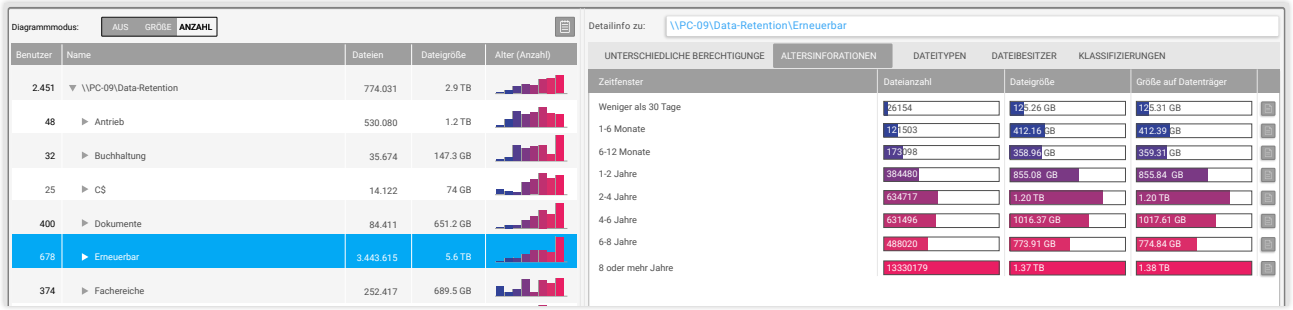
ANALYSE UND REPORTS FÜR FILESERVER

Effektive Berechtigungen erkennen, Datenberge finden - Data Owner bestimmen

migRaven GmbH
Alt-Moabit 59-61
10555 Berlin

GF: Thomas Gomell
T: +49 030 8095010-40
F: +49 030 8095010-41
E: info@migraven.com

www.migRaven.com

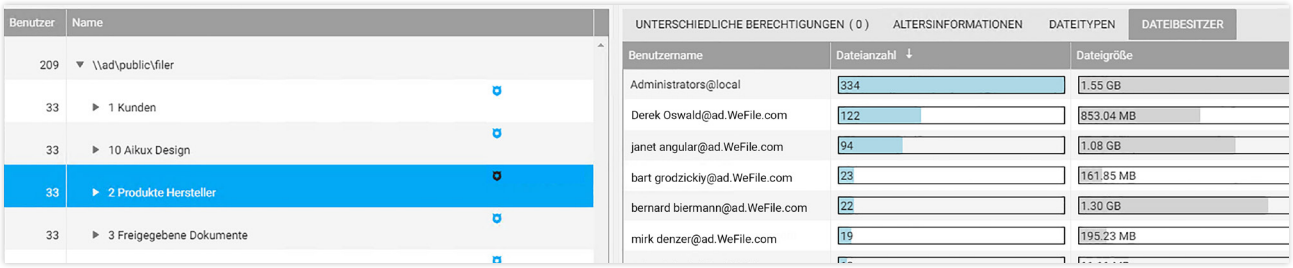


Visualisierung der Datenstruktur

Das für den Fachbereich entwickelte migRaven.24/7 Webinterface stellt auf der Home-Seite essentielle Informationen zur Datenstruktur übersichtlich dar und hilft dem Nutzer, ein Verständnis über seine Daten und Verzeichnisstrukturen zu gewinnen.

Konkret liefert die Home-Seite von migRaven.24/7 Ihren Mitarbeitern Antworten auf:

- Wie viele Verzeichnisse und Dateien gibt es?
- Welchen Speicherplatz nehmen die Dateien ein?
- Wie ist die Altersverteilung der Daten?
- Welche User haben zu den Verzeichnissen direkte Zugriffsberechtigungen?
- Welche Dateitypen befinden sich in den Verzeichnissen?
- Wer sind die Dateibesitzer innerhalb der Verzeichnisse?



Schlüsselfigur Data Owner

Sollen veraltete Daten aus dem produktiven Bereich des Fileservers verschwinden, wird in den meisten Fällen die IT-Administration aktiv. Diese Situation ist jedoch absurd, denn nur der Fachbereich bzw. der Dateibesitzer (Data Owner) ist über den Dateninhalt im Bilde und kann eine klare Aussage über die Relevanz und weitere Verwendung von Dateien treffen.

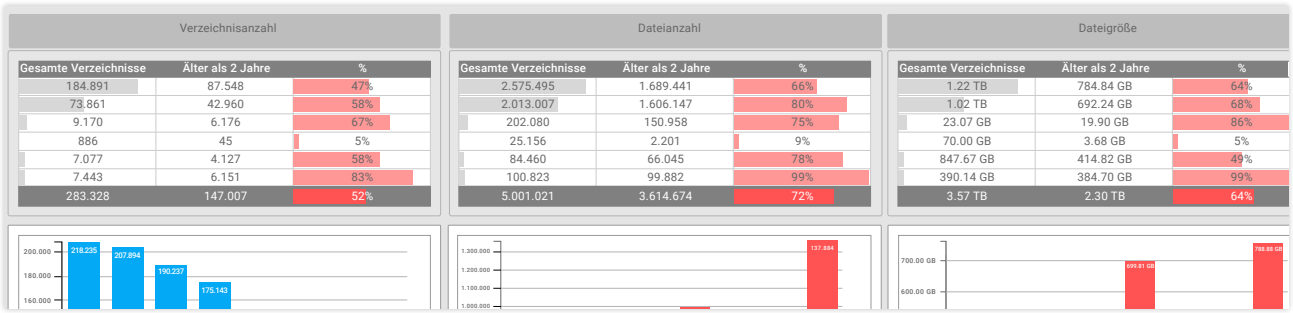
Mit den gewachsenen Strukturen mit tausenden von Dateien ist die Frage nach den Data Ownern innerhalb von Verzeichnissen jedoch alles andere als trivial.

Zuverlässige Identifikation der Data Owner

In migRaven.24/7 werden im Reiter Dateibesitzer die Anzahl der Dateien pro User angezeigt. Der User mit den meisten erstellten Dateien ist entweder selbst Data Owner oder weiß zumindest, wer es aus dem Kollegenkreis ist.

Ist der Data Owner eines Verzeichnisses ermittelt, können dem entsprechenden User auf dem Verzeichnis die Data Owner-Rechte mit einem Klick zugewiesen werden. So bekommt der Data Owner die Möglichkeit, sich selbst einen Überblick über die Dateien und die Struktur zu verschaffen und kann entscheiden ob

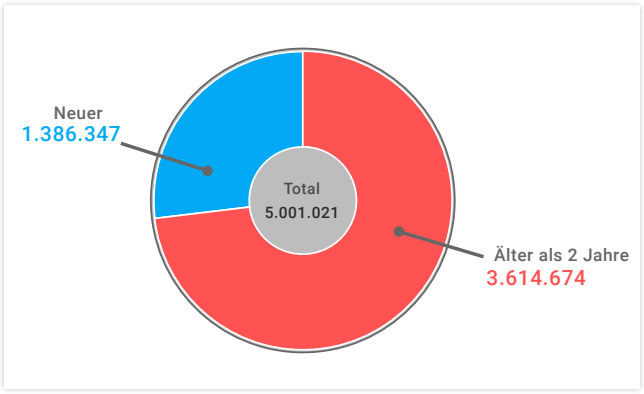
- bestimmte Verzeichnisse obsolet sind,
- Berechtigungen nicht mehr passend sind,
- Archivierungspolicies dem Verzeichnis zugewiesen werden sollten.

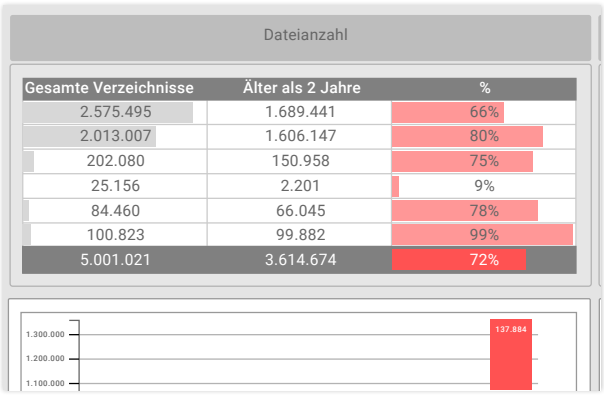


Obsolete Data Report

Am Anfang jeder Optimierung steht die Analyse des Ist-Zustandes: Dieser Report zeigt Ihnen deshalb schnell und übersichtlich, was mit Windows-Bordmitteln nur schwer zu machen ist: Wo sich in Verzeichnissen große Datenmengen abgelagert haben und wie alt diese bzw. die sie enthaltende Struktur sind. Dabei stellen Sie selbst ein, ab welchem Zeitraum Daten als veraltet oder zumindest überaltert gelten sollen und sehen dann, auf wie viele der auf einem Share vorhandenen Verzeichnisse und Dateien das zutrifft bzw. wie groß der belegte Speicherplatz dieser Dateien insgesamt ist. Zudem werden diese Werte im Verhältnis zur Gesamtmenge der Daten dargestellt – nicht selten mit dem Ergebnis, dass 70% und mehr der Daten längst hätten archiviert oder gelöscht werden können.

Dank des Obsolete Data Reports können Sie zielgerichtet Maßnahmen gegen diese Datenberge ergreifen und so die Effizienz aller Nutzer im Umgang mit dem Filesystem steigern.



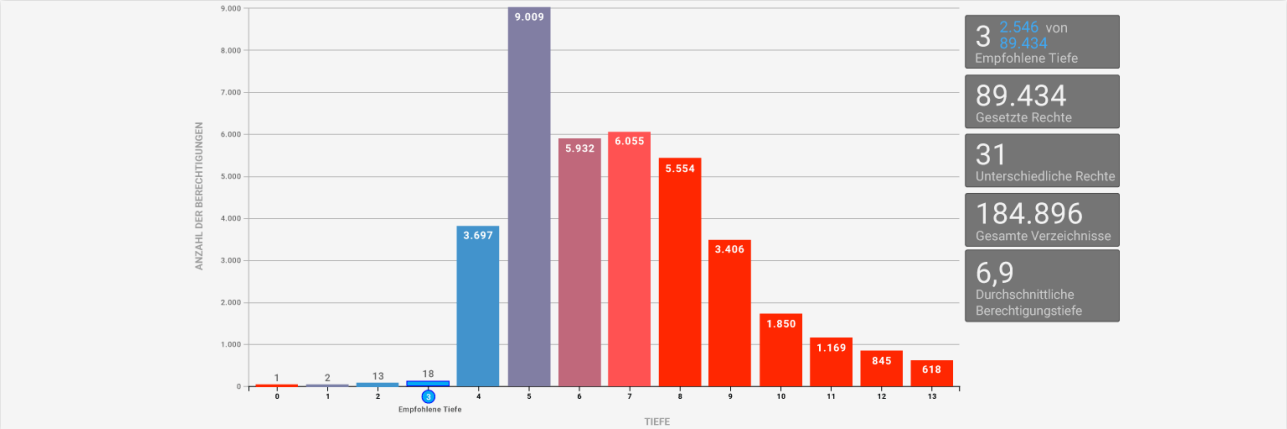


Daten älter als 2 Jahre

Der Obsolete Data Report von migRaven.24/7 zeigt Ihnen schnell und übersichtlich, was mit Windows-Bordmitteln nur schwer zu machen ist: Wo sich in Verzeichnissen große Datenmengen abgelagert haben und wie alt diese bzw. die sie enthaltende Struktur sind.

Problembewusstsein

Die beschriebene Situation ist auch in Ihrem Unternehmen, wenn es denn schon einige Jahre existiert, sehr wahrscheinlich Realität. Mit dem Obsolete Data Report erhalten Sie Gewissheit darüber, ob Ihr bisheriges Datenmanagement funktioniert hat.



Best Practice Report

Der Best Practice Report liefert dem Administrator detailliert wichtige Kennzahlen bezüglich der Microsoft Best-Practices-Compliance der Berechtigungen auf dem eingelesenen Laufwerk. Finden Sie unkompliziert heraus, wo beispielsweise Berechtigungen zu tief reichen (mehr als 3 Ebenen), Vererbungen unterbrochen werden oder User direkt berechtigt sind. Diese Informationen sind zur Vorbereitung einer Fileserver-Restrukturierung oder beim Bereinigen des Active Directorys unverzichtbar!

Berechtigungsebenen

Um die Administration von Berechtigungen so einfach wie möglich zu gestalten, sollten Berechtigungen nicht zu tief vergeben werden. Dabei hat sich Ebene 3 der Verzeichnisstruktur als optimale Verzeichnistiefe erwiesen. Denn jedes unterhalb von Ebene 1 liegende explizite Recht macht es notwendig, dass auch Listberechtigungen aufgebaut werden, damit der User überhaupt zum eigentlichen Verzeichnis gelangen kann. Der Report zeigt Ihnen im Detail, wie tief die Berechtigungen in Ihrer Umgebung reichen und die sich daraus ergebende durchschnittliche Berechtigungstiefe.

Vererbungsunterbrechung

Die Unterbrechung von Vererbungen sollte genau wie Deny-Berechtigungen vermieden werden. Auch wenn es in bestimmten Situationen als sinnvoll erscheinen kann, provoziert dieses Vorgehen im weiteren Lebenszyklus des Systems zusätzlichen Aufwand, z.B. wenn es notwendig wird, Berechtigungen zu vererben. Der Report zeigt Ihnen alle unterbrochenen Vererbungen. Empfohlen ist hier, grundsätzlich nach dem Least Privilege Principle zu arbeiten: Immer nur soviel Berechtigungen vergeben, wie tatsächlich benötigt werden. Dies macht eine Betrachtungsumkehr bei der Berechtigungsvergabe notwendig. Man setzt Rechte nicht von oben, sondern von unten. Dies bedeutet, dass man z.B. auf der Ebene über einem explizit vergebenen Modify-Recht nur noch Listberechtigungen benötigt, damit dies funktioniert.

Direkt berechtigte Personen

Eine weitere Empfehlung ist die Verwendung von Gruppen für die Berechtigungsvergabe. Gruppen ermöglichen es überhaupt erst, Rechte für viele User zu vergeben. Denn Access Control Lists (ACL) sind grundsätzlich beschränkt und es kommt leicht zu Performanceproblemen, wenn zu viele ACLs vorhanden sind. Der Report zeigt, wie viele User in einer Umgebung direkt berechtigt sind, die keine Administratoren sind. Nach Best Practice sollte man nach dem Prinzip A-G-DL(oder G, oder U)-P arbeiten: Der Account kommt in eine Rollengruppe (G), diese in Berechtigungsgruppen (DL) – diese wiederum wird zum Mitglied der P(ACL).

Es ist aber durchaus sinnvoll in bestimmten Fällen auf die Rollengruppe zu verzichten, wenn z.B. die Userkombination nur für ein einziges Verzeichnis benötigt wird. Genau dann verwendet man A-()-DL-P – die User werden zum direkten Mitglied in der Berechtigungsgruppe. Das stellt sicher, dass keine User direkt in einer ACL berechtigt sind.

Verwaiste ACE

Verwaiste ACEs entstehen, wenn ein Account aus dem AD gelöscht wird ohne die ACE Einträge zu entfernen. Dies ist kein technisches Problem, sondern ein „Schönheitsfehler“, der sich natürlich auch auf das Reporting auswirkt.