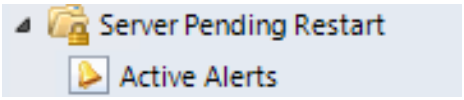
Server Pending Restart Monitoring



1. Table of Contents

1. Table of Contents 2
2. Release history 2
3. Background 3
4. Overview 3
5. Pending restart condition detection 4
6. The Management Pack 5
   6.1. Overview 5
   6.2. Two state unit monitor 5
      6.2.1. Monitor Configuration 6
      6.2.2. Overridable monitor properties: 6
   6.3. Alert Rule 9
      6.3.1. Rule Configuration 9
      6.3.2. Overridable rule properties 9
7. Alerting 11
8. About Apajove 14

2. Release history

Version	Comment
1.0.1.10	Initial Release

Introducing the ‘Server Pending Restart Monitoring’ management pack for System Center Operations Manager.

3. Background

This management pack was inspired from an existing, and very popular, management pack from David Allen – 'SCOM Pending Reboot Management Pack'. This provides alerting when certain conditions on the monitored server are detected and requires the server to be restarted.

We wanted to build on this idea, but at same time, introduce an enhanced level of monitoring.

4. Overview

A number of scenarios are evaluated to determine whether the target computer is pending a restart. Additionally, each of the scenarios can be overridden to tailor to your monitoring needs. For example, if your only requirement is to determine whether the monitored computer is pending a restart as a result of Windows Update automatic updates, then you simply enable this condition detection via override.

By default, all condition detections are disabled. You simply enable the condition detections as required using Operations Manager overrides.

5. Pending restart condition detection

Component Based Servicing (CBS)

Any component-based servicing which has taken place on the target computer, and requires a restart, the following registry location will store a 'PendingReboot' value - 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\'.

Pending Computer Rename and/or Domain Join operations

Computer rename operations are checked by evaluating the following registry locations and values

- 'SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName\'
- 'SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName\'

Domain join operations are checked by evaluating the following registry key and value:

- 'SYSTEM\CurrentControlSet\Services\Netlogon'
    - Value: 'JoinDomain'

Pending File Rename Operations

File rename operations are checked using the following registry key and value:

- 'SYSTEM\CurrentControlSet\Control\Session Manager\',
    - Value: 'PendingFileRenameOperations'.

File rename operations are triggered most commonly by anti-virus products when removing and updating virus definitions and / or .dat files.

System Center Configuration Manager (SCCM)

Any activity performed by the SCCM Client which results in a system pending restart is checked by executing a WMI query against the SCCM client ('ROOT\ccm\ClientSDK') on the target computer.

Windows Update / Auto Update

Post Windows Update / Auto update operations which result in the target computer requiring a restart are checked using the following registry key and value:

- 'SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\',
    - Value: 'RebootRequired'

6. The Management Pack

6.1. Overview

The “Server Pending Restart” management pack contains a monitor and a rule.

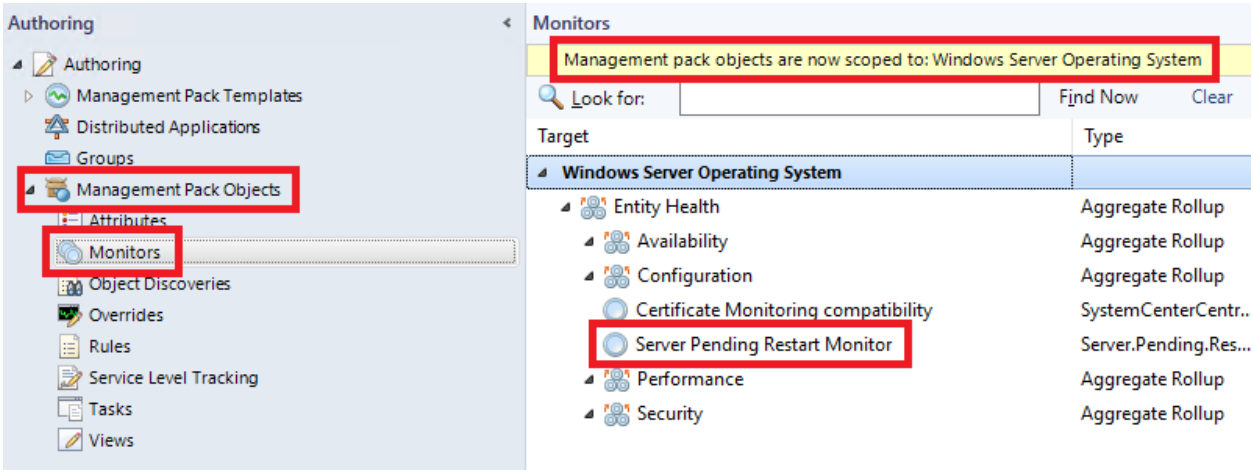
The **monitor** is enabled by default and is configured to change the 'Configuration' health state of the target Windows Server Operating System. When the 'Is Reboot Pending' value equals 'False', the monitor will detect the healthy condition and return to a healthy state.

The **rule**, which is disabled by default has the exact same condition detection behaviour as the "Server Pending Restart Monitor". This rule can be enabled as an alternative to the "Server Pending Restart Monitor" when the presentation of health state changes is not required.

Both the monitor and rule evaluate each of the condition detections described above (which have been enabled via override) in the same way using a PowerShell script. If one or more of the pending restart condition detections returns ‘True’, a warning alert is triggered.

6.2. Two state unit monitor

Authoring workspace view:



6.2.1. Monitor Configuration

- Monitor display name: "Server Pending Restart Monitor"
- Target: Windows Server Operating System
- Parent Monitor: Configuration
- Enabled: True

Monitor Condition	Operational State	Health State
NoRestartPending	No restart pending detected	Healthy
RestartPending	Restart pending detected	Warning

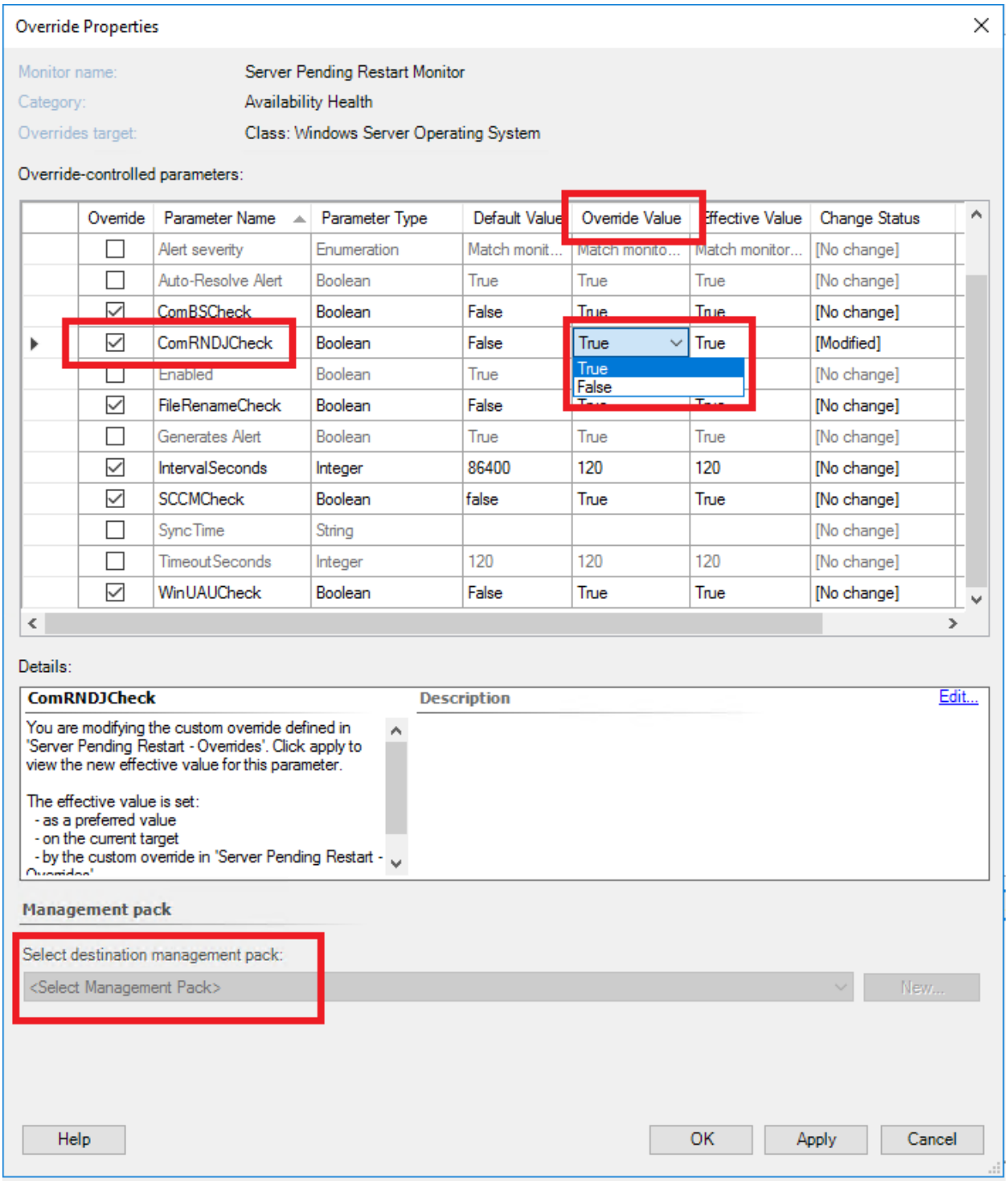
- Monitor Alert configuration
- Alert name: "Monitor Alert – Server pending restart detected"
- Priority: Medium
- Severity: Match monitor's health (Warning)

Monitor Condition	Operational State	Health State
NoRestartPending	No restart pending detected	Healthy
RestartPending	Restart pending detected	Warning

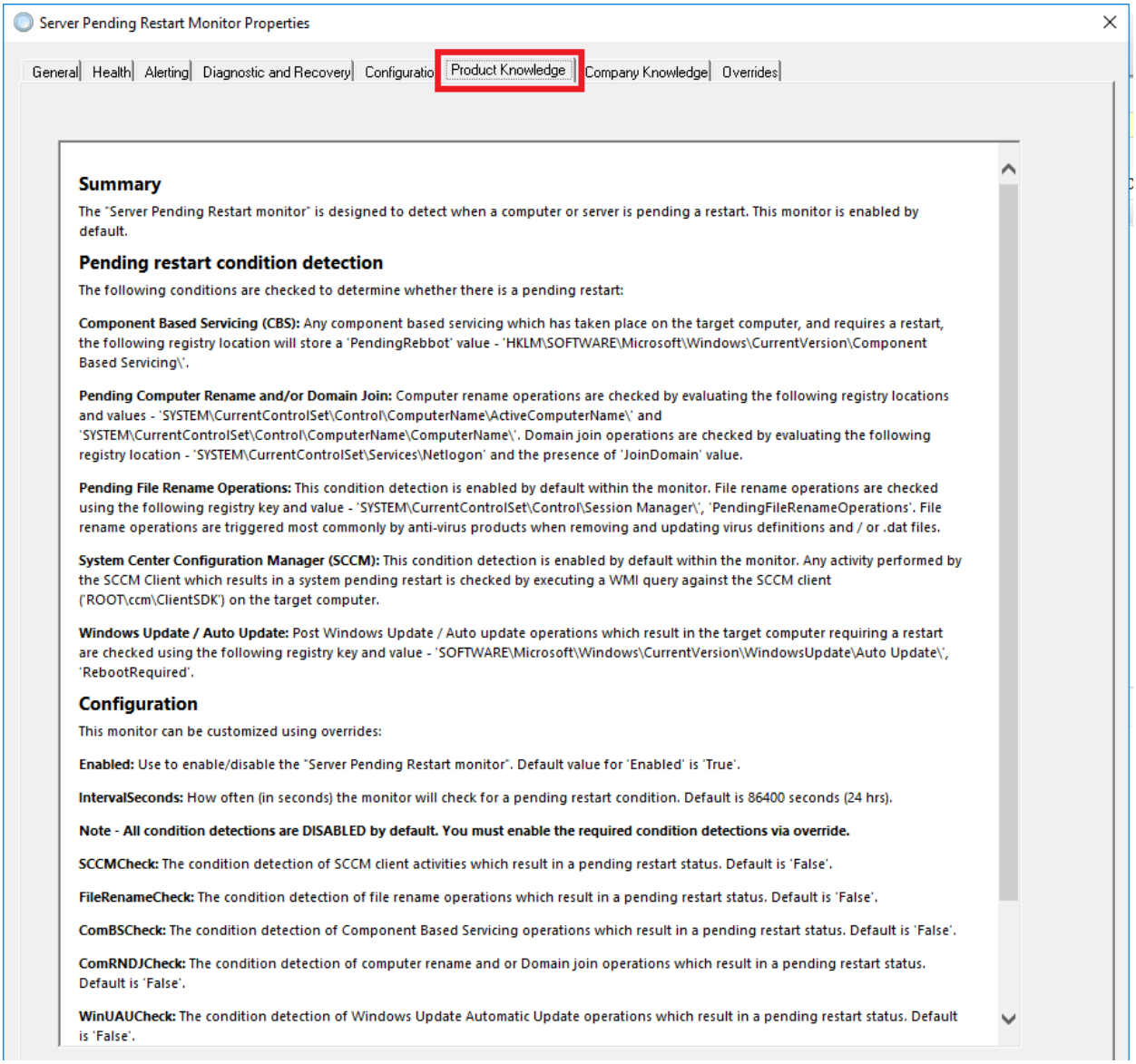
6.2.2. Overridable monitor properties:

Property	Comment	Default Value
Enabled	Use to enable/disable the "Server Pending Restart monitor".	TRUE
IntervalSeconds	How often (in seconds) the monitor will check for a pending restart condition.	86400 (24hrs)
SCCMCheck	The condition detection of SCCM client activities which result in a pending restart status.	FALSE
FileRenameCheck	The condition detection of file rename operations which result in a pending restart status.	FALSE
ComBSCheck	The condition detection of Component Based Servicing operations which result in a pending restart status.	FALSE
ComRNDJCheck	The condition detection of computer rename and or Domain join operations which result in a pending restart status.	FALSE
WinUAUCheck	The condition detection of Windows Update Automatic Update operations which result in a pending restart status.	FALSE
TimeoutSeconds	Timeout in seconds for the PowerShell script inside the monitor.	120

Monitor Override example:

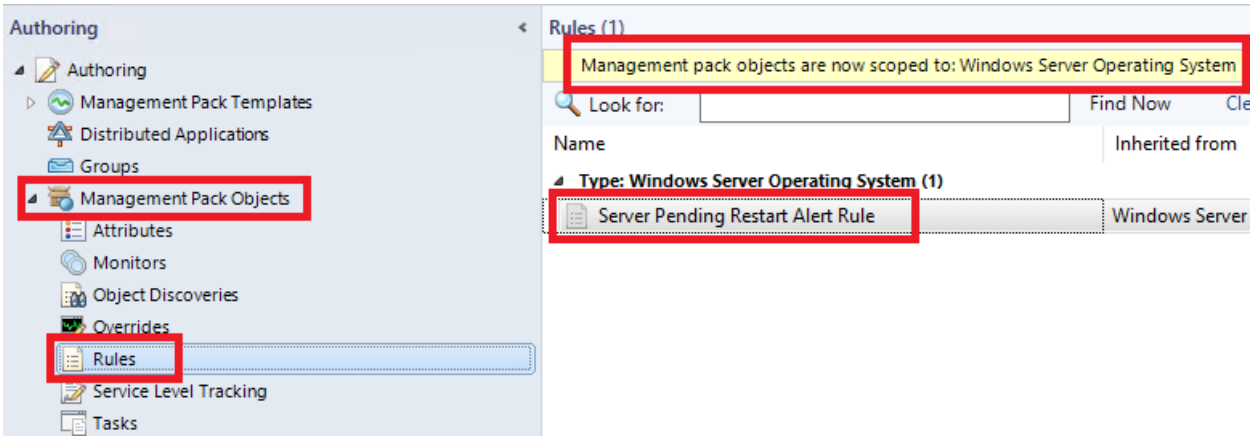


Monitor Product Knowledge:



6.3. Alert Rule

Authoring workspace view:



6.3.1. Rule Configuration

- Rule display name: "Server Pending Restart Alert Rule"
- Target: Windows Server Operating System
- Enabled: FALSE

Rule Alert configuration

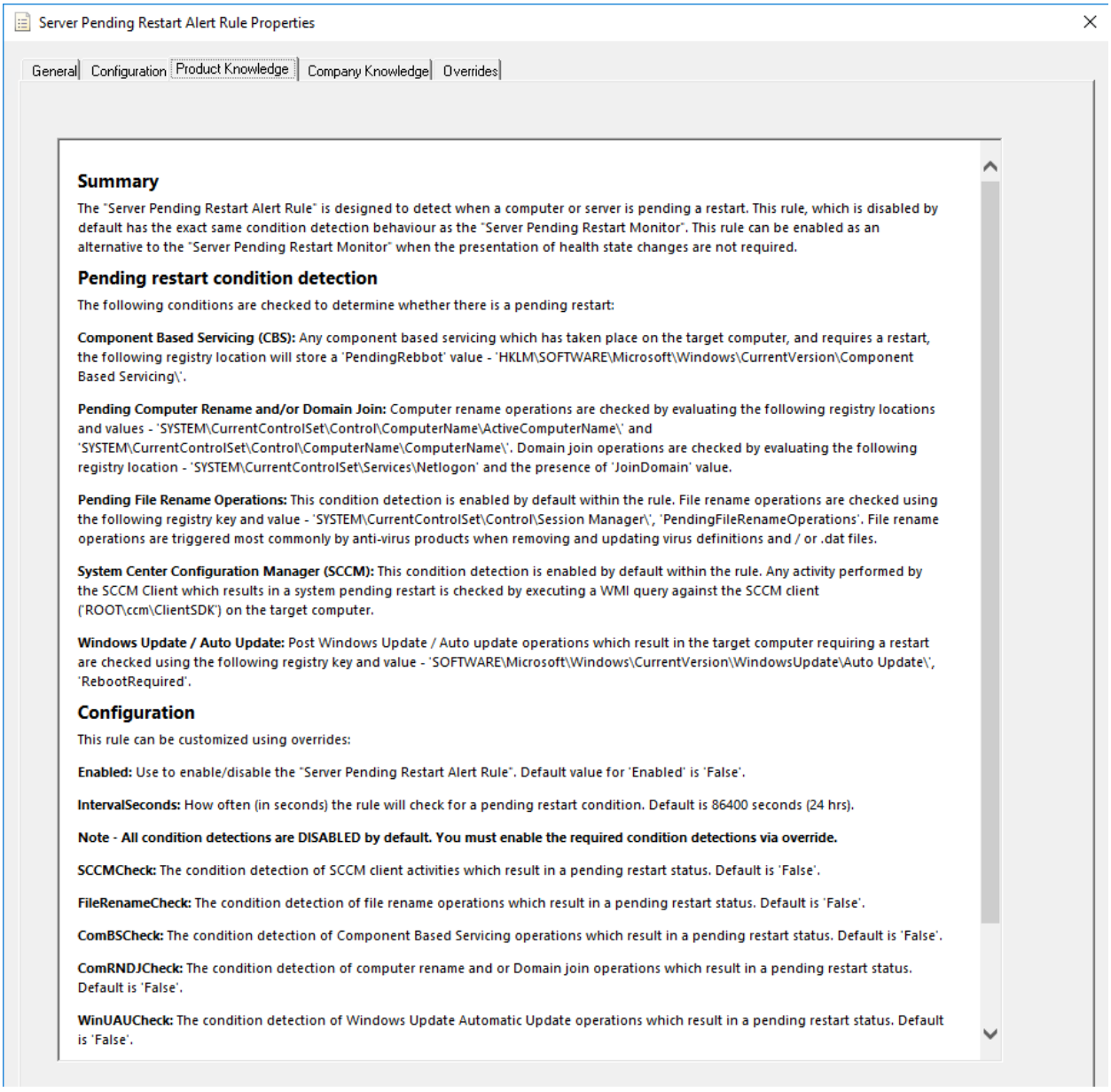
- Alert name: "Rule Alert - Server pending restart detected"
- Priority: Medium
- Severity: Warning

6.3.2. Overridable rule properties

Property	Comment	Default Value
Enabled	Use to enable/disable the "Server Pending Restart Alert Rule".	FALSE
IntervalSeconds	How often (in seconds) the monitor will check for a pending restart condition.	86400 (24hrs)
SCCMCheck	The condition detection of SCCM client activities which result in a pending restart status.	FALSE
FileRenameCheck	The condition detection of file rename operations which result in a pending restart status.	FALSE
ComBSCheck	The condition detection of Component Based Servicing operations which result in a pending restart status.	FALSE
ComRNDJCheck	The condition detection of computer rename and or Domain join operations which result in a pending restart status.	FALSE

WinUAUCheck	The condition detection of Windows Update Automatic Update operations which result in a pending restart status.	FALSE
TimeoutSeconds	Timeout in seconds for the PowerShell script inside the monitor.	120

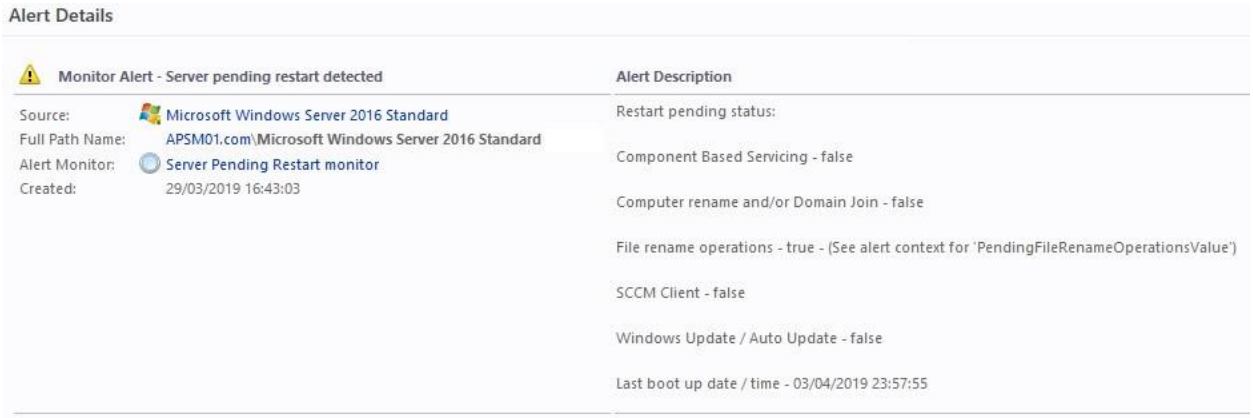
Rule Product Knowledge:



7. Alerting

Both the monitor and rule alerts contain the same level data within the description. Depending on whether certain condition detections are enabled or not, this is also reflected in the alert description:

Example 1:



Example 2:

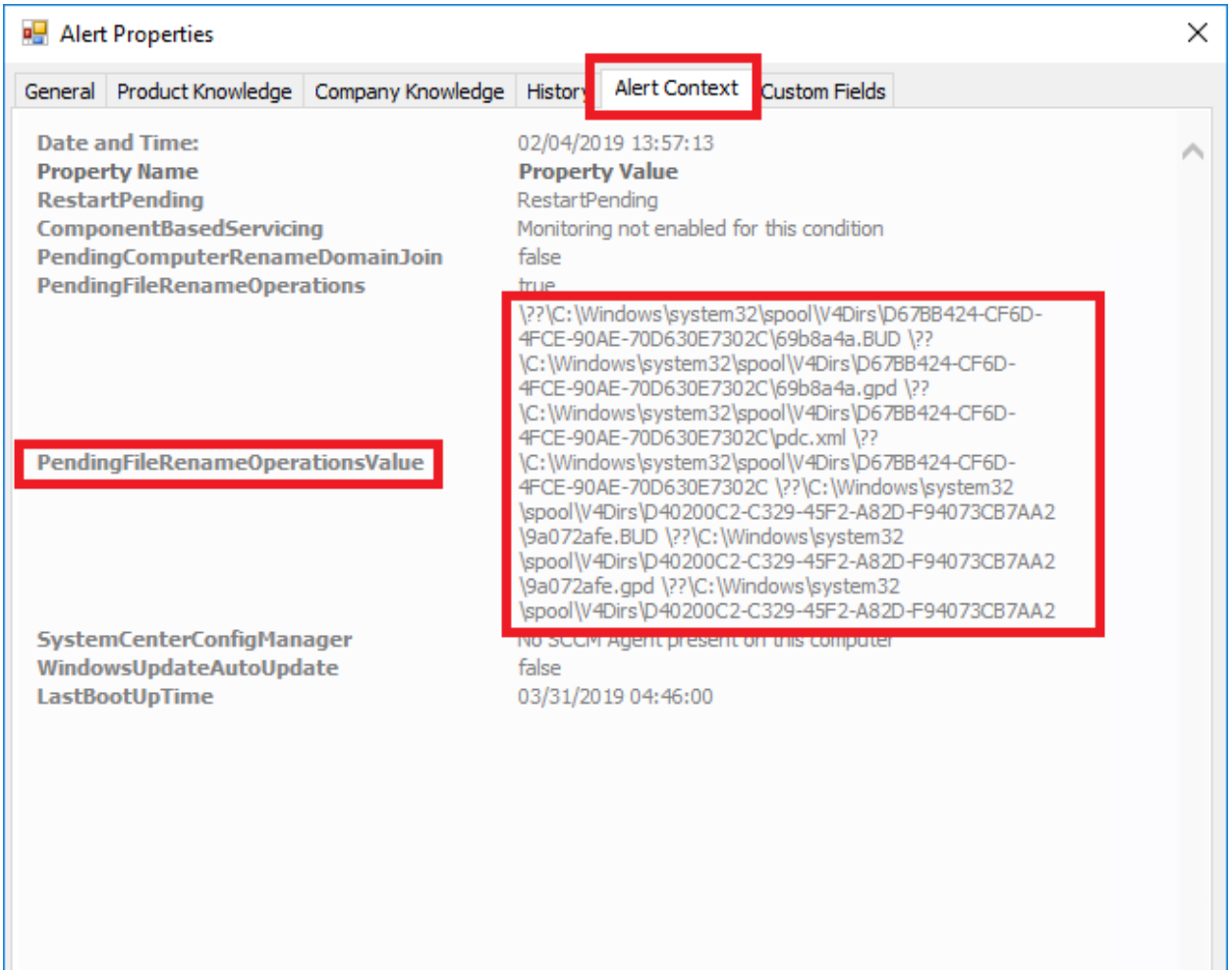
Alert Description
Restart pending status:
Component Based Servicing - false
Computer rename and/or Domain Join - false
File rename operations - true - (See alert context for 'PendingFileRenameOperationsValue')
SCCM Client - false
Windows Update / Auto Update - false
Last boot up date / time - 03/04/2019 23:57:55

Example 3:

Alert Description
Restart pending status:
Component Based Servicing - Monitoring not enabled for this condition
Computer rename and/or Domain Join - false
File rename operations - true - (See alert context for 'PendingFileRenameOperationsValue')
SCCM Client - No SCCM Agent present on this computer
Windows Update / Auto Update - false
Last boot up date / time - 03/31/2019 04:46:00

Example 4:

When condition detection has been enabled for 'File rename operations', the alert context tab contains the items associated with the file rename operations:



8. About Apajove

Apajove is a UK based provider of IT solutions using Microsoft System Center and related technologies. Offering a world-class consulting service, Apajove is led by a team of professionals who bring the highest level of experience and expertise available in the industry. With over 50 years' combined experience with Microsoft technologies, Apajove has established itself as one of the leading pure-Microsoft consultancies in the UK.

Apajove are also the suppliers of Callisto, the breakthrough HTML dashboard for System Center.

For more information, please contact us or see www.apajove.com/callisto

Microsoft Partner
Microsoft
Gold Datacenter
Gold Windows and Devices
Silver Application Development