

Symantec Endpoint Protection Infected Registry Flag Monitoring

Using a Powershell script and custom service



Table of Contents

Monitoring Network Shares.....	Error! Bookmark not defined.
Overview	3
Requirements.....	3
Workflow.....	3
Deployment	4
Importing and configuring the script	4
Script parameters and options	Error! Bookmark not defined.
Importing and configuring the custom service	6
Data being monitored.....	7
Information contained within the custom service	7

SEP Registry Check Status Information

Overview

N-able Technologies has developed a script and a custom service that allows to monitor a specific registry key set by Symantec Endpoint Protection, that reports on the infection status of the machine

To use it, the script must be run at periodic interval (we recommend every 4 hours, but the actual schedule is customizable), and a custom service must be deployed.

Requirements

This script was tested on Windows 8, but should work on all platforms as long as Symantec writes to the same registry location for all OS

Additionally, the script requires Powershell 2.0 and Microsoft .net 4

Workflow

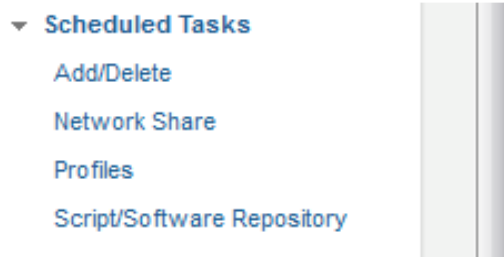
The script when run on a local computer will check a determined registry location, and will return the keyvalue back.

HKLM:\Software\Symantec\Symantec Endpoint Protection\currentversion\public-opstate

Deployment

Importing and configuring the script

1. Download the SEPIinfectedStatusRegistryCheck script from the N-able Resource Center (<http://nrc.n-able.com>) under COMMUNITY > Custom Services Policies section.
2. Import the Powershell script into the N-Central Script Repository
 - a. From the Service Organization Level (orange), go to the configuration menu, then to **Scheduled Tasks**,



- b. Select **Script/Software Repository**
- c. Click ADD and choose scripting, then click on BROWSE to select the script

Details

Type:	Scripting		
Name:	<input type="text" value="Get External IP and GeoLocation"/>		
Description:	<input type="text" value="get external ip addressand GeoLocation of a device"/>		
File Name:	<input type="text" value="GetExternalIPAndLocation.ps 1"/>	<input type="button" value="Browse ..."/>	<input type="button" value="Cancel"/>
Command Line Parameters:	<input type="text" value="GetExternalIPAndLocation.ps 1"/>		

- d. Once uploaded, it will be available for use
3. Create a Scheduled Task profile (as detailed below) to run the script every 1-4 hours (or as needed).
 - a. From the Customer level (green), go to the configuration menu, then to Scheduled Tasks, and click on profiles. Select ADD scripting task
 - i. Enter a name
 - ii. Select the script from the repository list
 - iii. Select the rule on which to apply the profile.
 - iv. Select the schedule and set it to recurring

- v. Select Custom if it needs to be scanned more frequently than hourly, and add all the times that are required, and leave the other fields default (every day, every month).

Schedule

Type:

Task Interval:

Interval:

Start Times:

Days of the Week:

☒ Every day

☐ Selected days

Mon Tue Wed Thu Fri Sat Sun

Days of the Month:

☒ Every day

☐ Selected days

Months of the Year:

☒ Every month

☐ Selected months

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

- vi. If desired, select notifications to be sent if the task fails to run.
- vii. Save the task. The task will now run at the specified times.

Importing and configuring the custom service

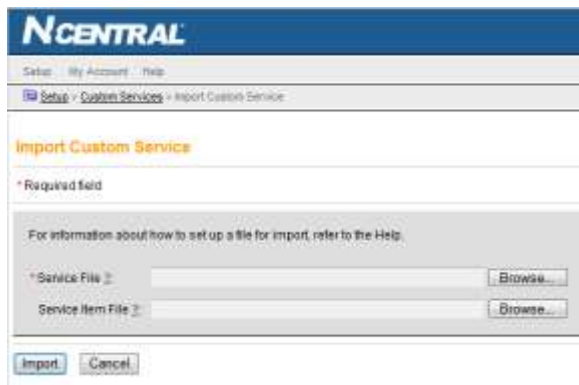
To import the custom service:

1. log on to the NAC by going to <http://YOURSERVER:10000> and logging in with your product administrator
2. go to **Custom Services** within the services section on the left

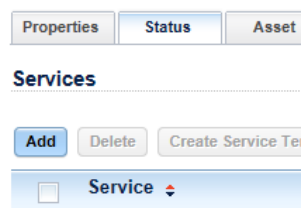


Import Service

3. Click on IMPORT SERVICE
4. Click on BROWSE and select the service file (xml file), then click on IMPORT



5. The service is now imported. Go to the N-Central GUI and select the device where to add the service. Go to the STATUS tab and click on ADD



6. From the list, enter a 1 besides Symantec Endpoing Protection – Infected Flag Check
Symantec Endpoint Protection - Infected Flag Check 0 -
7. Click on OK at the bottom of the list
8. The service will now report on the script data.

Data being monitored

Information contained within the custom service

The monitor will record 3 data points in WMI for N-Central to poll.

1. Does the Key exist (this will report on if the registry key exist. If it doesn't, it will go failed)
2. Is an infection found (if it is true, it goes failed)
3. Last Script Run Time (last time that the powershell script was run)



The screenshot shows the 'Service Status' window for a custom service. At the top, there is a 'Remote Control' button. Below it are tabs for 'Status', 'Service Details', 'Thresholds', 'Self Healing', and 'Reports'. The 'Status' tab is selected, showing the 'Service Status' section. It displays 'Current Status' as 'Normal' with a green checkmark, 'Scan Time' as '2013-Mar-01 18:59', and 'Transition Time' as '2013-Mar-01 18:54'. Below this is the 'Status Details' section, which contains a table with three rows of data points.

Description	Value	State	Thresholds
Does the Registry Key Exist	True	Normal	If Found: Normal, If Not Found: Failed
Is An Infection Detected	False	Normal	If Found: Failed, If Not Found: Normal
Last Script Run Time	03/01/2013 07:54:30	---	---

A 'Cancel' button is located at the bottom left of the window.