IT-Security

Permission analysis in Docusnap

TITLE	IT-Security
AUTHOR	Docusnap Consulting
DATE	12/12/2023
VERSION	4.0| valid from November 13, 2023

CONTENTS

1. INTRODUCTION

Permissions are essential for companies. Often it is difficult to get a structured and clean overview of which shares, and directories have which permissions, or which shares and directories a certain user or group of people may access.

With the help of IT security in Docusnap, these questions can be answered in the areas of file system, Exchange, and SharePoint.

As of 11/13/2023, it is not possible to perform an authorization analysis on the inventoried Exchange Online data.

In the file system area, share and NTFS permissions are used so that you can also determine the effective permissions of a user here. In addition, permissions for SharePoint servers, Exchange mailboxes, mailbox folders and public folders can be inventoried and analyzed.

This HowTo describes the implementation of the authorization analysis in Docusnap with all its functions and possibilities as well as application examples.

- Chapter 2 describes the authorization analysis for file systems in full - this includes, among others
    - Conditions for implementation
    - Directory reports, which output the permissions on shares / folders
    - Principal reports that output permissions for selected users / groups
    - Time-controlled execution of these reports
- Chapter 3 describes the authorization analysis of your SharePoint environment.
- Chapter 4 Authorization Analysis of the Exchange Infrastructure (On Premise)

1.1 GENERAL REQUIREMENTS

IT security can be analyzed in the areas of file system, Exchange and SharePoint. All of these areas require a full Active Directory inventory. The further necessary inventories can be found in the following table.

File system (Windows, CIFS, DFS)	Exchange	SharePoint
Active Directory Inventory (resolving SIDs and group affiliations)	Active Directory Inventory (resolving SIDs and group affiliations)	Active Directory Inventory (resolving SIDs and group affiliations)
Windows, CIFS, DFS (releases and their release permissions)		
DFS - the systems involved in DFS must be inventoried as Windows systems in order to be able to resolve local SIDs	Exchange inventory (mailboxes, public folders etc.)	SharePoint inventory (websites, document libraries etc.)
NTFS analysis		

Table 1 - IT Security Requirements

An overview of the required ports and permissions can be found in the HowTo Whitepaper Docusnap Inventory in the Docusnap Knowledge Base.

2. FILE SYSTEM (CIFS/DFS/WINDOWS)

2.1 REQUIREMENT

The successful permission analysis for file systems (NTFS, ReFS) requires the following inventories:

- Active Directory
- Windows, CIFS, DFS

Active Directory

An up-to-date Active Directory inventory is essential for authorization analysis. During the NTFS analysis SIDs are determined. These SIDs can be resolved to users and groups through the Active Directory inventory. The user and group structures are also known (group memberships).

In **step 3 - Active Directory** - of the Active Directory inventory, you can define an OU filter. Afterwards, only the selected OUs and the user and groups located there are inventoried. Please note that this setting may result in some SIDs not being resolved. Check the **Advanced option - Inventory all users and groups**.

Be sure to take a complete inventory of trusted domains as well. This is the only way to ensure that all SIDs can be resolved if authorizations have been assigned here.

Windows - CIFS - DFS

The later NTFS analysis aims at drives or shares. For these to be available for selection, the systems and services above them must also be inventoried: Windows, CIFS and DFS. During these inventories, the release authorizations are inventoried. These form the first part of the authorizations.

The following chapter describes the NTFS analysis, which inventories the second part of the permissions - the NTFS permissions.

2.2 NTFS ANALYSIS

NTFS analysis is used to read the NTFS authorizations and store them in the database. The NTFS analysis does not have archive data, which means that you can always only analyze the status.

The wizard for performing the NTFS analysis is located in the IT Security section, which can be accessed via the navigation bar.

In step 1 - Company selection - select the corresponding company

Step 2 - Authentication - requires a domain user with sufficient permissions to connect the shares and read the permissions.

In step 3 - Systems - you can now select the systems to be analysed via their drives or shares (use shares for Windows systems). The explicit selection of the shares to be analyzed has the advantage that shares that are not required are left out - e.g. administrative shares whose effective permissions are restricted to administrators.

Furthermore, you have the option of limiting the folder levels that are to be used for the NTFS analysis. This should be considered, as this setting has a considerable influence on the required database size (SQL-Express -10 GB).

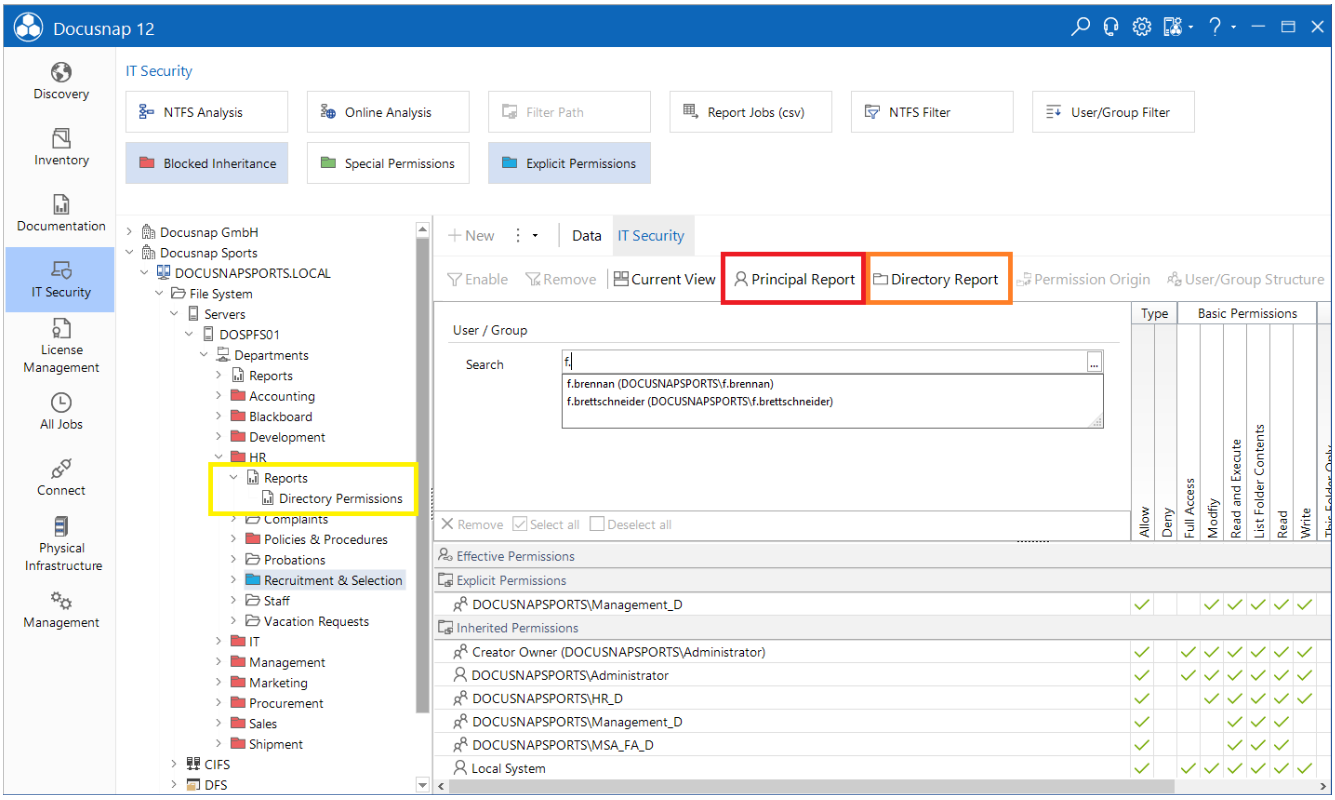
In order to also take into account drives or shares that did not yet exist during planning during scheduled inventories, the option For scheduled NTFS analyses: Automatically capture permissions of new drives/shares of already selected systems can be activated. New drives or shares from selected systems are then also inventoried.

If a filter is entered in the Drives column, newly found drives or shares are only inventoried if they match the filter.

In step 4 - DFS - you can select the DFS shares to be analyzed and limit the number of folder levels.

2.3 ANALYSIS - FILE SYSTEM

After the data has been collected, it can be analyzed in the next step. Both the Docusnap interface and reports are available for analysis.



User / Group

Search: f.

f.brennan (DOCUSNAPSPORTS\f.brennan)
f.brettschneider (DOCUSNAPSPORTS\f.brettschneider)

	Type		Basic Permissions					
	Allow	Deny	Full Access	Modfiy	Read and Execute	List Folder Contents	Read	Write
Explicit Permissions								
DOCUSNAPSPORTS\Management_D	✓			✓	✓	✓	✓	✓
Inherited Permissions								
Creator Owner (DOCUSNAPSPORTS\Administrator)	✓		✓	✓	✓	✓	✓	✓
DOCUSNAPSPORTS\Administrator	✓		✓	✓	✓	✓	✓	✓
DOCUSNAPSPORTS\HR_D	✓			✓	✓	✓	✓	✓
DOCUSNAPSPORTS\Management_D	✓				✓	✓	✓	
DOCUSNAPSPORTS\MSA_FA_D	✓				✓	✓	✓	
Local System	✓		✓	✓	✓	✓	✓	✓

Figure 1 - NTFS Analysis

2.3.1 SURFACE AREA

The Docusnap interface offers you the first opportunity to analyze the permissions assignment on the file system. You start the permissions analysis via the tree structure in the IT security area. Navigate in the tree structure to the desired share or folder:

- Your company - Your domain - File system server / CIFS / DFS.

In the data area you will first see the NTFS permissions (directly set and inherited) as well as the share permissions. Using the user-group search, you can also display effective permissions for selected users and/or groups here.

If blocked inheritances or directly set permissions are to be visible in the hierarchical structure, this can be activated in the toolbar.

2.3.2 REPORTS

The following reports are available for analyzing the file system.

- directory report
- principal report
- directories
- releases

A distinction is made between complex evaluations (directory and principal reports) and simple representations of ACLs (directories and releases). For complex evaluations, e.g. effective authorizations are calculated, and group memberships are dissolved.

directory report	**principal report**	**directories**	**releases**
Evaluation of effective and NTFS permissions from the point of view of the share / directory	Evaluation of effective and NTFS permissions from the point of view of the user / group	Display of NTFS permissions	Display of share and subdirectories
Execution of complex evaluations - dissolving group memberships (optional)	Execution of complex evaluations - dissolving group memberships (optional)	Representation of the ACLs of the directories	Representation of the ACLS of the shares and directories

2.3.2.1 DIRECTORY REPORT

The directory report shows the current permissions (share, NTFS, effective) from a share / folder. Within the wizard, you also have the choice of how many directory levels are to be considered during creation.

You determine the starting point of the directory report by selecting the appropriate share / folder within the tree structure. After you have made your selection, call the wizard for creating the **directory report in the** field of action.

The following selection of options is available. All options are described again in the user manual - which can be accessed via the F1 key.

Levels

- Number of levels that will be analyzed within the report

Settings

- Show changes only
    - Folders with only inherited permissions are not shown in the report
    - Only if the effective permissions have been changed (inheritance blocked, permissions set directly), these folders will be listed in the report
- Ignore share permissions
    - Only set NTFS permissions are analyzed
    - Share permissions are not taken into account
- Exclude domain administrators
- Show groups only
    - The report does not resolve the authorized groups recursively
    - Only the authorized groups and directly authorized users are listed
- Consider creator-owner permissions
    - If the creator-owners of folders change, this is not taken into account
    - If this is taken into account, the folders with changed creator owners are listed, even if the option Show only changes is activated.
- Show active users only
- Best Practice
    - Show only changes
    - Exclude domain administrators
    - Do NOT consider creator-owner permissions
    - Show active users only

View options

- Select the appropriate permissions to list in the report
- Best Practice:
    - For non-IT-savvy groups of people, list only effective permissions

Other

- Choose between the available report formats
  - Horizontal
  - Vertical
  - Excel
  - CSV
- Representation of each user
- Selection of additional ADS properties - e.g. department

Users/Groups Filter

- Exclude specific users and groups from the display in the directory report
- In chapter User/Group Filters you will learn how to perform predefined exclusions

2.3.2.2 PRINCIPAL REPORT

The User Report displays the corresponding permissions for the selected resources and folder levels for selected users or groups.

Before a user report can be created, you must add a selected user or group using the search box. You can then open the Create User Report Wizard.

The following options are available in the wizard. Detailed explanations can be found in the user manual - F1.

Levels

- Number of levels that will be analyzed within the report

Settings

- Show changes only
    - Folders with only inherited permissions are not shown in the report
    - Only if the effective permissions have been changed (inheritance blocked, permissions set directly), these folders will be listed in the report
- Consider creator-owner permissions
    - If the creator-owners of folders change, this is not taken into account
    - If this is taken into account, the folders with changed creator owners are listed, even if the option Show only changes is activated.
- Ignore share permissions
    - Only set NTFS permissions are analyzed
    - Share permissions are not taken into account
- Special permissions
    - If this option is enabled, the special permissions are also displayed in the report
- Show subfolders without permissions
    - Should folders to which the selected user / group have no permissions be listed in the report?

Other

- Choose between the available report formats
    - Horizontal
    - Vertical
    - Excel
    - CSV
- Representation of each user
- Selection of additional ADS properties - e.g. department

2.3.2.3 RELEASE/DIRECTORY REPORT

The tree structure contains additional reports for releases and directories. These reports do **not** reflect **effective permissions.** The reports give you release and NTFS permissions.

When you select Release as well as Report directories, the following setting options are available to you regarding the scope of the reports.

2.3.2.4 CREATE AND SEND REPORTS ON A SCHEDULED BASIS

The reports described above can also be scheduled and sent by e-mail. In this way, you can send the responsible persons an overview of the assigned authorizations at regular intervals - fully automatically!

You will find the **Schedule** button within the wizard for both the user and directory reports. You can now specify where the report is to be stored in the file system (step 2) and to whom the report is to be sent by e-mail (step 3). Please also note the file formats, which you can adjust below the **advanced options**. You can separate multiple recipients with a semicolon.

The report created on the file system can then be found in the following path:

- Your Path\Your company\Your domain\Servername\Release name

You can also create and send the share and directory report time-controlled after creation via the **Schedule as Job** button.

2.3.3 PERMISSION ORIGIN

If the analysis in the user interface or within a report reveals a permission that you would not have expected, you can use Docusnap to check the origin of this permission.

Why does the user have the appropriate permissions on this resource?

You can clarify this question using the permission origin. First add the user using the search field and choose the **permission origin** in the next step.

Now the origin of the NTFS as well as the release authorization and the resulting effective authorizations are derived.

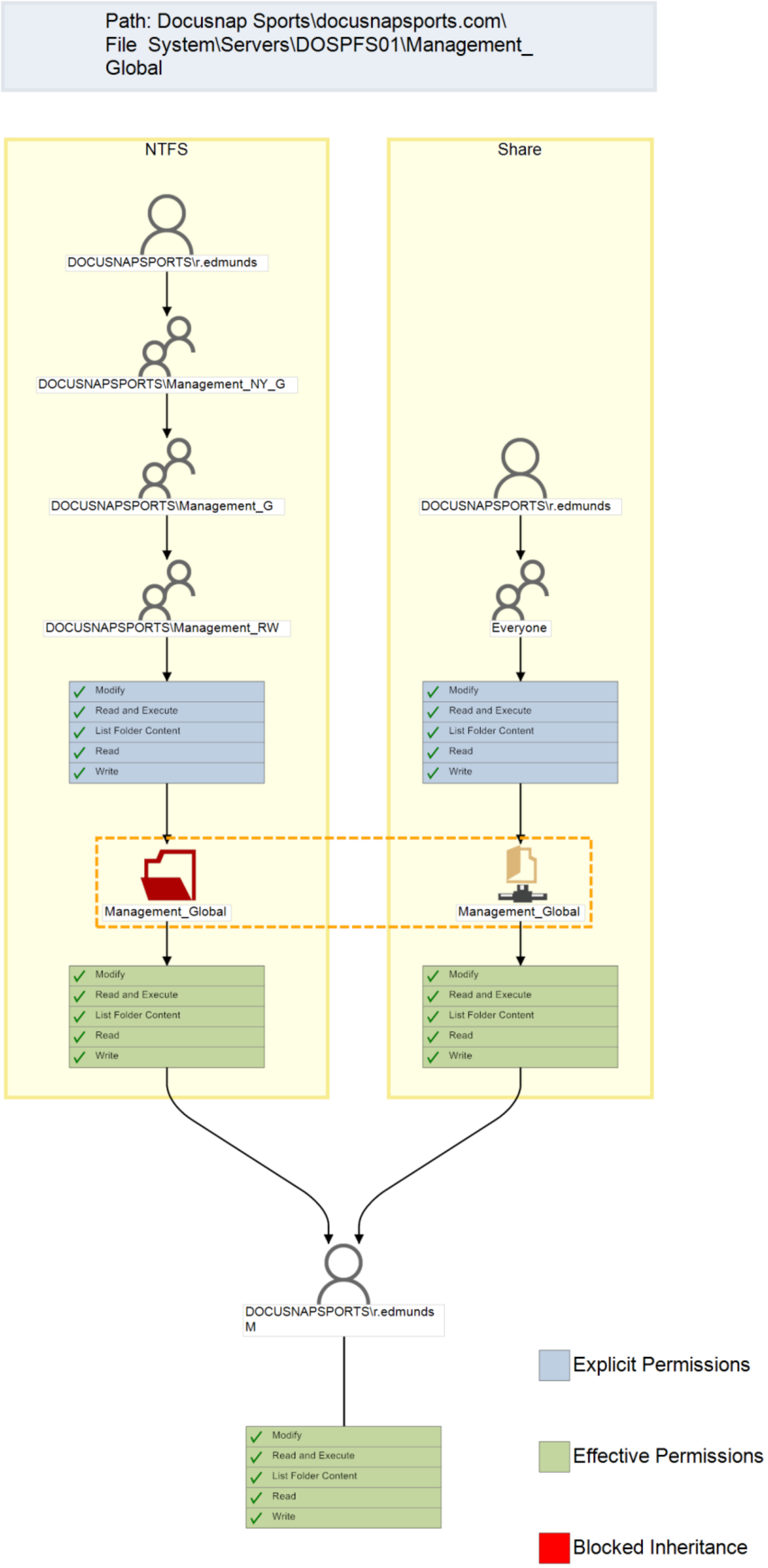


Figure 2 - Check permission origin

2.3.4 FURTHER TOPICS

The following section deals with further topics.

2.3.4.1 CUSTOMIZE DEFAULT SETTINGS

In the Options (title bar - cogwheel) - IT Security you have the option to customize the default settings for the NTFS analysis and the creation of the directory and principal report. The options selected here will be set by default in the future when you create a new directory report.

2.3.4.2 NTFS FILTER

You can use the NTFS filter to restrict the directories to be read. It is possible to specify directories that are to be inventoried. You can also exclude directories that are not required in the authorization analysis. You can also define a combination of directories to include and directories to exclude.

You call the NTFS filter via the control of the same name in the Miscellaneous area.

The following operators are available:

- Contains: The specified condition must be contained in the directory - the directory will then be inventoried.
    - If this operator is used, only the specified shares / directories are explicitly inventoried.
- Does not contain: The specified condition must not be contained in the directory - the directory will then not be inventoried.

2.3.4.3 ONLINE ANALYSIS

In addition to the so-called offline analysis - the inventory of the authorization via the previously discussed NTFS analysis - you can also perform an online analysis.

To do this, activate the online analysis using the control of the same name. In this course Docusnap tries to establish a connection to all inventoried Windows and CIFS systems as well as DFS shares.

This is useful if you need to "just do it fast" check the share and NTFS permissions of a less critical system. Here, too, you highlight folders in color whose inheritance has been deactivated or whose permissions have been set directly in addition to the inheritance.

Note that you cannot determine effective authorizations when using the online analysis. For this reason, no reports are available here.

2.3.4.4 REPORTING JOB (CSV)

If you want to create an extensive number of directory reports automatically at regular intervals, you can do this conveniently and quickly with a CSV file. Create a CSV file with the columns Domain, Host, Share/Path and Mail (sending the reports by mail).

Further information can be found in the corresponding HowTo in our Knowledge Base: Report Jobs (CSV).

2.3.4.5 USER/GROUP FILTER

When creating the directory report, there is a specific option to exclude domain administrators and other selected users and groups from the report. If you want to exclude these selected groups of people from the report on a recurring basis, you can do this using the **user/group filter** from the ribbon.

Click the New button to create a new filter, which will then be available to you when creating the directory report. In the **Search** area, add the group or user to the filter.

3. SHAREPOINT

3.1 REQUIREMENTS

To be able to evaluate the permissions of your SharePoint environment, the inventory of the SharePoint is required first. The permissions are automatically part of the inventory. In our Knowledge Base you will find a HowTo regarding the SharePoint inventory.

3.2 ANALYSIS

Similar to the permission analysis in file systems, it is also possible to perform evaluations for SharePoint environments. The user report and the directory report are also available. The current view of the matrix in the main window can also be generated.

The authorization analysis for SharePoint systems deals with the particularities of the underlying authorization concept. Only the individual authorizations are used here. Aggregation in authorization levels is not evaluated.

4. EXCHANGE

4.1 REQUIREMENT

To be able to evaluate Exchange permissions, you must first perform an inventory. The permissions must be part of the inventory. These can be enabled in the Exchange Scan Wizard - Step 3 - Advanced Options.

4.2 ANALYSIS

As with authorization analysis in file systems, it is also possible to perform evaluations for Exchange environments. The user report and the overview report (analogous to the directory report) are available. The current view of the matrix in the main window can also be generated.

The authorization analysis for Exchange systems deals with the special features of the underlying authorization concept. Both mailboxes and public folders can be viewed.

LIST OF FIGURES

VERSION HISTORY

Date	Description
08/22/2019	Document created
06/01/2020	Revision of the HowTo for Docusnap 11
06/01/2022	Screenshot update
09/27/2022	Revision of Chapter 2.2 – NTFS Analysis
11/13/2023	Version 4.0 – Revision of the HowTo for Docusnap 13