



WHITE PAPER

The Top 5 Threats in File Server Management

Introduction

To help comply with external regulations and ensure data security, organizations must audit their Windows® file servers. Performing Windows file auditing helps detect leaks and unauthorized modifications of sensitive data. File servers belong to the most complex assets in your IT Infrastructure. Moreover, they contain the most sensitive data, information, and knowledge. Unfortunately, the question of who has access to a folder is not easily answered by administrators. Managing the access rights situation of thousands of folders, with unique permissions and inherited rights, is an overly complex task if you rely only on standard Microsoft applications.

This paper will describe the top five threats in file server management and how SolarWinds® Access Rights Manager (ARM) can help you mitigate these threats. ARM is a powerful, affordable, and easy-to-use software solution designed to help IT and security administrators quickly analyze user authorizations and access permission to systems, data, and files—helping them protect their organizations from the risks of data loss and breaches.

#1: NO VISIBILITY INTO ACCESS RIGHTS

Improper access to file servers can put your critical data at risk, and determining who has access to file servers using the standard Windows O/S tools can be time-consuming and error-prone.

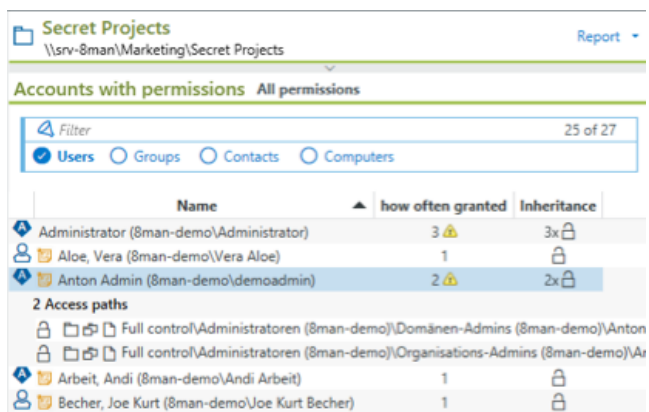
Access Rights Manager is designed to solve this crucial issue. It scans your file servers and instantly displays which users have access to the folder. By just clicking once on the desired folder, you are confronted with reality. In the example below, the “Secret Projects” folder is accessible by all the users displayed on the right side.

Active Directory			Name			how often granted	Inheritance
File server							
srv-Bman	\\srv-Bman		Administrator (Bman-demo\Administrator)			3	3x
Finanz	D:\Finanz	1 KB	Aloe, Vera (Bman-demo\Vera Aloe)			1	
GF	D:\GF	6 Bytes	Anton Admin (Bman-demo\demoadmin)			2	2x
Home	D:\Home	0 Byte	Arbeit, Andi (Bman-demo\Andi Arbeit)			1	
IT	D:\IT	1 KB	Becher, Joe Kurt (Bman-demo\Joe Kurt Becher)			1	
Marketing	D:\Marketing	162.79 MB	Burg, Johannes (Bman-demo\Johannes Burg)			1	
Events		0 Byte	Clean - Admin (Bman-demo\Clean - Admin)			1	
Flyer		1 KB	cradmin (Bman-demo\cradmin)			1	
Presse		4 Bytes	Dampf, Hans (Bman-demo\Hans Dampf)			1	
Produktbeschreibung BMAN		4 Bytes	Dave DataOwner (Bman-demo\Dave.DataOwner)			1	
Project Y		752 Bytes	Fred Chen (Bman-demo\Fred.Chen)			1	
Project X		162.79 MB	Frido Fleia (Bman-demo\Frido.Fleia)			2	2x
Secret Projects		0 Byte	Geber, Ann (Bman-demo\Ann.Geber)			2	2x
Vorlagen		4 Bytes	Hacke, Petra (Bman-demo\Petra.Hacke)			2	2x
Personal	D:\Personal	162.79 MB	Ka, Ede (Bman-demo\Ede Ka)			1	
Vertrieb	D:\Vertrieb	688 Bytes	Krise, Christiane (Bman-demo\Christiane.Krise)			1	
			Maria Makbetov (Bman-demo\Maria Makbetov)			1	

#2: MULTIPLE ACCESS PATHS TO DIRECTORIES

If you adopt state-of-the-art access rights management policies, you will never assign users directly to an ACL. Following Microsoft best practices, professionals use Active Directory permission groups for each set of folders to change their access rights quickly. The problem with this is administrators often have to deal with “grown”—or, better said—chaotic group structures in Active Directory. Users are often part of many groups, which can provoke multiple access paths to directories. Often, removing a user from one group does not restrict their access rights to a path because they are still given access by other unknown groups.

ARM displays multiple access paths for each folder. In the following example, Anton has two access paths to the “Secret Projects” folder.

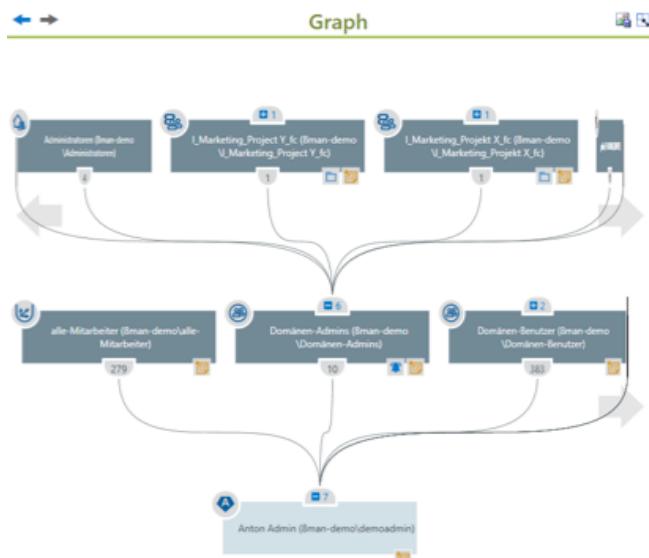


Name	how often granted	Inheritance
Administrator (8man-demo\Administrator)	3	3x
Aloe, Vera (8man-demo\Vera Aloe)	1	
Anton Admin (8man-demo\demoadmin)	2	2x

2 Access paths

- Full control\Administratoren (8man-demo)\Domänen-Admins (8man-demo)\Anton
- Full control\Administratoren (8man-demo)\Organisations-Admins (8man-demo)\Ar

The multiple access paths are due to memberships in two groups. By using the unique AD Graph, the administrator can identify the user's group structure and easily cut off one of the memberships.



#3: LOW ACCESS RIGHTS MAINTENANCE

Given that users change positions throughout the course of their career, usually their number of access rights grow within the company. This should not be the case. The “Principle of Least Privilege” teaches the importance of only granting access to the needed resources. Usually, the administrator has little or no information on where a user should have access. This must be clarified by management.

SolarWinds uses the concept of “data owners” to make sure a specific set of folders on the file server is maintained by only one person in charge. Usually, data owners are managers of a department. They determine which users have access to which resources. ARM has a review feature that empowers managers to review the access rights of their assigned folders.

In the following example, David Data Owner Manager is in charge of checking the access rights to the marketing folder. By using the checkbox on the left, he can decide who should no longer have access to his files. After reviewing every user, he can submit the requirements easily to the administrator. In most cases, Access Rights Manager will implement the changes automatically.

The screenshot displays the 'Recertification (2385)' window in SolarWinds ARM. The 'Configuration' section shows the path 'Isv-Brian\Organization\Marketing'. The main table lists access rights for the 'Marketing' folder, with columns for Folder, Type, Account, Direct access entry, Member Of, Expiration Date, Last Recertification, Action, and Comment. A sidebar on the right contains 'Reports' (Direct Audit report), 'Available Actions' (Remove, Deny), and a 'Progress' section with a pie chart showing 2385 Open, 0 Selected Action, and 0 Sent items. At the bottom, there is a 'Deactivate Windows' button and a message to 'Go to Settings to activate Windows'.

Folder	Type	Account	Direct access entry	Member Of	Expiration Date	Last Recertification	Action	Comment
Marketing	✓	Anton Adrian (Brian-demo\Anton Adrian)	Full	Domain Users (Brian-demo)				
Marketing	✓	Ja Brian (Brian-demo\Ja Brian)	Full	Domain Users (Brian-demo)				
Marketing	✓	Adrian Adminmanager (Brian-demo\Adrian Adminmanager)	Full	Domain Users (Brian-demo)				
Marketing	✓	David DO Marketing (Brian-demo\David DO Marketing)	Full	Marketing (Brian-demo), Domain Users (Brian-demo)				
Marketing	✓	Emily Employee (Brian-demo\Emily Employee)	Full	Marketing (Brian-demo), Domain Users (Brian-demo)				
Marketing	✓	Caroline Berggren (Brian-demo\Caroline Berggren)	Full	Marketing (Brian-demo), Domain Users (Brian-demo)				
Marketing	✓	Elyne Krog (Brian-demo\Elyne Krog)	Full	Marketing (Brian-demo), Domain Users (Brian-demo)				
Marketing	✓	Ludvig Karlsson (Brian-demo\Ludvig Karlsson)	Full	Marketing (Brian-demo), Domain Users (Brian-demo)				
Marketing	✓	David DO Finance (Brian-demo\David DO Finance)	Full	Domain Users (Brian-demo)				
Marketing	✓	David DO HR (Brian-demo\David DO HR)	Full	Domain Users (Brian-demo)				
Marketing	✓	David DO Manager (Brian-demo\David DO Manager)	Full	Domain Users (Brian-demo)				
Marketing	✓	David DO Sales (Brian-demo\David DO Sales)	Full	Domain Users (Brian-demo)				
Marketing	✓	Helena Helpdesk (Brian-demo\Helena Helpdesk)	Full	Domain Users (Brian-demo)				
Marketing	✓	Henry HR (Brian-demo\Henry HR)	Full	Domain Users (Brian-demo)				
Marketing	✓	Maggie Manager (Brian-demo\Maggie Manager)	Full	Domain Users (Brian-demo)				
Marketing	✓	Sebastian SAP (Brian-demo\Sebastian SAP)	Full	Domain Users (Brian-demo)				
Marketing	✓	DefaultAccount (Brian-demo\DefaultAccount)	Full	Domain Users (Brian-demo)				
Marketing	✓	krtdg (Brian-demo\krtdg)	Full	Domain Users (Brian-demo)				
Marketing	✓	User11 (Brian-demo\User11)	Full	Domain Users (Brian-demo)				
Marketing	✓	User10 (Brian-demo\User10)	Full	Domain Users (Brian-demo)				
Marketing	✓	User0 (Brian-demo\User0)	Full	Domain Users (Brian-demo)				
Marketing	✓	User1 (Brian-demo\User1)	Full	Domain Users (Brian-demo)				

#4: NONTRANSPARENT ACTIVITIES IN SENSITIVE DIRECTORIES

Through limiting access rights to sensitive directories, the primary step for additional security is achieved. As a second step, specialists recommend continuous monitoring of access rights by individual users, including their exact actions. This ensures full process transparency for sensitive data, information, and knowledge. ARM provides this data with its built-in logging capabilities, so you can track which users are performing actions within the files.

Title	Sensitive Directories Actions			
Comment	-			
Used time zone	W. Europe Standard Time (UTC+01:00:00)			

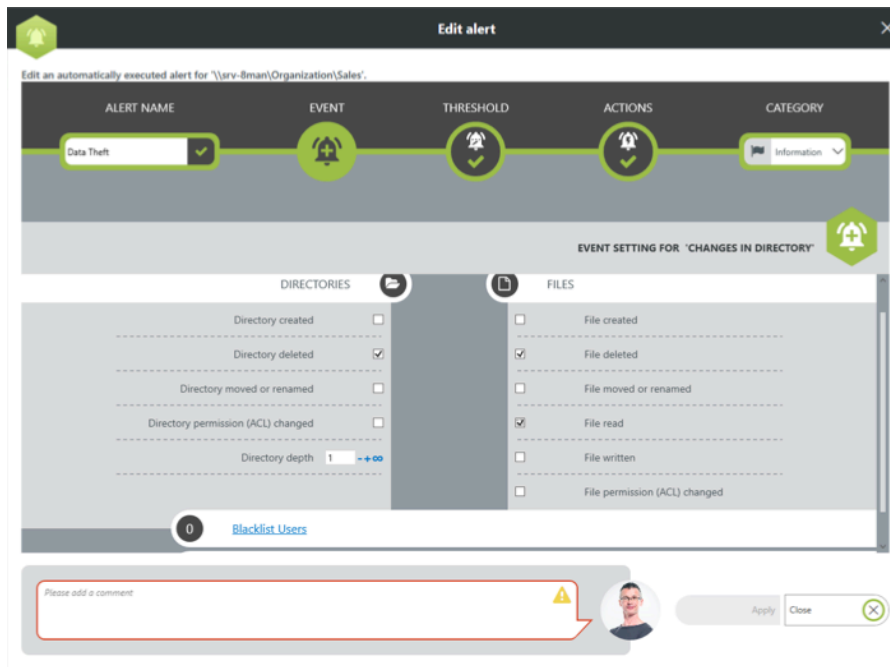
Scantime	8man-demo.local srv-8man	Active Directory File server	11/6/2018 10:00:02 PM 9/25/2018 8:11:50 AM	11/6/2018 10:00:02 PM 9/26/2018 12:04:05 PM
-----------------	-----------------------------	---------------------------------	---	--

Configuration	Reference period	9/24/2018 3:19:39 PM - 9/26/2018 3:19:39 PM		
	Selected resources:	+ D:\Organization (SRV-8MAN)		
	Monitored actions	All		

D:\Organization (SRV-8MAN)			
Time	Action Type	Author	New Path
D:\Organization			
9/26/2018 8:28:33 AM	Permissions changed	Administrator (8man-demo\Administrator)	
D:\Organization\Development			
9/26/2018 8:28:33 AM	Permissions changed	Administrator (8man-demo\Administrator)	
D:\Organization\Development\Documentation			
9/26/2018 8:28:33 AM	Permissions changed	Administrator (8man-demo\Administrator)	
D:\Organization\Development\Documentation\Internal deep dive			
9/26/2018 8:28:33 AM	Permissions changed	Administrator (8man-demo\Administrator)	
D:\Organization\Development\Documentation\Public			
9/26/2018 8:28:33 AM	Permissions changed	Administrator (8man-demo\Administrator)	
D:\Organization\Development\Roadmaps			
9/26/2018 8:28:33 AM	Permissions changed	Administrator (8man-demo\Administrator)	

#5: DATA THEFT & DELETION

Most data theft is committed by users with access rights. To efficiently capture security incidents, ARM focuses on user-initiated file server events. If these occur in unusually high numbers in a short period of time, ARM proactively informs all people responsible. In the case of data theft, the typical pattern consists of a user account that reads an unusually large number of files in a short period of time. Depending on the configuration, an alert is released immediately to inform the owner of the files. There is also the option to execute a script automatically after the incident. You can either monitor a whole server or specific folders. Many incidents in the past have shown how vulnerable companies are in matters of sabotage. Frustrated employees with access to vulnerable assets can do a lot of harm by deleting important files. To efficiently capture these security incidents, ARM allows you to release an alert if one user deletes many files quickly.



SEE HOW SOLARWINDS ACCESS RIGHTS MANAGER WORKS IN YOUR ENVIRONMENT

It's easy to see what ARM can do for you? Simply start a free [30-day trial](#), or [give us a call](#) and one of our specialists will arrange a personalized demo.

For a free trial, visit solarwinds.com/access-rights-manager/registration

To contact sales, visit solarwinds.com/company/contact-us

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.