

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

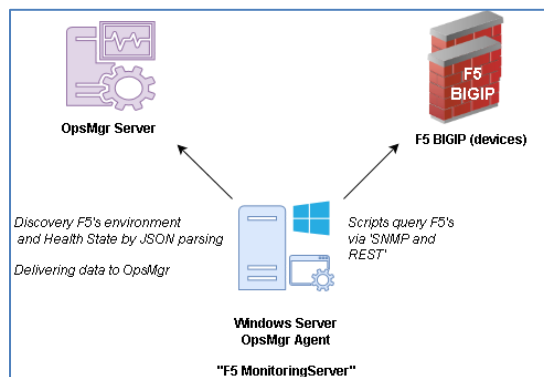
Gathering basic health state information and enabling alerting for key components for F5 Big-IP is the main idea for this this management pack.

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:

Monitoring

PoolStatus - Alerts (4)

Look for: Find Now Clear

Path	Source	Name	Resolution State	Created	Age
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...

Severity: Critical (4)

Alert Details

PoolStatus Issue

Alert Description

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

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

Alert Monitor: Monitor F5 BIGIP Application PoolStatus

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

Please check. PoolStatus System abnormal.

TestedAt: 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:

Monitoring

CPU - State (4)

Look for: Find Now Clear

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

Detail View

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

Display Name: F5-CPU 1 On vmva487.sig.dom

Full Path Name: F5-CPU 1 On vmva487.sig.dom

Id: 1

SystemNodeName: vmva487.sig.dom

Key: vmva487.sig.domF5-CPU1

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

Monitoring

System - State (2)

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

Detail View

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

Display Name	BIG-IP vmva486.sig.domF5 System
Full Path Name	BIG-IP vmva486.sig.domF5 System
SystemNodeName	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

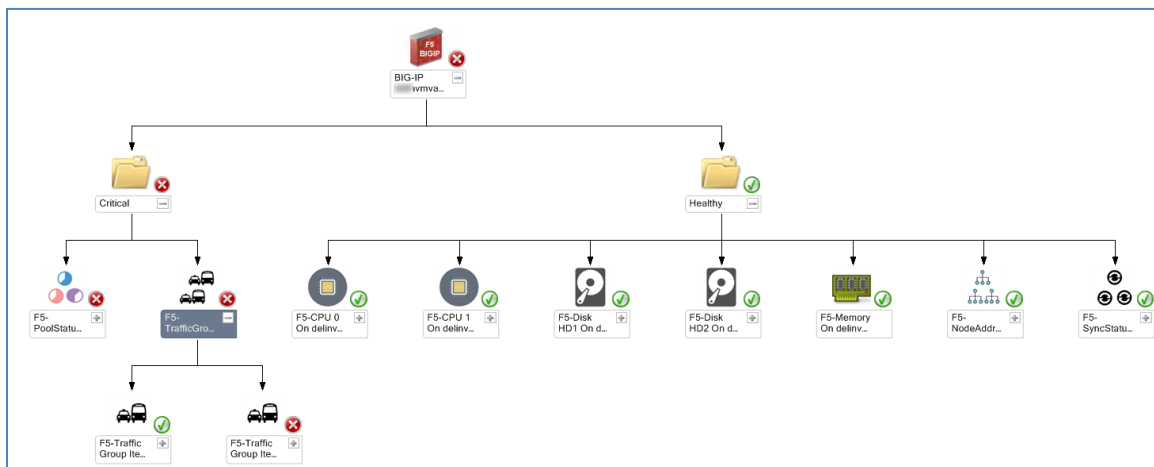
Tasks

State Actions

- Start Maintenance Mode...
- Edit Maintenance Mode Se...
- Stop Maintenance Mode...
- Personalize view...

Navigation

- Alert View
- Diagram View
- Event View
- Performance View
- State View
- DELINAlert
- Network Vicinity Dashboar...
- Object State Dashboard



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:

The screenshot shows the 'System » SNMP : Agent : Configuration' page. It has a navigation bar with 'Agent' and 'Traps' tabs. The 'Global Setup' section contains 'Contact Information' with 'Customer Name <admin@customer.com>' and 'Machine Location' with 'Network Closet 1'. The 'SNMP Access' section has a 'Client Allow List' table with columns for 'Type' (radio buttons for Host and Network) and 'Address'. The 'Host' radio button is selected. The 'Address' column contains a list of IP addresses: 127., 10.1.11.210, 172.19.20.0 / 255.255.255.0, and 10.5.4.0 / 255.255.254.0. There are 'Add', 'Edit', and 'Delete' buttons at the bottom of the list.

Type	Address
<input checked="" type="radio"/> Host <input type="radio"/> Network	
	127.
	10.1.11.210
	172.19.20.0 / 255.255.255.0
	10.5.4.0 / 255.255.254.0

The screenshot shows the 'System » SNMP : Agent : Access (v1, v2c) » Record Details' page. It has a 'Record Properties' section with a table containing the following information:

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

The screenshot shows the 'System » SNMP : Agent : Access (v1, v2c)' page. It has a 'Create...' button and a table with the following information:

Type	Community	Source	OID	Access
<input checked="" type="checkbox"/> IPv4	public	default		Read Only

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

System >> Users : User List >> ruben

Properties

Account Properties

User Name					
Partition	Common qryUsr				
Password	New: <input type="password"/> Confirm: <input type="password"/>				
Partition Access	<div>Role: <input type="text" value="Auditor"/> Partition: <input type="text" value="All"/> Add</div> <table><thead><tr><th>Role</th><th>Partition</th></tr></thead><tbody><tr><td>Auditor</td><td>[All]</td></tr></tbody></table> <div>Edit Delete</div>	Role	Partition	Auditor	[All]
Role	Partition				
Auditor	[All]				
Terminal Access	<input type="text" value="Disabled"/>				

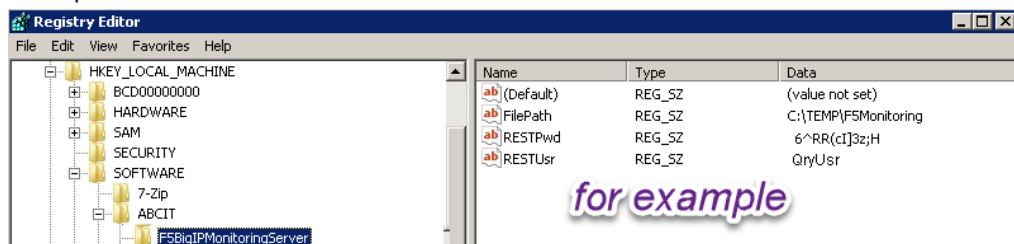
Auditor Role allows read only access to all partitions:

“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 RESTUser and RESTPwd according to the values configured above for the access.
 - [HKEY_LOCAL_MACHINE\SOFTWARE\ABCIT\F5BigIPMonitoringServer]
 - "RESTUser"="qryUser"
 - "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.