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.

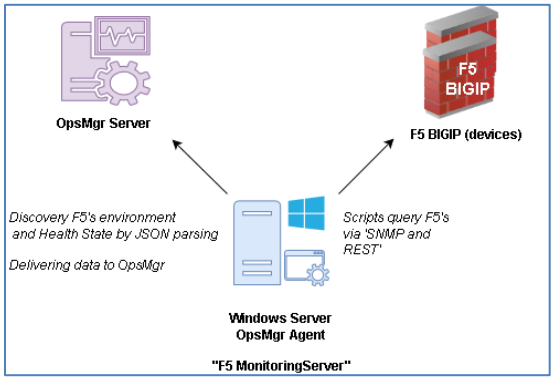
This MP is published as free software, feel free to use or customize it. – Consider the license terms.

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.

- Discoveries and Monitoring scripts in the F5 MP are interpreting the JSON files to provide OpsMgr Topology and Health information.



Configuration (Optional)

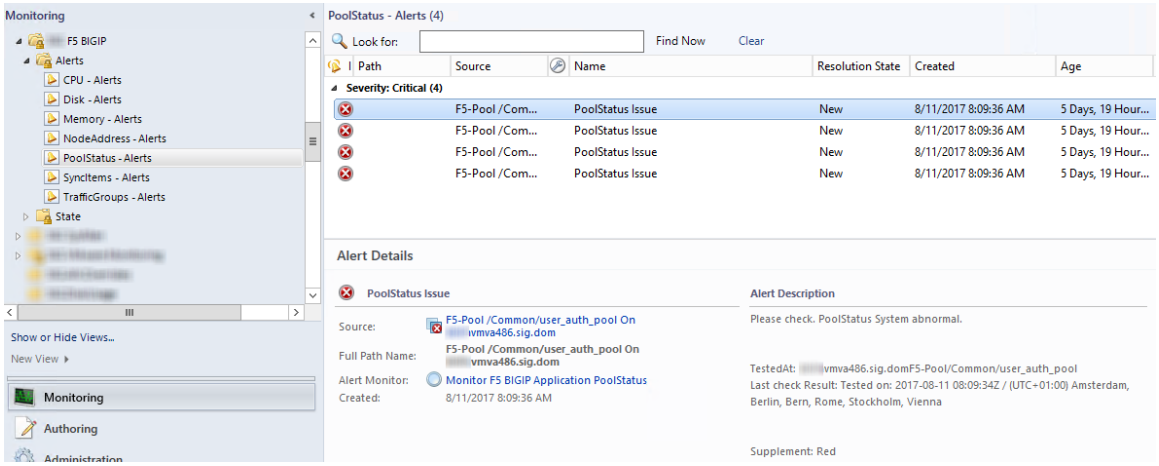
After importing the Management Pack the following Monitors may be configured:

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)

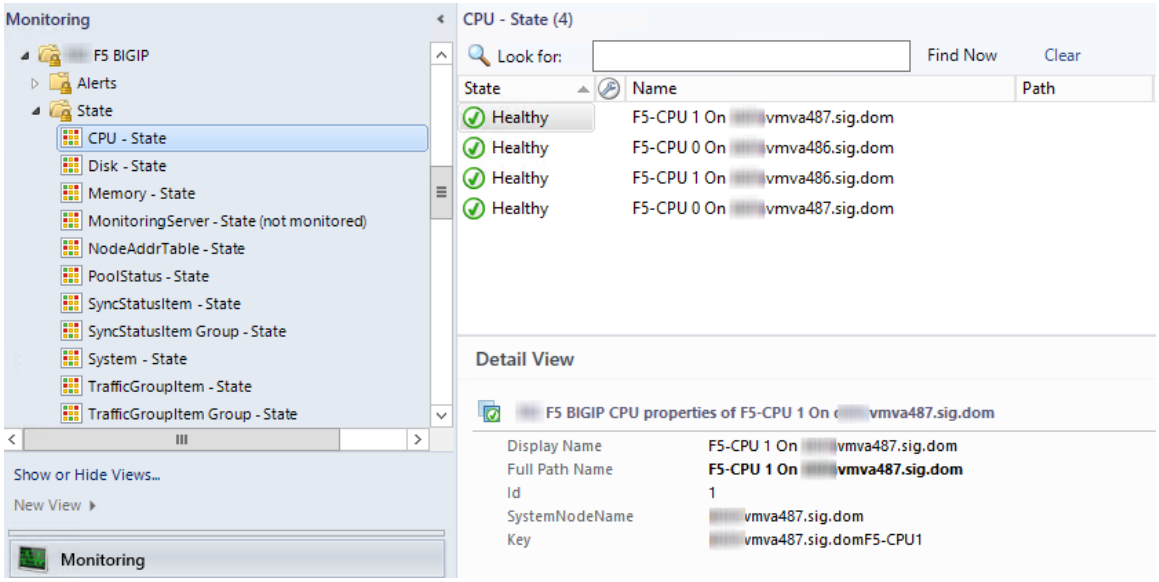
DisplayName	Monitoring Logic	Threshold	Frequency
.. System with PING	PING F5 BIGIP by IP address specified in the CSV file. If reachable Healthy, otherwise Critical	Na	300 sec.
.. System Disk	If free space less than 10% then Critical Otherwise Healthy	Default: 10%	300 sec.
.. System Memory	If Memory % 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

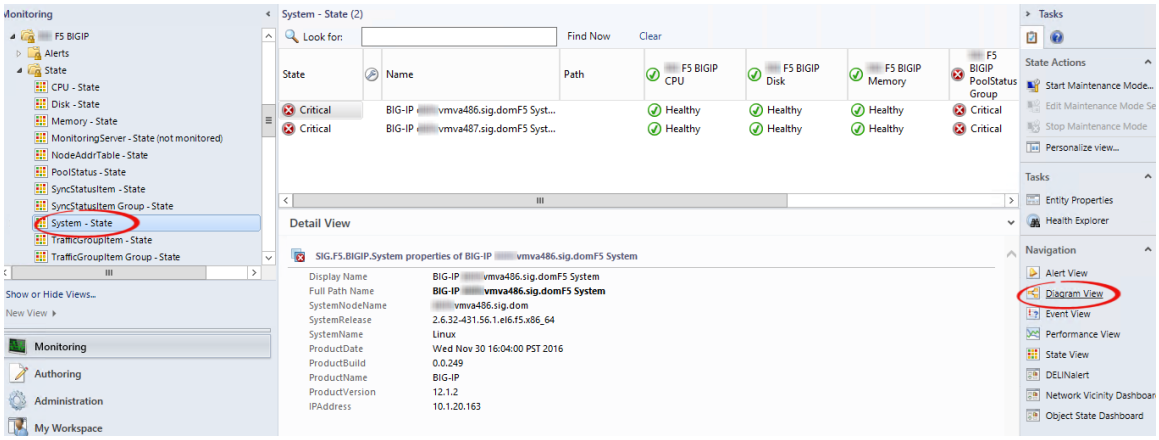
Alert views show details current breaches of configured threshold breaches:

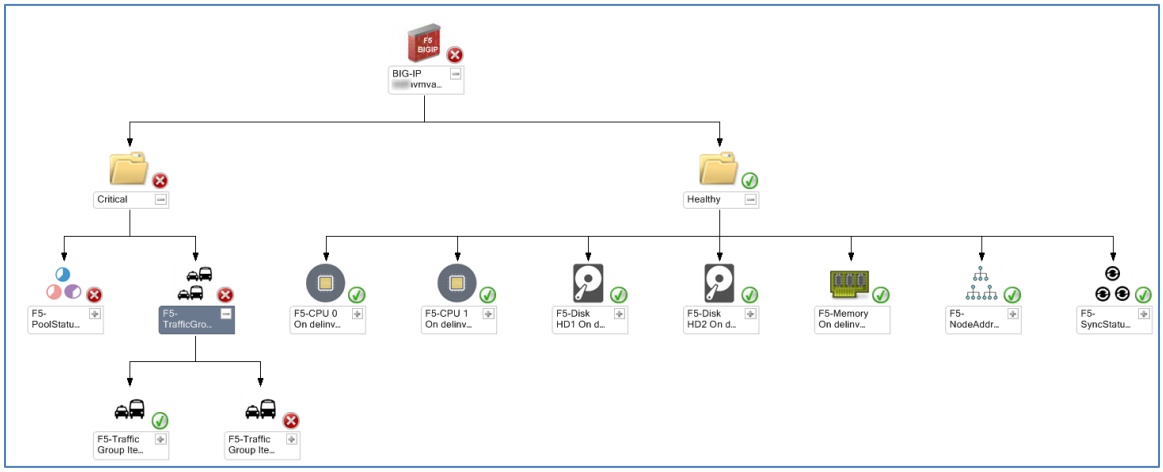


State view show the state of a particular item:



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





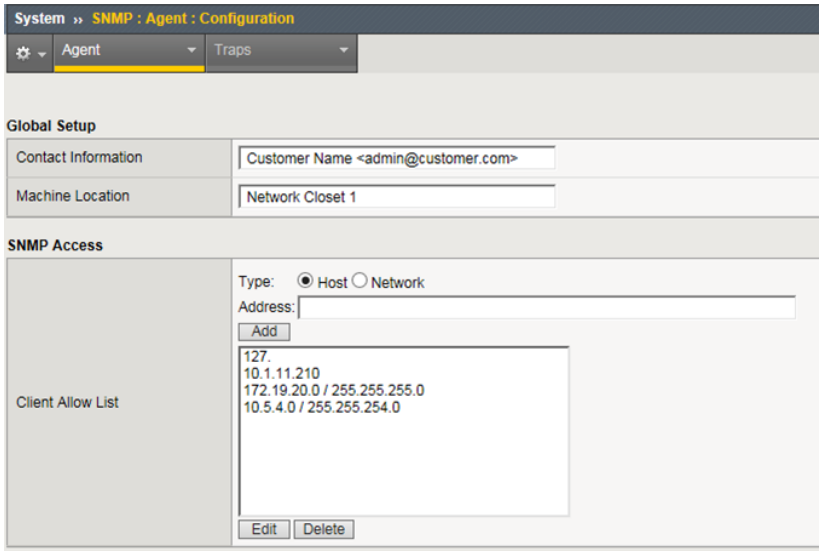
Preparation (Required)

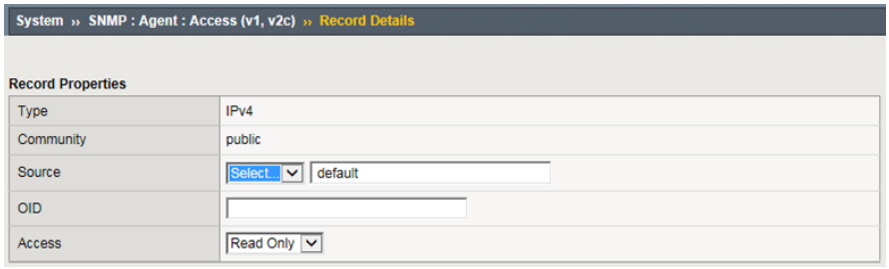
Settings in SCOM

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

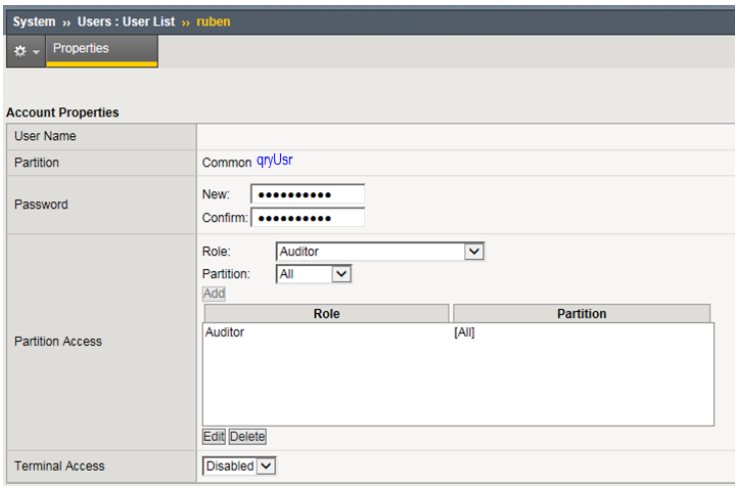
Settings on F5 BIGIP

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





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



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 OpsMgr Management Servers is required.

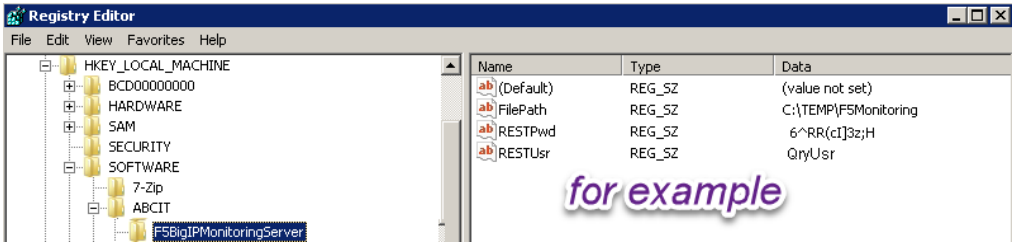
- Install the 64-Bit toolset from net-snmp. Available as free and open source software through http://www.net-snmp.org. Working version: net-snmp-5.5-2.x64.exe – higher should hopefully work as well.

- 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:



- 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

    - vmva486,10.1.20.163
    - vmva487,10.1.20.164

- 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 30 minutes
    - 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.