DATA ACCESS GOVERNANCE WITH NTFS PERMISSIONS

USING PERDEMIA'S PERMISSION ANALYZER TO GAIN INSIGHT INTO CURRENT NTFS RIGHTS WITHIN THE NETWORK

11 April 2021





1.	Introduction	. 3
]	Information requirements	.4
2.	Standard Windows tooling	. 5
I	PowerShell	. 5
3.	Approach with Perdemia's Permission Analyzer	.7
	Scanning the network	.7
(Creating reports	. 8



1. Introduction

It is common knowledge that most cases of data theft occur within the organization. No hacks from the outside, but people within the organization who (accidentally) unfairly have access to sensitive data. Apart from the financial damage, damage to reputation, this leads in many cases to legal violations, loss of intellectual property and problems in the customer relationships. See this <u>article</u> on <u>Digital Guardian</u> from this year in which 47 data security experts share their vision when it comes to protecting data and how the greatest risks come from within the organization. Employees are already cleared for most security measures and are already logged on to the network domain, they know the organization and can easily ask for additional rights. Although external attacks partly focus on weaknesses in the system, many hackers focus on existing authorized credentials through social engineering and phishing emails.

One of the complexities in the protection of data is that the solution doesn't rely on just one department. The business departments have the knowledge about the necessary authorizations and the sensitivity of data, while the IT Department has the knowledge about user groups, the rights structure and tooling. Both parties must find a balance between protection of data and supporting the business processes in which constant changes take place with accompanying pressure to ease the security principles. Who is now responsible for the protection of data and monitoring of policy?

Each organization starts with a clean design in the form of user groups, directory structures and processes, but as time passes this design blurs. Users request additional rights, projects use new approaches, departments reorganize or network data is restructured. Gradually there is a proliferation of rights and no longer can they be checked to see if the original design still applies, with all its consequences. Is the data still sufficiently protected? Do the defined groups still have the correct rights? And are temporarily acquired rights and group changes properly cleaned up? In other words, can we still rely on the design on paper with which strategic business goals, financial results, personal data, internal reviews and intellectual property are protected? We call this **Data Access Governance (DAG)**. Many companies in recent years have given priority to DAG and the protection of 'unstructured data', such as spreadsheets, presentations, documents and other data made by employees carrying out their day to day work. Gartner indicates that 80% of all data is unstructured. The first step in protecting this is the clarification, clean-up and organization of the current data and rights granted.

In this article we look at how Perdemia's Permission Analyzer can be used to support Data Access Governance and the way in which the below information requirements are addressed.



INFORMATION REQUIREMENTS

If we wish to gain insight into the current access rights, the following questions arise:

- 1. what are the effective rights for a specific user or group (including rights obtained through nested group memberships)?
- 2. where do the rights come from for a user? Through which folders and group memberships are the rights granted?
- 3. which groups and users have indirect access to a specific folder?
- 4. what happens if someone is placed in a group?
- 5. what are the rights for **all** users of a specific group and what exceptions apply?
- 6. can we validate and maintain consistency in the original security design for data access?

These information requirements increase in complexity, but even the most simple question, where someone has rights, is difficult to determine for a system administrator. The last two points are perhaps the most interesting because they contribute heavily to the validation of our security principles. We want to be able to characterize/segment users (everyone in an AD Group, a department in an LDAP organizational unit, or a private selection of employees) and we want to check the rights for a large number of users and this group. This group is allowed to view and edit certain data, or this group has absolutely **no** rights to certain data. This means that for each user the nested group memberships must be taken into account as, after all, the access rights can be obtained through nested groups. Furthermore, the overview must reveal what exactly the exceptions are and where the cause of the unwanted rights lies. In the end we want to be able to say in full confidence that **the policy for data access within the network is still applicable and consistent.**



2. Standard Windows tooling

If we rely on the standard Windows tooling then right away we encounter the first problems. NTFS rights are granted to directories and files via one of the thirteen "*special*" rights, or several "*simple*" rights which amount to a combination of special rights. The users, groups, and permissions (Access Control Entries) together constitute the Access Control List for a file or directory. Because this information is directly linked to a directory or file but not centrally stored, a network administrator will state the need to check all the directory's one by one to come to an overview of rights. In addition, a user can inherit rights through membership in groups, which makes the whole thing even more complex and time consuming to get a realistic overview. Current versions of Windows in the directory properties offer a tab to determine the effective rights of a user, but unfortunately this option is only for an individual directory. There is also a number of command-line tools available that we will evaluate later.

POWERSHELL

We have the option to use PowerShell, a scripting solution from Microsoft that enables special tasks to be performed by the operating system. One of these tasks is the Get-Acl cmdlet to get the security descriptor of a file or directory. In combination with the Get-ChildItem cmdlet to browse a folder structure, we can use a script to export all Access Control List Entries (ACE's) to a CSV file. The command powershell can be typed in the command line. PS appears before the command prompt and now the entire powershell script can be pasted and performed:

```
Get-ChildItem "C:\MyFolder" -Recurse | Sort-Object FullName | %{
$Path = $_.FullName
$IsDirectory = $_.PsIsContainer
(Get-Acl $Path) | Select-Object `
@{n='Path';e={ "$Path, d=$IsDirectory" }},
@{n='Access';e={ [String]::Join("`n", $( $_.Access | %{
    "$($_.IdentityReference), $($_.AccessControlType), $($_.IsInherited),
    $($_.InheritanceFlags), $($_.PropagationFlags), $($_.FileSystemRights)" }))
}}
} | Format-list | Out-File -FilePath C:\temp\permission_export.txt -
Encoding UTF8
```

A major advantage of PowerShell scripts is that the job is run on the remote server. Only the result is sent to the requesting machine through the network. We were disappointed with the performance of these tasks, scanning 500.000 local files took 32 minutes, 30% CPU, 1 GB memory and resulted in a CSV file of 150 MB. Other tools, such as Perdemia's Permission Analyzer, scans the same file information in 20 minutes as well as writing it to a database. PowerShell offers a lot of options and cmdlets to apply filters or additional tasks. For example, to skip inherited rights we can apply the line below in the preceding script:



```
@{n='Access';e={ [String]::Join("`n", $( $_.Access | ?{!$_.IsInherited} | %{
```

And to exclude files from the export we can use the following:

```
Get-ChildItem "C:\MyFolder" -Recurse | Sort-Object FullName | ?{
$_.PsIsContainer } | %{
```

But then? Then we have all rights in a CSV file, without considering the group membership. We can of course do some basic checks and there are also ways in a PowerShell to read the Active Directory for group memberships, but even then it remains difficult to get the right information and requires substantial manual development.

If we look at the available tooling then we encounter a number of comprehensive management applications, as well as tools purely focused on reading access rights (ranging between \$200 and \$2500 USD depending on the license form) and a number of small free tools. The large packages are distinguished mainly in the extensive functionality, but do they also help us to provide the stipulated information requirements?



3. Approach with Perdemia's Permission Analyzer

Perdemia's Permission Analyzer is a targeted tool to gain control on the proliferation of NTFS rights. It offers a unique way to apply filters, look at results from different angles and can automatically check on the consistency of security principles by setting its own rules. Here we'll discuss some examples to see how the application works.

More than ten years ago, Perdemia's <u>Permission Analyzer</u> started as an application to reveal the NTFS rights per user or group. Now, the application has been completely rebuilt to version 2, in order to better fulfill information requirements stated in the <u>Introduction</u>. Permission Analyzer was rebuilt with the focus on performance and large amounts of data. The directory information and user information is therefore not all loaded into memory and it does not scan the network for every search, but it uses a database to gather all the information together and to apply filters. It's standard to use an embedded database (H2), but out-of-box the application also supports MSSQL Server, Oracle, MySQL, DB2, PostgreSQL and Derby.

SCANNING THE NETWORK

The application provides two 'views' from the menu, the Scan View and the Report View. In the Scan View the scan is configured by selecting the desired directories and OU's from the Active Directory. The directories can be added as network share, local directory, simply a server name (a search for network shares will automatically happen), or a text/zip file generated by a Powershell script included or EMC Isilon export from a NetApp filer. Incidentally, a <u>Scan Agents</u> can also be used that run locally on a file server and store the scan results in a central database. The Active Directory OU's are used to scan for group memberships. A scan can also be started automatically with various <u>command-line</u> <u>parameters</u>, which periodically refreshes the data.

7



Application Help	dition					- 🗆 ×
Application rich						
Folders to scan			ි LDAP OU's to scan			
Directory path	iscover network shares Add server PowerShell output file EMC Isile	on output file	LDAP Connection: Globa	al Catalog 🗸 🏷		
🗹 🌉 dataserver01	0 Yes Yes		Ldap container (base OU):			18
	0 Yes Yes 0 Yes	Yes Yes	Scope: Cont	ainer and sub containers		
C:\acl-exports\powershell-exp		Ne				
C:\Documents	0 Yes Yes	Yes	Object types: Users	and groups 🛛 🗸		
						🕂 Add 🛞 Update
			LDAP connection	LDAP base container	Search scope	Object types
	Add particular network shares or local		🗹 💭 Global Catalog	CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=	Container and sub containers	Users and groups
	directories to scan. Or scan all network shares		Primary domain controller	OU=Management,DC=mydomain,DC=com	Container and sub containers	Users and groups
	by adding a server or let PowerShell do the scanning and import the results from a txt file					
	acaming and import the results norm a cxt me					
				Add specific LDAP containers to		
				scan. Determine the depth and the		
				objects to scan.		
🗹 🏢 Clear all data from the databa	ise before scanning 📀 Test input source	🖋 Change 🛛 🗱 Delete			📀 Test	LDAP config X Delete
Q Scan results						
Scan results						
Date / time	Message					^
3-jun-2017 14:52:18	Start scanning directories					
🕡 3-jun-2017 14:52:25	Done scanning local groups on server dataserver01. Found 53 local groups					
🕖 3-jun-2017 14:52:28	Done scanning local groups on server dataserver02. Found 48 local groups					
🕖 3-jun-2017 14:52:32	Done scanning local groups on server localhost. Found 23 local groups					
	Start scanning server dataserver01					
🕖 3-jun-2017 14:52:32						
🛦 3-jun-2017 14:52:32	Skipping share: \\dataserver01\C\$		Observe the scan progress,	warnings and		
A 3-jun-2017 14:52:32 3-jun-2017 14:52:32	Skipping share: \\dataserver01\C\$ Start scanning directory \\dataserver01\Development including all levels of subdirect		Observe the scan progress, possible errors.	warnings and		
▲ 3-jun-2017 14:52:32 ② 3-jun-2017 14:52:32 ③ 3-jun-2017 15:24:11	Skipping share: \\dataserver01\C\$ Start scanning directory \\dataserver01\Development including all levels of subdirect Done scanning directory \\dataserver01\Development. Scanned 73256 directories and	236334 files.	possible errors.			
▲ 3-jun-2017 14:52:32 3-jun-2017 14:52:32 3-jun-2017 14:52:32 3-jun-2017 15:24:11 3-jun-2017 15:24:11	Skipping share:\\dataserver0\\C\$ Start scanning directory\\dataserver0\\Development including all levels of subdirect Done scanning directory\\dataserver0\\Development. Scanned 73256 directories and Start scanning directory\\dataserver0\\Customers including all levels of subdirector	l 236334 files. es	Observe the scan progress, possible errors. Tip: use this list to view the scheduled scan.			
▲ 3-jun-2017 14:52:32 7 3-jun-2017 14:52:32 7 3-jun-2017 14:52:32 7 3-jun-2017 15:24:11 7 3-jun-2017 15:24:11 7 3-jun-2017 15:39:18	Skipping June (UdatserveOIICS Start scanning directory (UdatserveOIIDevelopment including all levels of subdirect Done scanning directory (UdatserveOIIDevelopment: Scanned 7256 directories and Start scanning directory (UdatserveOICCustomers: Scanded 2856 directories and To Done scanning directory (UdatserveOICCustomers: Scanded 2856 directories and T	l 236334 files. es	possible errors. Tip: use this list to view the			
3-jun-2017 14:52:32 3-jun-2017 14:52:32 3-jun-2017 14:52:32 3-jun-2017 15:24:11 3-jun-2017 15:24:11 3-jun-2017 15:39:18 3-jun-2017 15:39:18	Skipping share: \\dataserve01\CS Start scanning directoy \\dataserve01\Development including all levels of subdirect Done scanning directoy \\dataserve01\Development. Scanned 73256 directories and Start scanning directoy \\dataserve01\Customers including all levels of subdirectori Done scanning directoy \\dataserve01\Customers including all levels of subdirectori Start scanning directory \\dataserve01\Customers inclu	1 236334 files. es 76987 files.	possible errors. Tip: use this list to view the			
▲ 3-jun-2017 14:52:32 ④ 3-jun-2017 14:52:32 ④ 3-jun-2017 15:24:11 ④ 3-jun-2017 15:24:11 ④ 3-jun-2017 15:39:18 ④ 3-jun-2017 15:39:18 ④ 3-jun-2017 16:13:45	Steping baine: VulatasenveOICS Start scanning directory VulatasenveOID@velopment including all levels of subdirect Done scanning directory VulatasenveOID@velopment. Scanned 73255 directories and Start scanning directory VulatasenveOIT.customers including all levels of subdirectori Done scanning directory VulatasenveOIT.customers including all levels of subdirectories Start scanning directory VulatasenveOIT.projects including all levels of subdirectories Done scanning directory VulatasenveOIT.projects. Scanned Start Scanterios and Start Start scanning directory VulatasenveOIT.projects. Scanned Start Scanterios and Start Start scanning directory VulatasenveOIT.projects. Scanned Start Scanterios and Start Start Scantery VulatasenveOIT.projects. Scanned Start Starterios and Start Start Scantery VulatasenveOIT.projects. Scanted Start Starterios and Start Start Scantery VulatasenveOIT.projects. Scanted Starterios and Starterios and Start Start Scantery VulatasenveOIT.projects. Scantery Starterios and S	1236334 files. es 76987 files. 87 files.	possible errors. Tip: use this list to view the		Scan the network (directories and LE	AP
 3-jun-2017 1452:32 3-jun-2017 1452:32 3-jun-2017 1452:821 3-jun-2017 15:24:11 3-jun-2017 15:39:18 3-jun-2017 15:39:18 3-jun-2017 16:13:45 3-jun-2017 16:13:45 	Slapping share: \u03d4tasevv010C5 Start scannig directoy \u03d4tasevv010Devlopment including all levels of subdirect Done scannig directoy \u03d4taserv010Devlopment. Scanned 7255 directories and Start scannig directoy \u03d4tasevv010Cutamores. Scanned 18486 directories Done scannig directoy \u03d4tasevv010Cutamores. Scanned 38486 directories and 15 start scannig directoy \u03d4tasevv010Cutamores. Scanned 38486 directories and 455 Brat scannig directoy \u03d4tasevv020Crejects. Including all level of subdirectos Done scannig directoy \u03d4tasevv020Crejects. Including all level of subdirectos Done scannig directoy \u03d4tasevv020Crejects. Scanned 1365 directories and 455 Brat scannig directoy \u03d4tasevv020Crejects. Scanned 1386 directories and 455 Brat scanned directoy \u03d4tasevv020Crejects. Scanned 1386 directories and 455 Brat scanned directoy \u03d4tasevv020Crejects. Scanned 1386 directories and 455 Brat scanned directories \u03d4tasevv020Crejects. Scanned \u03d4tasevv020	l 236334 files. es 76987 files. 87 files. es	possible errors. Tip: use this list to view the		containers).	
▲ 3-jun-2017 1452:32 3-jun-2017 1452:32 3-jun-2017 152:24:11 3-jun-2017 152:24:11 3-jun-2017 152:24:11 3-jun-2017 15:39:18 3-jun-2017 15:39:18 3-jun-2017 16:13:45 3-jun-2017 16:13:45 3-jun-2017 16:13:45	Slipping baine: \u03e4tasenve01ClS Start scannig directony \u03e4tasenve01Development inclusing all levels of subdirect Dene scannig directony \u03e4tasenve01Development, Scanned 7255 directories and Start scanning directony \u03e4tasenve01Development, Scanned 2888 directories and Dene scannig directony \u03e4tasenve01Development 2888 directories and Start scanning directony \u03e4tasenve01Development 2888 directories and Start scanning directony \u03e4tasenve01Development Dene scanning directony \u03e4tasenve01Development Start scanning directony \u03e4tasenve01Development Start scanning directony \u03e4tasenve01Developments and all levels of subdirectories Dene scanning directony \u03e4tasenve01Deprojects. Scanned 1982 directories and 498 Start scanning directony \u03e4tasenve01Deprojects. Scanned 1982 directories and 498 Dene scanning directony \u03e4tasenve01Deprojects. Started 1982 directories and 498 Dene scanning directony \u03e4tasenve01Deprojects. Started 1982 directories and 498 Dene scanning directony \u03e4tasenve01Deprojects. Started 1984 directories Dene scanning directony \u03e4tasenve01Deprojects. Started 1984 directories directories directories and 4984 directories directories and 4984 directories and 4984 directories directories and 4984 directories and 4	l 236334 files. es 76987 files. 87 files. es	possible errors. Tip: use this list to view the		containers). Schedule an automatic scan by start	ing the
 3-jun-2017 1452:32 3-jun-2017 1452:32 3-jun-2017 1452:821 3-jun-2017 15:24:11 3-jun-2017 15:39:18 3-jun-2017 15:39:18 3-jun-2017 16:13:45 3-jun-2017 16:13:45 	Slapping share: \u03d4tasevv010C5 Start scannig directoy \u03d4tasevv010Devlopment including all levels of subdirect Done scannig directoy \u03d4taserv010Devlopment. Scanned 7255 directories and Start scannig directoy \u03d4tasevv010Cutamores. Scanned 18486 directories Done scannig directoy \u03d4tasevv010Cutamores. Scanned 38486 directories and 15 start scannig directoy \u03d4tasevv010Cutamores. Scanned 38486 directories and 455 Brat scannig directoy \u03d4tasevv020Crejects. Including all level of subdirectos Done scannig directoy \u03d4tasevv020Crejects. Including all level of subdirectos Done scannig directoy \u03d4tasevv020Crejects. Scanned 1365 directories and 455 Brat scannig directoy \u03d4tasevv020Crejects. Scanned 1386 directories and 455 Brat scanned directoy \u03d4tasevv020Crejects. Scanned 1386 directories and 455 Brat scanned directoy \u03d4tasevv020Crejects. Scanned 1386 directories and 455 Brat scanned directories \u03d4tasevv020Crejects. Scanned \u03d4tasevv020	1 236334 files. es 76987 files. 87 files. es es 938 files.	possible errors. Tip: use this list to view the		containers).	ing the
▲ jun-2017 44532 ▲ jun-2017 14532 ■ jun-2017 152411 ■ jun-2017 152411 ■ jun-2017 153818 ■ jun-2017 153818 ■ jun-2017 161345 ■ jun-2017 161312 ■ jun-2017 161312 ■ jun-2017 161315	Slipping share: \u03e4tasenve010C5 Start scannig directoy \u03e4tasenve010Development including all levels of subdirect Done scannig directoy \u03e4tasenve010Development. Scanned 7255 directoris and Start scannig directoy \u03e4tasenve010Levelopment. Scanned 7255 directoris and Tat Done scannig directoy \u03e4tasenve010Levelopment (u03e5) directoris and 154 Start scannig directoy \u03e4tasenve020.Projects: Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects.Scanned 1326 directories and 459 start scannig directoy \u03e4tasenve020.Projects.Scanned 1327 directories and 270 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 271 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectority hoverthid level sub	1 236334 files. es 76987 files. 87 files. es es 938 files.	possible errors. Tip: use this list to view the		containers). Schedule an automatic scan by start	ing the
▲ 3-jun-2017 44532 ④ 3-jun-2017 14532 ④ 3-jun-2017 152411 ④ 3-jun-2017 152411 ④ 3-jun-2017 153918 ④ 3-jun-2017 153918 ④ 3-jun-2017 161345 ④ 3-jun-2017 161455 ④ 3-jun-2017 161712 ④ 3-jun-2017 161712	Slipping share: \u03e4tasenve010C5 Start scannig directoy \u03e4tasenve010Development including all levels of subdirect Done scannig directoy \u03e4tasenve010Development. Scanned 7255 directoris and Start scannig directoy \u03e4tasenve010Levelopment. Scanned 7255 directoris and Tat Done scannig directoy \u03e4tasenve010Levelopment (u03e5) directoris and 154 Start scannig directoy \u03e4tasenve020.Projects: Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects.Scanned 1326 directories and 459 start scannig directoy \u03e4tasenve020.Projects.Scanned 1327 directories and 270 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 271 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectority hoverthid level sub	1 236334 files. es 76987 files. 87 files. es es 938 files.	possible errors. Tip: use this list to view the		containers). Schedule an automatic scan by start	ing the
▲ jun-2017 44532 ▲ jun-2017 14532 ■ jun-2017 152411 ■ jun-2017 152411 ■ jun-2017 153818 ■ jun-2017 153818 ■ jun-2017 161345 ■ jun-2017 161312 ■ jun-2017 161312 ■ jun-2017 161315	Slipping share: \u03e4tasenve010C5 Start scannig directoy \u03e4tasenve010Development including all levels of subdirect Done scannig directoy \u03e4tasenve010Development. Scanned 7255 directoris and Start scannig directoy \u03e4tasenve010Levelopment. Scanned 7255 directoris and Tat Done scannig directoy \u03e4tasenve010Levelopment (u03e5) directoris and 154 Start scannig directoy \u03e4tasenve020.Projects: Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects.Scanned 1326 directories and 459 start scannig directoy \u03e4tasenve020.Projects.Scanned 1327 directories and 270 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 271 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectority hoverthid level sub	1 236334 files. es 76987 files. 87 files. es es 938 files.	possible errors. Tip: use this list to view the		containers). Schedule an automatic scan by start	ing the
▲ jun-2017 453:32 → jun-2017 453:32 → jun-2017 453:32 → jun-2017 1528:11 → jun-2017 1538:18 → jun-2017 1538:18 → jun-2017 16138:5 → jun-2017 16138:5 → jun-2017 1617:12 → jun-20	Slipping share: \u03e4tasenve010C5 Start scannig directoy \u03e4tasenve010Development including all levels of subdirect Done scannig directoy \u03e4tasenve010Development. Scanned 7255 directoris and Start scannig directoy \u03e4tasenve010Levelopment. Scanned 7255 directoris and Tat Done scannig directoy \u03e4tasenve010Levelopment (u03e5) directoris and 154 Start scannig directoy \u03e4tasenve020.Projects: Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects Including all level of subdirector Done scannig directoy \u03e4tasenve020.Projects.Scanned 1326 directories and 459 start scannig directoy \u03e4tasenve020.Projects.Scanned 1327 directories and 270 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 271 start scannig directoy \u03e4tasenve020.Projectoris.Scanned 1327 directories and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectoris and 273 start scannig directority hoverthid level subdirectority hoverthid level sub	1 236334 files. es 76987 files. 87 files. es es 938 files.	possible errors. Tip: use this list to view the		containers). Schedule an automatic scan by start	ing the

CREATING REPORTS

After the scan is complete the database can be used to make overviews. The Report View of the application displays the initial folder tree containing a summation of the rights found per directory or file. The folder icon indicates what rights are found and the columns next to a directory show the special rights. Without applying filters, the permission will mainly be set to "Full Control" with all the special rights, but after applying <u>filters</u> on a user or group, the unwanted rights can be viewed at a glance. In order to not clutter the folder tree the users are not instantly displayed in the folder tree, but rather across in <u>four tabs</u> under the folder tree

- Effective permissions: displays the effective rights of all users and groups in the selected folder that match the filter criteria. Each user or group can be folded out to see where the rights originate from.
- ACL on the file system: shows the rights (Access Control Entries) as they appear on the file system. This corresponds with the Security tab in Windows Explorer and includes the possibility to <u>adjust rights</u> from within the application.
- Trace the origin of permissions: provides the ability to create a user or group to pin down through which group memberships and parent folders the rights have been obtained.
- All matching users and groups: the previous tabs display information for the selected directory. This tab displays all unique users and groups that are found in the overview. Each user or group can be folded out to see where the rights are found and through which group.



Applyfilters ‰ 🗊 🗇 🖷 🖷 🖷 🖓 🥬 🔎	1 0														Quick file search: search o	n file name	_
*Member filters	The file tree displays an apprepated view of all t	he nermissions that match the filter. It sh	man a label with	h the rel		listing an		e of colu	max she	owing wi	hich some	ial narmir	tions an	nh a narmini	ions of various members, as each row in	a sum of all	-
	 retrieved permissions. Use the tabs at the bottom 	m of the screen to view more details on t	he selected dire	ectory or	file.		a numbe	- or cons		owing in	inch aper	an permu	anona abi	py eg. permiss	ions of rendos memoes, as each for a		
Filter on members	Path 35937 items found		Permission			1.8	10	2 -		12 1	177	6 0	21	2 2			
Saved member selections:	CA Employees		Read and ex	ecute		- 19	171										
	Filter O	n users or groups, sions and folder or files.	None			1		-					-				
stom 👻 🔛 🔀	¥ 1 2015		None														
	✓ III Projects		None														
fember filter options	✓ ■ Results		None														
lude	✓ IIII Clients		None											_		_	
Users 🖸 🖏 Groups	MCE Hospital		Modify			1	5	1 12		7 1	77	0	9				
	Y Nade Bank LC		Read and ex	ecute				-		-			2	Browse the tive permi	rough the directories and inspect the e issions based on your filter criteria. If yo	ffec-	
🌺 Built-in groups 🛛 🤗 Group memberships	E-mail prop	osal.txt	Read and ex			1		\$	T	1			2	have selec	cted multiple members then this view sl		
ude or exclude users/groups:	Evaluation.		Read and en	ecute				4	12				0	the sum o	of all permissions.		
clude or exclude users/groups:	Notes 2015	1608.doci	Read and en			18		4		1			0	A green b	ackground indicates explicit permission	6, 8	
1	Notes 2015	3714.docx	Read and en	ecute		1		-		1			2		background means explicit deny, light means inherited	NO.	
	Notes 2015	3829.doca	Read and ex	ecute		1		\$	1	1			0	allow.	and dely and the inclusion in the inclusion		
	Profits.xisa		Read and est	ecute		1		\$	-	-			0				
	Proposal.pc	1	Read and ex	ecute		1		1	1	-			0				
	Re results zip		Read and ex	ecute				\$		-			2				
Select one or more users or groups or	Screenshot.	ped	Read and ex			- 12		-	-	-			0				
exclude particular members.	> 2016		None					. 14					-				
	intranet		Read and en	ecute		1		\$	125	-							
	> Water and			ecute 1				14	-				0				
	View and modify permissions on	the Pin a member in the Tr		ecute	View all	the effec	ive permi	sions of	-	1			0				
	file system. This tab corresponds	with view the provenance of on the selected folder.	permissions		the use	s and gro	ups in the	overviev		DT	T	6 0	21	8 8			
	the Windows Security tab.	on the selected route.	1	ecute	1				_	-		-	2				
	Technical support		Read and ex	ecute	1	1		*	-	-			0				
					_				10	-							_
	B Effective permissions X Co ACL on the fi	le system 🛛 🏷 Trace the origin of pe	missions 🗾	7 All m	atching us	ers and gr	oups								Apply filter on th	e list 📝 🗋	
members from group or OU:	This tab displays all the members that are found inherited permissions for a particular user or gro					syed and	unfolding	a membe	er will di	isplay all	the appl	icable expl	licit Acce	ess Control Entri	ies and (if applicable) members of a gro	up. To view the	¢
And Annual Result	mounted permissions for a particular due of gr	buy, you can put a memoer in the mote	and daming the co	ontext in	and.												
TESTDOMAIN\Consultants [global group]	search user or group	2															
										-						1	
	Member	Permission	10	1 12	16 😭	6. 6	1 4	0	ø	PA		Inheritanc	e flags		From folder	1	
	 TESTDOMAIN/PWaxman 	Read and execute	1		\$	T	1			2							
	P TESTDOMAIN\Domain Users [global		n/a on thi		1		123			2		This folde	r, subfol	ders and files	\\dataserver01\data		
Frank and the second	TESTDOMAIN\Consultants [global gr	oup] Read and execute	13		1	100	and a			2		This folde	r, subfol	ders and files	Trade Bank LC		
Include or exclude all members of a particular group or LDAP OU.	> 2 TESTDOMAIN/RRounthwaite	Read and execute	1	1	1					P						_	
	> 2 TESTDOMAIN/SPurcell	Read and execute	1	6	-		1			P					Division in the second		
	> 2 TESTDOMAIN/SShridhar	The second se	1 2		1		40			P					Directly modify a on the file system		
		ew the effective permissions of each use group including group memberships.															

Through these four angles we can easily get answers to the first five information requirements. We can instantly view effective rights on all directories, we see per directory and user where the rights come from and we can filter out all the users of a particular group without losing the relationship between the rights and users. The latter helps us with the 5th information requirement (*"What are the right for all users of a specific group and where are the exceptions?"*). Finally, we want to know which users or groups are involved in the unwanted rights within the search results. By including multiple users/groups as a filter, or a filter of the *"All members from group" type*, in one bulk check an overview is created for a large group of users including nested group memberships. With the *Effective Permissions* and *All matching users and groups* tabs, we can subsequently zoom in on individual users.

The last information requirements is to run checks to keep the access rights consistent. Instead of notifying system administrators for each change, Permission Analyzer offers another solution. A set of filters can be stored as Policy in order to periodically check for unwanted rights. If search results are found on a Policy, the system administrator can be notified by email, with an HTML report of the rights found as an attachment. Also, the list of Policies with their status is available within the application. Loading of a Policy gives the possibility to zoom in on the results and thus solve the cause.

Example:

We make a policy in which it is stated: "Nobody from the group Freelancers can edit project data"

We want to create a report in which we get to see the unwanted rights so that we can save the filters as Policy. We add a member filter of the type "All members from group" and we select the group Freelancers. Then we add additional filters to the rights (we want to allow read access), and we report on the scopes folder \\\\dataserver01\\projects:





Tip: Use the Policy Wizard to get acquainted with the various filter options:

🖹 Create policy >
Policy type
This wizard guides you through a number of predefined policies. Remember you can save any set of filters as a new policy, but this wizard will limit the number of filters based on the selected policy to help you understand the possibilities.
Policy name:
Explicit user permissions for the group Intranet Developers
Policy description:
This policies checks all explicit user permissions of all members from the group Intranet Developers.
v
Policy type: [®] Only the members of particular groups are allowed to have permissions in the given folder(s) [®] [®] Members from particular groups are not allowed to have permissions in the given folder(s) [®] [®] Only particular users or groups are allowed to have explicit permissions in the given folder(s) [®] [®] [®] Particular users or groups are not allowed to have explicit permissions in the given folder(s) [®]
< Previous Next > Finish Cancel



The listing now shouldn't display any search results, which means that no unwanted rights have been found. We now store the filters as Policy:

🖹 Create a new policy	- D X									
Create a new policy										
create a reference to the filter selection v	filter, then that selection will show up as an option when creating the report. Using the selection will vithin the report and any modifications to the filter selection will result in all reports automatically king the option in the report will result in the report saving a copy of the filters and not change									
Policy name:	Permissions of freelancers in the Projects folder									
Report description:	All permissions excluding Read and Exceute permissions for everyone in the group Freelancers, scoped to the Projects folder.									
Report type:	Users/groups and all their explicit permissions $\qquad \lor$									
File type:	HTML with interactive table									
Target file path:	c:\permission reports\Permissions Freelancers in Projects folder.html									
Custom template path:										
E-mail recipient:	administrator@mydomain.com									
Policy alert threshold (file/folder count):	1									
Link to filter sets:	No filter sets have been selected									
Filters for this report:										
👷 Include (nested) group membership										
👫 Include all members from the group	TESTDOMAIN\Freelancers [global group]									
ACE's that have any of the fo	Ilowing permissions:									
P Read (allow)										
List folder content (allow)										
Read and execute (allow)										
Include folder \\dataserver01\project	5									
	Create Cancel									

By regularly running the policies via the <u>parameters</u> -scan and -allPolicies, we can periodically check the rights for consistency, without having to check each change in the folder structure manually. In the overview of Policies we can see the status of our rules at a glance and we can zoom in on the unwanted rights by loading a policy in the application:

Policies								
Policies								
A policy is a collection of filters that display unwanted permissions. The difference between a policy and in the details.	d a standard report is that a policy def	nes a combination of filters t	nat should not yi	eld any result	s. Should you have any search result items	that appear as ex	cceptions, then simply raise	the threshold val
Vame		Policy status	Result count	Threshold	Report type	File type	Last run	Last run messa
All members of the group Auditors (including individual group memberships) are only allowed to read a	data in \\dataserver02\Compliancy	Found permissions	5	1	Folders/files and the ACL with expand	CSV	jun 27 2017 16:12	OK
Explicit permissions in the Sales folder should only be assigned to the groups Pre-Sales, Consultants and	Finance	Passed	0	1	Folders/files and the sum of their per	HTML	jul 03 2017 11:57	OK
No one from the group External Employees should be able to modify project data		Passed	0	1	Folders/files and their Access Control	HTML HTML HTML HTML	jul 04 2017 20:56	OK
None of the files in \\dataserver01\projects should have explicity user permissions (only groups)		Passed	8	9	Folders/files and the sum of their per		jul 02 2017 20:57	OK
Only the group Project Management should be able to modify data in the Customers folder		Passed	0	1	Folders/files and the sum of their per		jun 30 2017 21:05	OK
Only the users Andrew Lawrence and Erin Simpson are allowed to modify data in HR\News\Events		Passed	0	1	Folders/files and the sum of their per		jun 29 2017 11:02	OK
Only users in the LDAP OU System Admins may access the folder \\dataserver01\Network\Config		Passed	0	1	Folders/files and their Access Control	HTML	jun 30 2017 11:02	OK
	💉 Edit policy details							
	2 Load policy into application							
	Q Quickly view policy results							
	Open report file							
	Run policy							
	Open destination folder in Ex	plorer						
	× Delete policy							
Run all policies								Clos

11 April 2021



AUDIT DASHBOARD

In addition to regularly running policies we can immediately discover a number of improvements for the Data Access Governance via the Audit Permission Analyzer's dashboard. This dashboard shows 18 different charts including a top 25 of users who have the most explicit rights (rights that may have to be regulated through a group membership), a top 25 of users with the most group memberships, the ratio between direct and indirect group membership, directories with the most explicit rights and much more. Many of these statistics instantly detect where the possible risks are if someone manages to get unauthorized access to the system.



The price of Permission Analyzer depends on the number of users and groups that is scanned and varies between \$149 and \$499 per year. A license is valid for a single machine on which the application is installed (not the number of servers scanned). A trial version is available online, as well as time-limited versions of each of the Permission Analyzer editions.