aikux.com

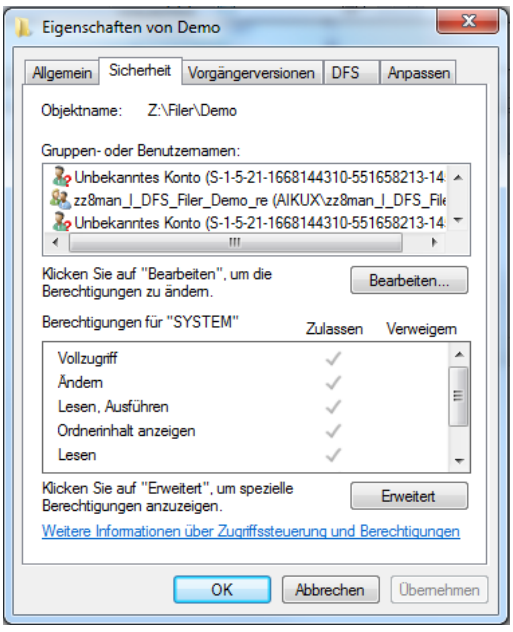
ACL-Cleaner

Das Werkzeug zum sicheren Entfernen von toten oder verwaisten SIDs

Was sind und wie entstehen tote bzw. verwaiste SIDs?
Viele Firmen und Organisationen haben gewachsene Fileserverstrukturen. Im Laufe der Jahre wurden immer wieder Berechtigungen gesetzt, mitunter auch falsch, so dass es nach dem Löschen der Accounts oder von Gruppen aus dem Active Directory ohne vorheriges Löschen der Einträge in der Access Control List (ACL) zu verwaisten SID-Einträgen in der ACE des Fileservers kommt.

Für die Steuerung der Zugriffsberechtigungen auf Fileserverressourcen empfiehlt sich die Nutzung von Domänen-Gruppen und Domänen-Accounts. Diese können direkt in die ACL der Verzeichnisse des Fileservers eintragen werden. Ein Domänen-Account oder eine Domänen-Gruppe besteht aus einer eineindeutigen Security-ID. Da diese SID für Menschen allerdings schlecht zu verwalten ist, wird dem Account auch noch ein Name gegeben. Windows arbeitet intern mit der SID – Administratoren arbeiten mit dem Namen. Wenn jetzt einem User oder einer Gruppe eine Berechtigung zugewiesen werden soll, dann sucht man den entsprechenden Account aus und weist diesem auf dem Fileserver die Berechtigungen zu. Im System geschieht noch etwas anderes: Auf Systemebene wird in der ACL nicht der Name vermerkt sondern die SID.

Wenn nun ein Account aus dem AD gelöscht wird, ohne dass vorher der Eintrag aus der ACL entfernt wurde, kann diese SID bei der nächsten Betrachtung der Sicherheitseinstellungen nicht mehr aufgelöst werden. Es steht kein Objekt im AD mit ihr in Referenz. Also kann und sollte dieser Eintrag auch entfernt werden.



Warum sollten verwaiste SIDs entfernt werden?
- erheblich verbesserte Übersicht
- Ausschluß bösartiger Manipulationen der SID-History mit nachfolgender unkontrollierter Rechtevererbung
- Vermeiden von Performanzverlusten

Wie entfernt der ACL-Cleaner tote oder verwaiste SIDs?
Alle Unternehmen und Organisationen, die das Werkzeug für das Rechtemanagement 8MAN im Einsatz haben, können mit 8MAN alle ACLs sichtbar machen, in denen sich verwaiste/ tote SIDs befinden. Diese können in einem CSV-Report aus 8MAN exportiert werden. Dann schlägt die Stunde für den ACL-Cleaner: Er ist in der Lage, die identifizierten ACLs zu bereinigen. Dazu wird der Export an den ACL-Cleaner übergeben, der nun der Reihe nach alle ACLs bereinigt. Nach dem nächsten Scan von 8MAN sind dann im Report für verwaiste/ tote SIDs keine Einträge mehr zu finden. Der ACL-Cleaner kann viele Stunden Arbeit und auch ein aufwendiges Scripting ersparen bzw. macht die Lösung des Problems erst möglich.

Empfohlene Systemvoraussetzungen:

Serverseitig:

- Microsoft Fileserver ab 2003, NetApp-Filer, EMC (weitere CIFs basierende Systeme)

Clientseitig (Ort der Installation des ACL-Cleaners):

- .net Framework 3.5 SP1 Vollinstallation
- Windows Server 2003 SP2 oder höher
- Windows XP SP3 oder höher
- RAM: 2 GB
- CPU: Aktueller Prozessor (min. 1 Kern)

aikux.com GmbH
Oldenburger Str. 37
10551 Berlin

Geschäftsführer: Thomas Gomell
Tel.: +49 (30) 8095010-40
Fax: +49 (30) 8095010-41
Email: info@aikux.com

www.aikux.com