DRITTSYSTEME AM ACCESS RIGHTS MANAGER

20 JAHRE FUTUREDAT

Totgesagte leben länger.

Wie eine CSV-Datei alles anbindet, was keinen Connector hat

Norbert Eggert · Senior Engineering Manager

VORAB

Es ist kurz nach dem Essen. Ich rede über Berechtigungsdaten.

Deshalb übernehmen das heute die Simpsons.

GRUNDLAGE

Der Access Rights Manager in einem Satz

Er liest aus Ihren Systemen, wer existiert, was es gibt und wer darauf zugreifen darf.

Er vergibt nichts selbst. Er zeigt, was längst vergeben ist.

VON HAUS AUS

Die vier gewohnten Quellen

Active Directory.

Benutzer, Gruppen, Mitgliedschaften

Filesystem.

Freigaben, Ordner, NTFS-Rechte

Exchange.

Postfächer, Stellvertretungen

SharePoint.

Websites, Listen, Bibliotheken

Sehr komfortabel. Und sehr Microsoft.

DIE LÜCKE

Und das Fachverfahren?

Das Archiv. Die Zeiterfassung. Die Maschinensteuerung in Halle 3. Kein Connector, aber sehr wohl Berechtigungen.

EASY CONNECT

Eine Tabelle genügt.

Jedes System, das exportieren kann, ist anbindbar — als CSV oder direkt aus der Datenbank. Das können praktisch alle.

BEISPIELSYSTEM

Springfield

Homer Marge Bart Lisa Maggie.

Eine Familie, ein Haus, keine Schnittstelle. Seit 1989 im Fernsehen und bis heute an kein System angebunden.

DIE MECHANIK

Vier Datenarten

1

Konten

Benutzer und Gruppen

2

Relationen

Wer ist Mitglied worin

3

Ressourcen

Alles, was berechtigt werden kann

4

Berechtigungen

Konto, Ressource, Recht

Dazu Attribute: aktiv, inaktiv, Typ. Mehr fragt ARM nicht ab.

Konten

Jedes Familienmitglied ist ein Konto. Die Gruppen sind ebenfalls Konten — sie stehen in derselben Datei.

Entscheidend ist nur eins: eine Kennung, die sich nicht ändert.

ACCOUNTS.CSV

Homer
Marge
Bart
Lisa
Maggie
Children
Parents
Simpson Family
Mr. Burns

Mr. Burns steht in keiner Familiengruppe. Konten müssen nirgendwo dazugehören.

Relationen

Zwei Spalten genügen: Mitglied und Gruppe. Homer ist in Parents, Parents gehört zur Familie.

Verschachtelte Gruppen löst ARM selbst auf — inklusive der Frage, woher ein Recht eigentlich kommt.

ACCOUNTRELATIONS.CSV

Homer	Parents
Homer	Simpson Family
Marge	Parents
Marge	Simpson Family
Bart	Children
Bart	Simpson Family
Lisa	Children
Lisa	Simpson Family
Maggie	Children
Maggie	Simpson Family

Ressourcen

Alles, was berechtigt werden kann. Die Hierarchie steckt im Pfad.

Springfield
- Simpson-House
  - Garage
    - **Car**
  - Living_Room
    - **Couch**
- Nuclear_Plant
  - **Control_Room**

Eine Zeile pro Ressource, vier Ebenen im Pfad.



Berechtigungen

Ressource, Konto, Recht. Welche Rechte es gibt, entscheidet das System — nicht ARM. Homer steuert das Werk übrigens direkt, nicht über eine Gruppe.

RESSOURCE	KONTO	RECHT
Springfield	Simpson Family	**Live**
Living_Room/Couch	Parents	**Sit**
Living_Room/Couch	Bart	**Sit**
Garage/Car	Parents	**Drive**
Nuclear_Plant/Control_Room	Mr. Burns	**Control**
Nuclear_Plant/Control_Room	Homer	**Operate**

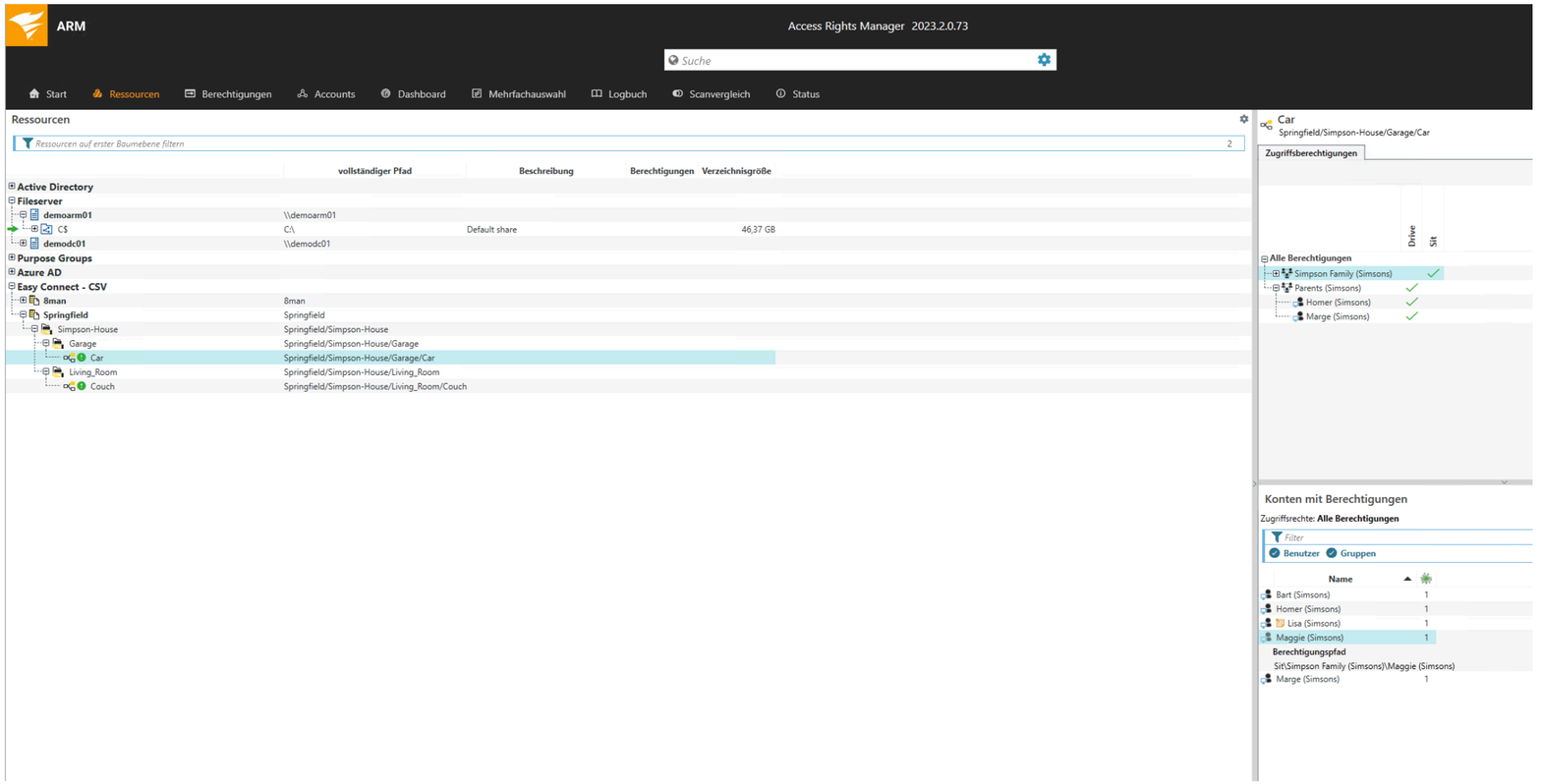
UND DANN DIE ATTRIBUTE

Maggie ist deaktiviert — und hat trotzdem Rechte.

Ein Attribut pro Konto, aktiv oder inaktiv. Daran hängt jede Auswertung über Konten, die es längst nicht mehr geben sollte.

IN ARM

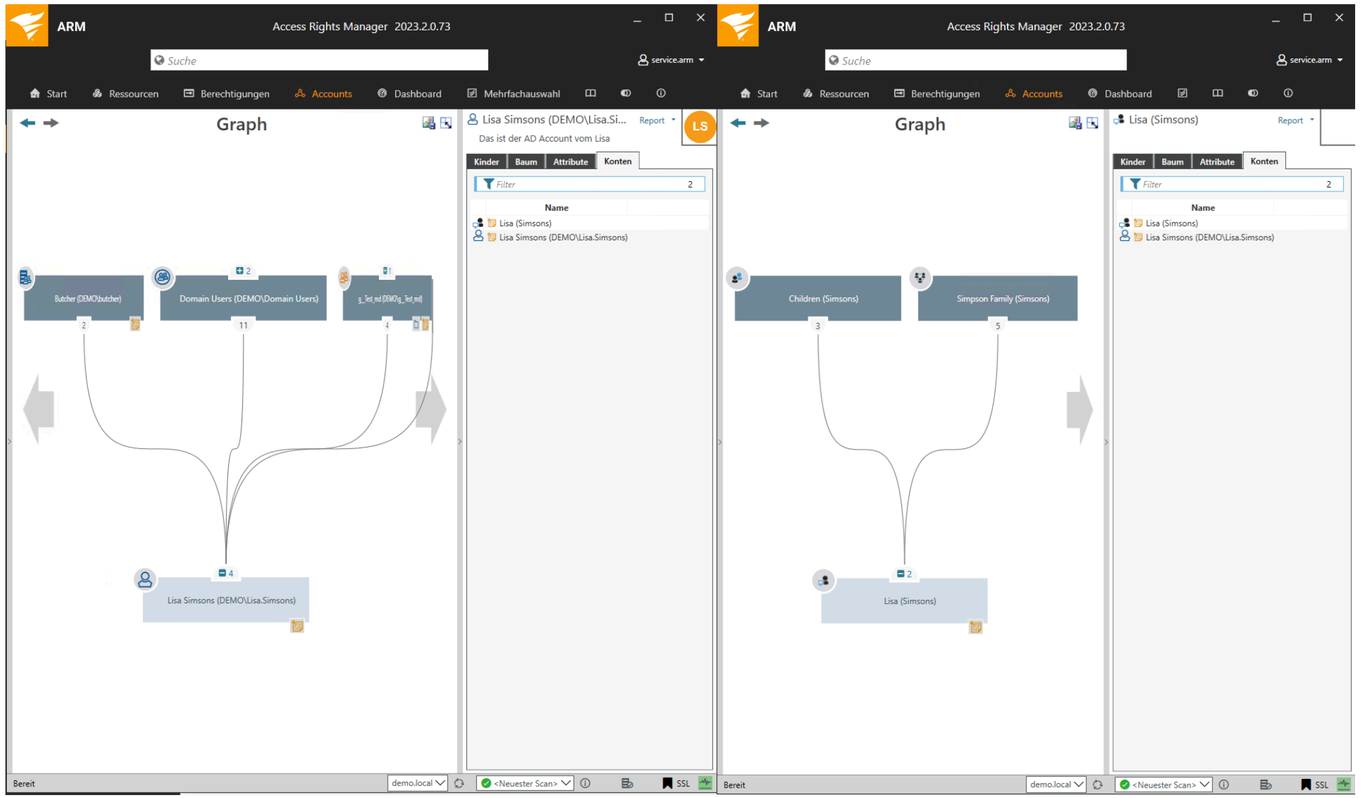
Springfield steht neben dem Fileserver



Eine Quelle im Ressourcenbaum wie jede andere — und rechts die aufgelöste Berechtigung am Auto.

KONTENMAPPING

Zwei Konten, eine Person



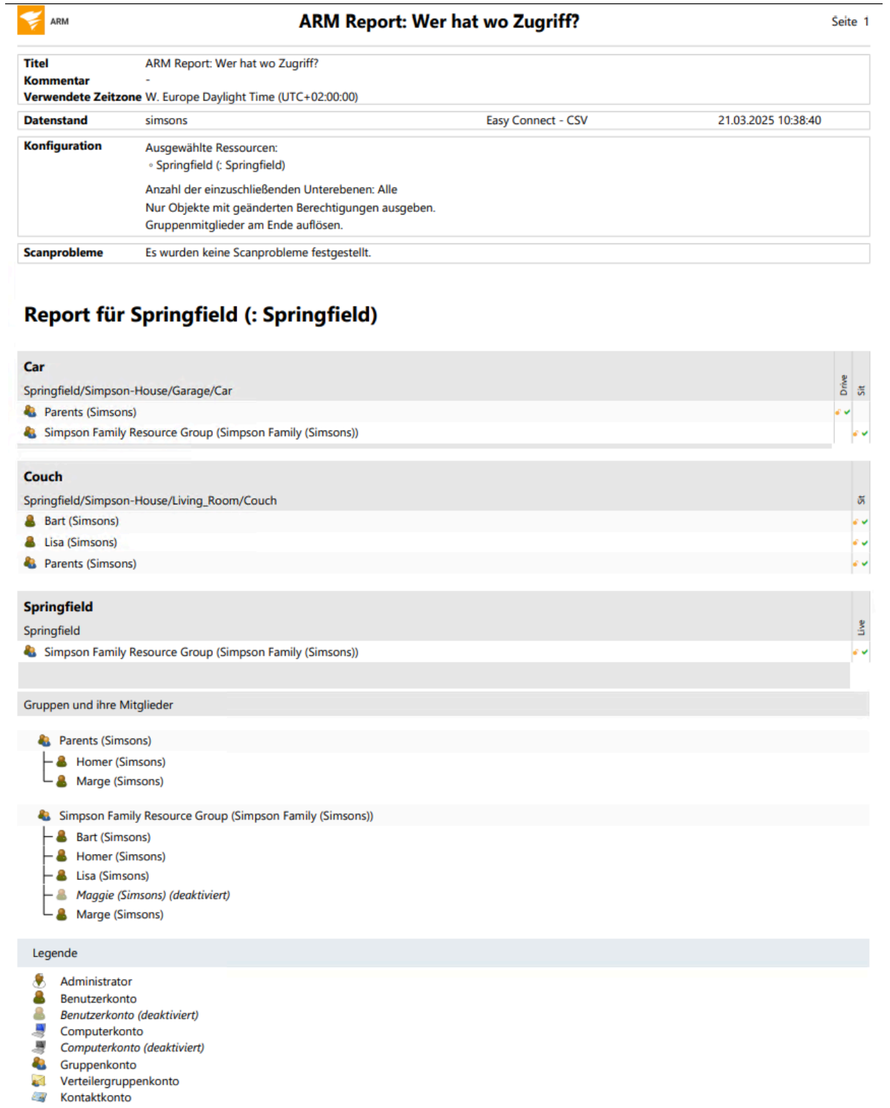
Das Konto aus der Tabelle wird mit dem AD-Konto verknüpft. Ab hier ist Lisa in jeder Auswertung dieselbe Person.

BERICHT

Wer hat wo Zugriff?

Derselbe Bericht wie für einen Fileserver. Nur dass die Ressource hier eine Couch ist.

Gruppen werden bis zum einzelnen Konto aufgelöst. Deaktivierte Konten stehen kursiv — Maggie inklusive.



ARM

ARM Report: Wer hat wo Zugriff?

Seite 1

Titel	ARM Report: Wer hat wo Zugriff?
Kommentar	-
Verwendete Zeitzone	W. Europe Daylight Time (UTC+02:00:00)
Datenstand	simsons — Easy Connect - CSV — 21.03.2025 10:38:40
Konfiguration	Ausgewählte Ressourcen: ◦ Springfield (: Springfield) Anzahl der einzuschließenden Unterebenen: Alle Nur Objekte mit geänderten Berechtigungen ausgeben. Gruppenmitglieder am Ende auflösen.
Scanprobleme	Es wurden keine Scanprobleme festgestellt.

Report für Springfield (: Springfield)

Car
Springfield/Simpson-House/Garage/Car — Drive, St
- Parents (Simsons)
- Simpson Family Resource Group (Simpson Family (Simsons))

Couch
Springfield/Simpson-House/Living_Room/Couch — St
- Bart (Simsons)
- Lisa (Simsons)
- Parents (Simsons)

Springfield
Springfield — Live
- Simpson Family Resource Group (Simpson Family (Simsons))

Gruppen und ihre Mitglieder

- Parents (Simsons)
  - Homer (Simsons)
  - Marge (Simsons)
- Simpson Family Resource Group (Simpson Family (Simsons))
  - Bart (Simsons)
  - Homer (Simsons)
  - Lisa (Simsons)
  - *Maggie (Simsons) (deaktiviert)*
  - Marge (Simsons)

Legende

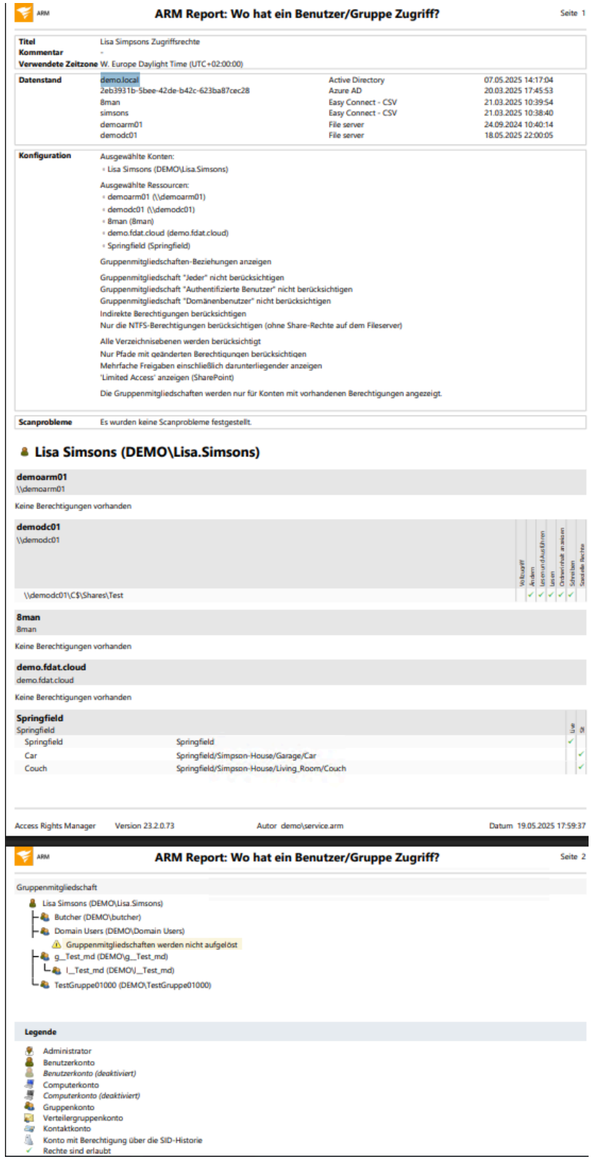
- Administrator
- Benutzerkonto
- *Benutzerkonto (deaktiviert)*
- Computerkonto
- *Computerkonto (deaktiviert)*
- Gruppenkonto
- Verteilergruppenkonto
- Kontaktkonto

BERICHT

Wo hat ein Benutzer Zugriff?

Ein Konto, sechs Datenquellen, ein Blatt Papier. Springfield steht darin zwischen Fileserver und Azure AD.

Das ist die Frage aus dem Austrittsprozess. Und die Frage der Revision.



ARM Report: Wo hat ein Benutzer/Gruppe Zugriff? Seite 1

Titel	Lisa Simsons Zugriffsrechte
Kommentar	
Verwendete Zeitzone	W. Europe Daylight Time (UTC+02:00:00)

Datenstand			
	demo.local	Active Directory	07.05.2025 14:17:04
	2eb1911b-5bee-42de-b42c-623ba87cec28	Azure AD	20.03.2025 17:45:53
	8man	Easy Connect - CSV	21.03.2025 10:39:54
	simsons	Easy Connect - CSV	21.03.2025 10:38:40
	demoarm01	File server	24.09.2024 10:40:14
	demodc01	File server	18.05.2025 22:00:05

Konfiguration

Ausgewählte Konten:
- Lisa Simsons (DEMO\Lisa.Simsons)

Ausgewählte Ressourcen:
- demoarm01 (\\demoarm01)
- demodc01 (\\demodc01)
- 8man (8man)
- demo.fdat.cloud (demo.fdat.cloud)
- Springfield (Springfield)

Gruppenmitgliedschaften-Beziehungen anzeigen

Gruppenmitgliedschaft "Jeder" nicht berücksichtigen
Gruppenmitgliedschaft "Authentifizierte Benutzer" nicht berücksichtigen
Gruppenmitgliedschaft "Domänenbenutzer" nicht berücksichtigen
Indirekte Berechtigungen berücksichtigen
Nur die NTFS-Berechtigungen berücksichtigen (ohne Share-Rechte auf dem Fileserver)

Alle Verzeichnisebenen werden berücksichtigt
Nur Pfade mit geänderten Berechtigungen berücksichtigen
Mehrfache Freigaben einschließlich darunterliegender anzeigen
'Limited Access' anzeigen (SharePoint)

Die Gruppenmitgliedschaften werden nur für Konten mit vorhandenen Berechtigungen angezeigt.

Scanprobleme	Es wurden keine Scanprobleme festgestellt.

Lisa Simsons (DEMO\Lisa.Simsons)

demoarm01
\\demoarm01

Keine Berechtigungen vorhanden

demodc01
\\demodc01

Vollzugriff | Ändern | Lesen und Ausführen | Lesen | Schreiben | Spezielle Rechte

\\demodc01\C$\Shares\Test

8man
8man

Keine Berechtigungen vorhanden

demo.fdat.cloud
demo.fdat.cloud

Keine Berechtigungen vorhanden

Springfield
Springfield

		Lesen	Schreiben
Springfield	Springfield	✓	
Car	Springfield/Simpson-House/Garage/Car	✓	✓
Couch	Springfield/Simpson-House/Living_Room/Couch	✓	✓

Access Rights Manager Version 23.2.0.73 Autor demo\service.arm Datum 19.05.2025 17:59:37

ARM Report: Wo hat ein Benutzer/Gruppe Zugriff? Seite 2

Gruppenmitgliedschaft

- Lisa Simsons (DEMO\Lisa.Simsons)
  - Butcher (DEMO\butcher)
  - Domain Users (DEMO\Domain Users)
    - Gruppenmitgliedschaften werden nicht aufgelöst
  - g_Test_md (DEMO\g_Test_md)
    - l_Test_md (DEMO\l_Test_md)
  - TestGruppe01000 (DEMO\TestGruppe01000)

Legende

- Administrator
- Benutzerkonto
- *Benutzerkonto (deaktiviert)*
- Computerkonto
- *Computerkonto (deaktiviert)*
- Gruppenkonto
- Verteilergruppenkonto
- Kontaktkonto
- Konto mit Berechtigung über die SID-Historie
- Rechte sind erlaubt

AUS DER PRAXIS

Wer darf eigentlich das Kraftwerk steuern?

Die Antwort stand in einer Tabelle, die keiner gelesen hat. Bei Ihnen heißt „Homer" wahrscheinlich anders — und „Mr. Burns" ist ein Dienstkonto von 2019.



DER NUTZEN

Eine Auswertung über alle Systeme statt sechs getrennter Listen.

Was jemand beim Austritt an Rechten hatte, steht danach in einem Bericht — auch für das Verfahren ohne Connector.

GRENZEN

Was die Tabelle nicht kann

Nur lesen

ARM zeigt die Rechte des Systems. Ändern müssen Sie dort, wo sie entstehen.

Stand des Exports

Der Bericht ist so aktuell wie der letzte Scan. Nächtlich reicht meistens.

Stabile Kennungen

Ändert das System seine IDs, ist die Historie weg. Das ist die einzige echte Hürde.

VORGEHEN

Von der Tabelle zum Betrieb

Verstehen

Welche Rechte kennt das System überhaupt

Struktur schaffen

Export definieren, Konten mappen

Betrieb

Geplanter Scan, nächtlich oder wöchentlich

Absichern

Berichte, Rezertifizierung, Nachweis

Seit 2010 am Markt und regelmäßig abgeschrieben

Das Produkt hat vier Eigentümer und mehrere Namen überlebt. Die Tabellenschnittstelle hat sich in dieser Zeit nicht geändert.

ZUM MITNEHMEN

20 JAHRE FUTUREDAT

Selbst die Simpsons kann man an ARM ankoppeln.

Ihr Fachverfahren also auch.

Norbert Eggert · Senior Engineering Manager · FUTUREDAT GmbH, Gera