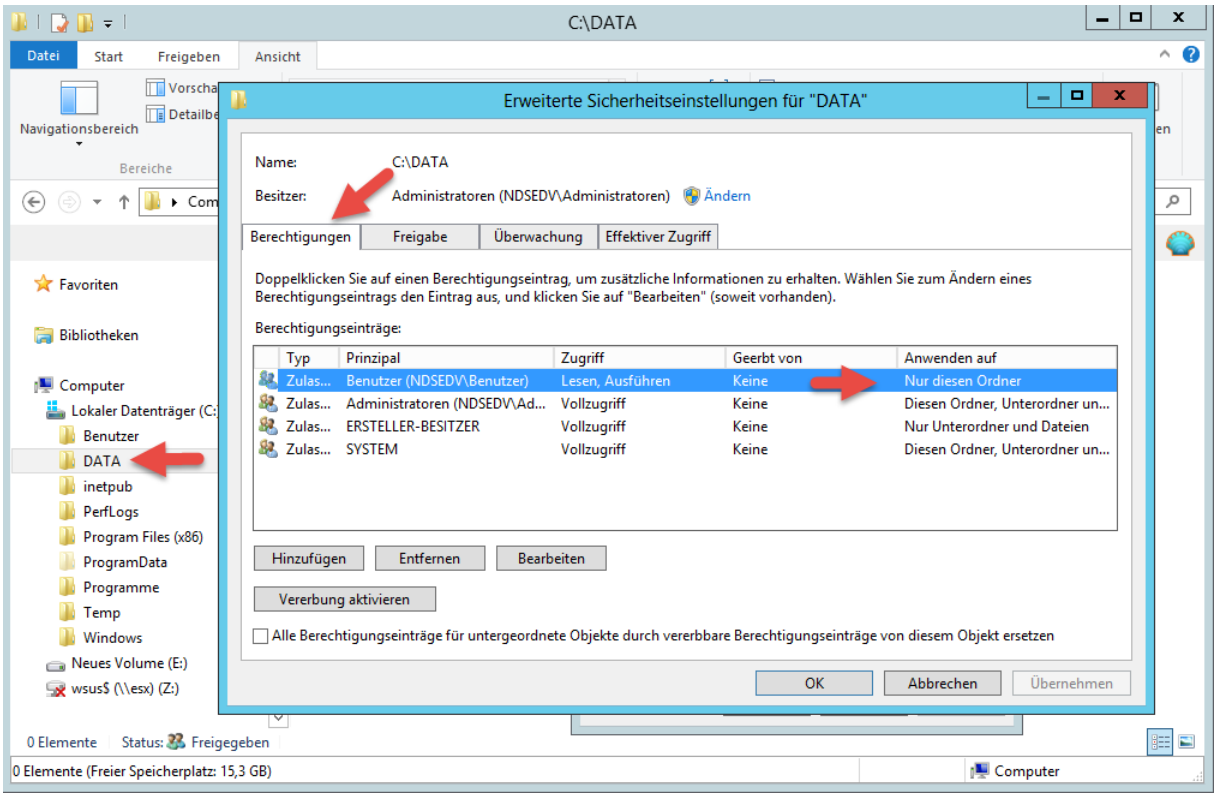
Das Tool lässt sich hier downloaden: https://www.der-windows-papst.de/ndsedv/wp-content/uploads/2015/11/ShrFlgs.zip

Der Befehl dazu lautet: shrflgs [\\winserver\data$](\\winserver\data$)

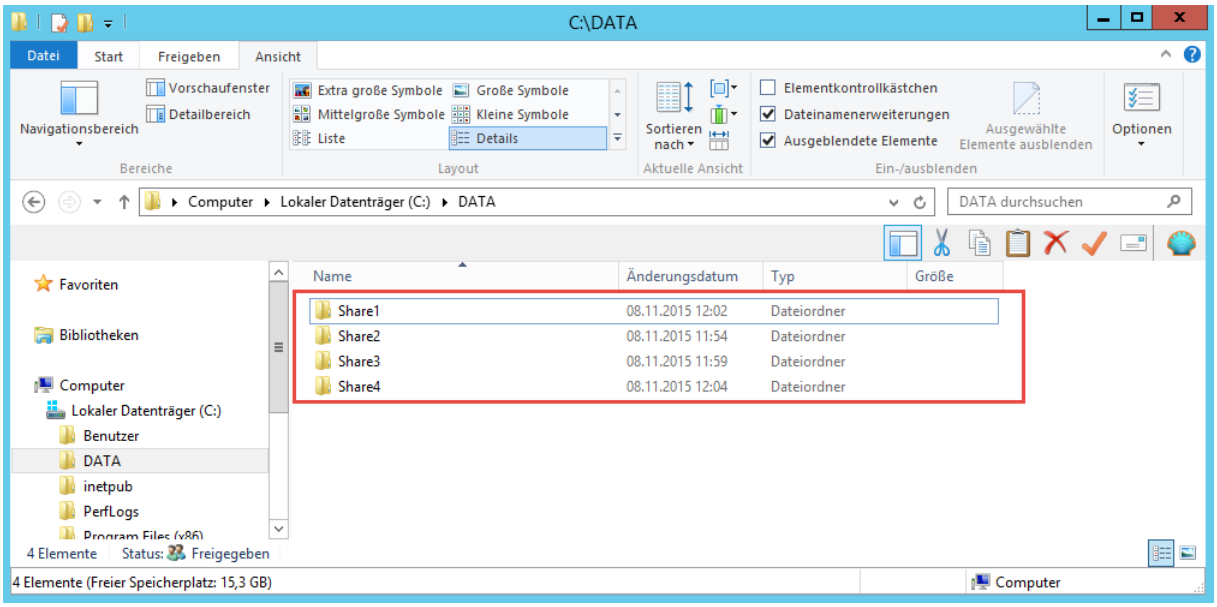


Server 2012 - NTFS Rechte und ABE

Auf die Freigabe \\winserver\data$ hat aktuell jeder Domänen-Benutzer Zugriff.

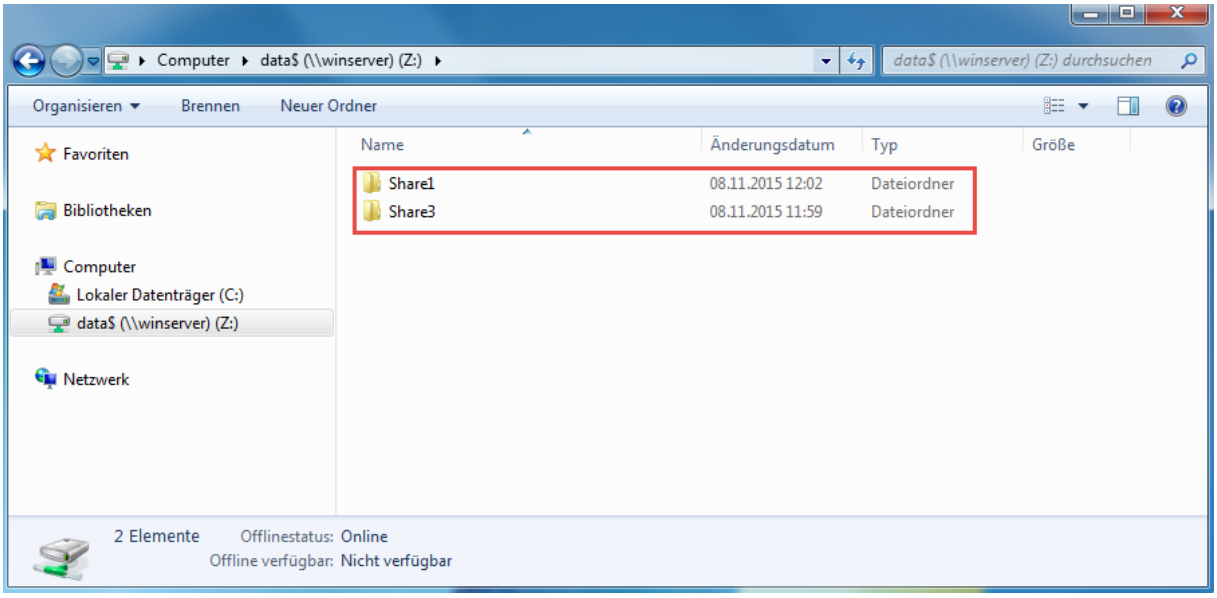


Der Einsprungs-Punkt ist dabei das Share Data$.

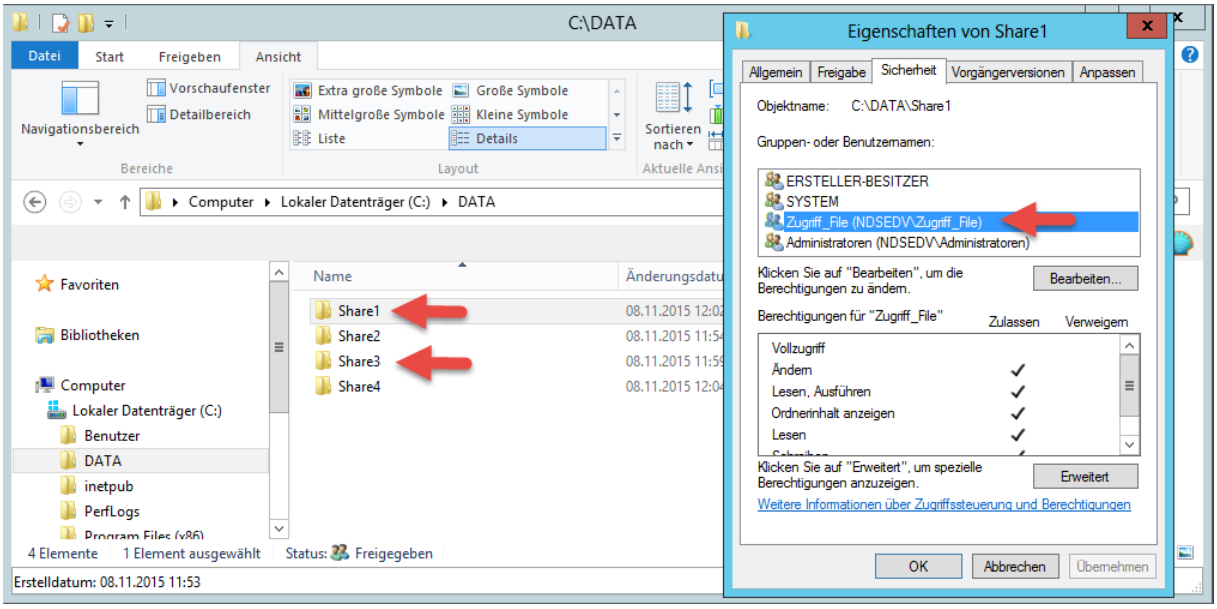


Es gibt also insgesamt 4 Ordner namens Share1-4. Der Ordnername ist vielleicht etwas unglücklich gewählt, weil es ja keine Shares sind.

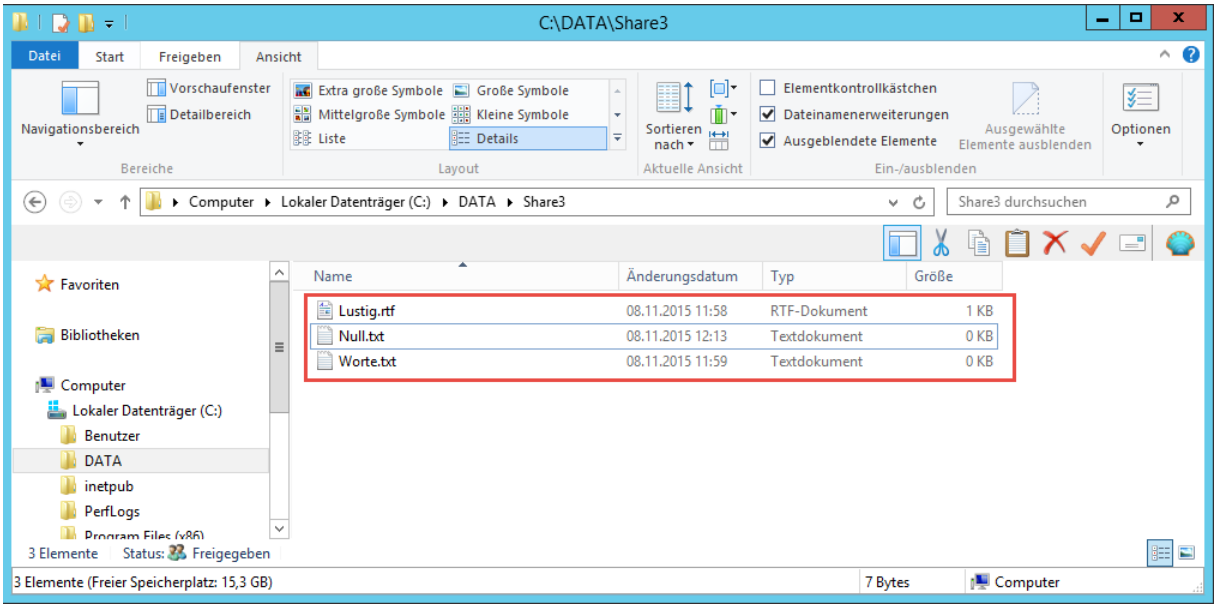
Ich starte den Client und öffne die Freigabe DATA$ und sehe nur 2 Ordner auf die ich explizit berechtigt bin.



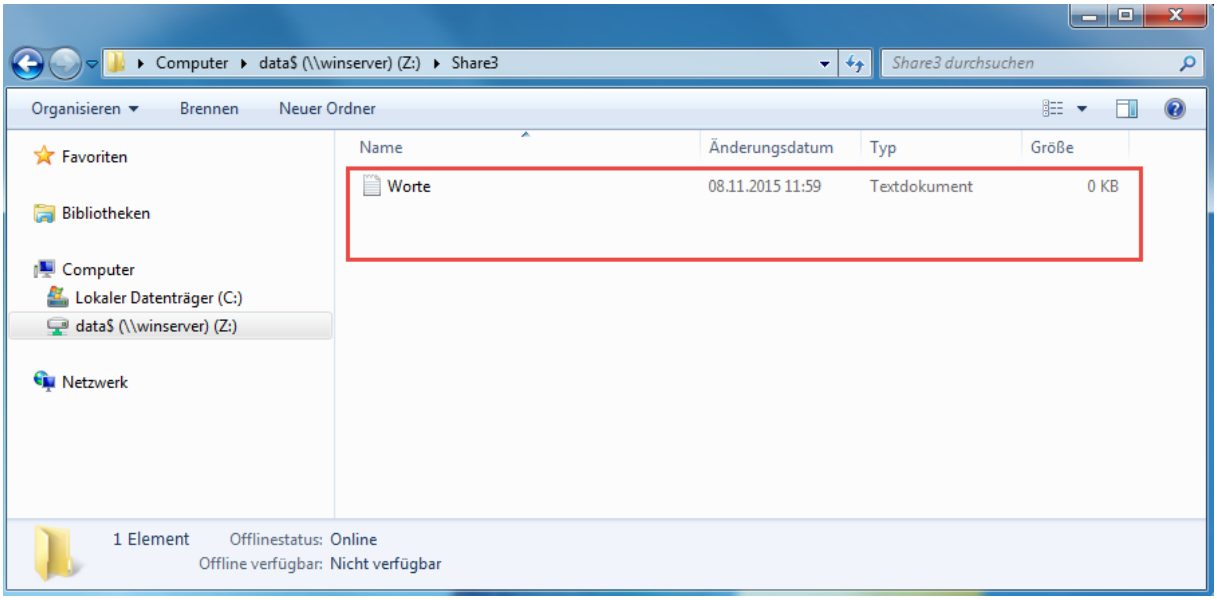
Gesteuert über die Zugriffsgruppe Zugriff_File. Auf Share2 und Share4 habe ich keinen Zugriff und kann diese somit weder sehen noch darauf zugreifen.



Ich sehe auch nur die Daten auf die ich berechtigt bin obwohl sich im Ordner Share3 mehrere Dateien befinden.



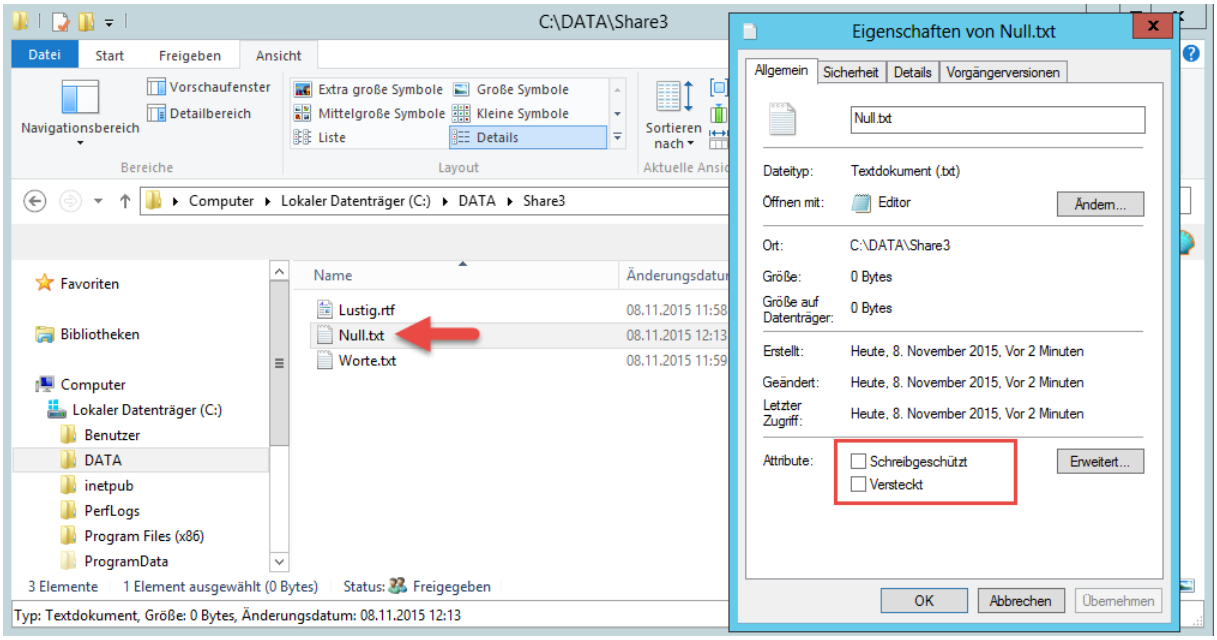
Berechtigt bin ich also nur auf eine Datei, und zwar auf die Datei „Worte".



Die beiden anderen Dateien sind auch nicht über das NTFS Attribut „Versteckt" ausgeblendet, das zeigt uns der nächste Screenshot.

Es wird alles über die Funktion „Zugriffsbasierte Aufzählung" gesteuert.

Server 2012 - NTFS Rechte und ABE



Erstellt von Jörn Walter www.der-windows-papst.de – 08.11.2015