The Top 5 Threats in File Server Management

solarwinds

solarwinds

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.

#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.

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.
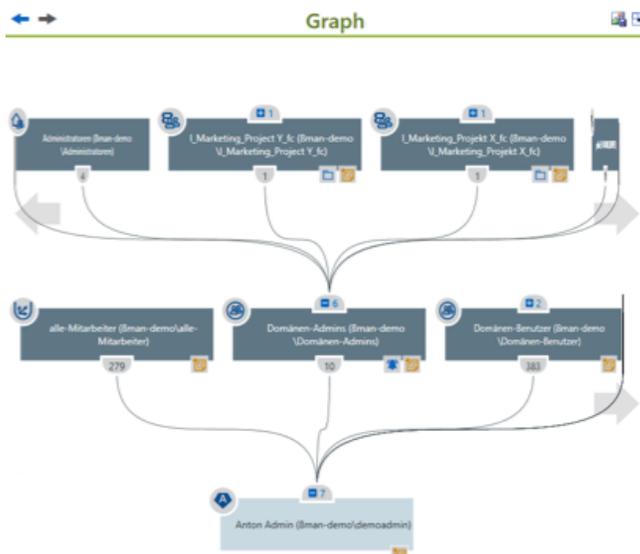
#3: LOW ACCESS RIGHTS MAINTENANCE

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.

#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	Active Directory	11/6/2018 10:00:02 PM	11/6/2018 10:00:02 PM
	srv-8man	File server	9/25/2018 8:11:50 AM	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.
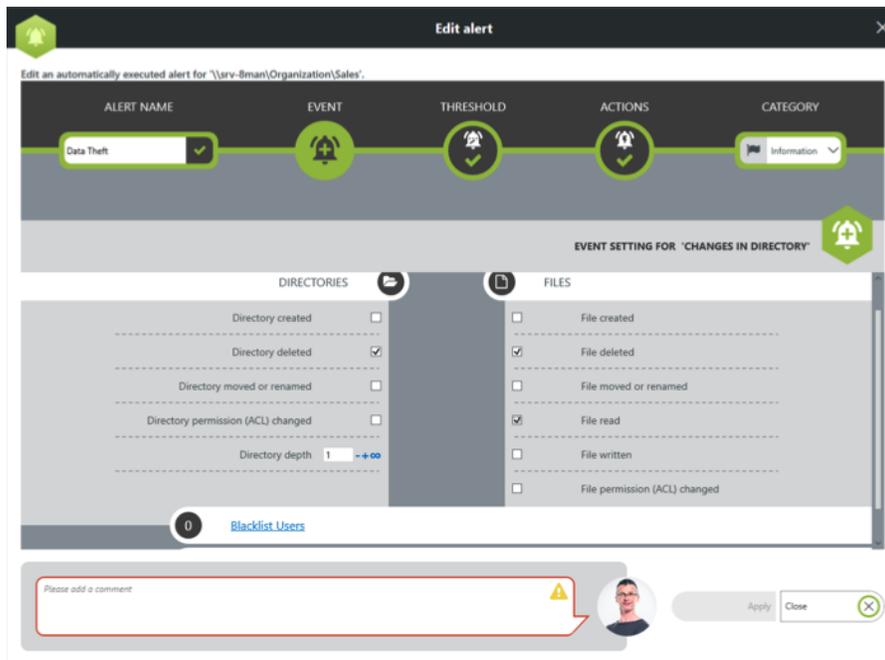
SEE HOW SOLARWINDS ACCESS RIGHTS MANAGER WORKS IN YOUR ENVIRONMENT

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