10 | 18 Sonderdruck für G + H Systems

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

# G+H Systems Daccord 1.6

www.it-administrator.de

G+H Systems Daccord 1.6

# Stopp, Zugriffskontrolle!

von Jürgen Heyer

Die Kontrolle der Zugriffsberechtigungen ist in einem Unternehmen unverzichtbar, um Manipulationen und unkontrollierten Datenabfluss zu vermeiden sowie die gesetzlichen Anforderungen zu erfüllen. Die Herausforderung besteht dabei darin, alle bestehenden Rechtestrukturen zu überwachen und sich nicht nur auf einen Teil zu beschränken. Hier greift Daccord an, das sich über Konnektoren für eine ganzheitliche Übersicht flexibel anbinden lässt. IT-Administrator wollte genauer wissen, wie gut der Überblick gelingt.

Quelle: Roberto Rizzo – 123RF

Geht es darum, in einem Verzeichnisdienst wie beispielsweise dem Active Directory (AD) den Überblick über die Rechte zu behalten, stehen dem Administrator diverse Werkzeuge zur Verfügung. Schwieriger wird es in heterogenen Umgebungen, wo die Benutzer und Rechte an mehreren Stellen verwaltet werden. Dann wird es zu einer Herausforderung, diese auszulesen und zusammengefasst darzustellen. Genau dieses Szenario adressiert Daccord der Firma G+H Systems aus Offenbach am Main. Die Software-Appliance nutzt Konnektoren, um die verschiedenen Rechtestrukturen abzufragen und zu analysieren. Diese Informationen lassen sich innerhalb von Daccord synchronisieren und zusätzlich anreichern. Das Produkt kommt mit einem Standard-Konnektorset, weitere vorgefertigte Konnektoren lassen sich hinzubuchen. Darüber hinaus sind auch Anbindungen an individuelle Lösungen für branchenspezifische Systeme möglich, indem der Hersteller einen passenden Konnektor programmiert.

Zu beachten ist, dass das System zur einfacheren Visualisierung der diversen Zugriffsberechtigungen dient, es ist aber nicht zu deren Administration gedacht. Dementsprechend gibt es nur einen lesenden Zugriff auf die Quellen. Das ist wichtig für das grundsätzliche Verständnis des Leistungsumfangs.

## Persönliche Betreuung bei der Einrichtung notwendig

Basis von Daccord ist ein Linux-System, wie es uns für den Test als OVA-Datei für den Import in unsere VMware-Plattform zur Verfügung gestellt wurde. Allerdings gibt es für die endgültige Einrichtung kein vorbereitetes Setup, sondern es sind einige Einstellungen wie die genutzte IP-Adresse sowie die Ports an mehreren Stellen manuell einzutragen. Für unsere Testbereitstellung unterstützte uns der Hersteller über ein Fernsteuerungstool.

In der Regel erfolgt die Einrichtung von Daccord durch den Hersteller persönlich vor Ort. Hintergrund dafür ist, dass sich das Produkt vorwiegend für den Einsatz in heterogenen Umgebungen anbietet, wo von unterschiedlichen Systemen Zugriffsrechte ausgelesen werden sollen, und dies den Einsatz unterschiedlicher Konnektoren erfordert, die allesamt individuell zu konfigurieren sind.

Was die Ersteinrichtung des Linux-Systems anbetrifft, gibt es laut Hersteller für den IT-Verantwortlichen zwei Möglichkeiten: Der erste, schnellere und zuverlässigere Weg ist die Installation via Appliance. Dazu stellt der Nutzer eine leere VM-Hülle bereit, in die ein ISO-Image eingehängt wird. Daraus findet die Installation des Betriebssystems, MySQL, Java und zuletzt Daccord statt. Bei der

### G+H Systems Daccord 1.6

**Produkt**
Programm zur Verwaltung von Zugriffsberechtigungen in heterogenen Umgebungen.

**Hersteller**
G+H Systems
www.daccord.de

**Preis**
Daccord kostet einmalig 35 Euro pro aktivem Benutzer zuzüglich 20 Prozent Wartung jährlich. Für größere Benutzerzahlen gibt es Staffelpreise.

**Systemvoraussetzungen**
Virtuelle Maschine mit 50 bis 60 GByte Plattenkapazität und 4 bis 8 GByte RAM.

**Technische Daten**
www.it-administrator.de/downloads/datenblaetter

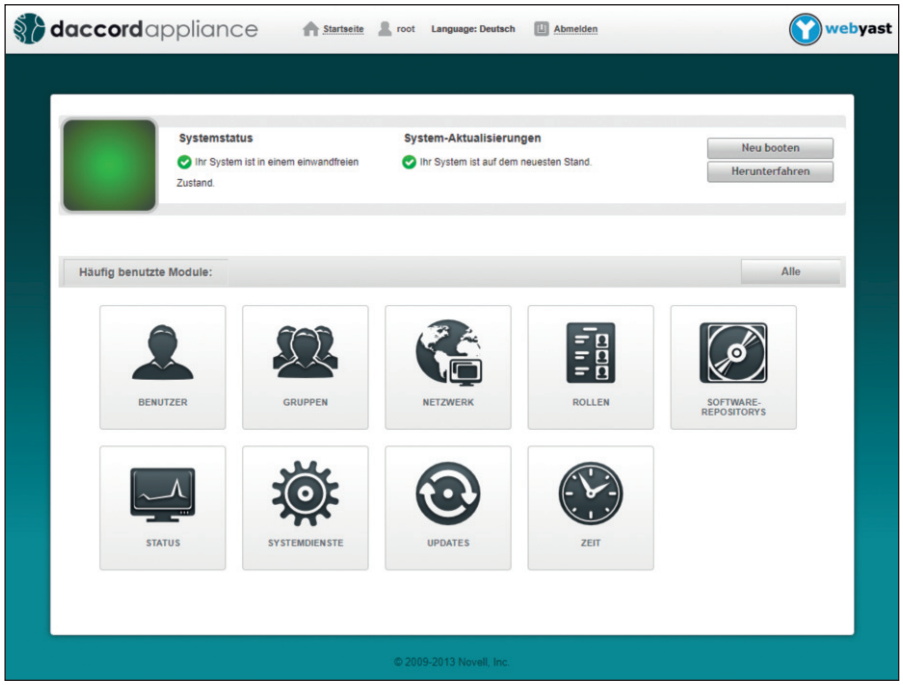


Bild 1: Teile der Appliance lassen sich über Yast konfigurieren, aber nicht sämtliche Einstellungen.

zweiten Variante bereitet der Anwender ein Linux-System inklusive der Komponenten wie MySQL und Java vor, um dann darauf Daccord über RPM-Pakete zu installieren.

Für den Einsatz in unserer Testumgebung konfigurierten wir die Anbindung an ein Active Directory mittels LDAP-Konnektor, der im Basislieferumfang enthalten ist. Bei der Einrichtung sind die LDAP-Informationen einzugeben sowie der Pfad zu den Benutzer- und Gruppeneinträgen. Nachdem Daccord auf die anliefernden Quellen nur lesend zugreift, reicht entsprechend ein Benutzer mit AD-Leserechten. Aus Sicherheitsgründen sollte auch tatsächlich nur ein leseberechtigter Benutzer verwendet werden, um das Schreiben konsequent zu unterbinden. Wie sich das Zurückschreiben im Sinne einer Automatisierung dennoch realisieren lässt, beleuchten wir später. Nach der Einrichtung dauerte es wenige Minuten, bis die Informationen aus dem AD in Daccord importiert waren und nach und nach angezeigt wurden.

Der Hersteller liefert zu Daccord eine übersichtliche Dokumentation als Download. Interessierte Administratoren können sich hier bereits gut einlesen und einen Überblick gewinnen. Die gesamte deutschsprachige Dokumentation ist ordentlich strukturiert und einfach verständlich.

## Beeindruckende Anbindungsmöglichkeiten

Um die Einsatzmöglichkeiten in einer heterogenen Umgebung genauer betrachten zu können, bekamen wir neben der Installation in unserer Laborumgebung einen Einblick auf ein umfassend eingebundenes System beim Hersteller. Dieser wirbt damit, dass bei einem großen Kunden über 400 Systeme regelmäßig ausgewertet werden und bisher jedes gewünschte System angebunden werden konnte – und sei es durch individuelle Programmierung.

Das Basispaket kommt standardmäßig mit Konnektoren für JDBC (Java Database Connection), CSV zum Einlesen von CSV-Dateien, Microsoft AD sowie LDAP. Damit sollte sich in der Regel der Großteil der Auswertungen realisieren lassen. Für die Erweiterung stehen eine Vielzahl an Konnektoren, Notifier und Request Handler zur Verfügung. So gibt es neben CSV auch Konnektoren für XML- sowie FLT-Dateien (Mainframe), MS NTFS, Novell NSS, MS Exchange, SharePoint, Novell Vibe, SAP, Office 365, Salesforce und zuletzt Google Apps.

Noch umfangreicher gestaltet sich die Übersicht einer Auswahl typischer Systemanbindungen. Zu nennen sind IAM-Systeme, Werkzeuge für das Endpoint-Management, weiterhin Speicher- und E-Mail-Systeme, diverse Bankensysteme, Helpdesk-Lösungen, Netzwerkmanagement sowie Monitoringsysteme. Der Hersteller nennt hier über 70 Beispiele. Aufgefallen ist uns dabei vor allem die umfangreiche Unterstützung von Bankensystemen mit allein 15 Positionen. Für eine individuelle Prüfung der Anforderungen empfiehlt sich auf jeden Fall eine Kontaktaufnahme mit dem Hersteller.

## Fest vorgegebene Oberfläche

Die Bedienung von Daccord erfolgt im Browser mittels Web-GUI. Nach der Anmeldung als Administrator erscheint das Admin-Frontend mit einigen Statistiken zu den verwalteten Personen und Systemen wie der Personenanzahl (gesamt, inaktiv, ausgetreten, ohne Benutzung), Personentypen (Interne, Externe, Andere) und dem Verlauf über die letzten Tage bis hin zu einem Monat. Für die einzelnen Benutzer gibt es User-Frontends mit entsprechend reduzierter Ansicht auf die eigenen Rollen und Rechte.

Die Ansichten sind fest vorgegeben und somit durch den Benutzer nicht individuell anpassbar. Auch ist kein Drilldown implementiert, um beispielsweise in einem Statistikfenster durch Anklicken eines Balkens wie der Gesamtanzahl der Benutzer mehr Details zu erfahren, etwa, welche Benutzer gezählt wurden. Der interaktiven Bedienung sind somit Grenzen gesetzt. Allerdings beschränkt sich die Funktionalität von Daccord auch auf die nachfolgend beschriebenen Möglichkeiten, die letztendlich keine komplexe Benutzerführung verlangen.

Sind mehrere Anbindungen implementiert und die Informationen zu den Personen, Benutzerkonten und Berechtigungen initial ausgelesen, kann die Arbeit mit Daccord beginnen. Eingangs erwähnten wir, dass das Tool eine MySQL-Datenbank nutzt, und zwar nicht nur zum Speichern der importierten Daten, sondern auch für eine ergänzende Anreicherung mit Zusatzinformationen wie der Unternehmensstruktur, um das Organigramm abzubilden oder um Details zu hinterlegen.

Um die Importe aus verschiedenen Quellen zu synchronisieren, also die jeweiligen

Benutzerinformationen einem gemeinsamen User-Objekt in Daccord zuzuweisen, gibt es verschiedene Möglichkeiten. Viele Firmen arbeiten beispielsweise mit Personalnummern. Sind diese Bestandteil der einzelnen Importe, so ist die Zuordnung verständlicherweise durch dieses gemeinsame Merkmal sehr einfach. Alternativ ist eine Zuordnung anhand des Namens möglich, im schlechtesten Falle bei keinerlei inhaltlichen oder logischen Gemeinsamkeiten ist eine manuelle Zuordnung erforderlich. Über entsprechende Regeln lässt sich die beste Vorgehensweise in Daccord hinterlegen, so dass dann innerhalb des Tools ein gesamtheitlicher Blick auf jeden Benutzer möglich ist.

## Rollen- und Berechtigungsmanagement im Fokus

Die wesentliche Funktion von Daccord besteht darin, ein umfassendes Rollen- und Berechtigungsmanagement einzurichten, um zu erkennen, wo einem Benutzer womöglich noch Rechte fehlen oder zu viele Rechte vergeben wurden. Die Bestätigung von Rechten wird in Daccord unter dem Schlagwort der "Zertifizierung" geführt.

Um wiederum bestehende Zertifizierungen zu prüfen, lassen sich Zeitintervalle hinterlegen, nach deren Ablauf die Berechtigung als sogenannte Rezertifizierung erneut zu bestätigen ist. Dies ermöglicht eine regelmäßige Compliancеprüfung, um sicherzustellen, dass es nicht auf Dauer Benutzer mit zu vielen Rechten gibt, nur weil sich beispielsweise deren Aufgaben geändert haben. Üblicherweise reklamiert ein Benutzer in so einem Fall fehlende Berechtigungen von sich aus sofort, bezüglich der Rückgabe nicht mehr benötigter Rechte dagegen agiert er eher zurückhaltend. Daccord kann hier die notwendige Kontrolle übernehmen.

Um die diversen Beziehungen zu hinterlegen, gibt es vier Managementsichten, genannt "Person Manager", "System Manager", "Rights Manager" und "Role Manager". Darüber hinaus existiert noch die Möglichkeit zum Eintragen von entsprechenden Vertretungen. Fällt ein Manager zum Beispiel wegen einer Krankheit für längere Zeit aus, kann ein anderer Manager mit Hilfe des Vertretungsmodus seine Vertretung übernehmen. Die Sicht Personenmanager beschreibt die Verantwortlichkeit der Personen in einem Unternehmen und bildet quasi die Organisationsstruktur ab.

Als Systemmanager werden die Personen hinterlegt, die für eines der importierten Systeme zuständig sind. Ein Systemmanager kann für das System, für das er verantwortlich ist, alle Benutzerkonten und Berechtigungen einsehen. Beispielsweise kann er sich anzeigen lassen, welche Benutzerkonten über einen gewissen Zeitraum wie beispielsweise 90 Tage nicht benutzt worden sind. Das hilft bei der Bereinigung und ist ein wertvoller Beitrag zur Erhöhung der Sicherheit. Die Sicht des Systemmanagers ist letztendlich immer systembezogen.

Der Rechtemanager wiederum kann alle Berechtigungen einsehen, für die er verantwortlich ist, auch systemübergreifend. Der Rollenmanager letztendlich sieht sämtliche Rollen, für die er als Verantwortlicher eingetragen ist, sowie deren Zuweisungen. Rollen werden aufgabenbezogen definiert, um so einfach prüfen zu können, ob die Mitarbeiter entsprechend ihrer Aufgaben die passenden Rechte besitzen. Die Beschreibung der unterschiedlichen Manager zeigt auf, dass es in Daccord unterschiedliche, sich durchaus überschneidende Sichten gibt entsprechend der Zuständigkeiten der einzelnen Administratoren.

Die bereits erwähnte (Re-)Zertifizierung betrifft die Rollen sowie die Berechtigungen. Hinsichtlich der Berechtigungen werden die importierten Rechte mit den in Daccord zertifizierten Berechtigungen verglichen, um so zu erkennen, ob die Vergabe passt. Die Rollen wiederum werden den Mitarbeitern je nach Aufgabe zugewiesen. Dann lässt sich bei einem Systemimport feststellen, ob ein Mitarbeiter aufgrund seiner Rollen in dem jeweiligen System die notwendigen Berechtigungen

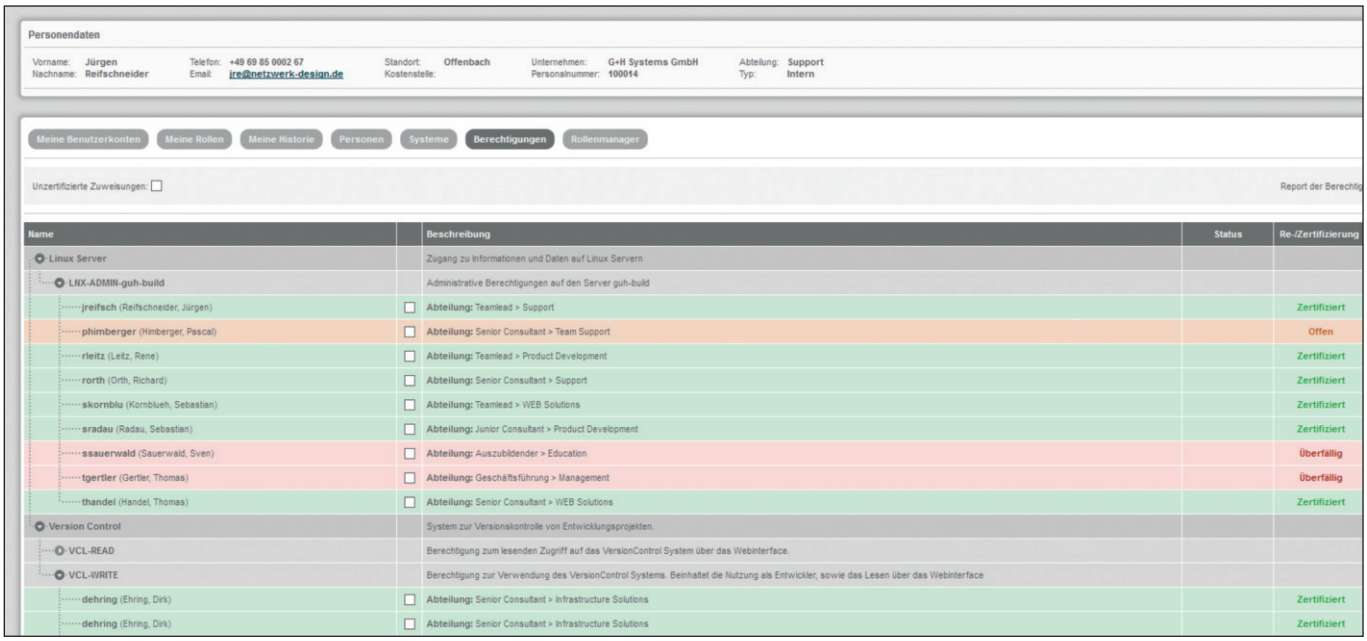


Bild 2: Die Berechtigungen auf die einzelnen Systeme listet Daccord übersichtlich auf und hinterlegt sie ihrem Status entsprechend farbig.

hat. Fehlen welche, muss der Manager dafür sorgen, dass der Mitarbeiter die Rechte bekommt. Falls dagegen zu viele Rechte vergeben sind – Daccord nennt dies Überberechtigungen – muss der Manager entscheiden, ob er die Rechte zertifiziert und damit legitimiert oder ob er dafür sorgen muss, dass die Rechte wieder genommen werden.

## Formulare für Änderungswünsche

Grundsätzlich ist Daccord, wie bereits erwähnt, nicht für die Administration gedacht, sondern vermittelt nur einen Blick auf den Status nach dem Motto "Nur gucken, nicht anfassen". Wie oben beschrieben ist es möglich, die ausgelesenen Informationen innerhalb von Daccord anzureichern und diese Anreicherung auch zu verändern. Die eingelesenen Daten lassen sich jedoch nicht direkt in Richtung der Importquellen zurückschreiben.

Es gibt aber die Möglichkeit einer Beantragung, mit der sich Klärungswünsche, Löschaufträge sowie Re-Zertifizierungsanfragen erfassen lassen. In allen Fällen öffnet sich ein Antragsformular zum Ausfüllen. Mit dem Abschicken lässt sich eine Aktion verknüpfen wie das Versenden einer E-Mail oder das Ansprechen einer Webservice-Schnittstelle eines anderen Systems wie beispielsweise einer IAM-Lösung (Identity- and Accessmanagement). Bereits im Basispaket enthalten sind ein Mail Request Handler für eine Aktionsbeantragung per E-Mail sowie ein Webservice Request Handler, um die SOAP-Webservice-Schnittstelle eines anderen Tools ansprechen zu können. Der Bearbeitungsstatus eines Antrags ist in Daccord bis zu dessen Abschluss einsehbar.

## Über die Ansichten verteiltes Reporting

Daccord verfügt über keinen eigenen Bereich zum Berichtswesen. Vielmehr finden sich auf den einzelnen Übersichtsseiten kleine Schaltflächen zur Berichtsausgabe in den Formaten PDF und/oder Excel. Die Reporte sind fertig vorbereitet und nicht durch Filter oder Ähnliches anpassbar. Denkbar ist bei einer Excel-Ausgabe allenfalls eine anschließende Filterung oder Gestaltung.

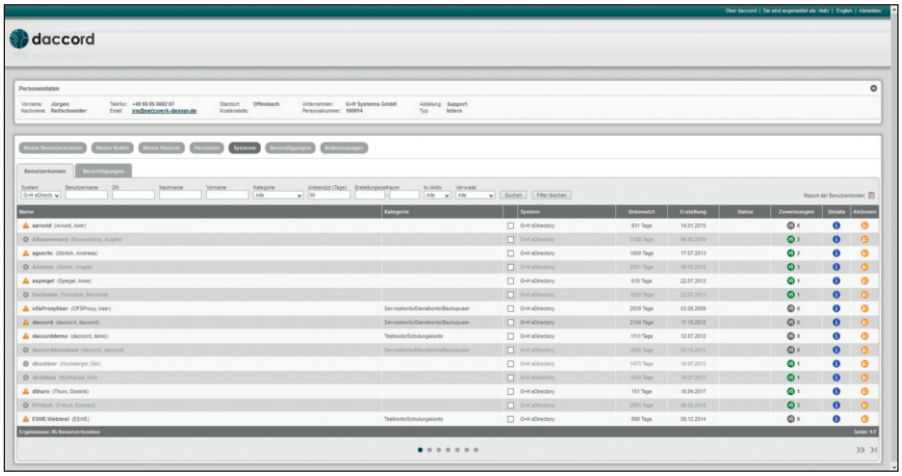


Bild 3: Unbenutzte Accounts sind bekanntlich ein Sicherheitsrisiko, Daccord listet diese auf Wunsch auf.

Um Änderungen nachzuvollziehen, zeichnet Daccord alle Aktionen eines Benutzerkontos auf. Diese sind in einer Übersicht chronologisch aufgelistet und lassen sich nach verschiedenen Kriterien filtern. Die angezeigten Aktionen sind in die zwei Arten "Prozess" und "Systemereignis" unterteilt. Zu jeder gelisteten Aktion lassen sich wiederum die einzelnen Prozessschritte anzeigen. Nach Anklicken erscheint ein Fenster mit Detailinformationen wie die Attribute und dessen Werte.

## Fazit

Daccord eignet sich für heterogene Umgebungen, wo mehrere Benutzer diverse Berechtigungen auf unterschiedlichen Systemen haben und diese überwacht werden sollen. Das Tool wird umso interessanter, je mehr Systeme es im Unternehmen gibt, in denen individuelle Berechtigungen zu pflegen sind. Daccord ist ausschließlich zur Analyse der Berechtigungen gedacht, sodass für das Erfassen ein Benutzer mit Leserechten reicht. Beeindruckend ist die Unterstützung von über 400 Systemen, wobei der Hersteller auf Anfrage auch individuelle Anpassungen vornimmt. Auch wenn das Tool nicht für die Rechteadministration gedacht ist, lassen sich Änderungsanträge beispielsweise per E-Mail verschicken oder an eine Webservice-Schnittstelle übergeben, um so eine Aktion zu initiieren. Denkbar ist auch die Anbindung an ein Ticketsystem oder eine IAM-Lösung, die dann Berechtigungen ändert.

Gut gefallen hat uns, dass sich Daccord für Complianceprüfungen eignet und die Berechtigungssituation aus verschiedenen Sichten auflistet. Dies können sowohl fehlende Rechte sein als auch unerwünschte Überberechtigungen, die wieder entfernt werden sollten. Nicht ganz trivial ist die Einrichtung, die in der Regel durch den Hersteller erfolgt. Auch die Bedienung könnte insgesamt etwas intuitiver sein inklusive einer Drilldown-Möglichkeit. *(jp)*

### So urteilt IT-Administrator

| | |
|---|---|
| Inbetriebnahme | 6 |
| Bedienung | 7 |
| Funktionsumfang | 8 |
| Anbindungsmöglichkeiten | 9 |
| Berichtswesen | 7 |

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

### Dieses Produkt eignet sich

**optimal** für heterogene Umgebungen, in denen an mehreren Stellen Rechte vergeben sind. Daccord ermöglicht hier eine übergreifende Sicht und Complianceprüfung.

**bedingt** für Umgebungen, wo die Rechte nur an wenigen Stellen vergeben werden. Zu bewerten ist hier, wie wichtig eine globale Übersicht ist.

**nicht**, sofern die Rechte nur an einer Stelle vergeben werden. Dies ist in der Regel mit den vorhandenen Bordmitteln zu lösen und erfordert kein zusätzliches Tool.