AdminInfo Management Pack for OpsMgr

This MP intents to give Windows Administrators useful information about their Server environment.

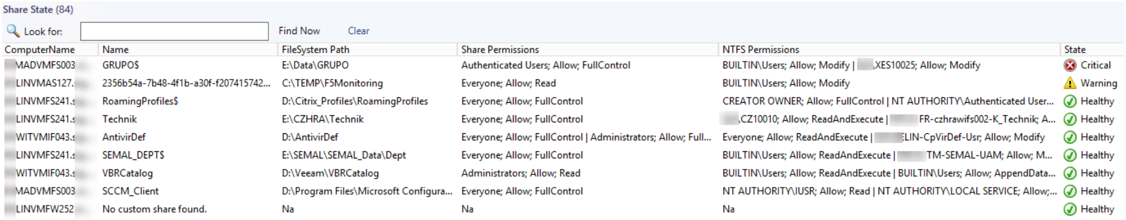
Current it contains two main parts

1) Find shares and alert in case of weak permissions
2) Display 'good to know' information which can help to facilitate trouble shooting.

Introduction

Alert on weak share permissions

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.

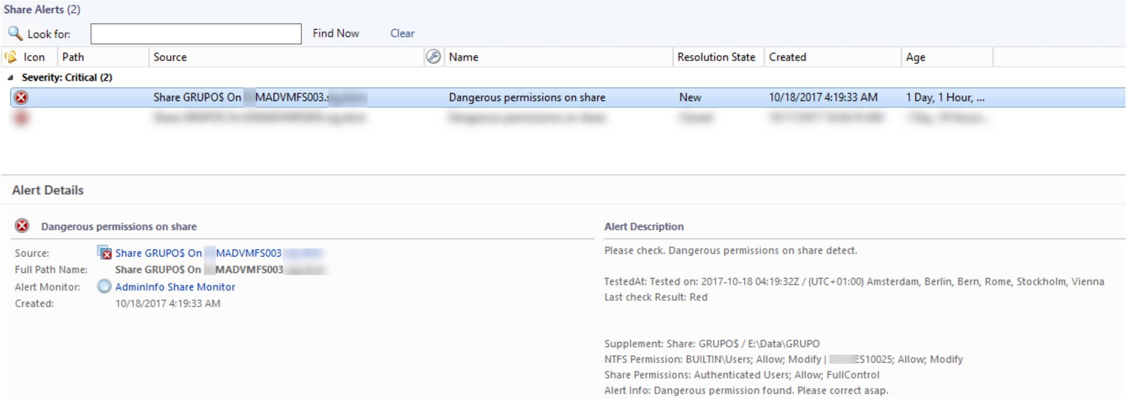


Share State (84)

Look for: Find Now Clear

ComputerName	Name	FileSystem Path	Share Permissions	NTFS Permissions	State
[redacted]MADVMFS003[redacted]	GRUPO$	E:\Data\GRUPO	Authenticated Users; Allow; FullControl	BUILTIN\Users; Allow; Modify | [redacted]XES10025; Allow; Modify	✖ Critical
[redacted]LINVMAS127.[redacted]	2356b54a-7b48-4f1b-a30f-f207415742...	C:\TEMP\F5Monitoring	Everyone; Allow; Read	BUILTIN\Users; Allow; Modify	⚠ Warning
[redacted]LINVMFS241.[redacted]	RoamingProfiles$	D:\Citrix_Profiles\RoamingProfiles	Everyone; Allow; FullControl	CREATOR OWNER; Allow; FullControl | NT AUTHORITY\Authenticated User...	✓ Healthy
[redacted]LINVMFS241.[redacted]	Technik	E:\CZHRA\Technik	Everyone; Allow; FullControl	[redacted]CZ10010; Allow; ReadAndExecute | [redacted]FR-czhrawifs002-K_Technik; A...	✓ Healthy
[redacted]WITVMIF043.[redacted]	AntivirDef	D:\AntivirDef	Everyone; Allow; FullControl | Administrators; Allow; Full...	Everyone; Allow; ReadAndExecute | [redacted]LIN-CpVirDef-Usr; Allow; Modify	✓ Healthy
[redacted]LINVMFS241.[redacted]	SEMAL_DEPT$	E:\SEMAL\SEMAL_Data\Dept	Everyone; Allow; FullControl	BUILTIN\Users; Allow; ReadAndExecute | [redacted]TM-SEMAL-UAM; Allow; M...	✓ Healthy
[redacted]WITVMIF043.[redacted]	VBRCatalog	D:\Veeam\VBRCatalog	Administrators; Allow; Read	BUILTIN\Users; Allow; ReadAndExecute | BUILTIN\Users; Allow; AppendData...	✓ Healthy
[redacted]MADVMFS003[redacted]	SCCM_Client	D:\Program Files\Microsoft Configura...	Everyone; Allow; FullControl	NT AUTHORITY\IUSR; Allow; Read | NT AUTHORITY\LOCAL SERVICE; Allow;...	✓ Healthy
[redacted]LINVMFW252[redacted]	No custom share found.	Na	Na	Na	✓ Healthy

State View showing share objects and their state



Share Alerts (2)

Look for: Find Now Clear

Icon	Path	Source	Name	Resolution State	Created	Age
◢ Severity: Critical (2)						
✖		Share GRUPO$ On [redacted]MADVMFS003.[redacted]	Dangerous permissions on share	New	10/18/2017 4:19:33 AM	1 Day, 1 Hour, ...
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Alert Details

✖ Dangerous permissions on share

Source: Share GRUPO$ On [redacted]MADVMFS003[redacted]
Full Path Name: Share GRUPO$ On [redacted]MADVMFS003[redacted]
Alert Monitor: AdminInfo Share Monitor
Created: 10/18/2017 4:19:33 AM

Alert Description

Please check. Dangerous permissions on share detect.

TestedAt: Tested on: 2017-10-18 04:19:32Z / (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Last check Result: Red

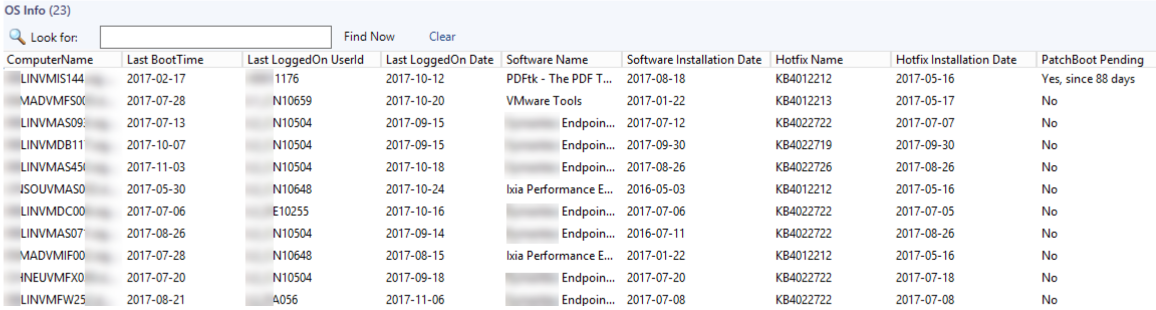
Supplement: Share: GRUPO$ / E:\Data\GRUPO
NTFS Permission: BUILTIN\Users; Allow; Modify | [redacted]ES10025; Allow; Modify
Share Permissions: Authenticated Users; Allow; FullControl
Alert Info: Dangerous permission found. Please correct asap.

Alert View showing critical alerts on weak share permission condition

Good to know about your Windows Servers

Most issues in production environment happen because something was changed.
A few lines of code can reveal useful information which may help pointing to the cause of the issue.

The view OS Info shows: Last Boot Time, Last logged on User's SamAccountName, Last logged on date, Last software that was installed, Date of the last installed software, Last installed Hotfix, Date of the last installed Hotfix and if a Reboot is pending (assuming that each Hotfix requires a Reboot to apply).



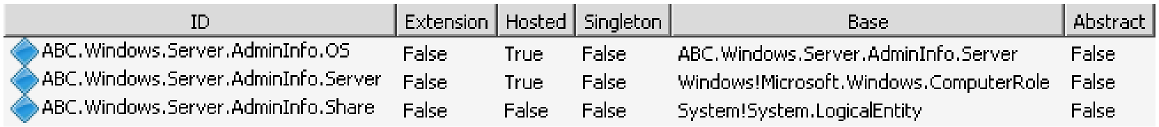
ComputerName	Last BootTime	Last LoggedOn UserId	Last LoggedOn Date	Software Name	Software Installation Date	Hotfix Name	Hotfix Installation Date	PatchBoot Pending
[redacted]LINVMIS144[redacted]	2017-02-17	[redacted]1176	2017-10-12	PDFtk - The PDF T...	2017-08-18	KB4012212	2017-05-16	Yes, since 88 days
[redacted]MADVMFS0[redacted]	2017-07-28	[redacted]N10659	2017-10-20	VMware Tools	2017-01-22	KB4012213	2017-05-17	No
[redacted]LINVMAS09[redacted]	2017-07-13	[redacted]N10504	2017-09-15	[redacted] Endpoin...	2017-07-12	KB4022722	2017-07-07	No
[redacted]LINVMDB11[redacted]	2017-10-07	[redacted]N10504	2017-09-15	[redacted] Endpoin...	2017-09-30	KB4022719	2017-09-30	No
[redacted]LINVMAS45[redacted]	2017-11-03	[redacted]N10504	2017-10-18	[redacted] Endpoin...	2017-08-26	KB4022726	2017-08-26	No
[redacted]ISOUVMAS0[redacted]	2017-05-30	[redacted]N10648	2017-10-24	Ixia Performance E...	2016-05-03	KB4012212	2017-05-16	No
[redacted]LINVMDC00[redacted]	2017-07-06	[redacted]E10255	2017-10-16	[redacted] Endpoin...	2017-07-06	KB4022722	2017-07-05	No
[redacted]LINVMAS07[redacted]	2017-08-26	[redacted]N10504	2017-09-14	[redacted] Endpoin...	2016-07-11	KB4022722	2017-08-26	No
[redacted]MADVMIF00[redacted]	2017-07-28	[redacted]N10648	2017-08-15	Ixia Performance E...	2017-01-22	KB4012212	2017-05-16	No
[redacted]INEUVMFX0[redacted]	2017-07-20	[redacted]N10504	2017-09-18	[redacted] Endpoin...	2017-07-20	KB4022722	2017-07-18	No
[redacted]LINVMFW25[redacted]	2017-08-21	[redacted]A056	2017-11-06	[redacted] Endpoin...	2017-07-08	KB4022722	2017-07-08	No

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.

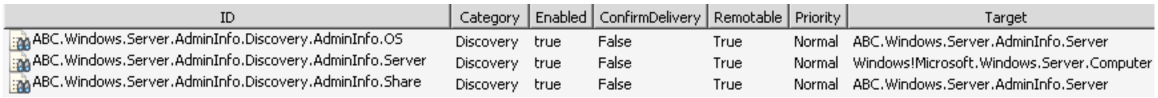
For shares and for 'OS'   a dedicated class is required as well. Only if you have a dedicated class, objects can have a health state that you can monitor.



ID	Extension	Hosted	Singleton	Base	Abstract
ABC.Windows.Server.AdminInfo.OS	False	True	False	ABC.Windows.Server.AdminInfo.Server	False
ABC.Windows.Server.AdminInfo.Server	False	True	False	Windows!Microsoft.Windows.ComputerRole	False
ABC.Windows.Server.AdminInfo.Share	False	False	False	System!System.LogicalEntity	False

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	Category	Enabled	ConfirmDelivery	Remotable	Priority	Target
ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.OS	Discovery	true	False	True	Normal	ABC.Windows.Server.AdminInfo.Server
ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.Server	Discovery	true	False	True	Normal	Windows!Microsoft.Windows.Server.Computer
ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.Share	Discovery	true	False	True	Normal	ABC.Windows.Server.AdminInfo.Server

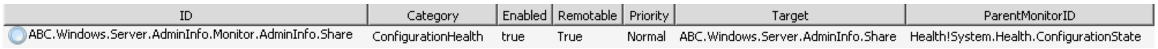
First discovery **ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.Server** is used to find '…AdminInfo.Server' objects. Targeted are all Windows servers (which are already monitored by SCOM). The FilteredRegistryDiscoveryProvide' scans the registry and if the key HKLM\SOFTWARE\Microsoft exists, the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

Third discovery '**ABC.Windows.Server.AdminInfo.Discovery.AdminInfo.OS** 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 every 8 hours.

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.



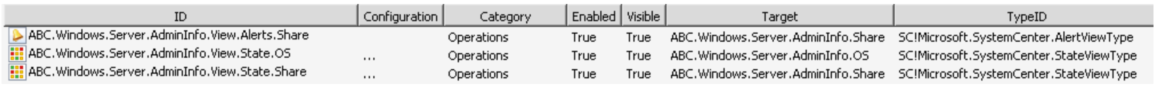
ID	Category	Enabled	Remotable	Priority	Target	ParentMonitorID
ABC.Windows.Server.AdminInfo.Monitor.AdminInfo.Share	ConfigurationHealth	true	True	Normal	ABC.Windows.Server.AdminInfo.Share	Health!System.Health.ConfigurationState

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**.

Another view **OS Info** is based on a State View and provide all collected information to 'OS'.

Both views can be found in a folder named **ABC.Windows.Server.AdminInfo.Folders**.



ID	Configuration	Category	Enabled	Visible	Target	TypeID
ABC.Windows.Server.AdminInfo.View.Alerts.Share		Operations	True	True	ABC.Windows.Server.AdminInfo.Share	SC!Microsoft.SystemCenter.AlertViewType
ABC.Windows.Server.AdminInfo.View.State.OS	...	Operations	True	True	ABC.Windows.Server.AdminInfo.OS	SC!Microsoft.SystemCenter.StateViewType
ABC.Windows.Server.AdminInfo.View.State.Share	...	Operations	True	True	ABC.Windows.Server.AdminInfo.Share	SC!Microsoft.SystemCenter.StateViewType