10 | 20 Sonderdruck für G+H Systems

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

G+H Systems Daccord Microsoft Edition

www.it-administrator.de

G+H Systems Daccord Microsoft Edition

Das Dickicht lichten

von Jürgen Heyer

Je größer das Active Directory und das Filesystem werden, desto schwerer ist es, veraltete oder ungenutzte Benutzer- oder Dienstkonten zu finden sowie die effektiven Rechte im Dateisystem zu ermitteln. Hier setzt die neue Daccord Microsoft Edition an, um die Situation zu analysieren und auf Auffälligkeiten sowie Schwachstellen hinzuweisen. IT-Administrator wollte genauer wissen, wie gut der Überblick gelingt.

In der Oktober-Ausgabe 2018 hatten wir uns die damals aktuelle Version Daccord 1.6 angesehen. Deren Fokus war es, in heterogenen Umgebungen, wo die Benutzer und Rechte an mehreren Stellen verwaltet werden, die verschiedenen Rechtestrukturen abzufragen und zu analysieren.

Inzwischen hat der Hersteller G+H Systems aus Offenbach die "Daccord Microsoft Edition" entwickelt, die sich auf die Berechtigungen und Benutzerkonstellationen im Active Directory (AD) sowie im NTFS-Filesystem konzentriert. Die Software arbeitet als eigenständiges Linux-System und nutzt Agenten zum Zugriff auf die Microsoft-Umgebung.

Zu beachten ist, dass die Edition zur einfacheren Visualisierung der diversen Zugriffsberechtigungen dient, sie ist aber nicht zu deren Administration gedacht. Dementsprechend ist auch nur ein lesender Zugriff auf das AD sowie die Fileserver notwendig. Das ist wichtig für das grundsätzliche Verständnis zum Leistungsumfang. Zum Testzeitpunkt stand die Software kurz vor der Veröffentlichung und wir konnten einen Blick darauf werfen.

Installation mit Linux-Umweg

Was den überzeugten Windows-Administrator am meisten wundern dürfte, ist der Umstand, dass die Daccord Microsoft Edition auf einem Linux-System läuft und eine entsprechende Installation voraussetzt. Zur Auswahl stehen drei Linux-Varianten (siehe Kasten), wobei wir uns für OpenSuse Linux 15.1 mit Gnome Desktop entschieden. Wichtig ist in dem Fall, dass bei der Installation der genannte Desktop gewählt wird und nicht KDE, weil es sonst bei der Daccord-Installation zu einem Konflikt mit der benötigten MariaDB kommt.

Dass eine Einrichtung auch jemandem ohne besondere Linux-Kenntnisse gelingen kann, hat der Testautor selbst ausprobieren können. Letztendlich erforderte die Installation keine besonderen Eingaben und zog sich alle aktuellen Pakete aus dem Internet. Das Schwierigste war es, anschließend SSH zu aktivieren, um dann beispielsweise mit WinSCP das Daccord-Installationsskript auf das System zu kopieren. Ebenfalls wichtig ist, dass die DNS-Namensauflösung korrekt funktioniert, da andernfalls Daccord den Domain Controller für die AD-Anbindung nicht findet. Sind diese Voraussetzungen erfüllt, kann der Administrator mit dem Quick Start Guide beginnen, der ihn auf 72 Seiten durch die weitere Installation sowie die Grundeinrichtung führt.

72 Seiten mag viel klingen, es sind aber letztlich viele Screenshots und der Admin muss nur einige Male mit der Maus klicken, um diverse Dinge wie eine Collector Engine, eine Policy Engine und einen CSV- sowie einen NTFS-Connector anzulegen und zu konfigurieren. Dabei kann er durchweg die Standardeinstellungen übernehmen und muss nur die eine oder andere IP-Adresse eintragen, ein administratives Benutzerkonto für das Daccord-Portal erstellen sowie einen Benutzer für den lesenden Zugriff auf das AD angeben. In der ersten Version ist der Zugriff auf ein AD begrenzt, die Anbindung mehrerer ADs soll mit einem der nächsten Updates kommen.

Der CSV-Connector dient dem Import aktueller Personendaten, wobei dieser Import im Rahmen der Installation oder auch später erfolgen kann. Diese Personendaten dienen als Referenz für den Abgleich mit dem AD-Inhalt, worauf wir weiter unten noch eingehen. Weiterhin

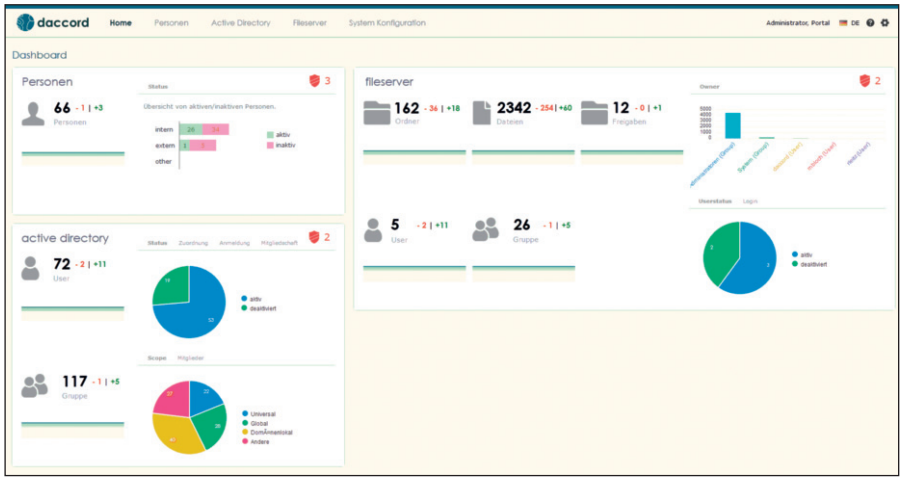

Bild 1: Das Dashboard liefert die wichtigsten Kennzahlen auf einen Blick und ermöglicht durch einen Drilldown eine einfache Bedienung.

kann der Verantwortliche über den erwähnten NTFS-Connector sämtliche Fileserver anbinden, deren Berechtigungen Daccord analysieren soll. In diesem Zuge sind die zu prüfenden Laufwerke auszuwählen. Auf jedem Fileserver wiederum ist ein Agent zu installieren. Während dessen Konfiguration ist ein Benutzerkonto anzugeben, das die Berechtigung zum Anmelden als Dienst besitzt, da der Agent später im Hintergrund läuft. Der Quick Start Guide hilft hier detailliert bei der Einrichtung. Daccord erlaubt das Anbinden beliebig vieler Fileserver.

Nach dem Einrichten dauert es eine gewisse Zeit, bis die ersten Ergebnisse auf der Benutzeroberfläche erscheinen. Um die Bereitstellung von Daccord zukünftig noch weiter zu vereinfachen und die Linux-Einrichtung zu umgehen, arbeitet der Hersteller bereits daran, die komplette Software als Docker-Image bereitzustellen. Mithilfe von Windows Docker muss sich der Administrator dann gar nicht mehr mit Linux auseinandersetzen und bekommt letztendlich einen fertigen Container mit der lauffähigen Daccord-Software. Zum Veröffentlichungszeitpunkt dieses Tests dürfte die Docker-Variante bereits verfügbar sein.

Intuitive grafische Oberfläche

Die Bedienung von Daccord erfolgt im Browser mittels WebGUI. Gegenüber dem Test im Herbst 2018 präsentiert sich die Oberfläche weitaus moderner, bunter und ansprechender mit integrierten grafischen Statistiken. Nach der Anmeldung gelangt der Benutzer auf ein Dashboard mit den wichtigsten Informationen, aufgeteilt in die vier Bereiche "Personen", "Active Directory", "Systeme" sowie "Fileserver". Diese Punkte finden sich neben dem Eintrag "Home" für das Dashboard auch in der Kopfzeile der Oberfläche wieder. Im Gegensatz zur Ansicht von 2018 ist die Bedienung jetzt deutlich intuitiver geworden, da der Administrator auf die einzelnen Elemente das Dashboards klicken kann und dann über einen Drilldown dazu weitere Informationen erhält.

Symbolische Schutzschilder in Ampelfarben mit einer Zahl daneben weisen auffällig auf erkannte kritische Probleme beziehungsweise Schwachstellen hin, die der Administrator sich genauer ansehen und beseitigen sollte. Ein Klick darauf reicht, um eine entsprechende Auflistung zu bekommen. Ein nächster Klick auf einen Eintrag wiederum liefert weitere Detailinformationen. In den anderen Ansichten neben dem Dashboard sind ebenfalls Schutzschilder zu finden, hier mit kleinen rot oder gelb unterlegten Zahlen, um so auf Probleme entsprechend ihrer Kritikalität hinzuweisen.

Weitere groß dargestellte Kennzahlen in den Bereichen liefern unter anderem Informationen, wie viele Benutzer importiert wurden, wie viele Benutzer und Gruppen es im AD gibt sowie die Anzahl der Ordner, Dateien, Freigaben, Benutzer und Gruppen auf den Fileservern. Kleinere Zahlen jeweils daneben in Rot und Grün zeigen die Veränderungen seit dem letzten Einlesen an. So ist schnell erkennbar, in welchem Umfang in den einzelnen Bereichen und bei den Kennzahlen Änderungen aufgetreten sind.

Genauer Blick auf den Benutzerstamm

Sofern im Rahmen der Einrichtung noch keine Mitarbeiter über die erwähnten CSV-Dateien importiert wurden, sollte dies nun geschehen, um so Referenzdaten vorliegen zu haben, gegen die das System prüfen kann. Wichtig ist es dabei, den aktiven Mitarbeiterstamm zu importieren und diesen auch regelmäßig zu aktualisieren. Um die Daten im passenden Umfang bereitzustellen, lässt sich ein vorbereitetes Template herunterladen, das die Spalten angibt, die zu befüllen sind. Der Administrator muss also darauf achten, dass er die Benutzerdaten passend liefert, sonst ist ein Import nicht möglich. Der Mitarbeiterstamm kann aus verschiedenen Quellen stammen, beispielsweise aus SAP oder von einer HR-(Human Resources)-Software, die zur Personalverwaltung verwendet wird.

Sind die Benutzer importiert, führt Daccord verschiedene Prüfungen durch, sowohl einen Vergleich der importierten Benutzerinformationen mit den AD-In-

Daccord Microsoft Edition

Produkt
Programm zur Überprüfung von Zugriffsberechtigungen in Windows-Umgebungen.

Hersteller
G+H Systems
www.daccord.de

Preis
Daccord kostet einmalig 19,20 Euro pro aktivem AD-Benutzer zuzüglich 20 Prozent Wartung jährlich für die Folgejahre. Für größere Benutzerzahlen gibt es Staffelpreise.

Systemvoraussetzungen
Virtuelle Maschine mit 100 GByte Plattenkapazität, zwei CPUs, 8 GByte RAM.

Betriebssysteme: SuSE Linux Enterprise Server 12 SP2, SP3 oder SP4 oder OpenSuse 15.1 Textversion oder Gnome Desktop sowie CentOS Linux release 8.1.1911.

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

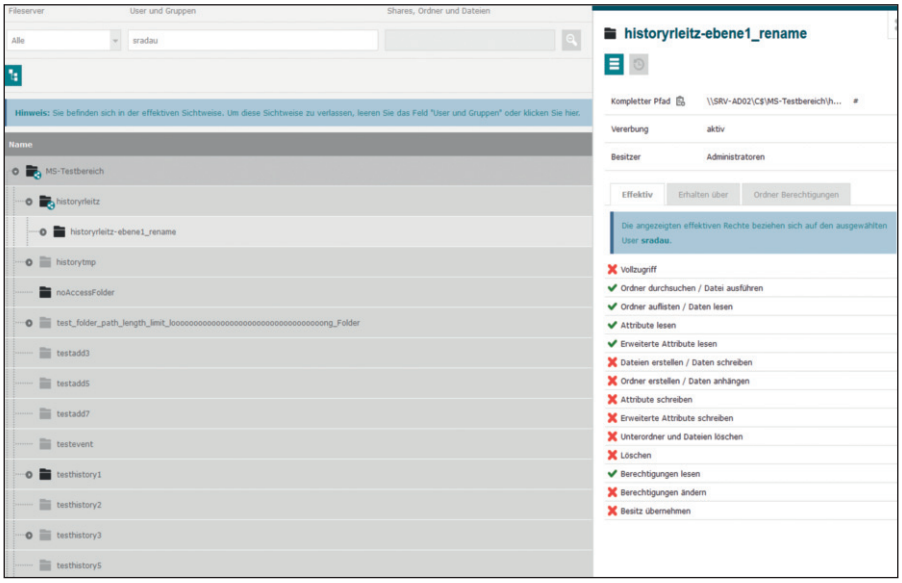

Bild 2: Daccord zeigt die effektiven Rechte für Benutzer und Gruppen übersichtlich an sowie auf welchem Weg die Rechte zustande kommen.

halten als auch eine Prüfung der AD-Informationen gegenüber dem bei der Einrichtung importierten Richtlinienkatalog. So findet Daccord beispielsweise Konten von ausgeschiedenen Benutzern, die im AD noch aktiv sind und damit ein mögliches Sicherheitsrisiko darstellen. Ebenso findet das Programm Mitarbeiter ohne einen Verantwortlichen, inaktive Verantwortliche oder Konten mit identischen Benutzernamen. Auch deckt es Personen auf, die für sich selbst verantwortlich sind.

Prüfungen von Benutzerrechten innerhalb des AD dienen dazu, Konten zu finden, die beispielsweise das Recht haben, als Dienstkonto zu fungieren, oder die sich direkt in lokalen Gruppen befinden. Weiterhin weist das System darauf hin, wenn die Anzahl der Domänen-Admins auffällig groß ist oder wenn es mit sich selbst verschachtelte Gruppen gibt. Gut gefallen hat uns, dass Daccord nicht nur die nackten Informationen liefert, sondern auch Hinweise, gegen welche Empfehlungen verstoßen wird.

Basis ist hier das bei der Einrichtung importierte Richtlinienpaket, das Best Practices enthält, Empfehlungen aus dem BSI-Maßnahmenkatalog sowie aus der ISO 27001. Neben dem universellen Paket ist es möglich, sich für individuelle Richtlinien in Absprache mit dem Hersteller ein eigenes Paket schnüren zu lassen und dieses zu importieren. Es gibt auch bereits Überlegungen zum Bau eines Richtlinien-Builders für den Administrator, was aber noch zu konkretisieren ist. Eine gute Unterstützung ist, dass Daccord in der eigenen Datenbank jegliche Änderungen erfasst, sodass es eine genaue Historie gibt und sich alles detailliert nachvollziehen lässt.

Detaillierte Analyse der Fileserver-Berechtigungen

Administratoren von Berechtigungen im Dateisystem von Windows-Fileservern wissen, dass die Sicht der Bordmittel eher rudimentär ausfällt und es nach wie vor schwierig ist, die effektiven Rechte auf einen Blick zu erkennen. Oft bekommen Benutzer im Laufe der Zeit immer mehr Rechte und es ist irgendwann nicht mehr genau ersichtlich, was hier zu viel ist und nicht mehr benötigt wird. Regelmäßige Compliance-Prüfungen helfen dabei, 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. Aus Sicht des Unternehmens sollte es aber das Ziel sein, den Benutzern genau die Rechte zu geben, die sie zur Erfüllung ihrer Aufgaben benötigen. Daccord kann hier die notwendige Kontrolle übernehmen. Für die Anzeige der Berechtigungen und Freigaben kennt Daccord zwei Verfahren. Ist kein Benutzer und keine Gruppe ausgewählt, erfolgt die Anzeige vom Umfang her vergleichbar mit den Windows-Bordmitteln, nur optisch etwas besser aufbereitet. Möglichkeiten zum Ändern gibt es aufgrund des nur lesenden Zugriffs nicht.

Wählt der Administrator im Kopfbereich der Ansicht einen Benutzer oder eine Gruppe aus, so listet Daccord auf einem Registerblatt die effektiven Rechte für dieses Objekt auf. Um noch mehr zu erfahren, kann der Administrator auf ein anderes Registerblatt umschalten, wo er sieht, auf welchem Weg das gewählte Objekt Rechte auf eine Freigabe oder ein Verzeichnis erhalten hat. Hier kann es zu Überlappungen kommen, wenn beispielsweise ein Benutzer bestimmte Rechte auf eine Freigabe durch direkte Zuweisung sowie durch eine Gruppenzugehörigkeit bekommt. Wichtig sind letztlich die effektiven Rechte. Wenn diese nicht passen, kann sich der Administrator über Daccord genau informieren, an welcher Stelle er etwas ändern muss.

Neben dieser individuellen Analyse prüft Daccord die Fileserver-Laufwerke ebenso gegen ein Richtlinienpaket und ermittelt, wo die Vererbung unterbrochen ist, wo Rechte (außer an "Administrators" und "System") vergeben wurden, wo "Jeder" berechtigt ist, welche Benutzerkonten Vollzugriff haben und ob es Anmeldungen als lokaler Administrator gab. Auch ermittelt Daccord globale Gruppen mit direkten Berechtigungen, verwaiste SIDs, in der Regel unerwünschte direkte Berechtigungen von Benutzern und einiges mehr.

Wir haben uns im Test die Rechtestruktur auf typischen Fileservern angesehen und merkten schnell, dass Daccord deutlich übersichtlichere Informationen liefert und das auch viel einfacher, als es mit Windows-Bordmitteln möglich ist. Bei der Arbeit mit Daccord ist zu beachten, dass der Zugriff wie erwähnt ausschließlich lesend erfolgt und keinerlei Administration möglich ist. Vielmehr vermittelt das Werkzeug einen Blick auf den Status. Für Änderungen muss der Administrator somit auf die Windows-Bordmittel oder

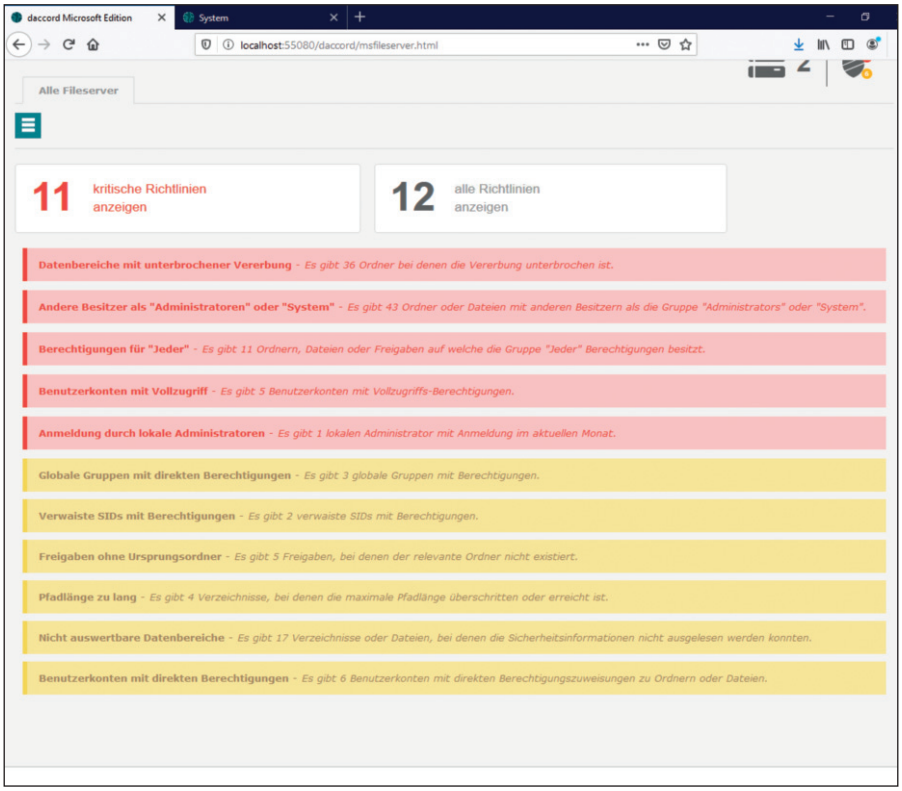

Bild 3: Daccord prüft das Dateisystem auf Richtlinienverstöße und hilft dadurch bei der Beseitigung von Schwachstellen und Sicherheitslücken.

ein anderes Tool zugreifen. Dann muss er bei Daccord eine nochmalige Analyse veranlassen und kann sich anschließend die Rechte erneut ansehen. Das mag auf den ersten Blick etwas umständlich erscheinen, letztlich aber sollte davon auszugehen sein, dass sich ein Administrator bei der Rechtevergabe auskennt und Daccord in erster Linie zur zusätzlichen Kontrolle verwendet.

Über die Ansichten verteiltes Reporting

Daccord verfügt über keinen eigenen Bereich, in dem das Berichtswesen zusammengefasst ist. Vielmehr finden sich auf den einzelnen Übersichtsseiten kleine Schaltflächen zur Berichtsausgabe im PDF-Format, teils auch als CSV-Datei. Die Reporte sind fertig vorbereitet und nicht durch Filter oder Ähnliches anpassbar, im Falle von CSV ist eine anschließende Filterung in Excel denkbar.

Um Änderungen zu erkennen, vergleicht Daccord die diversen Importe der Benutzer und der Fileserver-Berechtigungen und erstellt daraus chronologische Ansichten der Historie. So kann ein Betrachter schnell erkennen, wann was geändert wurde. Der Änderungszeitraum lässt sich in mehreren Schritten zwischen den letzten sieben und 180 Tagen filtern.

Fazit

Die Daccord Microsoft Edition eignet sich ideal für komplexe Windows-Umgebungen, in denen für viele Benutzer im Active Directory diverse Datei- und Freigabeberechtigungen auf unterschiedliche Fileserver vergeben wurden und diese überwacht werden sollen. Das Tool wird umso interessanter und hilfreicher, je mehr Benutzer, Gruppen und Fileserver es im Unternehmen gibt, wo individuelle Berechtigungen zu pflegen sind. Die Erweiterung der Unterstützung von einem auf mehrere ADs ist fest geplant.

Für einen typischen Windows-Administrator ist der Umstand sicher ungewöhnlich, dass die Software unter Linux läuft und eine entsprechende Installation erforderlich ist, um anschließend Daccord zu installieren. Die Einrichtung erwies sich im Test als so einfach, dass Linux-Grundkenntnisse durchaus ausreichen. Der Hersteller arbeitet zudem an einem optionalen Docker-Image, das zum Veröffentlichungszeitpunkt dieses Tests bereits verfügbar sein sollte. Damit erübrigt sich auf Wunsch die gesamte Installation.

Die Daccord Microsoft Edition ermöglicht Compliance-Überprüfungen sowohl für die Benutzerpflege als auch die Rechtevergabe im Dateisystem und kommt dazu mit vorbereiteten Richtlinienpaketen. Nicht mehr genutzte Benutzeraccounts oder welche mit zu vielen Rechten lassen sich auf diese Weise gut ermitteln. Auch liefert Daccord eine übersichtliche Darstellung der effektiven Berechtigungen im Dateisystem für Benutzer und Gruppen. Gut gefallen hat uns zudem die Historienfunktion, um Änderungen an den Benutzern und Rechten detailliert nachvollziehen zu können. Zu beachten ist, dass die Software die Informationen nur einliest und anzeigt, aber keine Änderungen ermöglicht. Diese müssen mit den Windows-Bordmitteln oder anderen Werkzeugen erfolgen. Interessierte können sich die Installationsdateien samt Quickstart-Guide herunterladen und für sieben Tage testen. *(dr)* IT

So urteilt IT-Administrator

Setup und Einrichtung	4
Bedienung und GUI	7
Benutzerpflege	8
Berechtigungsanalyse	9
Auswertung der Historie	8

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

Dieses Produkt eignet sich

optimal für komplexe Windows-Umgebungen mit vielen Benutzern und Gruppen, wo an mehreren Stellen Rechte vergeben sind. Daccord ermöglicht hier eine übergreifende Sicht und Compliance-Prüfung.

bedingt in Umgebungen, wo die Rechte nur an wenigen Stellen vergeben werden und es nur wenige Benutzer gibt. Zu bewerten ist hier, inwiefern dann ein Mehrwert gegeben ist.

nicht, sofern die Rechte nur an einer Stelle vergeben werden. Dies ist in der Regel einfach mit den vorhandenen Windows-Tools zu prüfen.