Monitor F5 BIGIP with OpsMgr

Basic Management Pack which provides general health state and alerting for the following components:

- CPU, Disk and Memory
- SyncStatus, PoolStatus, NodeAddress and TrafficGroups

Introduction

Gathering basic health state information and enabling alerting for key components for F5 Big-IP is the main idea for this this management pack.

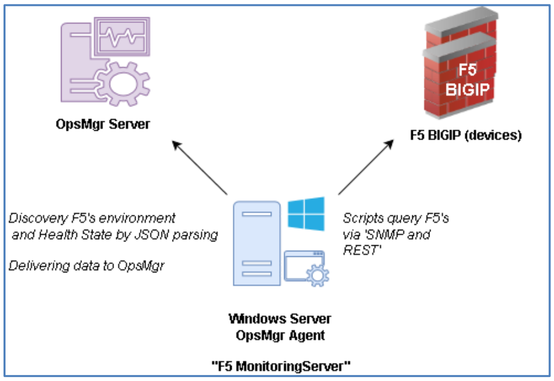
Under the hood PowerShell and a mixture between REST and SNMP is used to pull information out of the F5 appliance. Reason for the mixture is that some information was only exposed in SNMP, some other only via REST. Required steps are documented below.

This MP is published as free software, feel free to use or customize it. – Consider the license terms.

Design

- A Windows Server, taking the role of 'F5 Monitoring Server' queries firewall appliances via SNMP and REST.

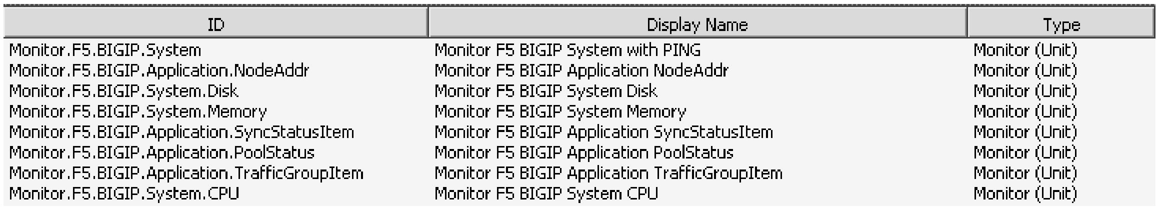
- A Scheduled Task is launching PowerShell scripts which perform the queries and storing the result in JSON files locally. Those files are used for discovering and monitoring F5 components (e.g. CPU, Memory, …)


OpsMgr Server
F5 BIGIP
F5 BIGIP (devices)
Discovery F5's environment and Health State by JSON parsing
Delivering data to OpsMgr
Scripts query F5's via 'SNMP and REST'
Windows Server
OpsMgr Agent
"F5 MonitoringServer"

- On the first run the F5 MPs' monitoring scripts it will share the folder which is specified in the 'FilePath' that you need to specify in the registry. The share name is 'OUrF5InfoForSCOM$', permissions are set to READ for Everyone.

Configuration (Optional)

After importing the Management Pack the following Monitors may be configured:

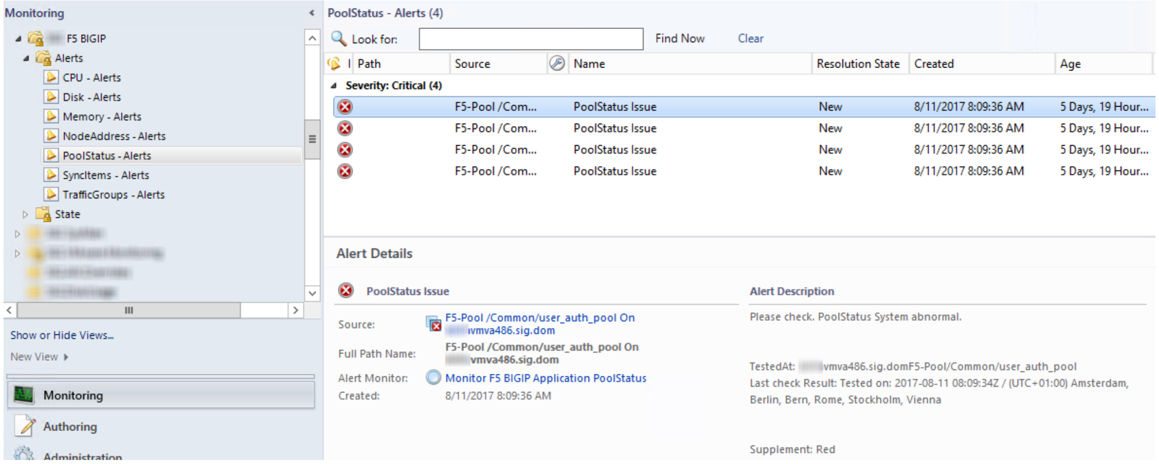


ID	Display Name	Type
Monitor.F5.BIGIP.System	Monitor F5 BIGIP System with PING	Monitor (Unit)
Monitor.F5.BIGIP.Application.NodeAddr	Monitor F5 BIGIP Application NodeAddr	Monitor (Unit)
Monitor.F5.BIGIP.System.Disk	Monitor F5 BIGIP System Disk	Monitor (Unit)
Monitor.F5.BIGIP.System.Memory	Monitor F5 BIGIP System Memory	Monitor (Unit)
Monitor.F5.BIGIP.Application.SyncStatusItem	Monitor F5 BIGIP Application SyncStatusItem	Monitor (Unit)
Monitor.F5.BIGIP.Application.PoolStatus	Monitor F5 BIGIP Application PoolStatus	Monitor (Unit)
Monitor.F5.BIGIP.Application.TrafficGroupItem	Monitor F5 BIGIP Application TrafficGroupItem	Monitor (Unit)
Monitor.F5.BIGIP.System.CPU	Monitor F5 BIGIP System CPU	Monitor (Unit)

DisplayName	Monitoring Logic	Threshold	Frequency
.. System with PING	PING F5 BIGIP by IP address specified in the CSV file. If reachable Healthy, otherwise Critical	Na	300 sec.
.. System Disk	If free space less than 10% then Critical Otherwise Healthy	Default: 10%	300 sec.
.. System Memory	If Memory % in Use less than Threshold, then Healthy Otherwise Critical	Default: 80%	300 sec.
.. System CPU	If Idle % is less than Threshold than Critical Otherwise Healthy	Default: 10%	300 sec.
.. Application SyncStatusItem	If itemState equals 'connected' or 'in sync' then Healthy Otherwise Critical	Default: connected, in sync	900 sec.
.. Application PoolStatus	Check if EnabledState is 'enabled' If poolAvailableStatus is green or blue than Healthy, if yellow then Warning, if red than Critical, other color results in Warning	Na	300 sec.
.. Application TrafficGroupItem	If failoverstatus equals to active or standby than Healthy Otherwise Critical	Na	900 sec.
.. Application NodeAddr	Check if SessionState is 'enabled' If MonitorStatus is 'up' then Healthy, otherwise Critical	Na	300 sec.

Usage

Alert views show details current breaches of configured threshold breaches:



PoolStatus - Alerts (4)

Path	Source	Name	Resolution State	Created	Age
Severity: Critical (4)					
	F5-Pool /Com...	PoolStatus Issue	New	8/11/2017 8:09:36 AM	5 Days, 19 Hour...
	F5-Pool /Com...	PoolStatus Issue	New	8/11/2017 8:09:36 AM	5 Days, 19 Hour...
	F5-Pool /Com...	PoolStatus Issue	New	8/11/2017 8:09:36 AM	5 Days, 19 Hour...
	F5-Pool /Com...	PoolStatus Issue	New	8/11/2017 8:09:36 AM	5 Days, 19 Hour...

Alert Details

PoolStatus Issue

Source: F5-Pool /Common/user_auth_pool On [redacted]vmva486.sig.dom

Full Path Name: F5-Pool /Common/user_auth_pool On [redacted]vmva486.sig.dom

Alert Monitor: Monitor F5 BIGIP Application PoolStatus

Created: 8/11/2017 8:09:36 AM

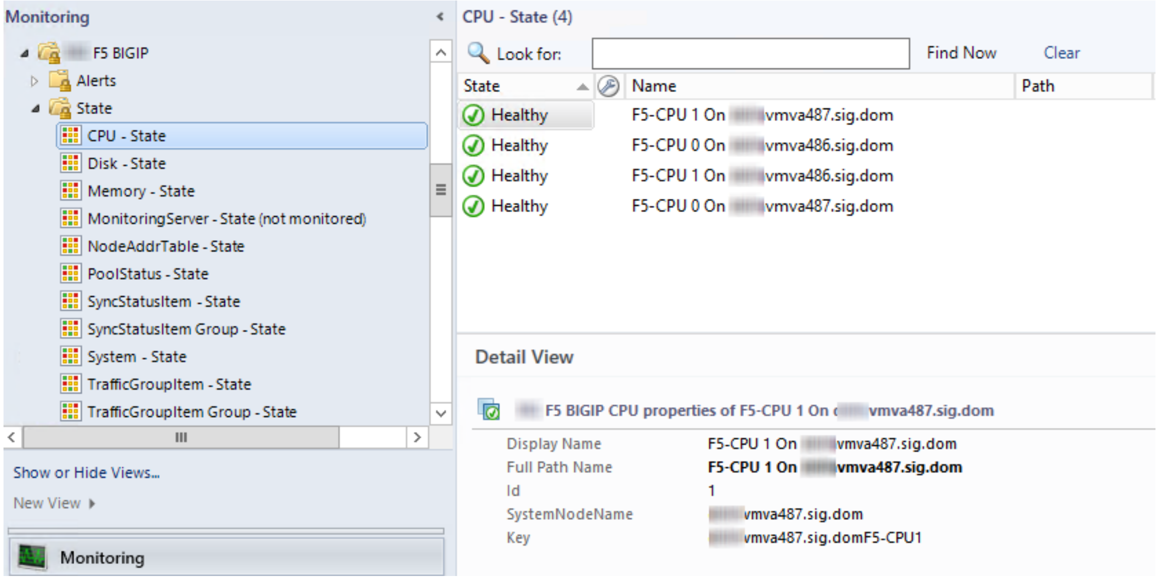
Alert Description

Please check. PoolStatus System abnormal.

TestedAt: [redacted]vmva486.sig.domF5-Pool/Common/user_auth_pool
Last check Result: Tested on: 2017-08-11 08:09:34Z / (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Supplement: Red

State view show the state of a particular item:



CPU - State (4)

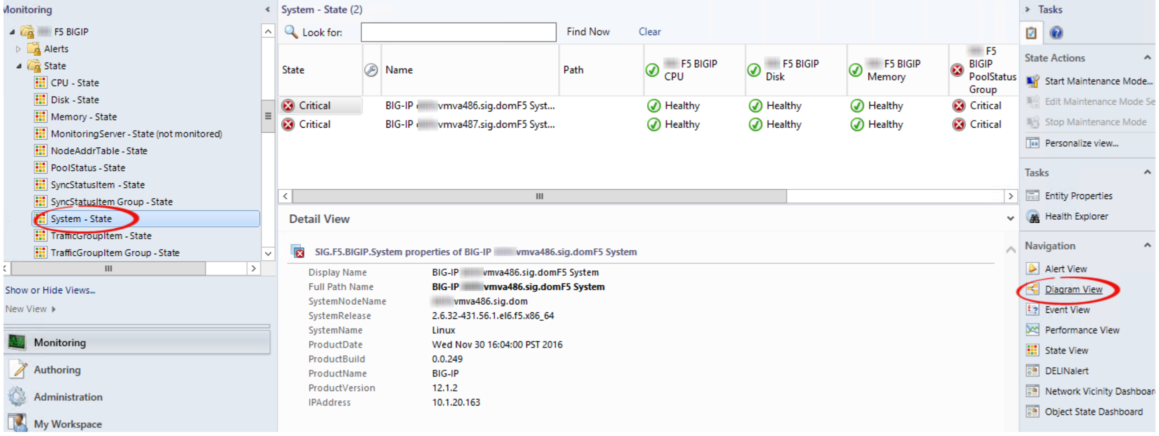
State	Name	Path
Healthy	F5-CPU 1 On [redacted]vmva487.sig.dom	
Healthy	F5-CPU 0 On [redacted]vmva486.sig.dom	
Healthy	F5-CPU 1 On [redacted]vmva486.sig.dom	
Healthy	F5-CPU 0 On [redacted]vmva487.sig.dom	

Detail View

[redacted] F5 BIGIP CPU properties of F5-CPU 1 On [redacted]vmva487.sig.dom

Display Name	F5-CPU 1 On [redacted]vmva487.sig.dom
Full Path Name	**F5-CPU 1 On [redacted]vmva487.sig.dom**
Id	1
SystemNodeName	[redacted]vmva487.sig.dom
Key	[redacted]vmva487.sig.domF5-CPU1

See the whole system by opening the diagram view on “system”:



Monitoring

- [redacted] F5 BIGIP
  - Alerts
  - State
    - CPU - State
    - Disk - State
    - Memory - State
    - MonitoringServer - State (not monitored)
    - NodeAddrTable - State
    - PoolStatus - State
    - SyncStatusItem - State
    - SyncStatusItem Group - State
    - System - State
    - TrafficGroupItem - State
    - TrafficGroupItem Group - State

Show or Hide Views...

New View ▸

Monitoring

Authoring

Administration

My Workspace

System - State (2)

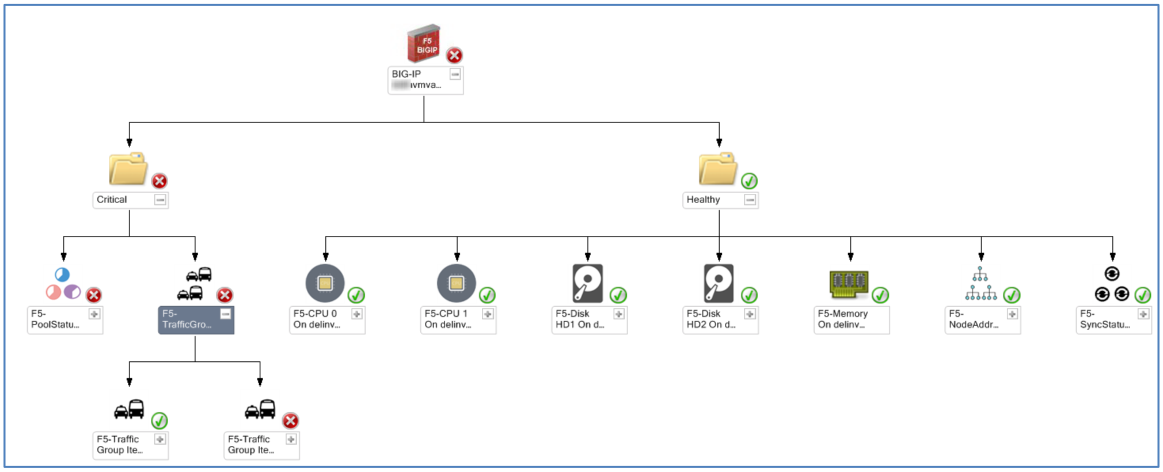
Look for: Find Now Clear

State		Name	Path	[redacted] F5 BIGIP CPU	[redacted] F5 BIGIP Disk	[redacted] F5 BIGIP Memory	[redacted] F5 BIGIP PoolStatus Group
Critical		BIG-IP [redacted]vmva486.sig.domF5 Syst...		Healthy	Healthy	Healthy	Critical
Critical		BIG-IP [redacted]vmva487.sig.domF5 Syst...		Healthy	Healthy	Healthy	Critical

Detail View

SIG.F5.BIGIP.System properties of BIG-IP [redacted]vmva486.sig.domF5 System

Display Name	BIG-IP [redacted]vmva486.sig.domF5 System
Full Path Name	**BIG-IP [redacted]vmva486.sig.domF5 System**
SystemNodeName	[redacted]vmva486.sig.dom
SystemRelease	2.6.32-431.56.1.el6.f5.x86_64
SystemName	Linux
ProductDate	Wed Nov 30 16:04:00 PST 2016
ProductBuild	0.0.249
ProductName	BIG-IP
ProductVersion	12.1.2
IPAddress	10.1.20.163



Preparation (Required)

Settings in SCOM

Create an empty Override Management Pack to store customizations. You might for instance wish to change the frequency that discovery runs.

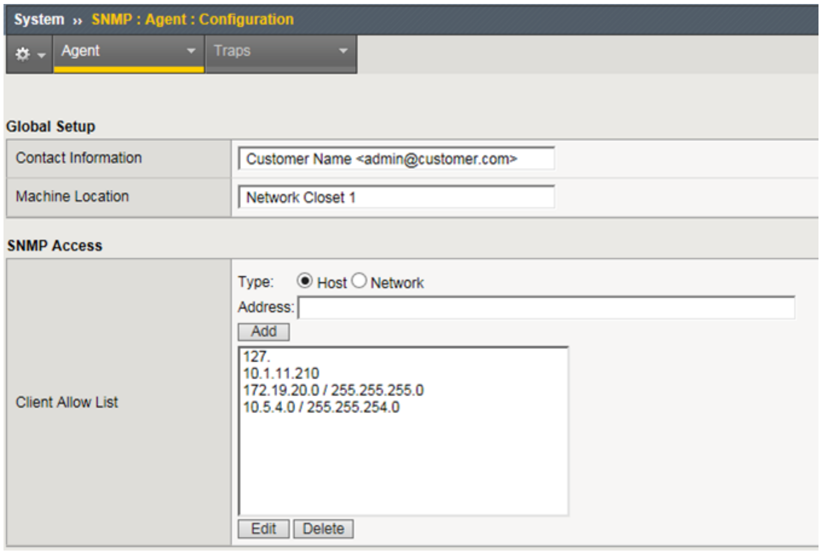
Settings on F5 BIGIP

To work properly setup a hostname for your appliance and maintain this name in DNS.

The name need also to be added to the CSV file mentioned below in the 'Settings on F5 Monitoring Server' section.

A certificate must be deployed to the web console. – Self signed certificates are also ok.

To allow SNMP access, change to the SNMP Agent configuration and maintain the Client Allow List and specify the community settings:



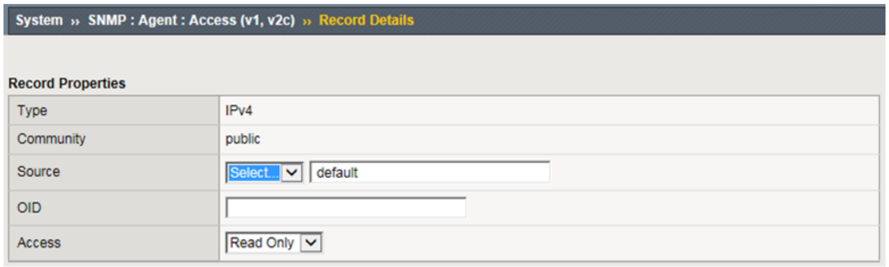
System » SNMP : Agent : Configuration

Global Setup

Contact Information	Customer Name <admin@customer.com>
Machine Location	Network Closet 1

SNMP Access

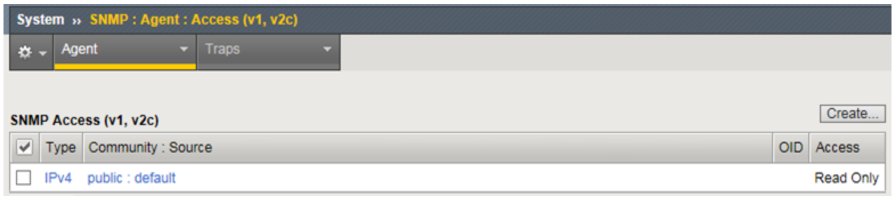
Client Allow List	Type: ● Host ○ Network Address: 127. 10.1.11.210 172.19.20.0 / 255.255.255.0 10.5.4.0 / 255.255.254.0



System » SNMP : Agent : Access (v1, v2c) » Record Details

Record Properties

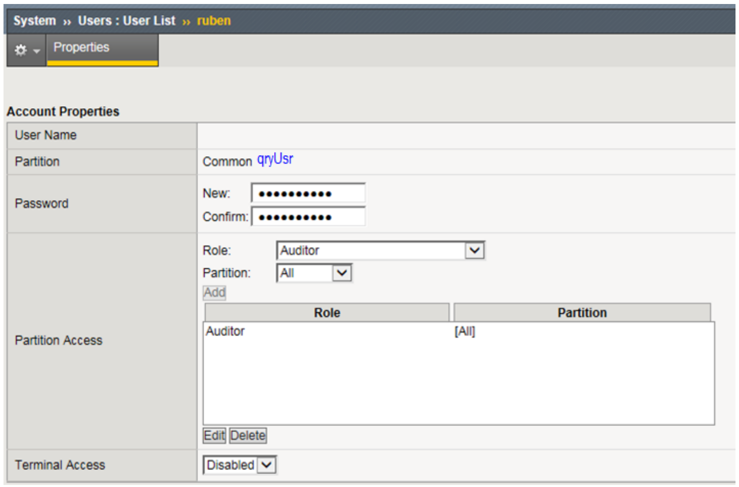
Type	IPv4
Community	public
Source	Select... default
OID	
Access	Read Only



SNMP Access (v1, v2c)

☑	Type	Community : Source	OID	Access
□	IPv4	public : default		Read Only

Querying via REST is made possible by creating an user account and assigning it Auditor permissions to all Partitions.



Account Properties

User Name	
Partition	Common qryUsr
Password	New: ●●●●●●●●●●● Confirm: ●●●●●●●●●●●
Partition Access	Role: Auditor Partition: All Add
Terminal Access	Disabled

Role	Partition
Auditor	[All]

Auditor Role allows read only access to all partitions:

"This role grants users permission to view all configuration data on the system, including logs and archives. Users with this role cannot create, modify, or delete any data, nor can they view SSL keys or user passwords. Users with the Auditor role have access to all partitions on the system, and this partition access cannot be changed."

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-user-account-administration-11-6-0/3.html

Settings on F5 Monitoring Server

- PowerShell version >= 5 on the 'F5 Monitoring Server' and on the SCOM Management Servers is required.

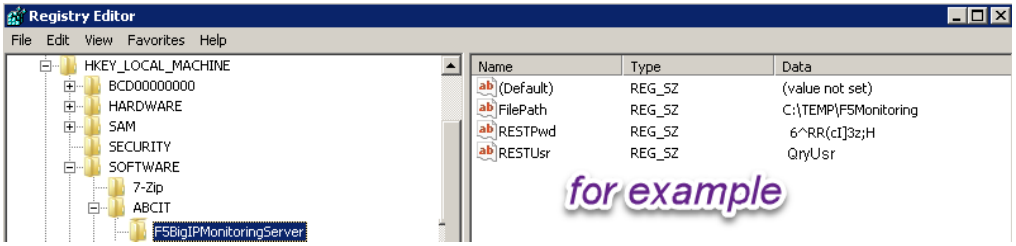
- Install the 64-Bit toolset from net-snmp. Available as free and open source software through http://www.net-snmp.org. Working version: net-snmp-5.5-2.x64.exe – higher should hopefully work as well.

- Download both F5 Mibs from your appliance, unpack them (e.g. 7zip) and store them in the directory net-snmp's shared snmp mibs are stored C:\usr\share\snmp\mibs)
  - https://<YourF5ApplianceName>/docs/mibs/mibs_f5.tar.gz
  - https://<YourF5ApplianceName>/docs/mibs/mibs_netsnmp.tar.gz

- Configure net-snmp in order to load all MIBs (C:\usr\etc\snmp\snmp.conf), add the following line:
  - mibs +ALL

- Set the following registry key on 'F5 Monitoring Server'.
  - The directory 'FilePath' needs to be created and be changed.
    - [HKEY_LOCAL_MACHINE\SOFTWARE\ABCIT\F5BigIPMonitoringServer]
      - "FilePath"="C:\\TEMP\\F5Monitoring"
  - Set the RESTUsr and RESTPwd according to the values configured above for the access.
    - [HKEY_LOCAL_MACHINE\SOFTWARE\ABCIT\F5BigIPMonitoringServer]
      - "RESTUsr"="qryUsr"
      - "RESTPwd"="Passw0rd"

  - Example screenshot:



Name	Type	Data
(Default)	REG_SZ	(value not set)
FilePath	REG_SZ	C:\TEMP\F5Monitoring
RESTPwd	REG_SZ	6^RR(cI]3z;H
RESTUsr	REG_SZ	QryUsr

- Maintain the Names and IP addresses of the F5 appliances in a CSV file name ‘**F5-BigIP-Hosts.csv**’ which must be placed in the path which is configured as ‘**FilePath’,** keep the header-row, e.g.:
    - HostName,IPAddress,Port
    - vmva486,10.1.20.163
    - vmva487,10.1.20.164,8443

    Port information is optional, 443 is chosen then.

- Create scheduled tasks on the ‘F5 Monitoring Server’ to launch both PowerShell scripts. The more often the scripts are executed the earlier information is visible in OpsMgr; e.g. every 15 minutes. – Files created by the scripts are also used for monitoring purposes.
    - F5-Discovery-rest.ps1
    - F5-Discovery-snmp.ps1

- Note: The directory specified in “FilePath” will be shared as a hidden share and made readable for Everyone. NTFS permissions are inherited. Ensure that the OpsMgr Management Server can access the file remotely.