migRaven.one
Migration und Konsolidierung

Microsoft Active Directory (AD) aufräumen

Microsoft Active Directory (AD) aufräumen

Die erste Version des AD wurde mit Windows 2000 im Jahre 2000 zur Verfügung gestellt. In vielen Unternehmen existiert das AD auch schon seit diesem Jahr. Das AD ist dabei das System in der Unternehmens-IT, das den meisten Veränderungen und Anpassungen unterworfen ist, weil kontinuierlich Accounts erzeugt, angepasst und gelöscht werden. Und es werden Gruppen erstellt, miteinander verschachtelt, Rechte darüber vergeben, wieder entzogen.

Seit der Einführung hat das AD immer wieder Funktionserweiterungen erfahren, die hauseigenen Tools zur Verwaltung haben sich aber nicht in gleichem Umfang entwickelt. Man kann über das Tool „Benutzer und Computer" Objekte erzeugen und bearbeiten, allerdings bleiben die Strukturen und die großen Zusammenhänge eher verborgen.

Gruppen im AD – tendenziell immer viel zu Viele

Ein AD kann man auf verschiedene Weisen strukturieren. Darunter gibt es Strukturen, die sehr übersichtlich sind, weil sie einer hierarchischen Struktur – beispielsweise Organisationseinheiten im Unternehmen – entsprechen. Parallel gibt es aber immer auch noch die eher undurchsichtigen Gruppenstrukturen, die über Jahre ohne eine klare Konvention gewachsen sind.

Diese machen mit 80% den bei weitem größten Teil der Gruppen aus und sie wurden ausschließlich zur Steuerung von Berechtigungen im Filesystem erzeugt. Dabei ist das Filesystem selbst ständig starken Veränderungen unterworfen. Verzeichnisse, die gestern erstellt und mit Berechtigungsgruppen versehen wurden heißen heute ganz anders, liegen an einer anderen Stelle oder wurden wenige Stunden später wieder gelöscht. In den seltensten Fällen werden die Gruppen entsprechend angepasst bzw. wieder gelöscht!

Auf jeden Nutzer kommen 2-3 Berechtigungsgruppen im AD

Unterm Strich kommen so auf einen einzelnen User etwa 2 bis 3 Berechtigungsgruppen im AD. Und das Schlimmste ist, dass man dieses undurchsichtige „Gruppengestrüpp" weiterhin zur Steuerung von Sicherheitseinstellungen verwendet. Dadurch sind Fehlkonfigurationen vorprogrammiert; denn mit den Microsoft Bordmitteln sind diese großen Gruppenstrukturen nachträglich nur noch sehr schwer zu durchdringen.

Man kann die verschachtelten Gruppenberechtigungen mit einer russischen Matrjoschka-Puppe vergleichen: Auf den ersten Blick sieht man nicht genau, was alles drinsteckt! Weist man also beispielsweise einer Gruppe ein Recht auf dem Filesystem zu, kann ohne aufwändige Analyse gar nicht erkennen, wer dadurch alles effektiv berechtigt wird. So kann es schnell passieren, dass man

eigentlich einen kleinen Benutzerkreis über eine entsprechende Gruppe, z.B. „Personalabteilung“ berechtigen möchte. Und dann wird über eine Verschachtelung die Gruppe „Domänen-Benutzer“ in eben dieser Gruppe mitberechtigt. Im Ergebnis sind dann alle Accounts auf dem Verzeichnis der Personalabteilung berechtigt.

AD aufräumen, aber wie… migRaven.one mit Graphen Datenbank kann mehr und das schneller

Kommt dann für die IT-Abteilung die Zeit, dass genau diese Strukturen – beispielsweise im Zuge der Einführung einer Identity & Access Management Lösungen – bereinigt und aufgeräumt werden müssen, steht diese vor einer schier unlösbaren Aufgabe.

migRaven.one stellt hier auf der Basis seiner auf der Graphentheorie basierenden neo4j-Datenbank ein einzigartiges Framework zur einfachen Analyse der Gruppen und Berechtigungen auf der Basis von logischen Ansätzen zur Verfügung.

Das Active Directory beinhaltet primär Objekte, die untereinander mehr oder weniger zueinander in Beziehung stehen. Und Beziehungen zwischen Objekten bilden die Grundlage der Graphentheorie: User stehen über Gruppenmitgliedschaften mit anderen Usern in Beziehung. Die Beziehungen werden wiederum über Berechtigungen im Filesystem erweitert. Die Aufgabe ist nun, die vorgegebenen vergleichbaren Werte wie z.B. das Department mit den tatsächlich existierenden Verbindungen auszuwerten. Wo relationale Datenbanken Stunden oder Tage für die Berechnung brauchen, kann das migRaven Framework Antworten in Minuten liefern. Und das in Umgebungen mit Userzahlen jenseits der 50.000 User Grenze und Datenmengen im Terrabyte-Bereich.

Ein Beispiel: Compliance Check

Compliance Check von Rollengruppen – Sind die Rollengruppen sauber mit den richten Accounts gefüllt?

Input: Rollengruppen

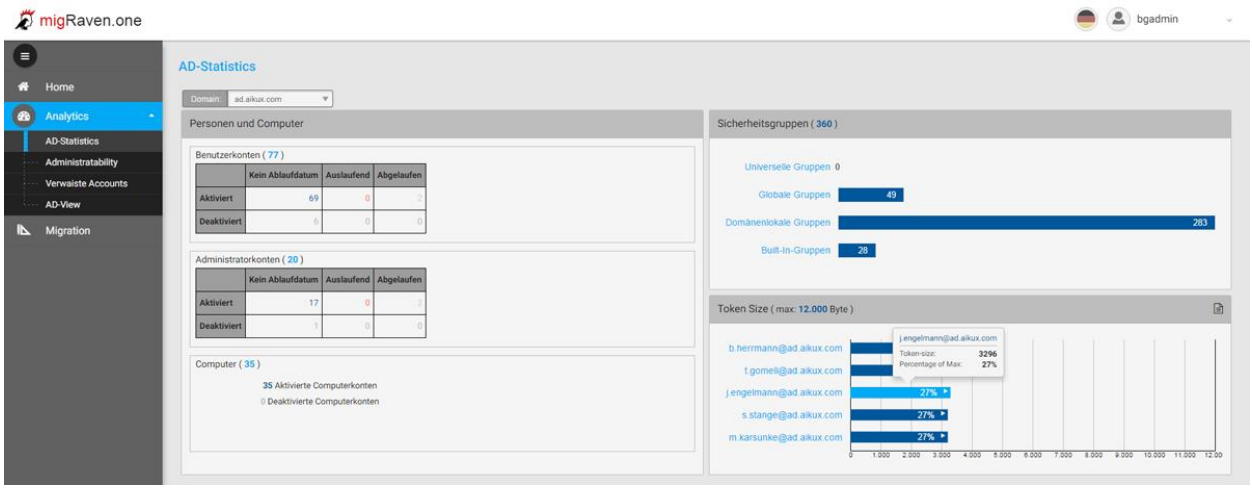
Output: Liste aller Rollengruppen, die Accounts aus unterschiedlichen Abteilungen beinhalten incl. Aller Details zu den Überschneidungen

Die User- und Gruppeninformationen aus dem Active Directory und die Berechtigungen des Filesystems werden in die interne Datenbank importiert und bilden die Grundlage für einzigartige Auswertungen, um die Strukturen und Abhängigkeiten zu verstehen und sie unmittelbar bereinigen zu können.

Fragen, die man ans AD stellen sollte

Diese Kennzahlen bzw. -werte helfen z.B. das vorhandene Active Directory besser zu verstehen und ggf. zu bereinigen:

- Verschachtelungstiefen von Gruppen,
- Anzahl aller Gruppen, die verwaist sind: Keine Mitgliedschaft, keine Mitglieder, keine Beziehung zu ACE,
- Anzahl der Objekte, die keinerlei Beziehung mehr zum Filesystem haben,
- Berechtigungstiefen im Filesystem (Optimierung der Verwaltung),
- Vorkommen Direktberechtigungen von User Accounts,
- Verwaiste User: Accounts, die schon seit gewisser Zeit nicht mehr genutzt werden,
- Tokensize: Berechnungen der tokenzize für jeden einzelnen Account,
- Konsistenzüberprüfungen von Gruppen: In welchen Gruppen sind die Accounts der Abteilungen zu welchem Anteil Mitglied (Nützlich zur Ableitung von Profilen auf der Basis von Profilen),
- Erweiterte Konsistenzüberprüfungen von Gruppen: In welchen Gruppen sind die Accounts der Abteilungen zu welchem Anteil Mitglied und welche anderen Abteilungen haben außerdem noch Mitglieder zu welchem Anteil in den Gruppen. (Nützlich zum Abgleich von Profilen),



Screenshot: AD Analytics in der aktuellen migRaven.one Version.

Eigene Abfragen gegen das AD erstellen

Bestimmte Sichten stellt migRaven.one direkt zur Verfügung andere Analysen können direkt speziell für ihre Fragestellungen entwickelt werden. Die Basis liefert immer die migRaven Datenbank auf der Basis der Graphentheorie.

Ein Beispiel für eine direkte Abfrage in der Datenbank über die Sprache „Cypher“:

```
MATCH (a2:ADAccount)
where a2.type="person" and not a2.department=""
with distinct a2.department as department
MATCH (a1:ADAccount)
where a1.type="person" and a1.department=department
Optional MATCH (a:ADAccount)<-[:rel_member*..]-(g)
where a.type="person" and a.department=department and not g.domain='local'
with g,a, count(distinct a1) as Anzahl, department
optional match (g)-[:rel_member*..]->(b)
where b.type="person" and not b.department = department
with g,b,a,count( b) as abt, Anzahl

return
distinct 'Die Gruppe:', ( g.name + "@" + g.domain) as Diese_Gruppe,
"enthält:", (count(distinct a)) + " Mitglieder" as enthält_x_Mitglieder,
"aus der Abteilung ", a.department as ade , " die insgesammt aus ", Anzahl,
" Mitgliedern besteht was einem Anteil von ", (( (count(distinct a)
/tofloat( Anzahl))*100 ) + " %") as c, " entspricht." ,
"Außerdem gibt es noch ", count(distinct b), " Mitglieder aus der Abteilung
", b.department as ab, " was einem Anteil von ", (( (count(distinct b)
/tofloat( count(distinct a)))*100 ) + " %" ) as d, " von der Gruppe "
,a.department, " zur Abteilung ", b.department as ab1, " entspricht." as b
order by Diese_Gruppe, enthält_x_Mitglieder desc
```

Das Ergebnis dieser Abfrage: Die Gruppe „RG_Abteilung_Administration“ enthält nur 4 Mitglieder aus der Abteilung „Administration“, die insgesamt aus 5 Mitgliedern besteht, und somit einem Anteil von 80% entspricht. Außerdem gibt es noch 2 Mitglieder aus der Abteilung „Marketing“ was einem Verhältnis von 4 zu 2 der Abteilung „Administration“ zur Abteilung „Marketing“ entspricht.

Folgerung: Die Gruppe muss bereinigt werden! Oder die Department-Informationen stimmen nicht.
In beiden Fällen sollte man tätig werden.

aikux.com development GmbH
Wiclefstraße 18
10551 Berlin

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

www.migraven.com