

PERMISSION ANALYZER V2.3

ARCHITECTURAL OVERVIEW AND SCREENSHOTS


Reports NTFS permissions from the file system combined with user and group data from the Active Directory

PROBLEM DESCRIPTION:

In a Windows environment it is not possible to view file permissions (NTFS) by user or group. This makes it very hard to insure the operational integrity and security of your network.

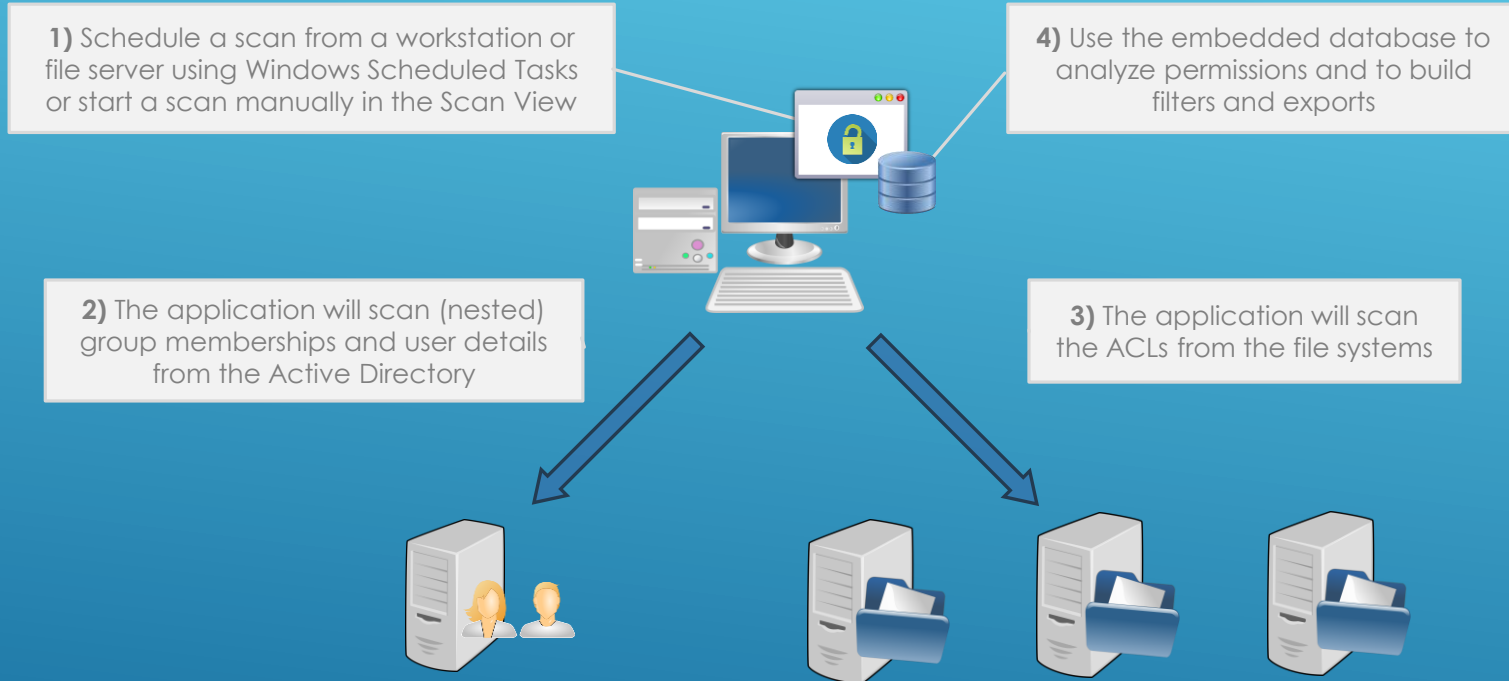
SOLUTION:

Perdemia has released Permission Analyzer v2, a Windows application that scans your network on NTFS permissions and stores all information in a database. Users can run reports by creating filters that include or exclude members, permissions, files, or folders.



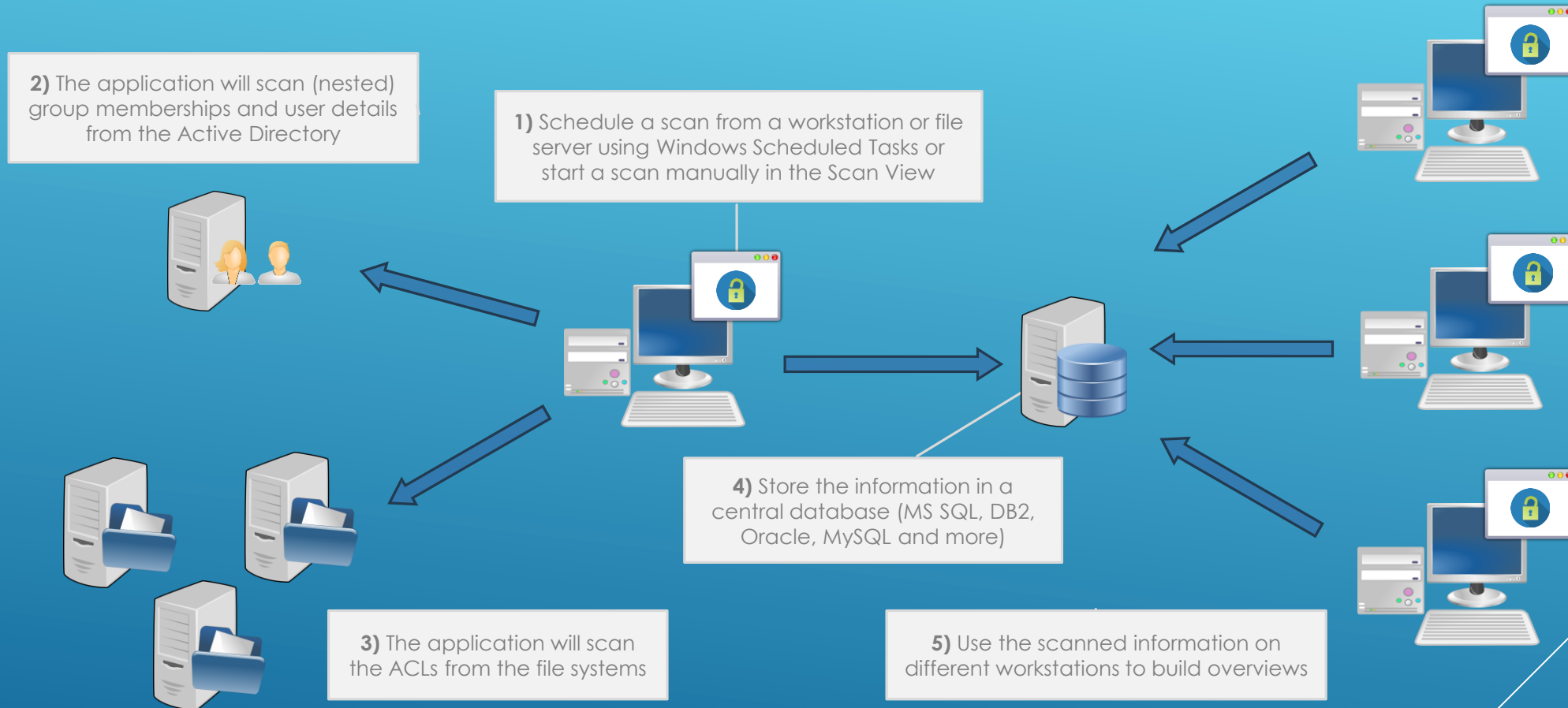
PERMISSION ANALYZER WITH EMBEDDED DATABASE

Use the embedded database to scan NTFS permissions and to create overviews:



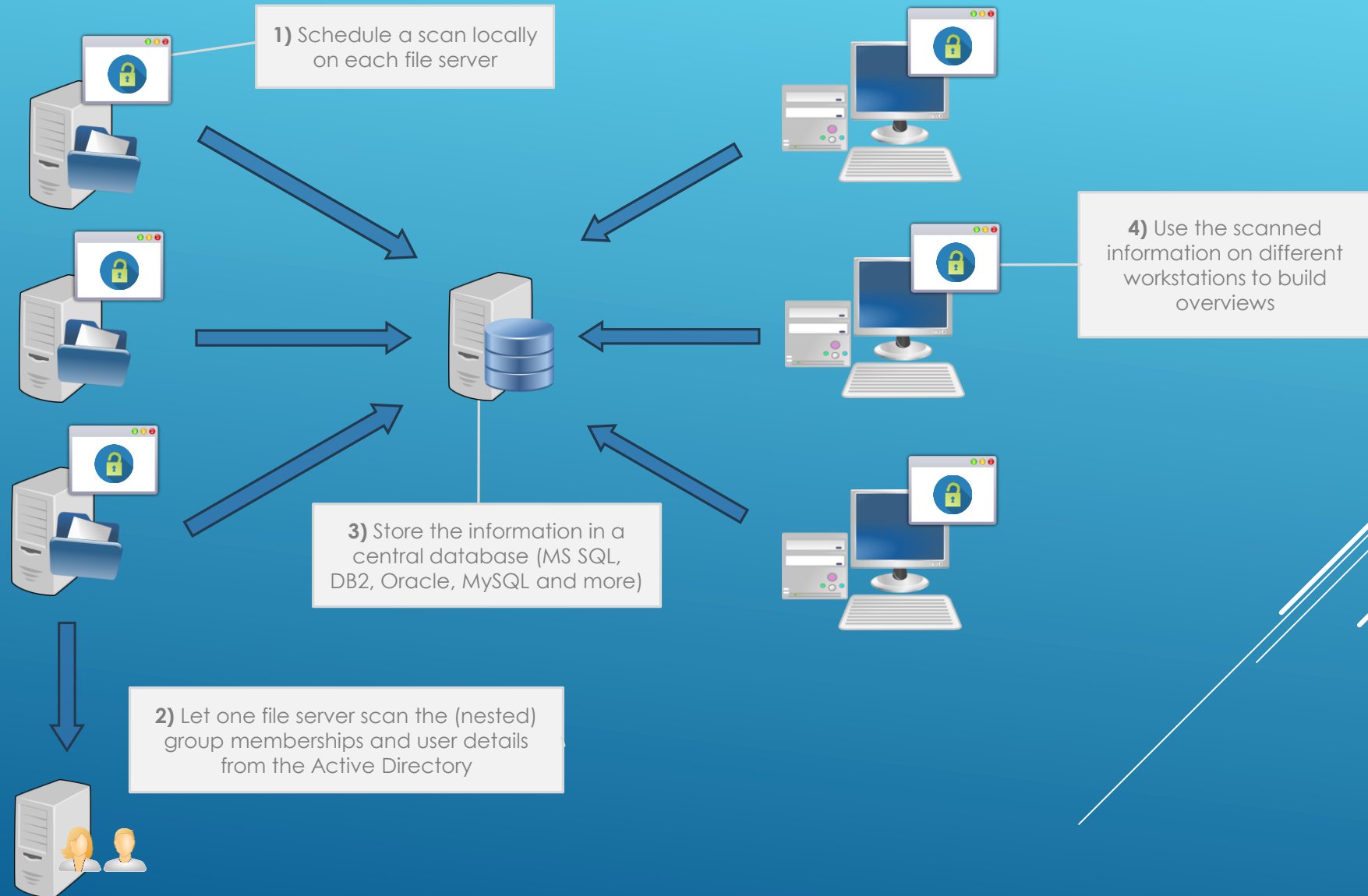
PERMISSION ANALYZER WITH A CENTRAL DATABASE

Use a central database server to scan NTFS permissions and to share network data, filter definitions and reports:



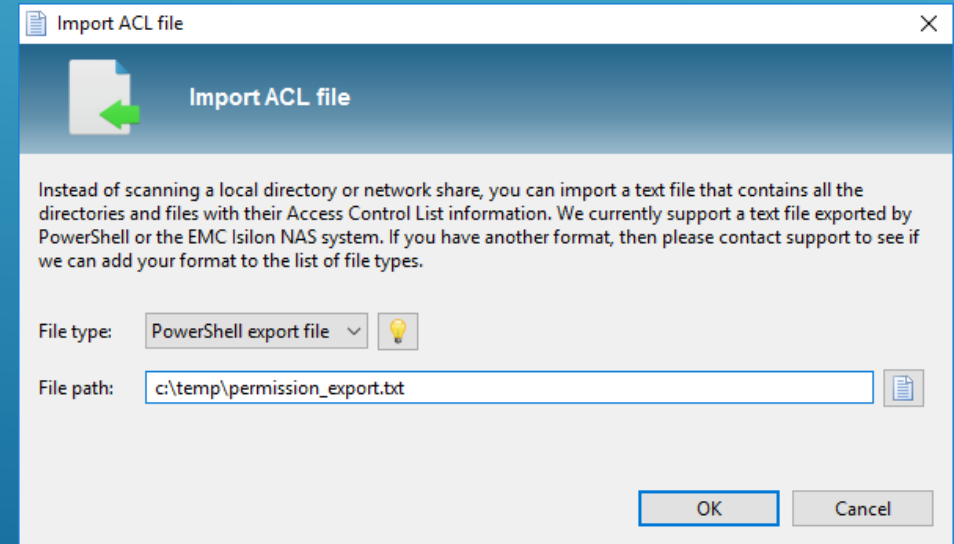
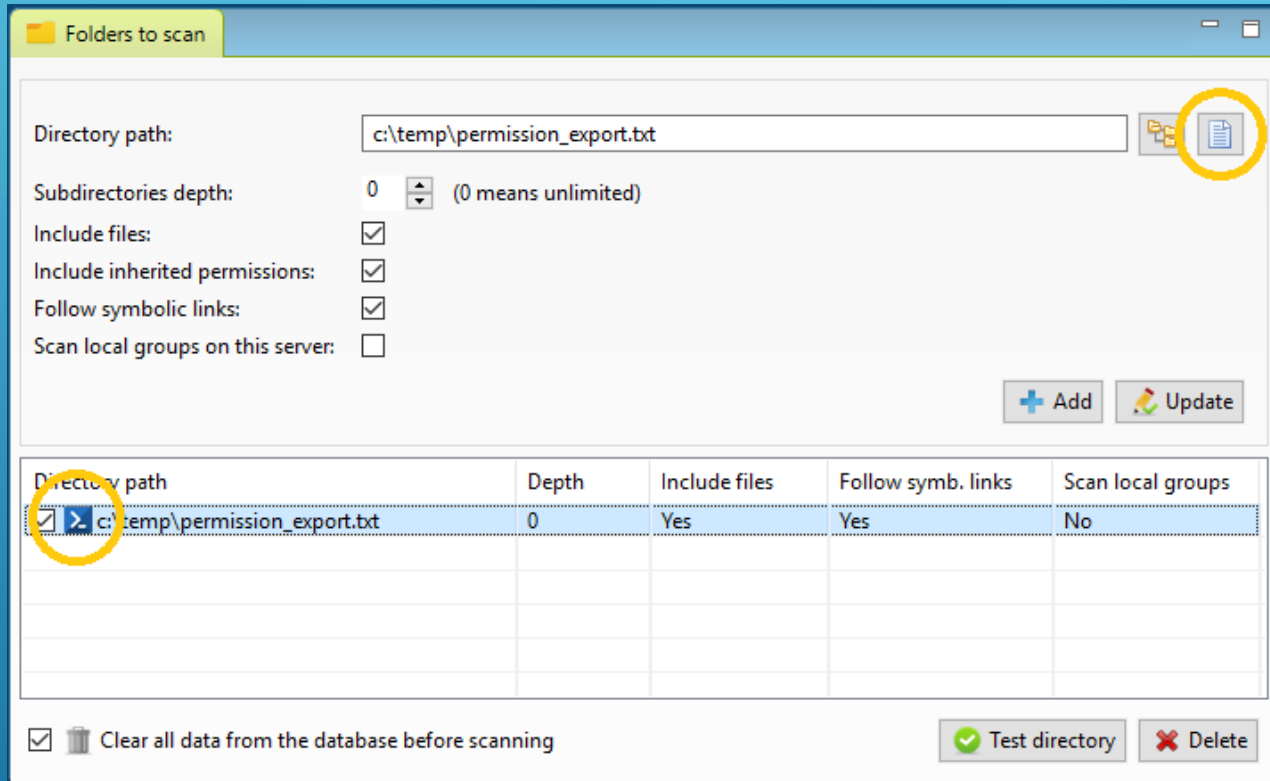
PERMISSION ANALYZER WITH SCAN AGENTS

Install Permission Analyzer on each file server and scan files locally while using a central database server to share information:



PERMISSION ANALYZER WITH POWERSHELL SCRIPTS

Run a PowerShell script to export the ACL's to a text file. This text file can be imported into Permission Analyzer



SCANNING THE NETWORK

The background is a blue gradient, transitioning from a lighter blue at the top to a darker blue at the bottom. On the right side, there are several white, parallel diagonal lines that create a sense of motion or scanning.

OPEN THE SCAN VIEW TO ADD DIRECTORIES AND LDAP OU'S

Permission_Analyzer

File Help

Folders to scan

Directory path:

Subdirectories depth: 0 (0 means unlimited)

Include files:

Follow symbolic links:

Scan local groups on this server: (servers will never be scanned more than once)

Directory path	Depth	Include files	Follow symb. links	Scan local groups
<input checked="" type="checkbox"/> \\dataserver01\projects	0	Yes	Yes	Yes
<input checked="" type="checkbox"/> \\development\applications	3	Yes	Yes	Yes

Add the network shares or local directories to scan. Optionally, scan the local groups of the server.

LDAP OU's to scan

LDAP Connection: Global Catalog

Ldap container:

Search scope: Container and sub containers

Search object types: Users and groups

LDAP connection	LDAP base container	Search scope	Object types
<input checked="" type="checkbox"/> Global Catalog	CN=Dev,OU=Distribution Groups,DC=gp...	Container and sub containers	Users and groups
<input checked="" type="checkbox"/> Primary domain contr...	ou=Management,dc=mydomain,dc=com	One level of sub containers, but not the container it...	Only groups

Add specific LDAP containers to scan. Determine the depth and the objects to scan.

Scan results

Date / time	Message
21-feb-2015 9:05:59	Start scanning directories
21-feb-2015 9:06:13	Done scanning local groups on server dataserver01. Found 53 local groups.
21-feb-2015 9:06:13	Done scanning local groups on server development. Found 33 local groups.
21-feb-2015 9:06:13	Start scanning directory \\dataserver01\projects including all levels of subdirectories
21-feb-2015 9:32:17	Done scanning directory \\dataserver01\projects. Scanned 73256 directories and 236334 files.
21-feb-2015 9:32:17	Start scanning directory \\development\applications including 1 levels of subdirectories
21-feb-2015 9:45:17	Done scanning directory \\development\applications. Scanned 39871 directories and 65391 files.
21-feb-2015 9:45:17	Scanned a total of 113127 directories and 301725 files.
21-feb-2015 9:45:17	Done scanning directories
21-feb-2015 9:45:17	Start LDAP containers
21-feb-2015 9:45:17	Preparing LDAP scan
21-feb-2015 9:45:17	Start scanning users using connection [Global Catalog] and baseDN [CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=mydomain,DC=com]
21-feb-2015 9:48:32	Done scanning users using connection [Global Catalog] and baseDN [CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=mydomain,DC=com]. Found 133 users.
21-feb-2015 9:48:32	Start scanning groups using connection [Global Catalog] and baseDN [CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=mydomain,DC=com]

No scan in progress

Observe the scan progress, warnings and possible errors.
Tip: use this list to view the results of a scheduled scan.

Scan the network (directories and LDAP containers).
Schedule an automatic scan by starting the application with the "-scan" parameter.

CONFIGURE MORE LDAP CONNECTIONS IN THE PREFERENCES

The screenshot shows the 'LDAP connections' configuration window. At the top, there are tabs for 'Network', 'Internet', 'E-mail', 'Security', 'Database', and 'Advanced'. The main area is titled 'LDAP connections' and contains 'LDAP connection details' with the following fields:

- Connection name: Primary domain controller
- Host name: domaincontroller.domain.com
- Host port: 636
- Username DN (optional for GSSAPI / Kerberos): admin@domain.com
- Password (optional, asked when required): *****
- Encryption: SSL/TLS
- Authentication: Simple

Below the form is a table with the following data:

Connection name	Host name	Host port	Username	Password	Encryption	Authentication
Primary domain ...	domaincontroller.doma...	636	admin@domain.com	*****	SSL/TLS	Simple

At the bottom right, there are buttons for '+ Add', 'Update', 'Test connection', and 'Delete'.

Three yellow callout boxes provide instructions:

- 1) Configure your domain controllers and/or global catalogs.
- 2) Configure a bind user and select an authentication type: simple, SASL or Kerberos
- 3) Add and test your LDAP connections!

BUILDING THE OVERVIEWS

The background is a blue gradient, transitioning from a lighter blue at the top to a darker blue at the bottom. On the right side, there are several white, parallel diagonal lines that create a sense of movement and depth, extending from the bottom right towards the top right.

OPEN THE REPORT VIEW AND BUILD YOUR FILTERS

Permission Analyzer - Consultant edition
 Application Reports Policies Help

Apply filters Quick file search: search on file name

Member filters **Permission filters** **Folder filters**

Filter on members

Saved member selections: Custom

Member filter options

Include:

- Users
- Groups
- Built-in groups
- Group memberships

Include or exclude users/groups:

Effective permissions | **ACL on the file system** | **Trace the origin of permissions** | **All matching users and groups**

Apply filter on the list

The file tree displays an aggregated view of all the permissions that match the filter. It shows a label with the relevant permission and a number of columns showing which special permissions apply e.g. permissions of various members, as each row is a sum of all retrieved permissions. Use the tabs at the bottom of the screen to view more details on the selected directory or file.

Path: 35937 items found

- Employees
- Finance
 - 2015
 - Projects
 - Results
 - Clients
 - MCE Hospital
 - Trade Bank LC
 - E-mail proposal.bt
 - Evaluation.docx
 - Notes 20150608.docx
 - Notes 20150714.docx
 - Notes 20150829.docx
 - Profits.xlsx
 - Proposal.pdf
 - results.zip
 - Screenshot.png
 - 2016
 - Intranet
 - Marketing
 - ...
 - Technical support

Permission

Path	Permission	Special Permissions
Employees	Read and execute	...
Finance	None	...
2015	None	...
Projects	None	...
Results	None	...
Clients	None	...
MCE Hospital	Modify	...
Trade Bank LC	Read and execute	...
E-mail proposal.bt	Read and execute	...
Evaluation.docx	Read and execute	...
Notes 20150608.docx	Read and execute	...
Notes 20150714.docx	Read and execute	...
Notes 20150829.docx	Read and execute	...
Profits.xlsx	Read and execute	...
Proposal.pdf	Read and execute	...
results.zip	Read and execute	...
Screenshot.png	Read and execute	...
2016	None	...
Intranet	Read and execute	...
Marketing	Read and execute	...
...	Read and execute	...
Technical support	Read and execute	...

Filter on users or groups, permissions and folder or files.

Browse through the directories and inspect the effective permissions based on your filter criteria. If you have selected multiple members then this view shows the sum of all permissions.

A green background indicates explicit permissions, a dark red background means explicit deny, light red means inherited deny and white means inherited allow.

Select one or more users or groups or exclude particular members.

View and modify permissions on the file system. This tab corresponds with the Windows Security tab.

Pin a member in the Trace tab to view the provenance of permissions on the selected folder.

View all the effective permissions of all the users and groups in the overview.

All members from group or OU:

TESTDOMAIN\Consultants [global group]

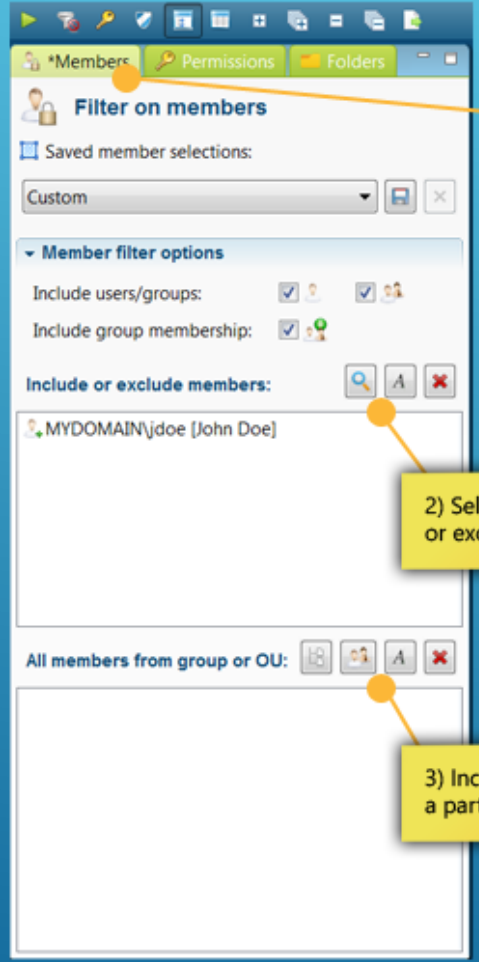
search user or group

Member	Permission	Inheritance flags	From folder
TESTDOMAIN\PWaxman	Read and execute		
TESTDOMAIN\Domain Users [global group]	Read and execute (n/a on thi...	This folder, subfolders and files	\\dataserver01\data
TESTDOMAIN\Consultants [global group]	Read and execute	This folder, subfolders and files	Trade Bank LC
TESTDOMAIN\RRounthwaite	Read and execute		
TESTDOMAIN\SPurcell	Read and execute		
TESTDOMAIN\SShridhar	Read and execute		

View the effective permissions of each user or group including group memberships.

Directly modify ACE's on the file system

FILTER FOR MEMBERS

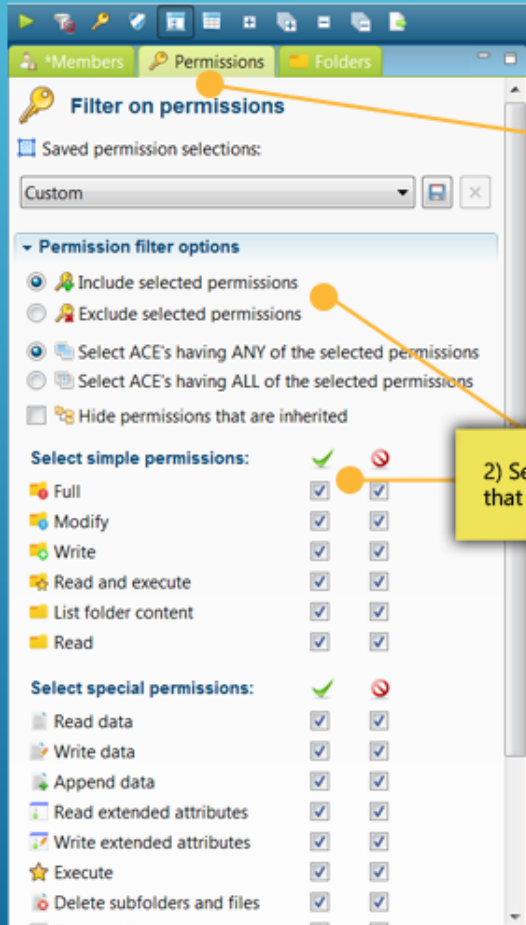


1) Filter on users or groups

2) Select one or more users or groups or exclude particular members.

3) Include or exclude all members of a particular group or LDAP OU.

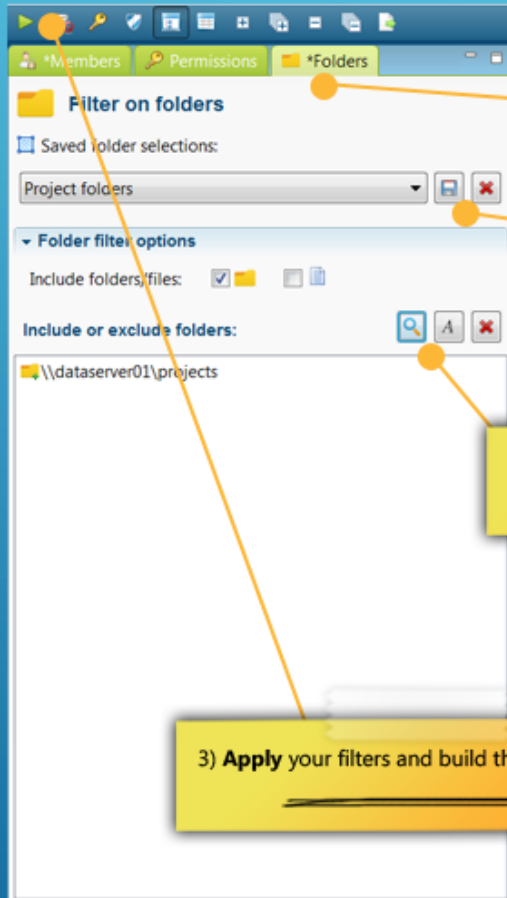
FILTER FOR PERMISSIONS



Filter on specific simple or special permissions

2) Select the 'allow' and/or 'deny' permissions that you want to include or exclude.

FILTER FOR FOLDERS



1) Filter on folders or files

Tip: save your filters as a selection

2) Select specific folders or use a wild card filter on the folder name

3) **Apply** your filters and build the overview!

USE THE TRACE VIEW AND VIEW THE ORIGIN OF PERMISSIONS

Permission Analyzer - Consultant edition

Application Reports Policies Help

Apply filters

Quick file search:

Filter on members

Member filter options

Include:

- Users
- Groups
- Built-in groups
- Group memberships

Include or exclude users/groups:

Select one or more users or groups or exclude particular members.

View the effective permissions of each user or group on the selected file including group memberships.

View and modify permissions on the file system. This tab corresponds with the Windows Security tab.

View all the effective permissions of all the users and groups in the overview.

Filter on users or groups, permissions and folder or files.

Browse through the directories and inspect the effective permissions based on your filter criteria. If you have selected multiple members then this view shows the **sum** of all permissions.

A green background indicates explicit permissions, a dark red background means explicit deny, light red means inherited deny and white means inherited allow.

Effective permissions

ACL on the file system

Trace the origin of permissions

All matching users and groups

Hide inherited permissions

This tab displays all permissions that apply to a specific member as well as the provenance of those permissions, e.g. through which (nested) group membership or superior directory the permissions were granted. Put a member in this tab using the context menu on the members in one of the other tabs.

Show permissions for member: TESTDOMAIN\SPurcell [Sean Purcell]

Path	Permission	Via group	Inheritance flags
\\dataserver01\data	Read and execute (explicit)	TESTDOMAIN\Domain Users [global group]	This folder, subfolders and files
Finance	None		
2015	None		
Projects	None		
Results	None		
Clients	None		
Trade Bank LC	Read and execute (explicit)	TESTDOMAIN\Consultants [global group]	This folder, subfolders and files

Read data (explicit)

Pin a member in the Trace tab to view the provenance of permissions on the selected folder.

Hide inherited permissions

All members from group or OU: TESTDOMAIN\Consultants [global group]

Include or exclude all members of a particular group or LDAP OU.

DEFINE REPORTS

Report details

Report name: Project folders for John Doe

Report description: Overview of the explicit permissions for John Doe, limited to the folder \\dataserver01\pro

Report type: Effective permissions

FileInfo type: HTML with dynamic table

Target file path: c:\reports\johndoe.html

Custom template path:

E-mail recipient: admin.support@mycompany.com

Link to filter sets: Projects folder

Filters for this report:

- Projects folder
 - Only include folders
 - Include folder \\dataserver01\projects
 - Include (nested) group membership
 - Include member MYDOMAIN\jdoe [John Doe]
 - Hide permissions that are inherited from a parent folder

Create Cancel

1) Save all your filters as a **report**. Load reports quickly in the overview or export them to a file.

2) Select the report type and the way the data is presented.

3) Select the file type:
- Plain HTML
- HTML with dynamic table (filter, sort and search functionality)
- CSV

4) Besides the file export, send the report to someone by e-mail (optional)

Tip: schedule your reports by starting the application with the parameters -report "my report". Add multiple -report parameters at once.

EXPORT TO HTML OR CSV

Directories and files found: 10

PERMISSION ANALYZER - TRACE REPORT

The Trace report displays permission information for all members that match the selected filter criteria. For each member the report will show all applicable Access Control Entries and where they come from, meaning via what group membership. All permissions excluding Read permissions for everyone in the group Freelancers scoped to the projects folder.

Filters applied:

- Include (nested) group membership
- Include all members from the group MYDOMAIN\Freelancers [global group]
- Exclude ACE's that have any of the following permissions:
 - Read and execute (allow)
 - List folder content (allow)
 - Read (allow)
- Include folder \dataserver01\projects

Column visibility:

- File path
- Members
- Permission text
- Special permission
- ACE flags
- Via group

Show 200 entries

Search:

Member	Permission	Read data Write data Append data Execute Read attributes Write attributes Read extended attributes Write extended attributes Delete subfolders and files Delete Read permissions Change permissions Take ownership	Via group	ACE flags
\\dataserver01\projects\Change requests				
MYDOMAIN\jdoe [John Doe]	Modify (explicit)		MYDOMAIN\Project Office [global group]	This folder, subfolders and files
\\dataserver01\projects\Development				
MYDOMAIN\jmurphy [Jane Murphy]	Full (explicit)		MYDOMAIN\Testers [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development\Calculation application				
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)		MYDOMAIN\Testers [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development\Calculation application\appidcertstorecheck.exe				
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)		MYDOMAIN\Testers [domain local group]	This file only
\\dataserver01\projects\Development\Calculation application\Design				
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)		MYDOMAIN\Testers [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development\Calculation application\Design\cifs.sys				
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)		MYDOMAIN\Testers [domain local group]	This file only
\\dataserver01\projects\Finance				
MYDOMAIN\jdoe [John Doe]	Special (explicit)		(direct)	This folder, subfolders and files
\\dataserver01\projects\HR				
MYDOMAIN\jdoe [John Doe]	Full (inherited)		MYDOMAIN\HR Admins [global group]	This folder, subfolders and files
\\dataserver01\projects\HR\employees				
MYDOMAIN\jdoe [John Doe]	Change permissions (explicit)		(direct)	This folder and subfolders
MYDOMAIN\jdoe [John Doe]	Full (inherited)		MYDOMAIN\HR Admins [global group]	This folder, subfolders and files
\\dataserver01\projects\Proposals				
MYDOMAIN\jdoe [John Doe]	Modify (explicit)		(direct)	This folder, subfolders and files

DEFINE POLICIES TO CHECK FOR UNWANTED PERMISSIONS

Policies

A policy is a collection of filters that display unwanted permissions. The difference between a policy and a standard report is that a policy defines a combination of filters that should not yield any results. Should you have any search result items that appear as exceptions, then simply raise the threshold value in the details.

Available policies:

Name	Policy status	Result count	Threshold	Report type	File type	Last run
Explicit user permissions for the group Intranet Developers	Failed	10	1	Folders/files and matching group members	HTML with interactive table	okt 12 2016 20:04
External employees should not have permissions in the Finance Data folder	Passed	12	13	Folders/files and the sum of their permissions	HTML with interactive table	okt 10 2016 20:18
Only people in the group Human Resources should have permissions in the Employee folder	Passed	0	1	Folders/files and their Access Control List	HTML with interactive table	okt 15 2016 20:04
Only the network administrators should have access to the file server BACKUP01	Passed	0	1	Folders/files and their Access Control List	HTML with interactive table	okt 15 2016 20:04

- Edit policy details
- Load policy into application
- Quickly view policy results
- Open report file
- Run policy
- Open destination folder in Explorer
- Delete policy

Run all policies

Close

AUDIT DASHBOARD

Permission Analyzer - Consultant edition

Application Help

Directory: All

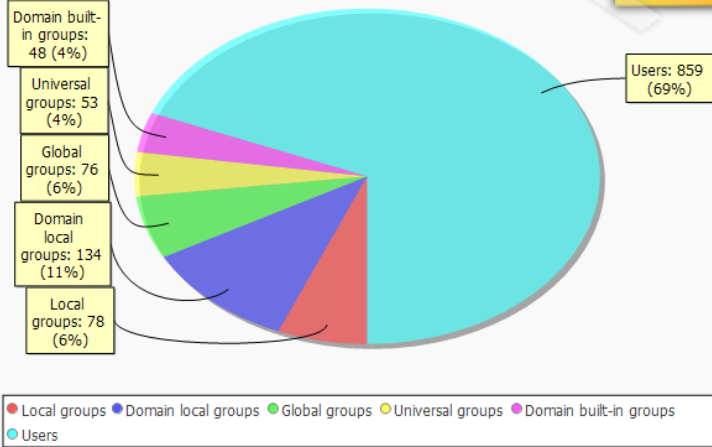
Audit category: Users and groups

Build all charts

Reset all charts

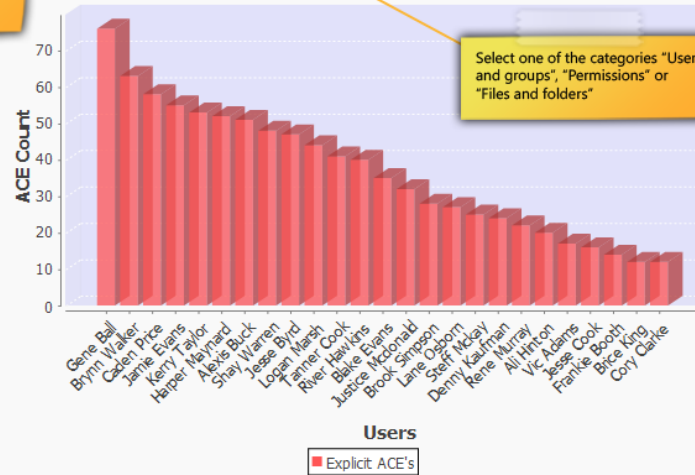
Users and groups from LDAP

Select a directory to scope the data

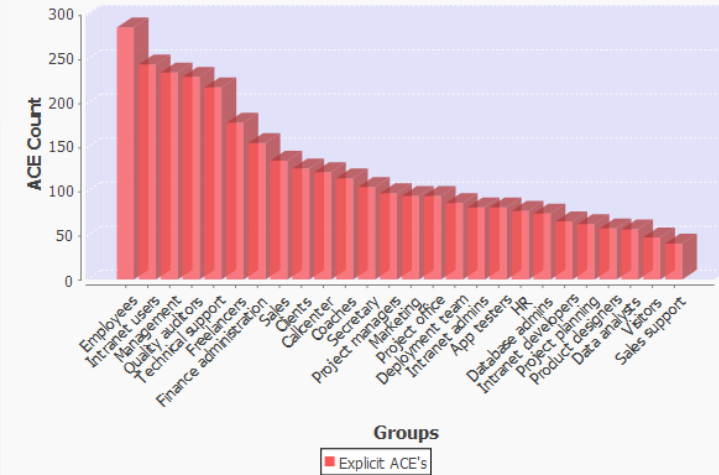


Top 25 of users with most explicit ACE's

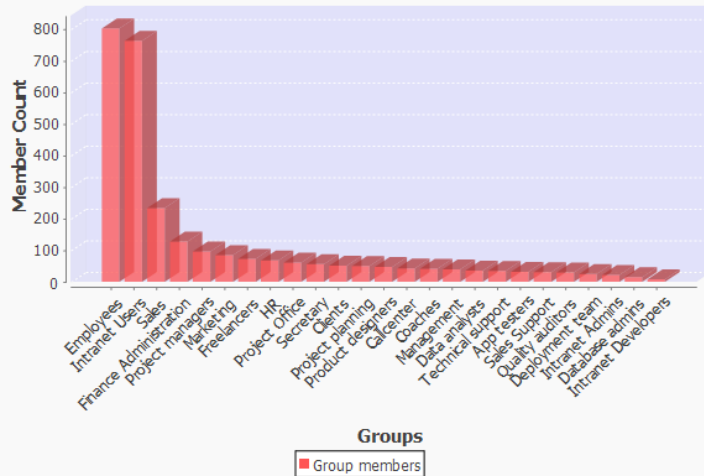
Select one of the categories "Users and groups", "Permissions" or "Files and folders"



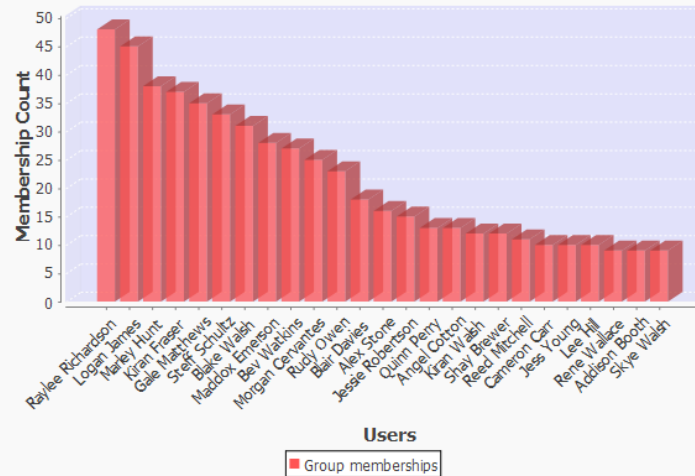
Top 25 of groups with most explicit ACE's



Top 25 of groups with most members



Top 25 of users with most group memberships



Group complexity: Indirect memberships (6798) / all memberships (13454)

