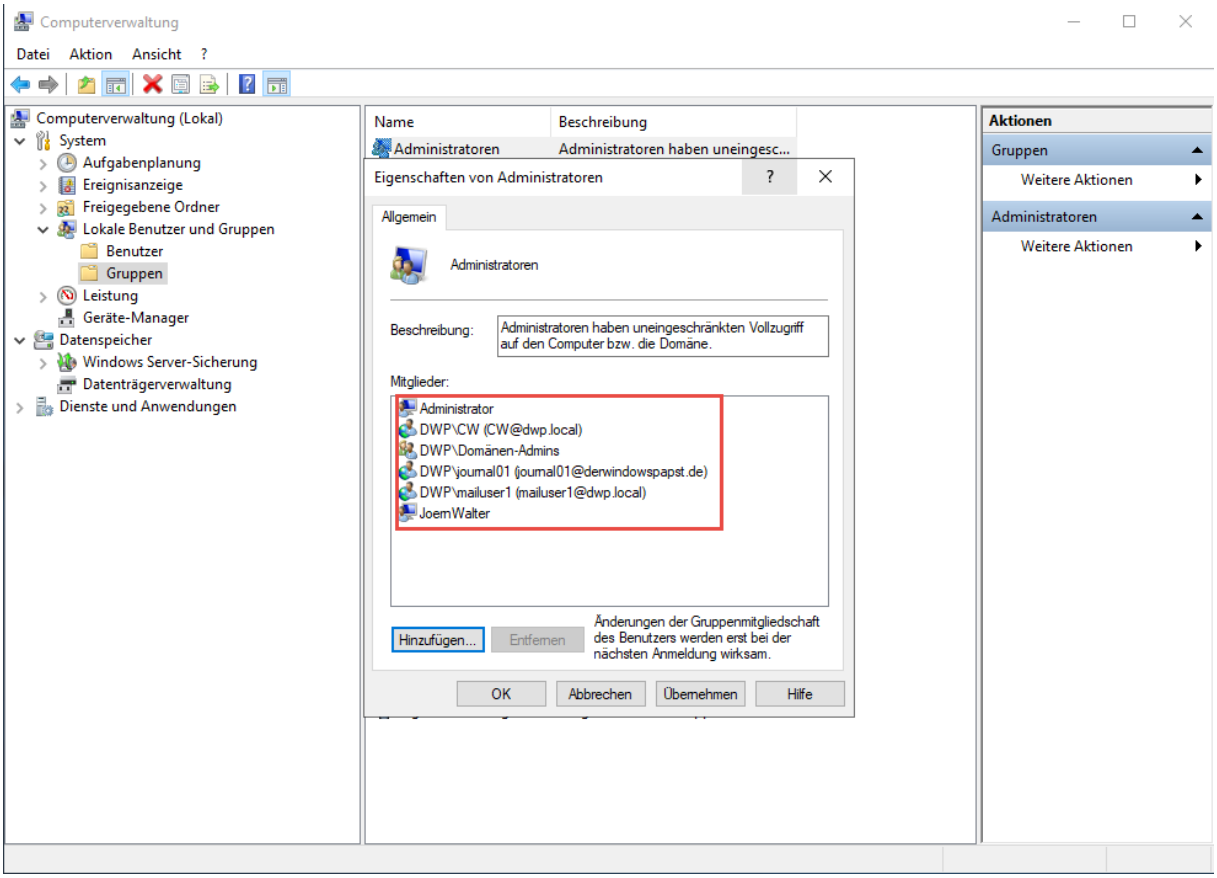
Lokale Administratoren managen

Das Problem ist, das im Laufe der Zeit viele Einzelpersonen auf einem Server zum lokalen Admin heraufgestuft wurden, eine oder mehrere Gruppen hinzugefügt wurden die wiederum Mitglieder enthalten. Es wird zu einem Wildwuchs.

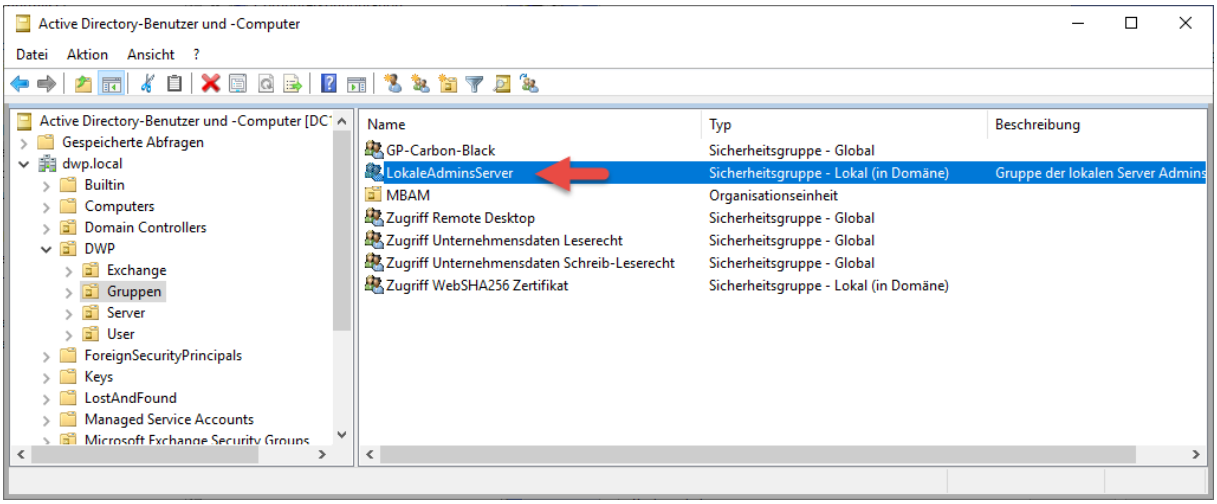
An dieser Stelle muss dringend etwas passieren.

Die Ausgangslage:



Das Ganze lässt sich sehr gut über eine Gruppenrichtlinie steuern. Mit einer Gruppenrichtlinie entfernen wir die einzelnen Benutzer und diverse Gruppen und fügen nach der Erstellung eines Konzepts neue hinzu.

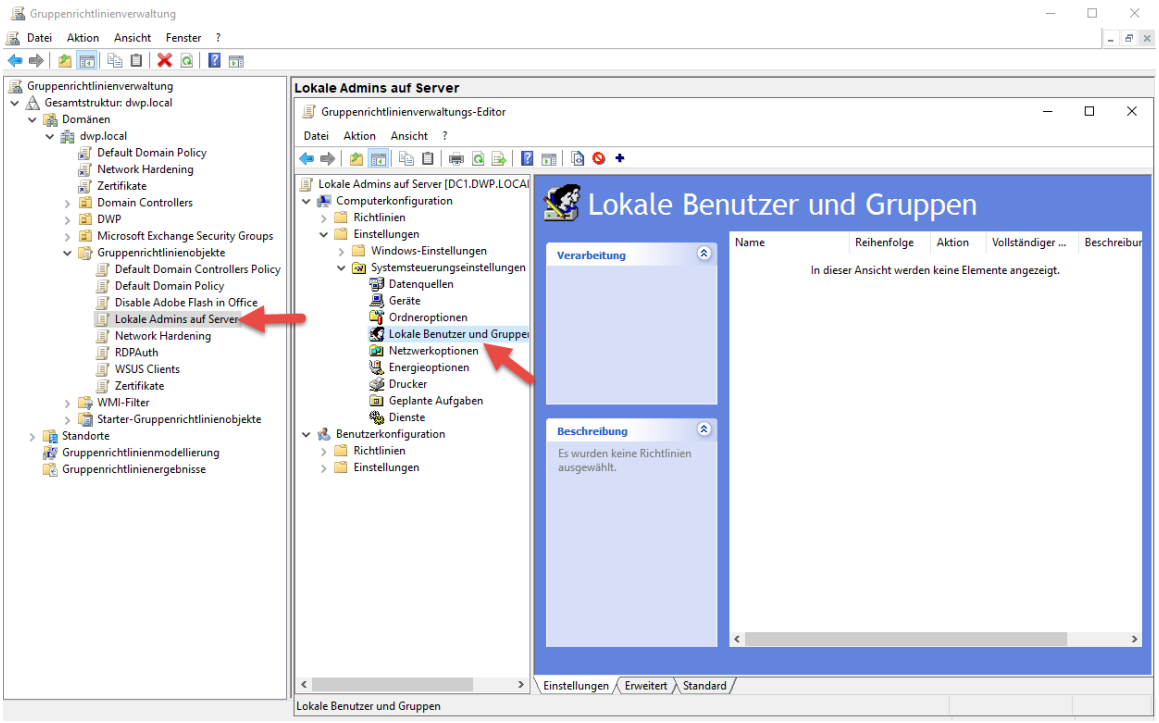
Zuerst erstellen wir im Active-Directory anlehnend an das erstelle Konzept eine neue Sicherheitsgruppe namens LokaleAdminsServer.



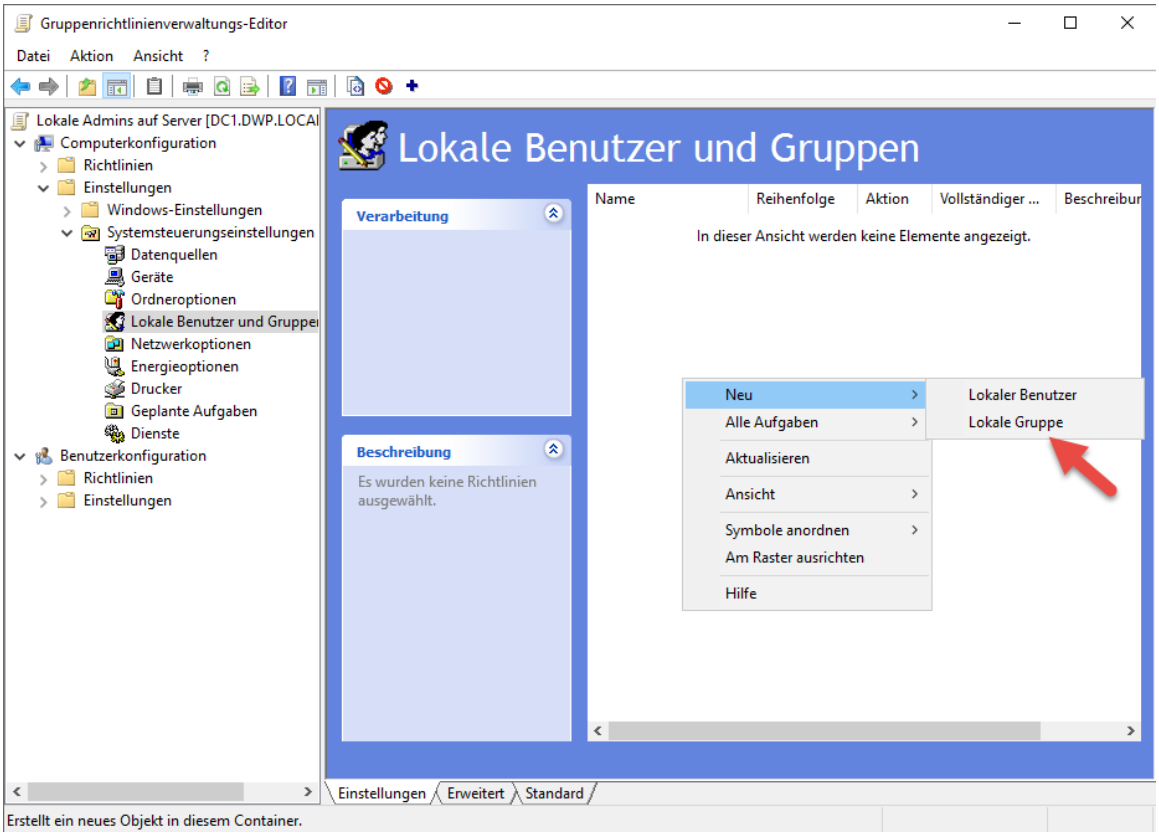
Lokale Administratoren managen

Die Gruppe enthält alle nötigen Benutzer, die auf den Servern tatsächlich das Recht benötigen. Die Anleitung ist nur ein Beispiel und soll die Vorgehensweise etwas näherbringen.

Danach erstellen wir ein neues GPO mit dem Namen Lokale Admins auf Server.

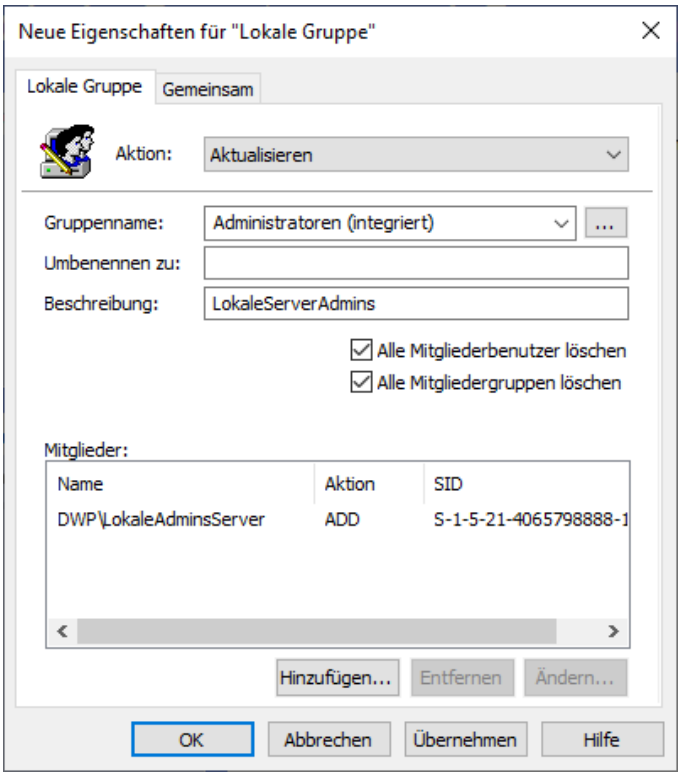


Als nächstes konfigurieren wir eine Lokale Gruppe.



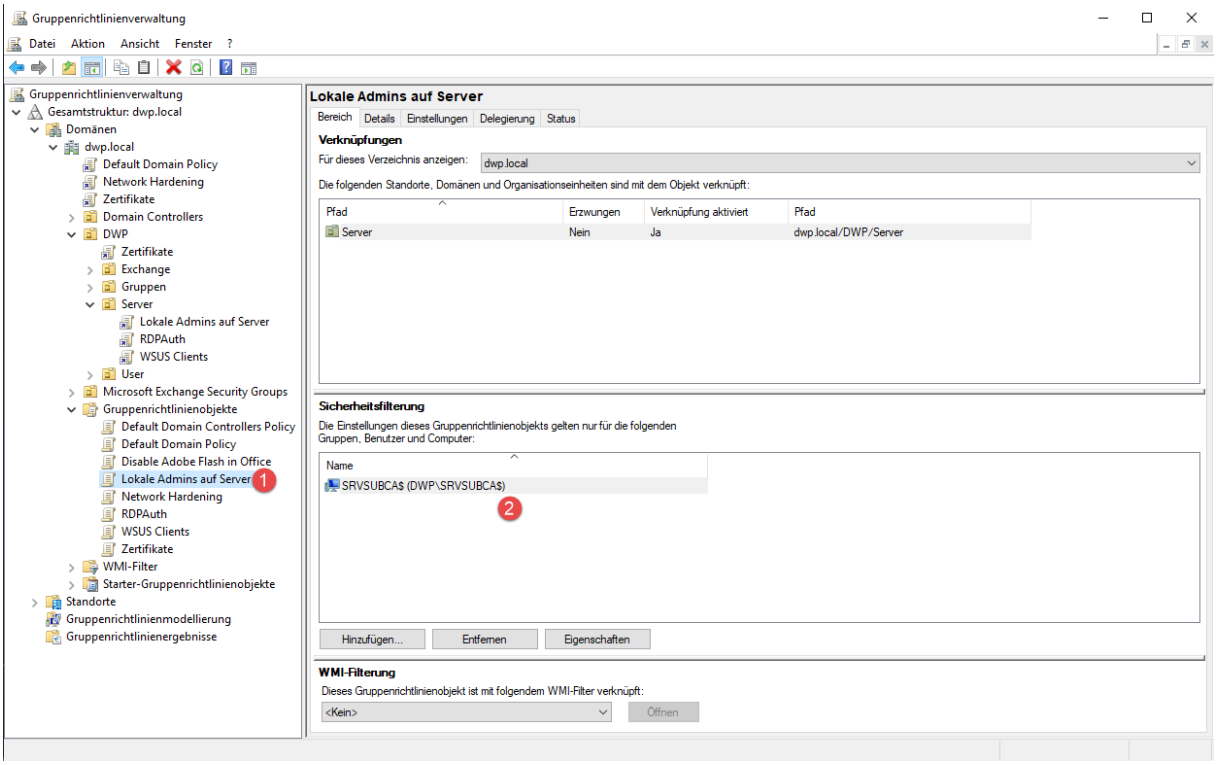
Lokale Administratoren managen

Die Konfiguration könnte so aussehen. Wir fügen der lokalen Gruppe der Administratoren eine neue Gruppe hinzu, und zwar die die wir zuvor im Active Directory angelegt haben (LokaleServerAdmins). Diese neue Gruppe sollte jetzt alle Benutzer enthalten, die die Server administrieren sollen. Zeitgleich, mit dem Setzen der Haken in Alle Mitgliederbenutzer löschen und Alle Mitgliedergruppen löschen entfernen wir den alten Wildwuchs. Der gute Nebeneffekt beim Setzen dieser Haken ist, das alle künftigen Benutzer und Gruppen die hinzugefügt werden, wiederrum im GPO Turnus (90 Minuten +-) entfernt werden.

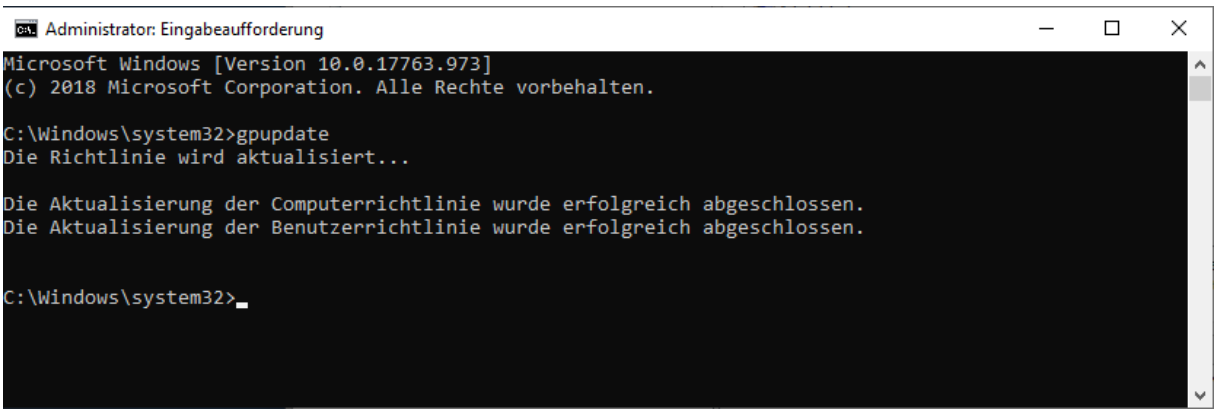


Lokale Administratoren managen

Jetzt verlinken wir das neue Gruppenrichtlinienobjekt auf die entsprechende OU und fügen die Server besser mittels einer Sicherheitsgruppe der Sicherheitsfilterung hinzu.

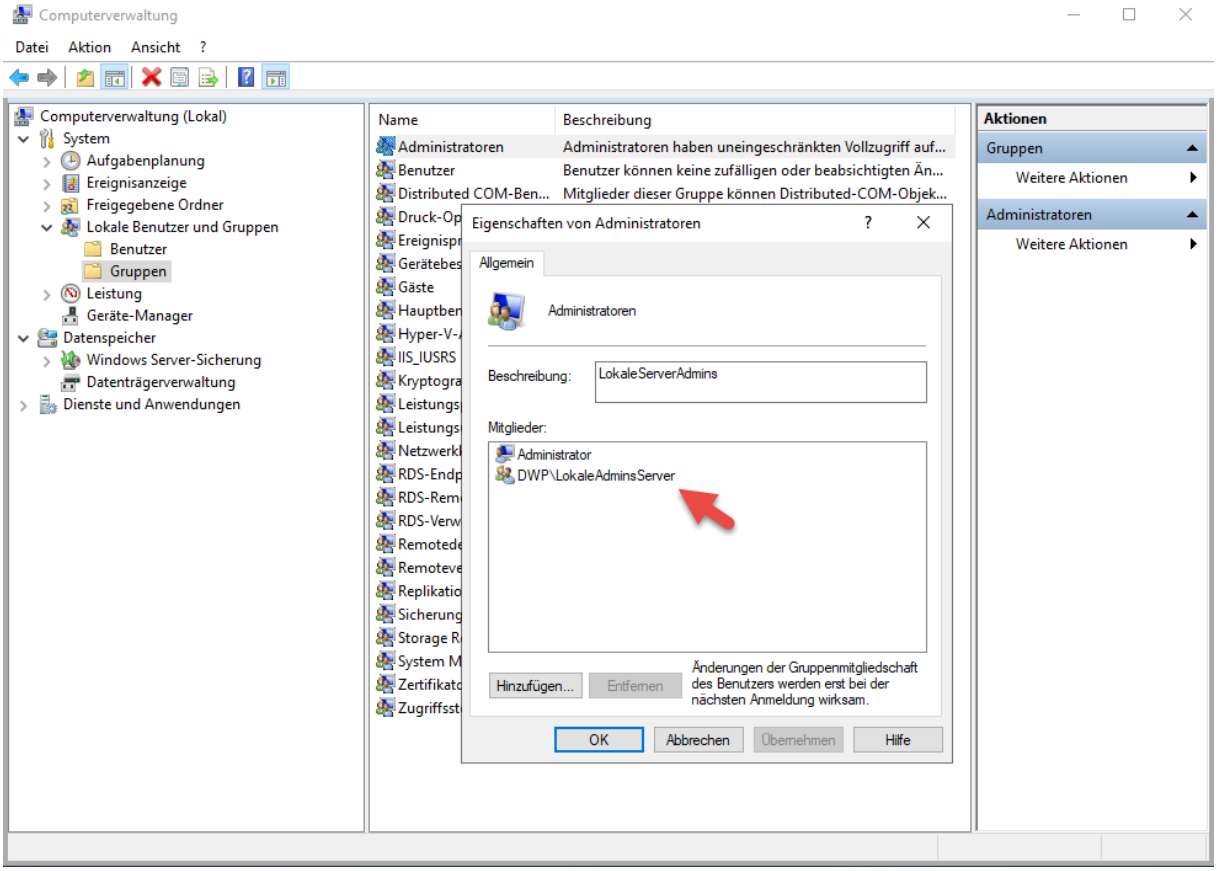


Nach einer Wartezeit oder durch das manuelle Ausführen von GPUPDATE werden die Richtlinien aktualisiert.

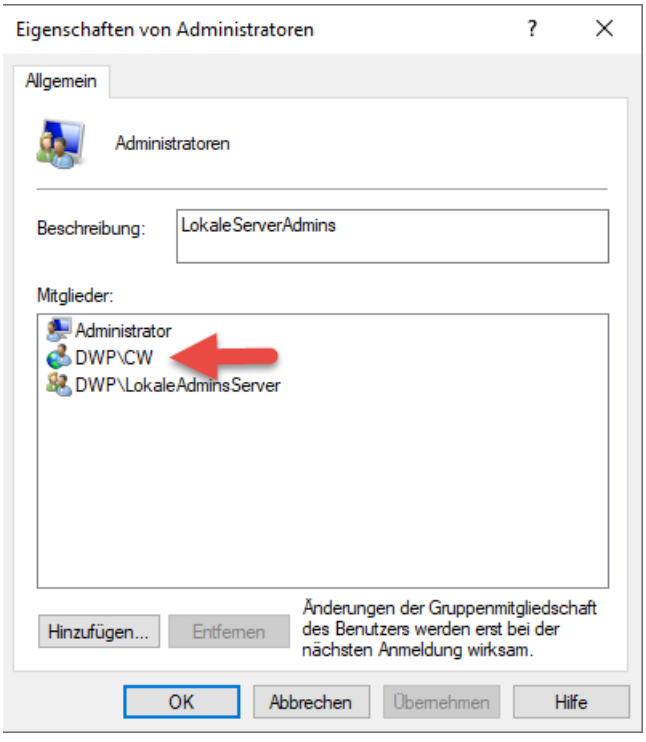


Lokale Administratoren managen

Nach der Aktualisierung sollte die neue Richtlinie gegriffen haben und nur noch die von uns gewünschte Sicherheitsgruppe vorhanden sein.

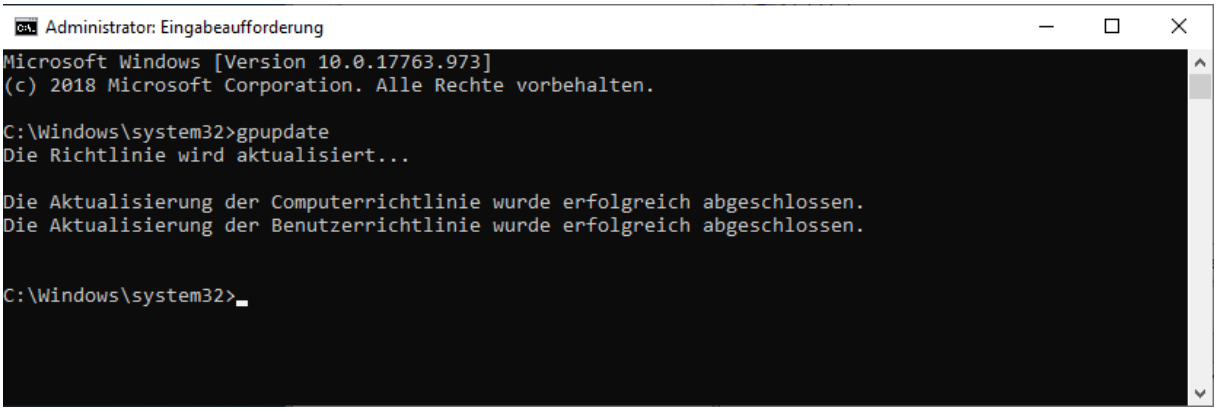


Fügt jetzt jemand unberechtigterweise wieder einen einzelnen Benutzer oder Gruppe hinzu, wird diese wieder entfernt.

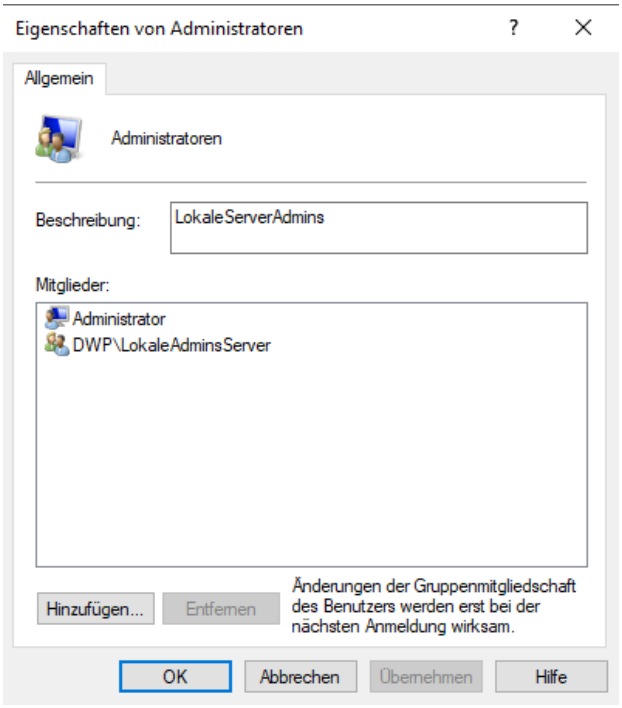


Lokale Administratoren managen

Nach einer Wartezeit oder durch das manuelle Ausführen von GPUPDATE werden die Richtlinien aktualisiert.



Auf diese Weise halten wir Ordnung und Transparenz und erhöhen die Sicherheit im Unternehmen, was der wesentliche Faktor ist.



Bitte erarbeitet vorher ein Konzept und denkt an die technischen Benutzer!