

Windows-Übung: NTFS-Dateiüberwachung

1. NTFS-Objektüberwachung testen

1.1 Objektzugriffsüberwachung aktivieren (Gruppenrichtlinie)

Melden Sie sich als Mitglied der Gruppe **Administratoren** an.
Aktivieren Sie in den Gruppenrichtlinien die Überwachung der Objektzugriffsversuche (erfolgreiche und fehlgeschlagene Versuche überwachen).

1.2 Überwachungseinträge konfigurieren (Ordneigenschaften)

Erstellen Sie den Ordner **C:\Test**.
Lassen Sie sämtliche Zugriffe überwachen.

1.3 Zugriffsversuche

Erstellen Sie im Ordner **C:\Test** die Datei **test.txt**.

1.4 Überwachungsprotokoll auswerten (Ereignisanzeige)

Schauen Sie sich das Überwachungsprotokoll an.

2. Beispiel

Erstellen Sie einen Benutzer **verdaechtig**
und die Ordner **C:\Erlaubt** und **C:\Verboten** mit jeweils einer Datei **test.txt**.
Der Benutzer **verdaechtig** erhält Lesezugriff auf den Ordner **C:\Erlaubt**
und keinen Zugriff auf **C:\Verboten**.
Ausserdem sollen sämtliche Zugriffe des Benutzers **verdaechtig** auf die beiden Ordner mitprotokolliert werden.
Melden Sie sich als **verdaechtig** an und versuchen Sie, die beiden Dateien zu löschen.
Schauen Sie sich das Überwachungsprotokoll an.

3. Überwachung wieder deaktivieren

Deaktivieren Sie die Objektzugriffsversuche wieder und löschen Sie alle angelegten Ordner und Benutzer.