Symantec Endpoint Protection Infected Registry Flag Monitoring

Using a Powershell script and custom service

Table of Contents

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

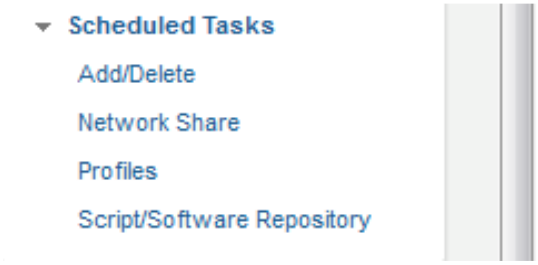
The script when run on a local computer will check a determined registry location, and will return the keyvalue back.

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

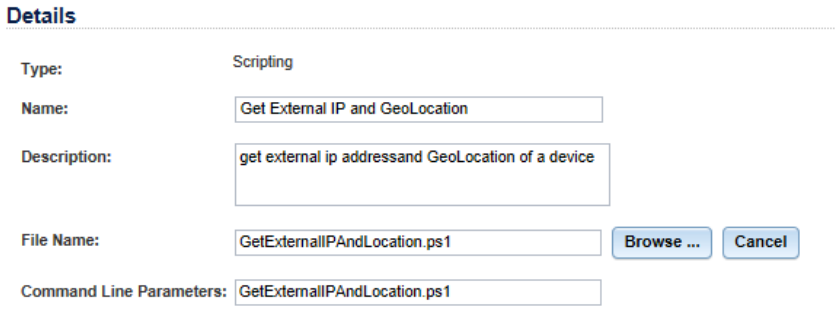
Deployment

Importing and configuring the script

1. Download the SEPInfectedStatusRegistryCheck 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



    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).

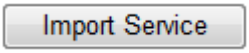
vi. If desired, select notifications to be sent if the task fails to run.

vii. Save the task. The task will now run at the specified times.

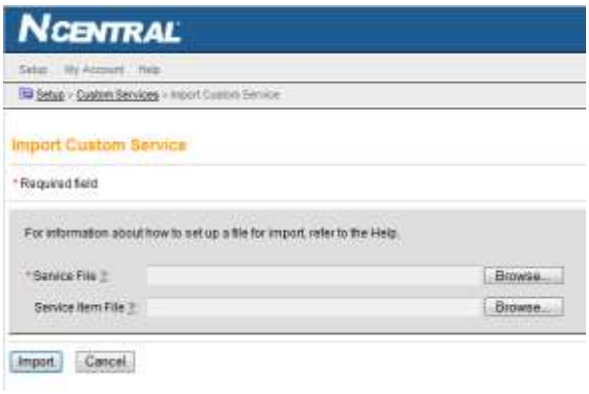
Importing and configuring the custom service

To import the custom service:

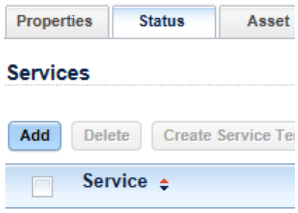
1. log on to the NAC by going to httpS://YOURSERVER:10000 and logging in with your product administrator
2. go to **Custom Services** within the services section on the left

3. Click on IMPORT SERVICE 

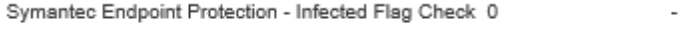
4. Click on BROWSE and select the service file (xml file), then click on IMPORT



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



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)