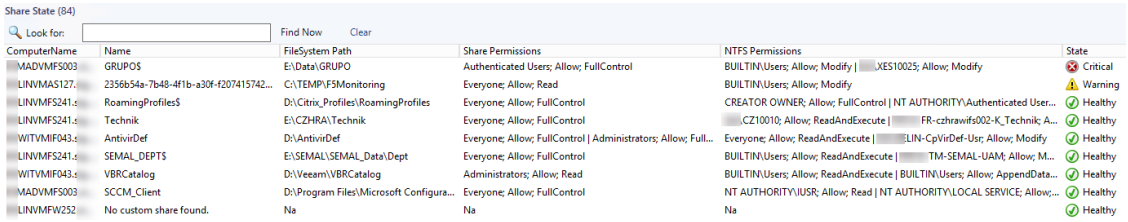
AdminInfo Management Pack for OpsMgr

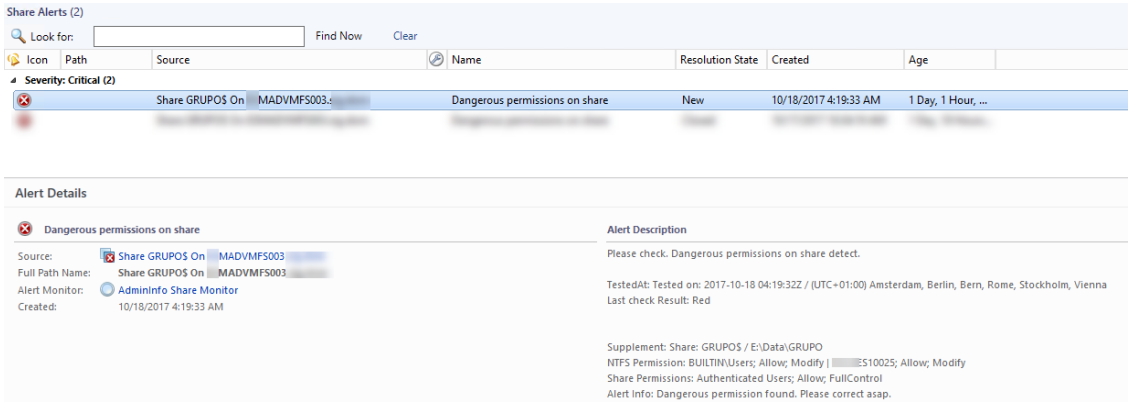
Find shares and alert in case of weak permissions is the primary intention of this free Management Pack. – Other purposes will come.

Introduction

Giving application developers or supporting 3rd parties administrative access to servers is sometimes needed. With a few clicks, a file share is created, providing convenient way to transfer files from and to the server. Unfortunately, keeping the default permissions can lead in some unwanted results. Ransomware that scans the network for vulnerabilities and encrypts everything that is accessible, may even cause serious service outages.



State View showing share objects and their state



Alert View showing critical alerts on weak share permission condition

Management Pack components

Classes

Everything in SCOM that has a Health State is an object. Instead of targeting all Windows servers directly and changing their health state (green/yellow/red) directly according to the share information that is found with that MP, I decided to create a dedicated computer class named **ABC.Windows.Server.AdminInfo.Server**. The idea behind this is that the computer is still running great if only a share is misconfigured.

For the shares a dedicated class is required as well. Only if you have a dedicated class, objects can have a health state that you can monitor.

ID	Extension	Hosted	Singleton	Base	Abstract	Accessibility	Comment
ABC.Windows.Server.AdminInfo.Server	False	True	False	Windows!Microsoft.Windows.ComputerRole	False	Internal	
ABC.Windows.Server.AdminInfo.Share	False	False	False	System!System.LogicalEntity	False	Public	

Discoveries

The mechanism of finding objects that match the definition and storing it in the SCOM database is called discovery. There are different types of discoveries, starting from matching registry values over results of an WMI query to scripts that can cover everything. Targets define on which component the discovery shall run.

ID	Display Name	Type
Discovery.AdminInfo.Server	Discovery AdminInfo Server	Discovery (Custom)
Discovery.AdminInfo.Share	Discovery AdminInfo Share	Discovery (Custom)

First discovery **ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.Server** is used to find '…AdminInfo.Server' objects. Targeted are all Windows servers (which are already monitored by SCOM). The FilteredRegistryDiscoveryProvide' scans the registry and if the key HKLM\SOFTWARE\Microsoft exists, the object will be created. The interval is daily.

Second discovery '**ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.Share**' finds shares gathers some parameters. Targeted are the previously discovered '…AdminInfo.Server' – computer objects. The 'TimedPowerShell.DiscoveryProvider' triggers the 'DiscoverAdminInfoItems.ps1' – PowerShell script which does the logic. Interval is hourly.

Monitors

Monitors are for finding out which Health State an object has. As default monitors did not meet the requirement I created a dedicated one. **ABC.AdminInfo.ThreeState.Test.MonitorType** targets all objects of the class **ABC.Windows.Server.AdminInfo.Share**.
This monitor here uses PowerShell to determine the state of the share objects. Interval is quarterly.

ID	Display Name	Type
Discovery.AdminInfo.Server	Discovery AdminInfo Server	Discovery (Custom)
Discovery.AdminInfo.Share	Discovery AdminInfo Share	Discovery (Custom)

Views

To make all discovered shares and their health state visible a state view **Share State** is used. Most imported properties are shown in there. Shares that meet the error criteria will raise a critical alert. Those alerts are shown in the alert view **Share Alerts**.
Both views can be found in a folder named **ABC.Windows.Server.AdminInfo.Folders**.

ID	Display Name	Type
Discovery.AdminInfo.Server	Discovery AdminInfo Server	Discovery (Custom)
Discovery.AdminInfo.Share	Discovery AdminInfo Share	Discovery (Custom)