Die betreute Einführung der Lösung 8MAN für das User- und Berechtigungsmanagement in einer Microsoft-Umgebung durch die aikux.com GmbH

Einführung

Unternehmensstrukturen folgen einer eigenen Dynamik, weshalb auch die Dateiablagen der Notwendigkeit ständiger Anpassung unterliegen. Diese Anpassungen können der exponentiell wachsenden Datenmenge, dem Umstieg von Novell auf Microsoft oder auch nur der Umstrukturierung des Unternehmens geschuldet sein. Solange dabei die Daten nur von einem kleinen Fileserver auf einen größeren kopiert werden, ist das keine sonderliche Herausforderung, aber: Ein solcher Umzug bietet auch die geeignete Gelegenheit, die Strukturen auf den Systemen und vor allem die Berechtigungssituation einer Überprüfung und Optimierung zu unterziehen. Und ab diesem Zeitpunkt wird das Ganze kompliziert – auch in sonst eher überschaubaren Strukturen…

Aufgabenstellung

Die Einführung einer Lösung zur User- und Berechtigungsverwaltung in einem Microsoft-Netzwerk (AD). Damit werden folgende Ergebnisse erzielt:

1. Visualisierung der Berechtigungssituation
2. Vereinfachung der AD-Administration
3. Vereinfachung der Berechtigungsverwaltung
4. Sicherstellung der BSI-konformen Dokumentation und Nachvollziehbarkeit der Administration

Umsetzung

Obwohl 8MAN im Prinzip speziell für die o.g. Aufgabenstellung entwickelt worden ist, stößt die Software gerade bei Migrationsszenarien an Ihre Grenzen.

8MAN setzt zwar die Rechte an den Berechtigungsendpunkten und erstellt automatisch Listgruppen bzw. vergibt Listberechtigungen bis hinauf zum Share, allerdings immer nur für ein explizit berechtigtes Verzeichnis. Abhängig vom Inhalt des Verzeichnisses kann es bis zu einer Stunde oder länger dauern, bis dieses Verzeichnis von 8MAN seine Berechtigungen erhalten hat. Hier kommt nun migRaven ins Spiel. Damit können die Berechtigungen einfach überarbeitet und angepaßt und eine saubere Struktur erstellt werden. Weil das in einer Datenbank geschieht, ist die Zugriffssicherheit auf die einzelnen Verzeichnisses immer gewährleistet.

Die Einführung gliedert sich in folgende Arbeitsschritte:

1. Installation, Konfiguration und Dokumentation (Block 1)
2. Schulung am Produkt nach Vorgaben zur Verwendung (Block 1)
3. Sichtung der aktuellen Berechtigungssituation und Anpassung des alten oder Entwicklung eines neuen Berechtigungskonzeptes (Block 2)
4. Erarbeitung einer neuen Berechtigungsstruktur (Block 3)
5. Migration der alten Berechtigungen in das neue Berechtigungsmodell (Block 3)

Block 1 – Installation und Schulung – Ablauf (3 Tage)

Für die Installation sollten vom Auftraggeber folgende Rahmenbedingungen geschaffen werden:

Technische Anforderungen:

- 8MAN: 1 Windows Server 2008 R2, 2GB RAM, 50GB HDD, SQL Express 2008 R2, administrative Accounts für den Zugriff auf das AD und die Fileserver. Siehe auch: http://www.aikux.com/produkte/8man-systemanforderungen/
- migRaven: 1 Windows Server 2008 R2, 4GB RAM, 50GB HDD, Java Runtime, administrative Accounts für den Zugriff auf das AD und die Fileserver, 64Bit System für die Anwendung. Siehe auch: http://www.migraven.com/hilfe/systemvoraussetzungen-migraven/

Die Installation von 8MAN erfolgt als erster Schritt. Danach werden die Zielsysteme in 8MAN eingebunden (AD + Fileserver). Nach der Einbindung wird 8MAN alle benötigten Informationen sammeln und in die SQL-Datenbank importieren. Die Dokumentation erfolgt während der Installation (ca. 4 Stunden).

Nach der ersten Sichtung der bestehenden Konfiguration werden die Einstellungen für die Administration der Berechtigungen über 8MAN angepasst. Hier geht es vor allem um die Strategie der Namensvergabe für Gruppen und nach welchem Modell die Gruppen für die Berechtigungsvergabe aufgebaut werden sollen – Stichwort: A-G-DL-P. Außerdem muss die Strategie für die Vergabe der Listberechtigungen entwickelt werden. Das erfolgt unter Beachtung der zu erwartenden Gruppen ausgehend von der zu verwaltenden Berechtigungstiefe in den Verzeichnissen. Hier ist im Vorfeld die optimale Mischung aus Listgruppen (Größe des Kerberos Tokens) und den Listberechtigungen der expliziten Berechtigungsgruppen (Anzahl der ACEs) festzulegen. Um ein Ausufern der Tokengröße bzw. der ACE-Einträge zu verhindern, sollte die Tiefe des Berechtigungsendpunktes vier Ebenen nicht überschreiten. (ca. 4 Stunden)

Für die erfolgreiche Nutzung von 8MAN wird eine ausführliche Schulung durch einen erfahrenen 8MAN-Consultant dringend empfohlen. Dieser wird innerhalb der Schulung auf folgenden Themen eingehen (2 Tage):

- Wie kann man mit 8MAN User anlegen und welche Punkte sind dabei zu beachten (evtl. durch Unterstützung von Skripten)?

- Wie können Gruppen mit 8MAN angelegt werden?
- Wie können die Gruppenverschachtelungen des AD mit 8MAN bearbeitet werden?
- Wie können temporäre Gruppenmitgliedschaften gebildet werden?
- Wie kann ein sauberer Prozess für den Abteilungsübergang mit 8MAN abgebildet werden (Azubi-Effekt); alte Berechtigungen sollen nach Zeitraum X nicht mehr zugewiesen sein?
- Wie können Passwörter zurückgesetzt und User deaktiviert/ gelöscht werden?
- Wie können neue Verzeichnisse erstellt werden?
- Wie können die Berechtigungen mit 8MAN bearbeitet werden? Detailliertes Eingehen auf die unterschiedlichen Methoden des Gruppen-Wizards mit 8MAN (ca. 1 Tag)
- Wie können temporäre Berechtigungen auf Verzeichnisse vergeben werden?
- Dokumentation und Reporting-Funktionen
- Einrichten des Zugriffs auf 8MAN für die DataOwner
- Einrichten von regelmäßigen Reports
- Logging-Funktionen für die revisionssichere Auditierung von Berechtigungen

Alle genannten Punkte werden in praktischen Übungen vertieft.

Block 2 – empfohlen – Entwicklung eines neuen Berechtigungskonzeptes (1 Tag)

Erfahrungen zeigen, dass es bei den meisten Kunden notwendig ist, das bisherige Berechtigungskonzept zu überdenken und anzupassen. Dazu gehört auch, dass die vergebenen Berechtigungen gesichtet und auf ihre innere Logik überprüft werden. Nach Rücksprache mit den Fachabteilungen ist oft ein Aufräumen der Berechtigungen erforderlich. Hier ist ein wichtiger Punkt, wie im Block 1 erwähnt, die Tiefe der zu berechtigten Verzeichnisse. Auch ob schon ABE verwendet wird oder ob der Einsatz von DFS sinnvoll ist, sind Fragen, die in diesem Rahmen angesprochen werden sollten. Gerade hier, bei der Entwicklung eines neuen Konzeptes und auch beim späteren Umgang mit 8MAN sollten die Fachabteilungen aktiv eingebunden werden, denn nur dort weiß man tatsächlich, wer auf Grund seiner Aufgaben wo berechtigt sein muss.

Block 3 – empfohlen – Migration der Berechtigungen (5-15 Tage, nach Aufwand)

Die Microsoft-Bordmittel stellen leider nur unzureichende Unterstützung für die Administration von Berechtigungen zur Verfügung. Das führt dazu, dass in den meisten Unternehmen und Organisationen das Aufräumen der Berechtigungen dringend notwendig ist. Mit Hilfe von migRaven kann die Migration schnell und ohne schädlichen Einfluss auf die tägliche Arbeit umgesetzt werden.

Ziel ist es, zu optimalen Berechtigungen zu kommen. Dazu wird das AD in migRaven eingescannt, danach können die Shares eingescannt und bearbeitet werden. Alternativ kann auch eine XLS-Datei außerhalb des Systems erstellt werden, in der die einzelnen Berechtigungsendpunkte definiert und mit den entsprechenden Usern/ Gruppen berechtigt werden. Wenn es sich um eine Migration von Novell handeln sollte: Es genügt, die Trustee.xml aus den dem Novell-System zu exportieren und in migRaven zu importieren. Achtung: Die Gruppen und User müssen schon im AD vorhanden sein. Die aikux-Consultants unterstützen Sie gern bei der Umsetzung des AD-Imports.

Im nächsten Schritt erstellt migRaven eine neue, leere Verzeichnisstruktur, die entsprechend Ihrer Vorgaben berechtigt ist. An dieser Stelle spielt migRaven seine Stärken aus: Alle Daten, neue Berechtigungen, User und Gruppen werden in einer Datenbank erstellt und dank der Visualisierungsfunktion von migRaven kann man in der Datenbank sehen und überprüfen, was schließlich im Produktivsystem geschehen wird. Erst im letzten Schritt werden die neuen Gruppen ins AD und die ACEs ins Filesystem geschrieben. Daß migRaven auch die Listgruppen/ -berechtigungen erstellt, versteht sich dabei von selbst.

> **Übrigens: Die mit migRaven erstellten Gruppen sind dann 8MAN-ready: d.h. diese Gruppen, einschließlich der Listberechtigungen, werden von 8MAN als 8MAN-Gruppen erkannt und weiterverwendet.**

Erst nach der Umstellung der Berechtigungen auf „8MAN-AD-Gruppen“ kann 8MAN seine volle Leistung erzielen. Danach werden alle Berechtigungen halbautomatisch durch 8MAN verwaltet (Gruppen erzeugen, konsistent halten, löschen).

Für diese Maßnahme ist es von großer Bedeutung, den Kommunikationsprozess mit den Dateneigentümern aufzubauen und so „angenehm“, also so einfach wie möglich, zu gestalten. Denn es sind die Dateneigentümer, die wissen, wie die Berechtigungen sein sollen. Hier gilt es, die Möglichkeiten von 8MAN voll auszuschöpfen.

In einer letzten Anpassung werden dann die Berechtigungen in enger Zusammenarbeit mit den Kollegen aus der IT und einem Mitarbeiter von aikux.com neu gesetzt. Das kann nach Abstimmung durchaus im laufenden Betrieb erfolgen.

aikux.com GmbH, 31.01.2014

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