

Transparency in Windows File Systems

cMatrix Reporting

Transparent Permissions and Structures in Inherited Windows File Systems

Reviewers, auditors and supervisory authorities are demanding increasingly detailed proof that data, users and access rights are securely and transparently administered. Here, however, the people responsible for IT usually lack reliable information. The reason is inherited file systems with partly undocumented permissions. This lack of transparency significantly increases the labor required to conduct migration and consolidation projects.

Scan, Analyze, Report, Transparency

With cMatrix Reporting, organizations now have the important information about their file systems:

Who is permitted to do what?

Filter out and itemize all permissions, even in large file systems.

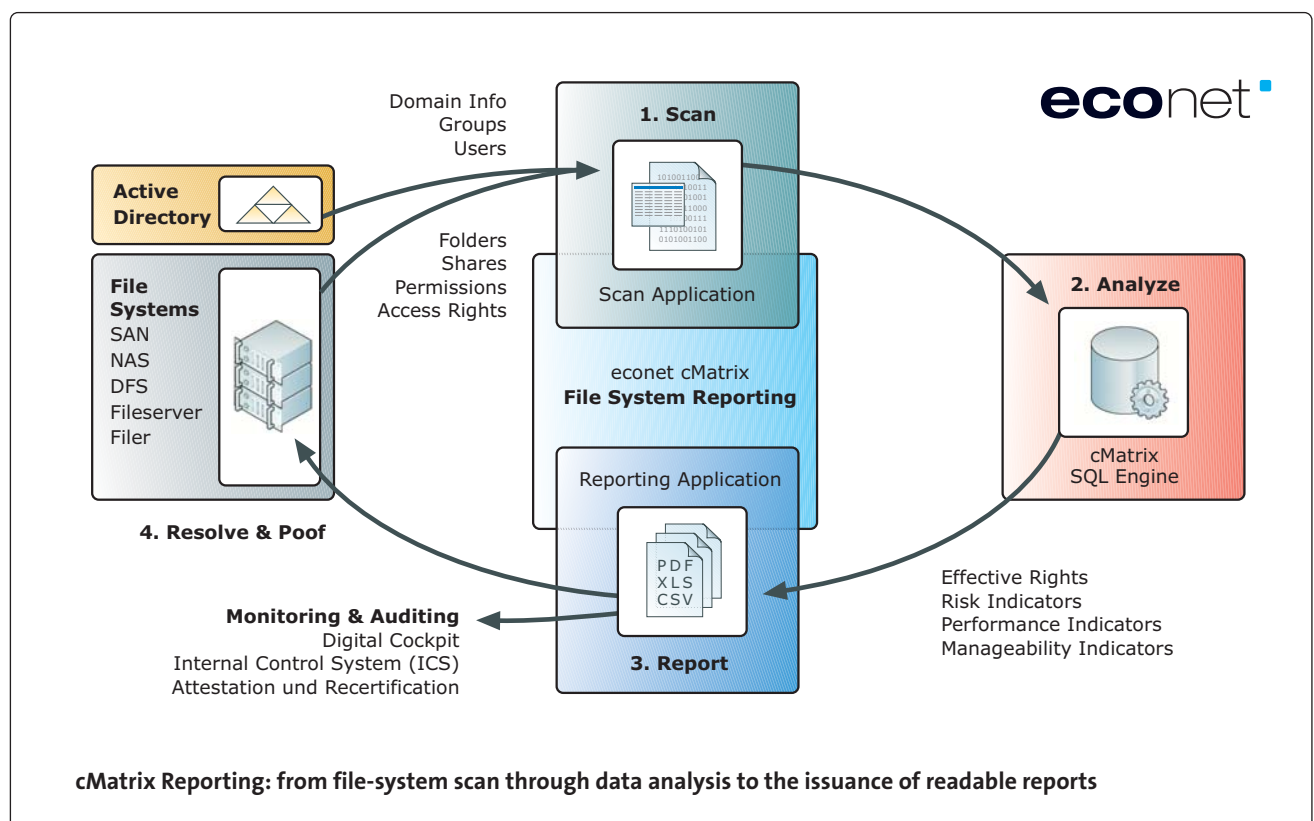
Where are the potential threats?

Identify, analyze and evaluate risks and weak points.

The information and indicators thus gained are issued in “readable” reports. These compliant and auditable reports provide the basis for the ongoing evaluation of risks. They can also be issued as journals containing proof of historical permissions.

The built-in standard reports answer important questions such as:

- Which users and/or which groups are authorized inside the examined area?
- Onto which directories is a particular user permitted, and in which ways is he permitted there?
- Which groups are the sources of these permissions?
- Who has permission for a particular folder, and in which ways is he permitted there?
- Who are the owners of the folders and shares?
- Which shares exist, and are they nested?
- Where do “special” permissions exist?
- Which files exceed the maximal path length?
- What differences have been detected compared to the previous evaluation?
- On which directories are orphaned user accounts still permitted?
- At which locations in the file system’s structure do the permissions change?
- What is the general status of the examined area with regard to security and manageability?





Greater information security: Identify effective permissions on folders and releases of folders – also within the framework of attestations and migration planning

Structured approach: Detect repeatable permissions and critical situations in file systems, compare them, and depict them in readable reports (in PDF, XLS and CSV formats)

Facilitate the evaluation of examined areas through performance indicators for risk and manageability (key risk indicators / key manageability indicators)

Better compliance conformity: Comply with obligations for documentation, keep track of changes, continually evaluate risks

Higher scalability: Reliable results, also in very large directory structures, even with several million folders

Save time and money: Completely automated scanning and reporting sequences after one-time-only configuration. These sequences can also be performed on a prescheduled basis, e.g. at night or on weekends. Several scans can run simultaneously over different areas. The generated reports can be automatically sent to specified recipients via e-mail.

Lastingly tidy permissions

To maximize information security and compliance conformity, it is recommended that access rights should be granted and changed according to thoroughgoing, rule-based processes. Automated request and approval workflows rely on the several-pairs-of-eyes principle to assure that coworkers only receive access to the “right” files.

Visit “Fileservice Management” at www.econet.de to learn more about how you can transform your file systems and permissions into a lastingly orderly state.

System requirements

Windows XP

Windows Vista

Windows 2003 Server

Windows 2008 Server

Systems must be in Active Directory

Supported database server

MS SQL server

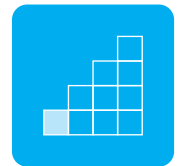
starting with version 2005

Would you like to test the solution?

We'll provide you with a free demonstration version.

From the overview reports to the filtered, detailed views: with cMatrix Reporting, you have the important information about your file system.

Name	Percentage	Set directly	Value
1. Scanned folders	-	-	2.360
2. Scanned permissions	-	-	16.235
3. Permissions after resolved group memberships	-	-	202.549
4. Users authorized in scanned folders	-	-	25
5. Groups authorized in scanned folders	-	-	20
6. Relation of groups to users	-	-	0,80
7. Folders with 'everyone' permissions *	9,75%	75	230
8. Folders with 'everyone full control' permissions *	0,21%	2	5
9. Folders with non-group/single user permissions	95,04%	23	2.243
10. Folders with just one single user permission	0,00%	0	0
11. Folders with non-inherited permissions (FSN)	4,24%	-	100
12. Relation of FSNs to users	-	-	4,00
13. Folders with deny permissions	2,92%	69	69



File System KPI Report



Key Risk Indicators (KRI) and Key Manageability Indicators (KMI)

Scope: C:\Users

Name	Percent	Value	KRI	KMI
Number of folders		2360	9	9
Number of users		25	9	9
Number of groups		20	8	9
Number of orphaned SIDs		0	10	
Number of scanned ACEs		16235	8	7
Number of permissions		202549		

Folders with everyone permissions				
Number	9,75 %	230	1	
Number without inherited permissions		75	1	6
Folders with nongroup permissions				
Number	95,04 %	2243	1	
Number without inherited permissions		23	8	8
Folders with everyone fullcontrol permissions				
Number	0,21 %	5	1	
Number without inherited permissions		2	1	9

Report "File System KPI":
Indicators for security and cost effectiveness evaluate the identified weak points

econet cMatrix Reporting:
A professional tool with a readily readable surface and simple operation

econet AG

Kaiser-Ludwig-Platz 5

D-80336 Munich

fon +49 (89) 514 51-0

fax +49 (89) 514 51-199

info@econet.de

www.econet.de



Gartner Inc. chose the econet AG as a "Cool Vendor" on the IAM market in 2009.