

EVALUATION GUIDE

HYCU SCOM Management Pack for F5 BIG-IP

Product version: 5.4

Product release date: May 2018

Document edition: First



Legal notices

Copyright notice

© 2015-2018 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5.

Microsoft is either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Squared Up is a registered trademark of Squared Up Ltd.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU
www.hycu.com

Contents

About this document	6
Purpose	6
Intended audience	6
Product deployment	7
Discover F5 BIG-IP devices as network devices in SCOM	7
Install the product	7
Configure F5 BIG-IP iControl REST API access	9
Configure iControl REST API access for F5 BIG-IP version 11.6.x or later	10
Configure HYCU F5 BIG-IP Device Action Account with SCOM Operations console	13
Set up Data Warehouse Action Account for F5 BIG-IP devices	13
Activate software evaluation license	14
Topology Diagram views	15
Topology Device Diagram view	15
Topology LTM Diagram view	15
Monitoring F5 BIG-IP system health	17
Monitoring CPU usage	17
Monitoring disk space	19
Monitoring memory usage	20
Monitoring network interfaces	22
Informing about unmonitored devices	23
License utilization monitoring	24
HYCU Management Pack for F5 BIG-IP Device (Reports)	25
Monitoring LTM module	29
Filtering virtual servers, pools, and pool members	36
Possibility to choose F5 monitor states which can create alerts	37
HYCU Management Pack for F5 BIG-IP LTM (Reports)	38

Monitoring ASM module	40
ASM Statistics dashboard	40
ASM Security Policies view	41
HYCU Management Pack for F5 BIG-IP ASM (Reports)	42
Monitoring DNS module	45
Monitoring wide IPs	45
Wide IPs view	47
Some of the F5 BIG-IP Devices in F5 DNS Sync Group are not in sync monitor	48
Using dedicated Squared Up dashboard pack	49
General on Squared Up	49
F5 BIG-IP (Comtrade) dashboard pack	49
Installation prerequisites	53
Acquiring the dashboard pack	53
Product information and latest updates	54
HYCU Customer Support and information	55
Customer Support	55
Company website and video channel	55
General information	56
Feedback	56

Chapter 1

About this document

Purpose

This guide is designed to be an aid for setting up HYCU SCOM Management Pack for F5 BIG-IP and testing specific product features. It instructs how to prepare environment for product evaluation, and demonstrates product functionalities and their value for key monitoring scenarios.

Intended audience

This guide is intended to be used by IT managers, F5 BIG-IP administrators, Microsoft System Center Operations Manager (SCOM) administrators, and other IT operations personnel who wish to evaluate HYCU SCOM Management Pack for F5 BIG-IP.

A prerequisite for using this guide is fair understanding of both F5 BIG-IP and SCOM.

Chapter 2

Product deployment

This chapter provides only a summary of the steps required for installation and configuration of HYCU SCOM Management Pack for F5 BIG-IP. For accurate instructions on how to install and configure the product, see the *HYCU SCOM Management Pack for F5 BIG-IP User Guide*.

Discover F5 BIG-IP devices as network devices in SCOM

Do the following:

1. Configure an SNMP community string on each F5 BIG-IP device that you plan to monitor.

For instructions, see the *HYCU SCOM Management Pack for F5 BIG-IP User Guide*, chapter *Environment preparation*, section *Configuring SNMP access to BIG-IP devices*.

2. Create an SNMP Run As account in SCOM. Then create and run the discovery rule in SCOM.

For instructions, see the *HYCU SCOM Management Pack for F5 BIG-IP User Guide*, chapter *Environment preparation*, section *Discovering BIG-IP devices as network devices in SCOM*.

After you complete the process, you should see F5 BIG-IP devices in the **Administration > Network Management > Network Devices** context of the SCOM Operations console.

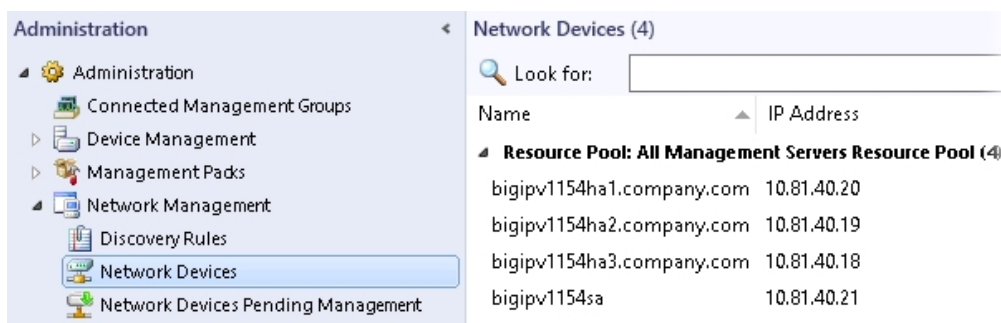


Figure 2-1: Network devices in SCOM

Install the product

Do the following:

1. On the SCOM management server designated for monitoring F5 BIG-IP, launch the HYCU.SCOP.MP.F5.BIG-IP.msi setup package and choose **Complete** for the setup type.
2. Management pack import can be performed only from one SCOM management server, because SCOM automatically deploys the imported management packs on other SCOM management servers in the same management group.

After management pack is imported, you should see F5 BIG-IP (by HYCU) folder in the Monitoring view of the SCOM Operations console.

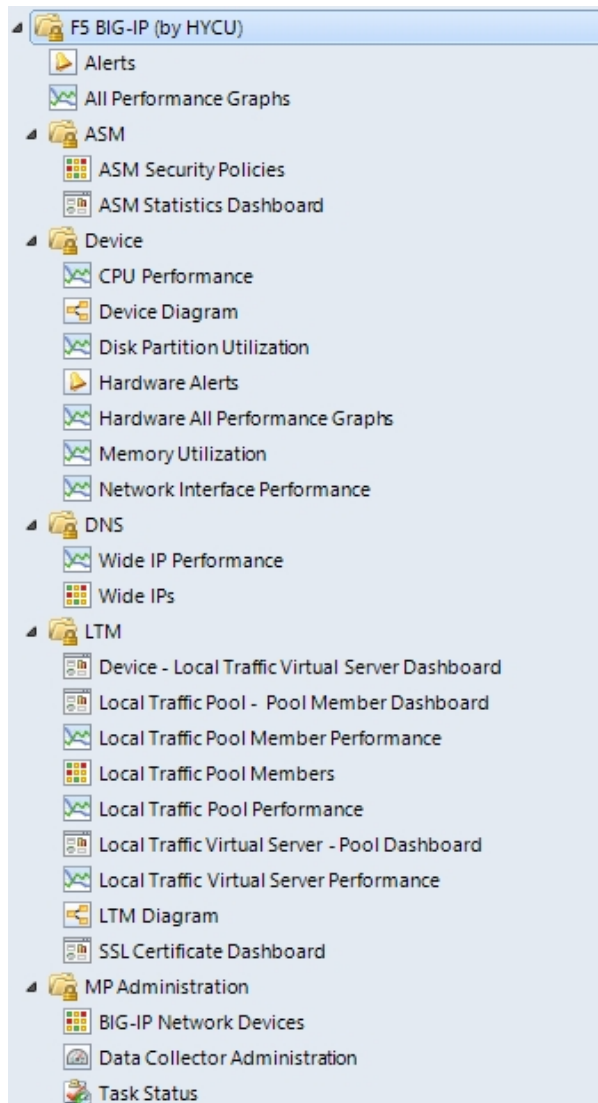


Figure 2-2: Elements of SCOM MP for F5 BIG-IP, as seen in the SCOM Operations console

3. The HYCU SCOM Data Collector for F5 BIG-IP component (this component is included if Typical or Complete installation is chosen) *must* be installed on all SCOM management servers that are members of the SCOM resource pool dedicated to F5 BIG-IP monitoring.

As a result, all SCOM management servers with the HYCU SCOM Data Collector for F5 BIG-IP component installed are listed in the **MP Administration > Data Collector Administration** view.

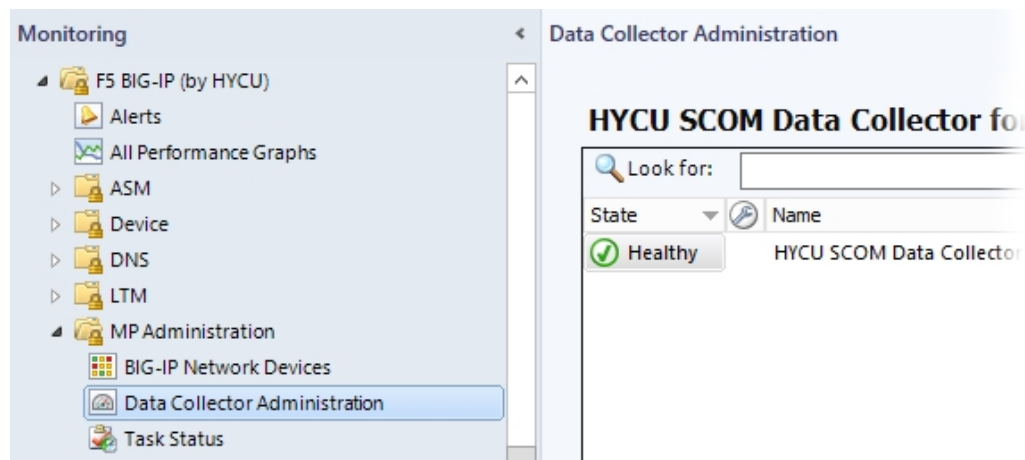


Figure 2–3: The Data Collector Administration view

Configure F5 BIG-IP iControl REST API access

The process for enabling monitoring of a F5 BIG-IP device through its iControl REST API consists of the following tasks:

1. Verify accessibility of a device from a SCOM management server.
2. On a BIG-IP device, configure a user account dedicated to device monitoring (referred to as *monitoring user account*).

You should complete the above process for *each* BIG-IP device that you plan to monitor and for *each* SCOM management server that you plan to use.

When configuring the monitoring user account, you can choose between two user account types (depending on the F5 BIG-IP version on your BIG-IP device). Your possibilities are as follows:

F5 BIG-IP version 11.6.x or later:

- Remote read-only user account
- Local read-only user account

F5 BIG-IP version 11.5.x:

- Remote administrative user account
- Local administrative user account

Section [“Configure iControl REST API access for F5 BIG-IP version 11.6.x or later”](#) on the next page contains an example procedure for configuring F5 BIG-IP iControl REST API access to a device with F5 BIG-IP version 11.6.x or later by using the BIG-IP Configuration Utility (graphical user interface).

For configuration instructions for all possible use cases, see the *HYCU SCOM Management Pack for F5 BIG-IP User Guide*, chapter *Environment preparation*, section *Configuring access to F5 BIG-IP devices*, subsection *Configuring F5 BIG-IP iControl REST API access*.

Configure iControl REST API access for F5 BIG-IP version 11.6.x or later

Verification

To verify accessibility of a device from the SCOM management server, do the following:

1. On a SCOM management server that you plan to use for monitoring, open a web browser, and go to the following webpage:

```
https://<IPaddress>
```

In this instance, <IPaddress> is the IP address of the chosen BIG-IP device.

2. Check if the BIG-IP Configuration Utility (web user interface) opens in the web browser.

To configure a read-only user account for monitoring a BIG-IP device, do the following:

1. Action in this step depends on the chosen user account type:
 - Remote user account:

Obtain a user name of the user account designated for monitoring your F5 BIG-IP devices from your network and systems administrator (in charge of the domain controller).

Important The chosen user account should not be part of a BIG-IP remote role group.
 - Local user account:

Proceed with the next step.
2. Open a web browser and log in to the BIG-IP Configuration Utility (web user interface) with a user account that has privileges to create BIG-IP user accounts.
3. Navigate to **System > Users > User List**.
4. Click **Create**.
5. Enter a value for the Account User Name option.

Example

Value of the Account User Name option in BIG-IP:

```
MyMonitoringAccountName
```

6. Action in this step depends on the chosen user account type:

- Remote user account:
Proceed with the next step.
 - Local user account:
Enter the password that you want to use for this user account
7. Assign the user account a user role other than No Access and Administrator.

Example

Assigned BIG-IP user role:

Guest

8. Click **Finished**.
9. On a SCOM management server that can access the BIG-IP device, run the following Windows PowerShell script:

```
Set-ReadOnlyAccess.ps1
```

The script is located in the

C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration tools directory. To retrieve its usage information and examples, run the `Get-Help .\Set-ReadOnlyAccess -detailed` command.

10. When prompted, enter the following information:
- IP address of the BIG-IP device on which you created the user account
 - Credentials of a user account that has administrative privileges in BIG-IP
 - User name of the created user account

Verification

Verification steps depend on the access authentication mode used by SCOM MP for F5 BIG-IP which in turn depends on the F5 BIG-IP version on the device.

F5 BIG-IP version 12.1.x or later:

Do the following:

1. On a SCOM management server that can access the BIG-IP device, run the following Windows PowerShell script:

```
Verify-TokenAccess.ps1 -DeviceIP <IPAddress> -UserName <UserName>
-Password <Password>
```

In this instance, `<DeviceIP>` is IP address of the BIG-IP device for which to verify access, and `<UserName>` and `<Password>` are user name and password of the configured monitoring user account.

The script is located in the C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration tools directory.

2. Check if the script output resembles the following:

```
StatusCode StatusDescription
-----
200 OK
```

F5 BIG-IP version 11.6.x:

Do the following:

1. On a SCOM management server that can access the BIG-IP device, open a web browser, and go to the following webpage:

```
https://<IPaddress>/mgmt/tm/cm/device?$select=version,managementIp
```

In this instance, <IPaddress> is the management IP address of the BIG-IP device.

2. Action in this step depends on the chosen user account type:
 - Remote user account:
When prompted for credentials, enter the user name of the monitoring user account that you have configured previously, and supply its password.
 - Local user account:
When prompted for credentials, enter the user name and password of the monitoring user account that you have configured previously.
3. Check if the response from the device is a valid JSON object that resembles the example output that follows.

Example

Device response from the F5 BIG-IP version 11.6.1:

```
{
  kind : "tm:cm:device:devicecollectionstate",
  selfLink :
  "https://localhost/mgmt/tm/cm/device?$select=version,managementIp&ver=11.6.1",
  items : [{
    managementIp : "10.49.14.127",
    version : "11.6.1"
  }]
}
```

Configure HYCU F5 BIG-IP Device Action Account with SCOM Operations console

Do the following:

1. Create Run As account (use account that was created and tested in the previous step).
2. Associate Run As Account with HYCU F5 BIG-IP Device Action Account.

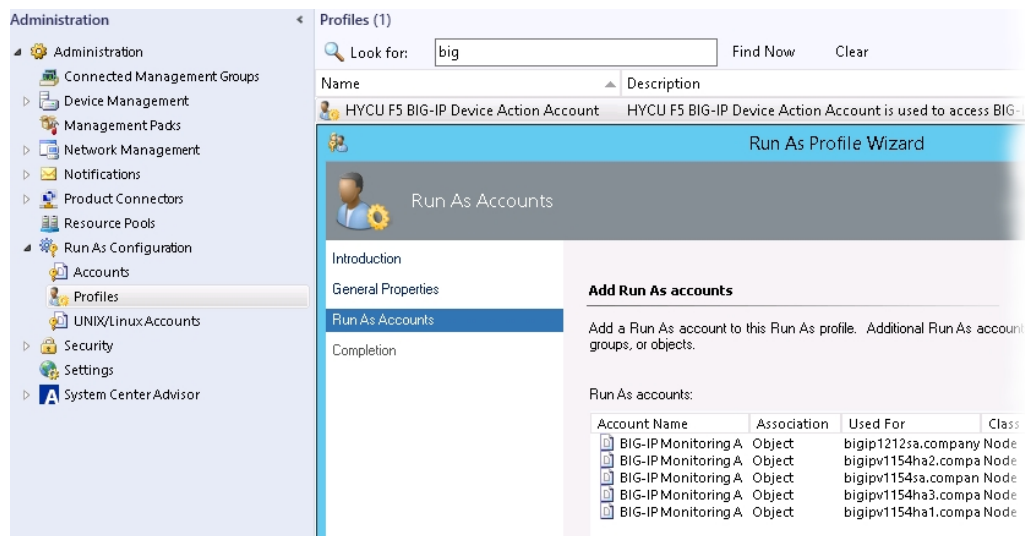


Figure 2-4: Assigning HYCU F5 BIG-IP Device Action Account for F5 BIG-IP devices discovered as network devices

Set up Data Warehouse Action Account for F5 BIG-IP devices

Do the following:

1. Select **Run As Configuration > Profiles**, double-click **Data Warehouse Action Account** and **Run As Account > Add**.
2. From the drop-down list, choose **Data Warehouse Action Account** and select **class**.
3. **Add** F5 Sync Failover Group and save configuration.

The Run As Profile Wizard window should resemble the figure that follows.

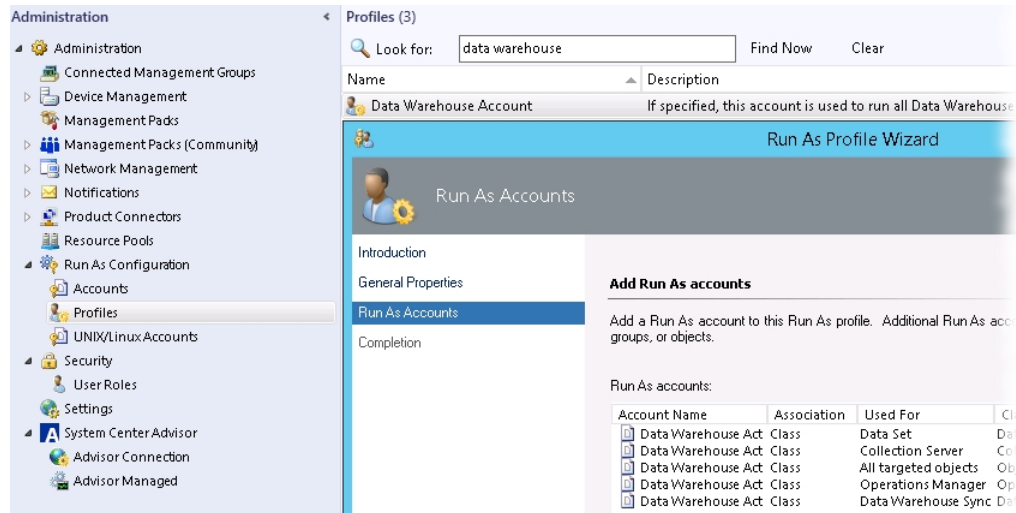


Figure 2-5: Assigning Data Warehouse Action Account

Activate software evaluation license

Do the following:

- Copy the license activation file `mpbigip_licact_new.dat` that you have received for the evaluation to the `%ProgramData%\Comtrade\Comtrade F5 Data collector` folder on all SCOM management servers on which HYCU SCOM Management Pack for F5 BIG-IP is installed.

Important F5 BIG-IP devices and their configuration objects can be discovered even when the product license is not activated, but monitors and rules provided by HYCU SCOM Management Pack for F5 BIG-IP do not function in this case.

Chapter 3

Topology Diagram views

Topology Device Diagram view

HYCU SCOM Management Pack for F5 BIG-IP automatically discovers all F5 BIG-IP resources. There is a topology view predefined in this management pack that provides quick overview across all F5 BIG-IP resources:

- F5 BIG-IP devices
- Host hardware (CPUs, disk partitions, NICs, memory)

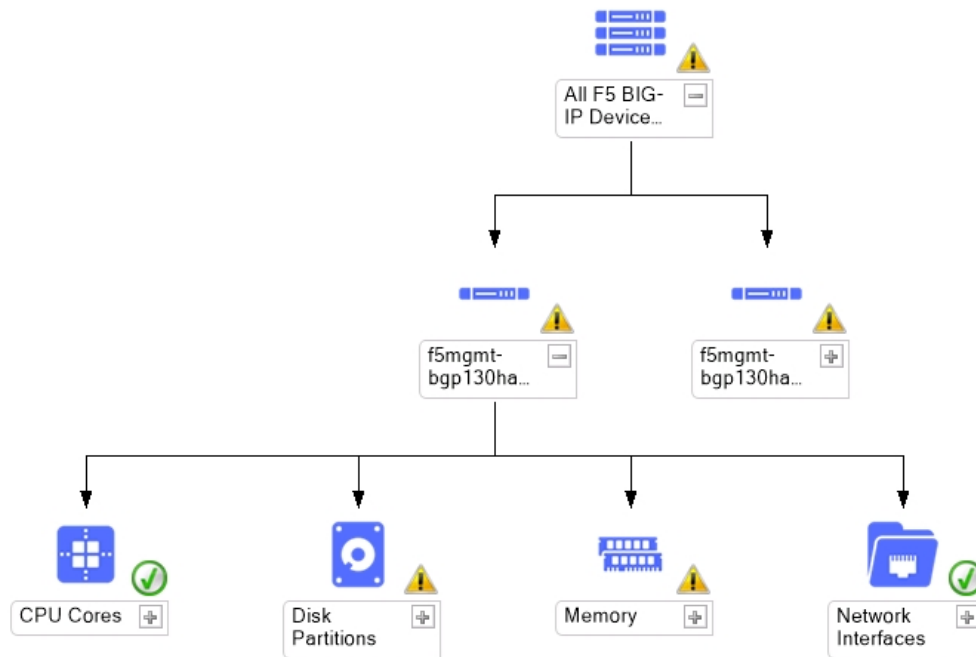


Figure 3-1: Topology device diagram shows all hardware components, their relationship, and health status

Topology LTM Diagram view

There is a predefined topology view available in HYCU SCOM Management Pack for F5 BIG-IP that provides quick overview of LTM topology:

- Traffic groups

- Active and passive devices
- F5 BIG-IP devices
- Host hardware (CPUs, disk partitions, NICs, memory)
- Virtual servers, pools, and pool members
- SSL certificates

HYCU SCOM Management Pack for F5 BIG-IP discovers traffic groups on the F5 BIG-IP device that contain at least one virtual server. As a result, these traffic groups are listed in the LTM diagram view. Virtual servers that are contained within that traffic group are shown in the diagram. Furthermore, it is possible to easily identify which devices are active and which are passive for that specific traffic group that is being displayed.

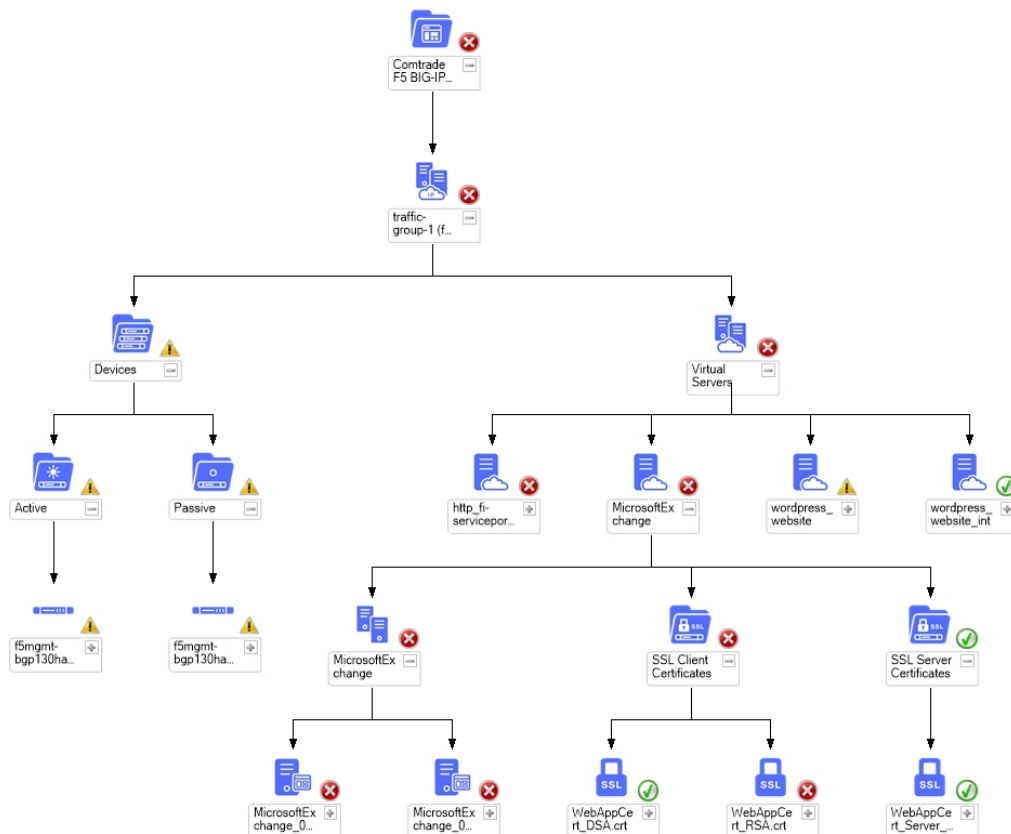


Figure 3-2: Topology LTM diagram shows all components, their relationship, and health status

Chapter 4

Monitoring F5 BIG-IP system health

Monitoring CPU usage

HYCU SCOM Management Pack for F5 BIG-IP automatically discovers all CPU cores and monitors CPU usage on a device and on a CPU core level.

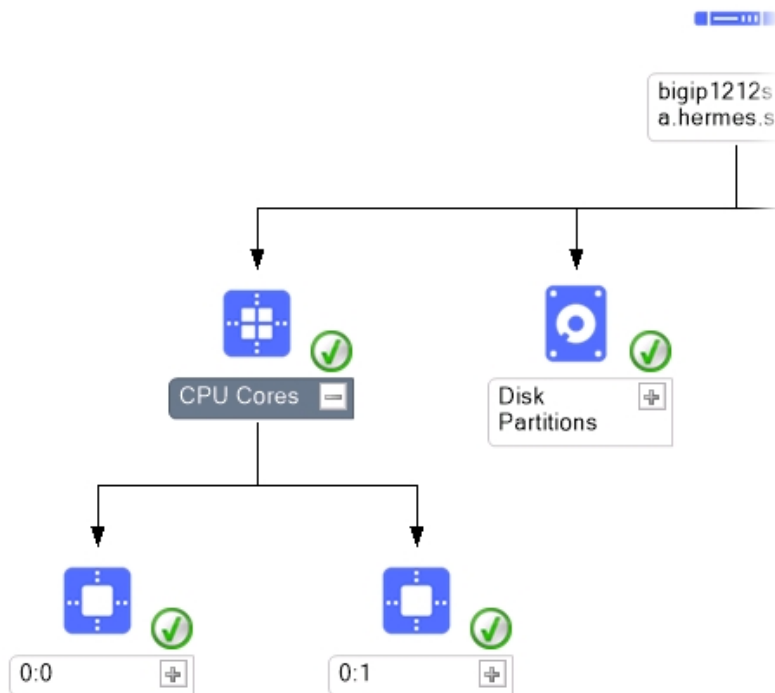


Figure 4-1: Topology device diagram shows all CPU cores discovered on F5 BIG-IP device

Alert Description

CPU usage on bigip1161ha1.hermes.si (10.49.39.240) device exceeds or is equal to the expected value. Extended high CPU utilization can degrade performance, and the system may eventually become unresponsive or reboot.

Figure 4-2: CPU Usage alert

CPU Performance graphs can be found in the **Monitoring > F5 BIG-IP Monitoring > Device > CPU Performance** view.

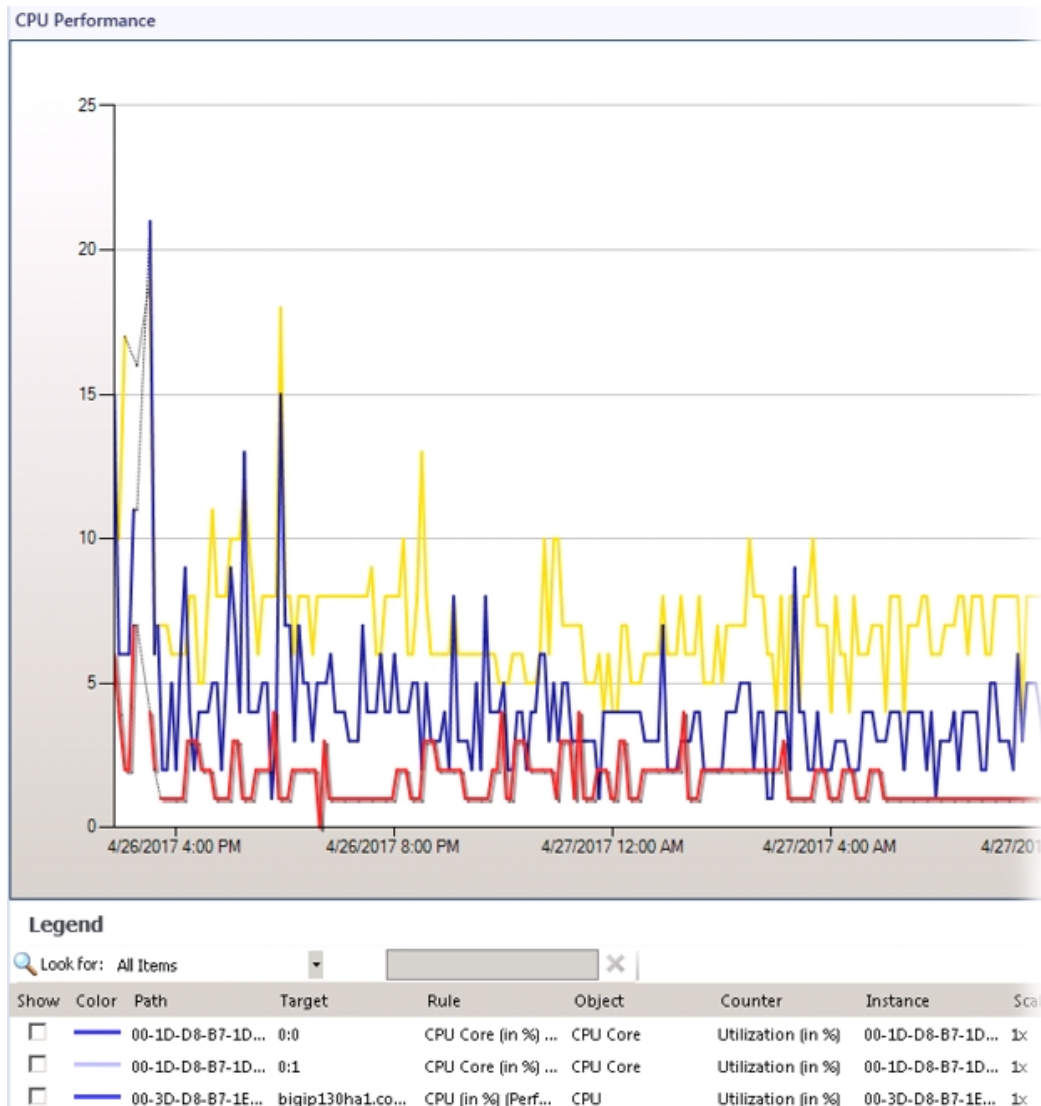


Figure 4-3: CPU Performance graphs can help with device CPU usage analysis

Monitoring disk space

Hard disk capacity monitoring on a F5 BIG-IP unit is critical for maintaining a healthy system. It is recommended that you periodically check disk space utilization and keep disk utilization at minimum. HYCU SCOM Management Pack for F5 BIG-IP automatically discovers and monitors disk usage and disk free space on a disk and partition levels.

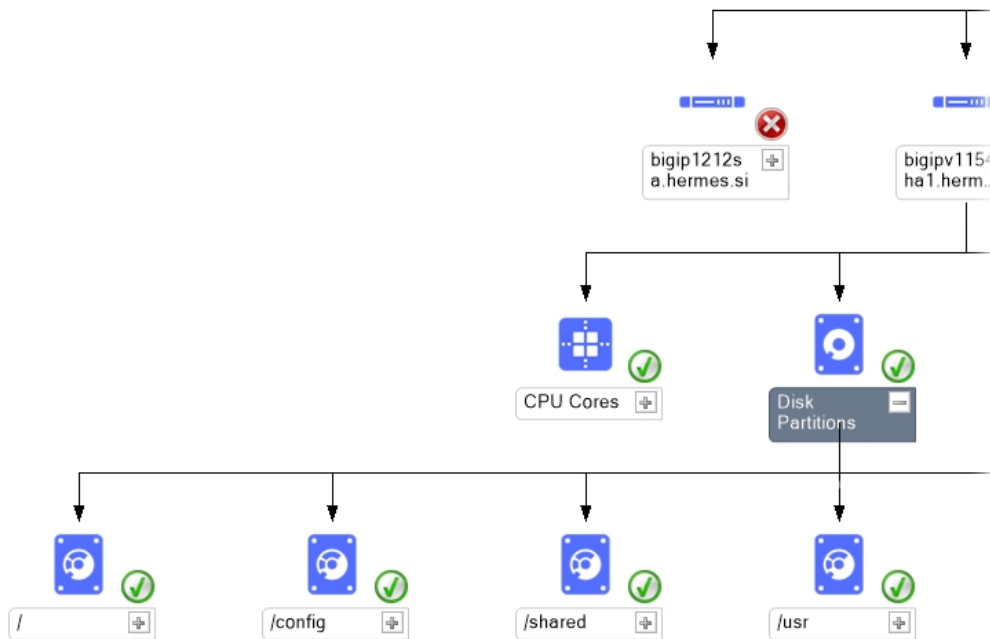


Figure 4-4: Topology device diagram shows all disk partitions discovered on F5 BIG-IP device

Alert Description

Free storage on bigipv1154ha2.hermes.si (10.81.40.19) device on partition /usr amounts to 20 % (506 MB) of total space. When the BIG-IP file systems become full, undesirable or unpredictable behavior may result.

Figure 4-5: Disk Utilization alert

Disk partition performance graphs can be found in the **Monitoring > F5 BIG-IP Monitoring > Device > Disk Partition Utilization** view.



Figure 4-6: Disk partition performance graph helps with disk space analysis

Monitoring memory usage

HYCU SCOM Management Pack for F5 BIG-IP enables you to monitor usage of:

- TMM memory
This is the amount of memory used by the TMM processes for traffic management.
- Other memory
This is the amount of memory used by non-TMM processes.

Alert Description

Other memory usage on bigipv1154ha2.hermes.si (10.81.40.19) device is higher than expected for normal operation. Please monitor this device's other memory consumption in more details.

Figure 4-7: Memory usage alert

Memory utilization performance graphs can be found in the **Monitoring > F5 BIG-IP Monitoring > Device > Memory Utilization** view.

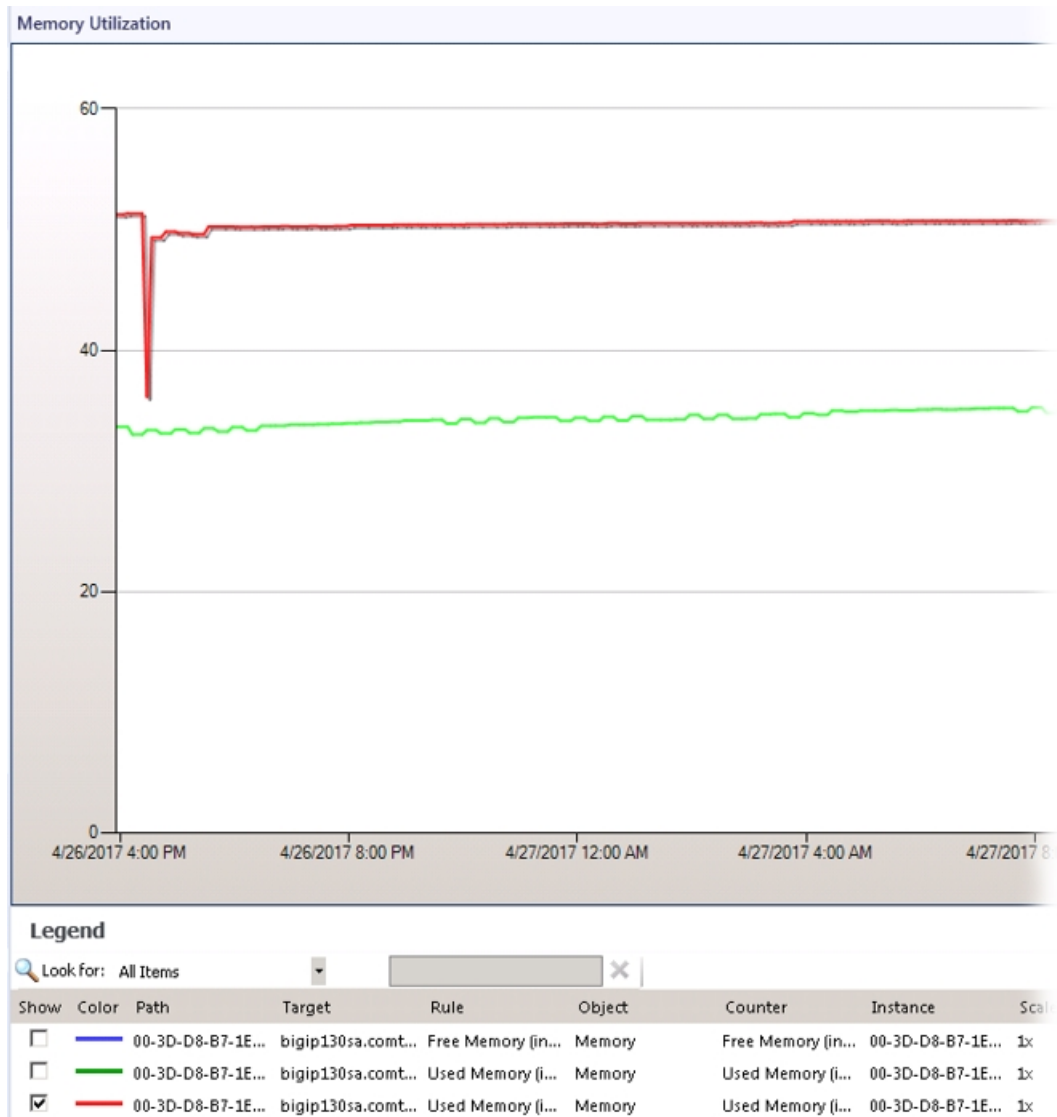


Figure 4-8: Memory utilization performance graphs

Monitoring network interfaces

HYCU SCOM Management Pack for F5 BIG-IP automatically discovers and enables monitoring of all network interfaces, including management interface and all other interfaces also known as TMM switch interfaces. TMM switch interfaces are those interfaces that the F5 BIG-IP system uses to send or receive application traffic.

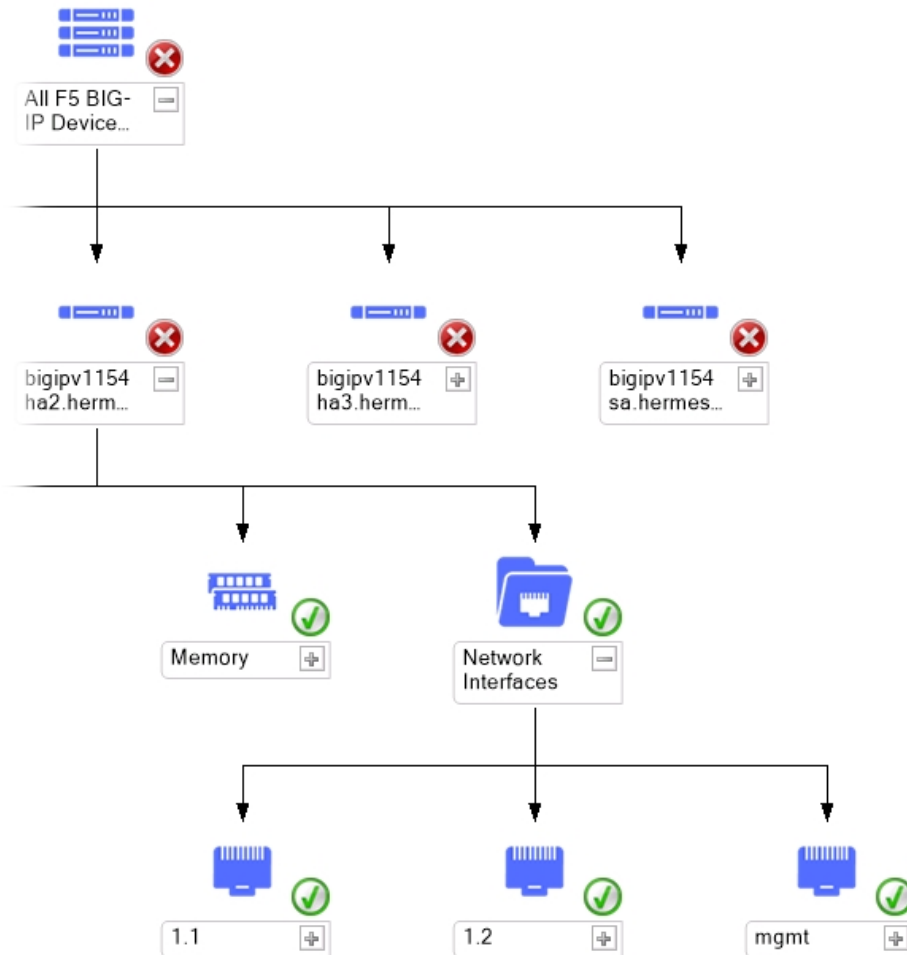


Figure 4-9: Topology device diagram shows mgmt and TMM interfaces

HYCU SCOM Management Pack for F5 BIG-IP monitors interface status and sends an alert to SCOM if the interface changes status to down or `uninit`. The default value for the Warning on UNINIT parameter is `false`. When switched to `true`, the monitor raises a warning alert on the UNINIT state.

Alert Description
Interface 1.1 on device bigipv1154sa.hermesi.si (10.81.40.21) is uninit.

Figure 4-10: Network interface status alert

Network Interface Performance graphs can be found in the **Monitoring > F5 BIG-IP Monitoring > Device > Network Interface Performance** view.

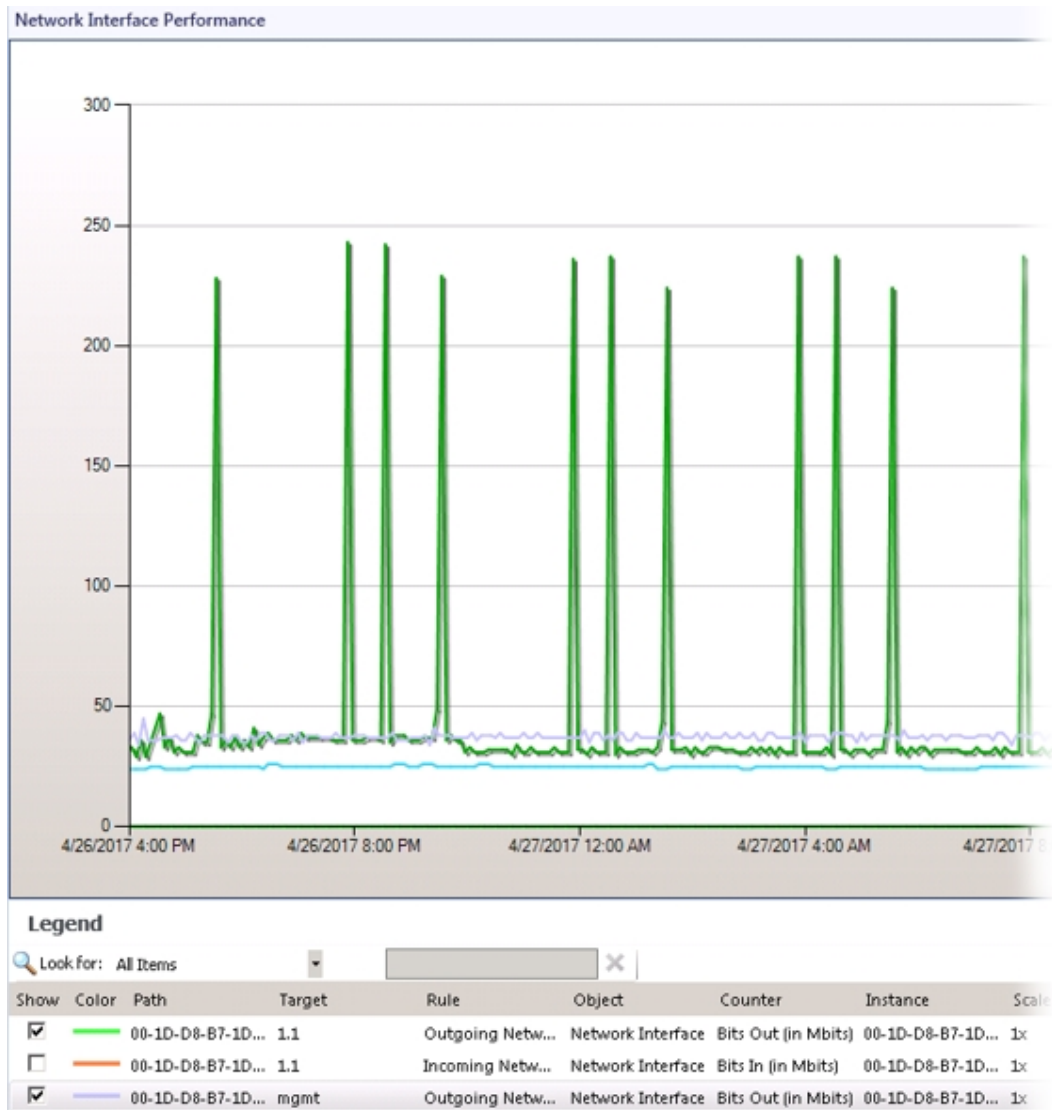


Figure 4-11: Network Interface Performance graphs show the amount of data received from or sent to the F5 BIG-IP node

Informing about unmonitored devices

F5 BIG-IP devices that are discovered in SCOM but cannot be monitored by HYCU SCOM Management Pack for F5 BIG-IP for some reason are set to critical and an alert is generated for each of them.

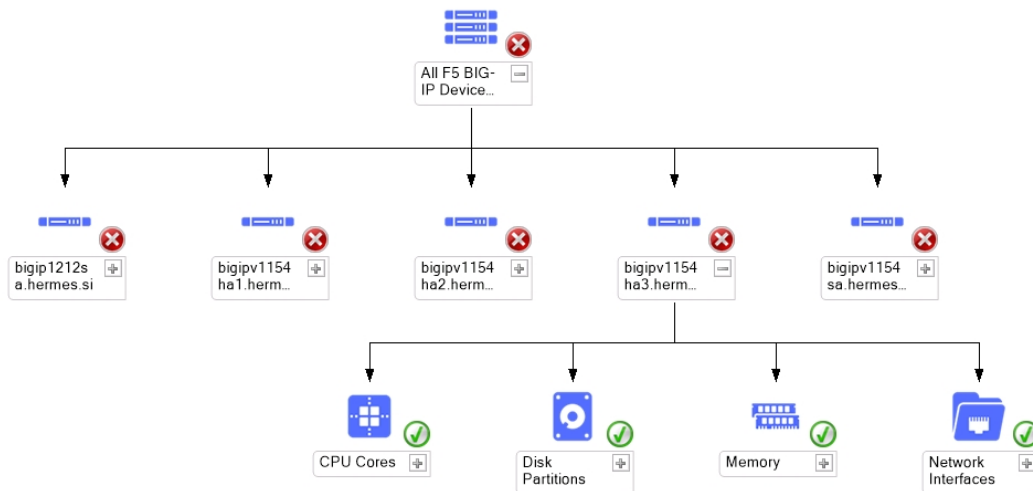


Figure 4-12: Topology device diagram shows all F5 BIG-IP devices

Alert Description

F5 BIG-IP Device bigip130ha4.comtrade.com (10.49.37.249) is not available for monitoring because data could not be obtained from the F5 BIG-IP Device

Figure 4-13: F5 BIG-IP device is unavailable for monitoring alert

License utilization monitoring

HYCU SCOM Management Pack for F5 BIG-IP generates an alert when inbound or outbound traffic exceeds limit determined by virtual edition license.

Alert Description

F5 BIG-IP mpbigip130ha3.comtrade.com (10.49.38.30) Outbound Bandwidth utilization is 60.9869 Mbps, this value exceeds 1% of licensed 5000 Mbps. In case where F5 BIG-IP License utilization is 100%, all applications delivered using this device will experience performance degradation. To identify all applications delivered using this device, see Device - Local Traffic Virtual Server Dashboard.

Figure 4-14: F5 BIG-IP Outbound Bandwidth utilization alert

Note License utilization monitoring is available only for F5 BIG-IP versions 12.1.x and later.

HYCU Management Pack for F5 BIG-IP Device (Reports)


To access HYCU Management Pack for F5 BIG-IP Device (Reports), do the following:

1. In the Monitoring view, expand **Monitoring** and click **F5 BIG-IP Monitoring**.
2. Select an F5 BIG-IP device in one of the following contexts:
 - **Device > Device Diagram View**
 - **LTM > Device - Local Traffic Virtual Server Dashboard**
 - **LTM > LTM Diagram View**
 - **MP Administration > BIG-IP Network Devices**
3. In the Task pane, choose one of the available F5 BIG-IP device reports:
 - **Device Performance**


This report displays the effect of user activity on the F5 BIG-IP device throughput and consumption of the device resources: CPU, memory, and disk. You can narrow the scope of data analysis to customizable business hours.
 - **Device Traffic Report**

This report shows traffic details on a specific BIG-IP device. You can choose to show traffic only during business hours, and select the time and days of the week of your business cycle.
 - **Inbound License Utilization (Top N)**

This report shows license inbound utilization details for a specific device. You can choose algorithms from the drop-down list (Top N or Bottom N).

 **Note** The report contains no data unless the Inbound License Utilization (in %) (Performance DB DW) rule is enabled.
 - **Outbound License Utilization (Top N)**

This report shows license outbound utilization details for a specific device. You can choose algorithms from the drop-down list (Top N or Bottom N).


 **Note** The report contains no data unless the Outbound License Utilization (in %) (Performance DB DW) rule is enabled.

By selecting the **Top N** (or **Bottom N**) algorithm in either of the two reports, you can identify which devices utilize their license the most (or the least), and you can plan ahead if you are going to need a better license by identifying growth trends on the report (or you can reorganize application deployment to better utilize this license).

Report tables (apart from the Device Performance report) present the following information:

- Sample count
- Minimum value

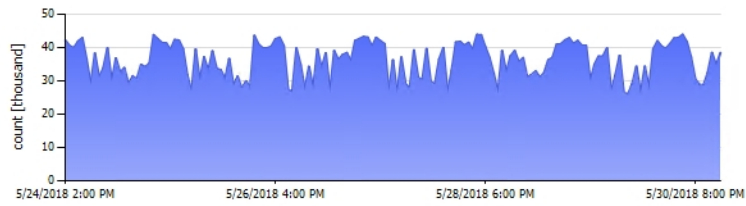
- Maximum value
- Average value
- Standard deviation

 **Note** License utilization reports are available only for F5 BIG-IP versions 12.1.x and later.

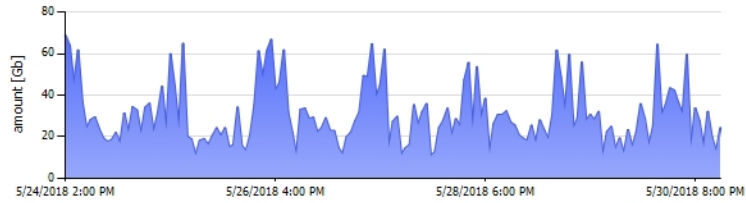
F5 BIG-IP Device: bigip131ha1.company.com (10.49.36.167)

USER ACTIVITY

USER CONNECTIONS



NETWORK TRAFFIC

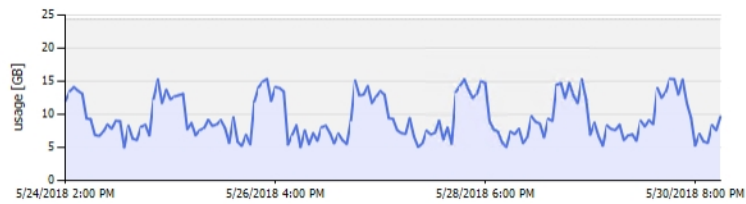


DEVICE PERFORMANCE

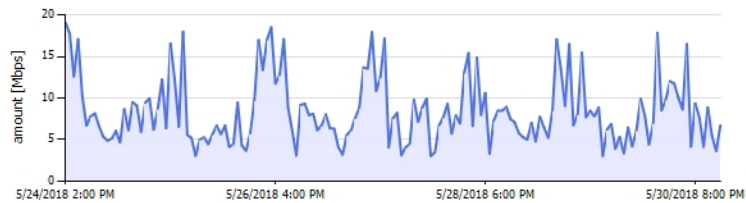
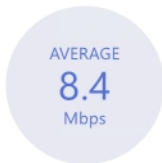
CPU USAGE



MEMORY USAGE



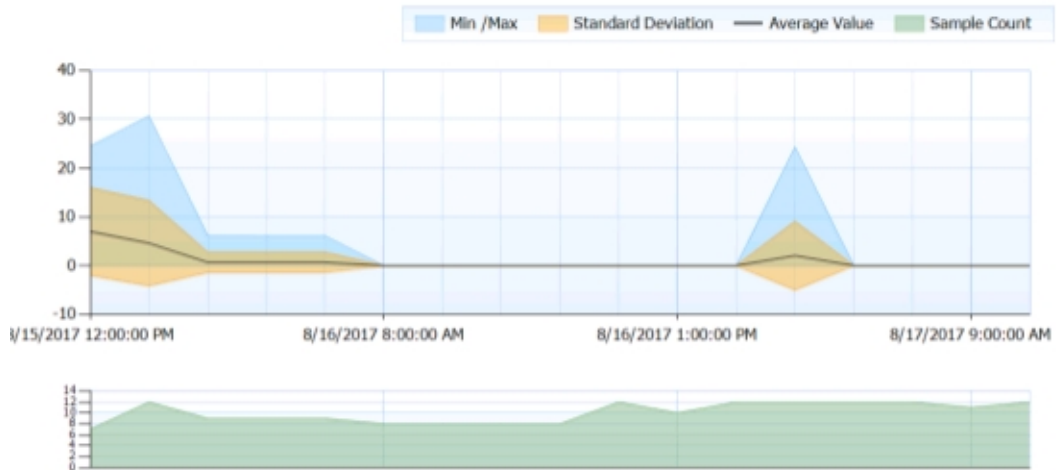
THROUGHPUT



DISK USAGE



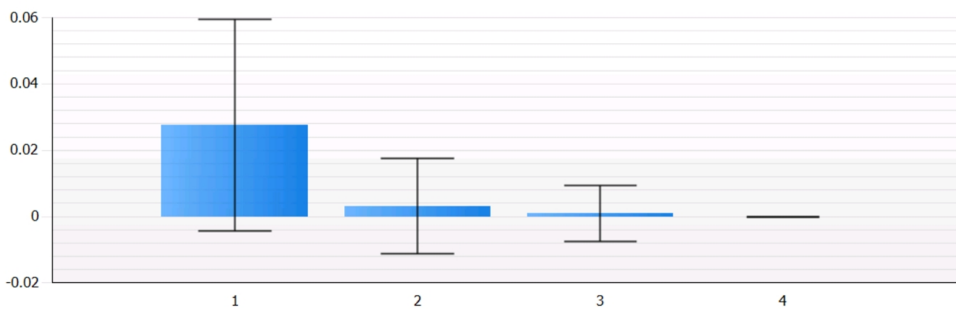
Figure 4-15: Graphical part of the Device Performance report



Sample Count : 171	Mn Value : 0.007672	Average Value : 0.8793
<input type="checkbox"/> Detail Table	Max Value : 30.68	Standard Deviation : 3.574

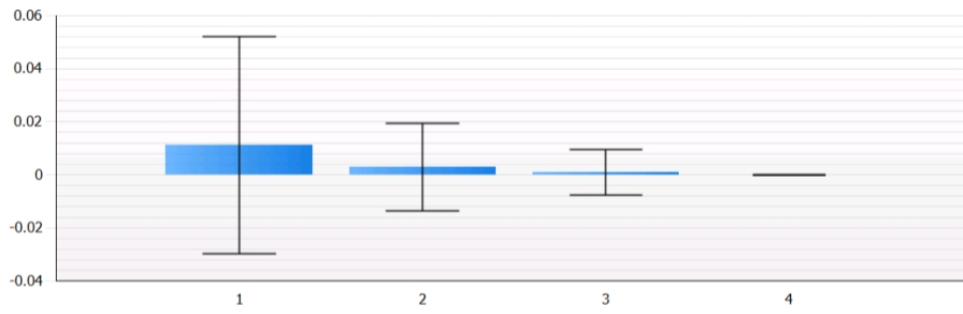
Interval	Sample Count	Mn Value	Max Value	Average Value	Standard Deviation
8/15/2017 12:00:00 PM	7	0.009834	24.52	7.009	8.973
8/15/2017 1:00:00 PM	12	0.0078	30.68	4.617	8.727
8/15/2017 2:00:00 PM	9	0.00821	6.157	0.6915	2.05
8/15/2017 3:00:00 PM	9	0.008039	6.109	0.6863	2.034
8/15/2017 4:00:00 PM	9	0.007791	6.107	0.6857	2.033
8/16/2017 8:00:00 AM	8	0.008095	0.008464	0.00823	0.0001539
8/16/2017 9:00:00 AM	8	0.007747	0.008095	0.007972	0.000142
8/16/2017 10:00:00 AM	8	0.007767	0.008275	0.008083	0.0001649
8/16/2017 11:00:00 AM	8	0.007672	0.008326	0.007976	0.0002676
8/16/2017 12:00:00 PM	12	0.008139	0.03311	0.02807	0.006691
8/16/2017 1:00:00 PM	10	0.0255	0.03306	0.02934	0.002757
8/16/2017 2:00:00 PM	12	0.02508	0.03301	0.02872	0.002962
8/16/2017 3:00:00 PM	12	0.01414	24.42	2.061	7.041

Figure 4-16: Device Traffic Report



	Object	Sample Count	Min Value	Max Value	Average Value	Standard Deviation
1	F5 BIG-IP: mpbigip130ha3.comtrade.com anduin_grp 00-2D-D8-B7-1C-16	246	0	0.31	0.0276	0.03196
2	F5 BIG-IP: mpbigip130sa.comtrade.com anduin_grp 00-2D-D8-B7-1C-13	166	0	0.12	0.003133	0.01432
3	F5 BIG-IP: mpbigip130ha4.comtrade.com					

Figure 4-17: Outbound License Utilization (Top N)



	Object	Sample Count	Min Value	Max Value	Average Value	Standard Deviation
1	F5 BIG-IP: mpbigip130ha3.comtrade.com anduin_grp 00-2D-DB-B7-1C-16	168	0	0.31	0.01125	0.0408
2	F5 BIG-IP: mpbigip130sa.comtrade.com anduin_grp 00-2D-DB-B7-1C-13	150	0	0.14	0.003	0.01656
3	F5 BIG-IP: mpbigip130ha4.comtrade.com	145	0	0.09	0.000955	0.008513

Figure 4-18: Inbound License Utilization (Top N)

Chapter 5

Monitoring LTM module

HYCU SCOM Management Pack for F5 BIG-IP automatically discovers:

- Traffic groups
- Active and passive devices
- Virtual servers
- Pools
- Pool members
- SSL certificates
- Connection between pools and virtual servers over LTM policies

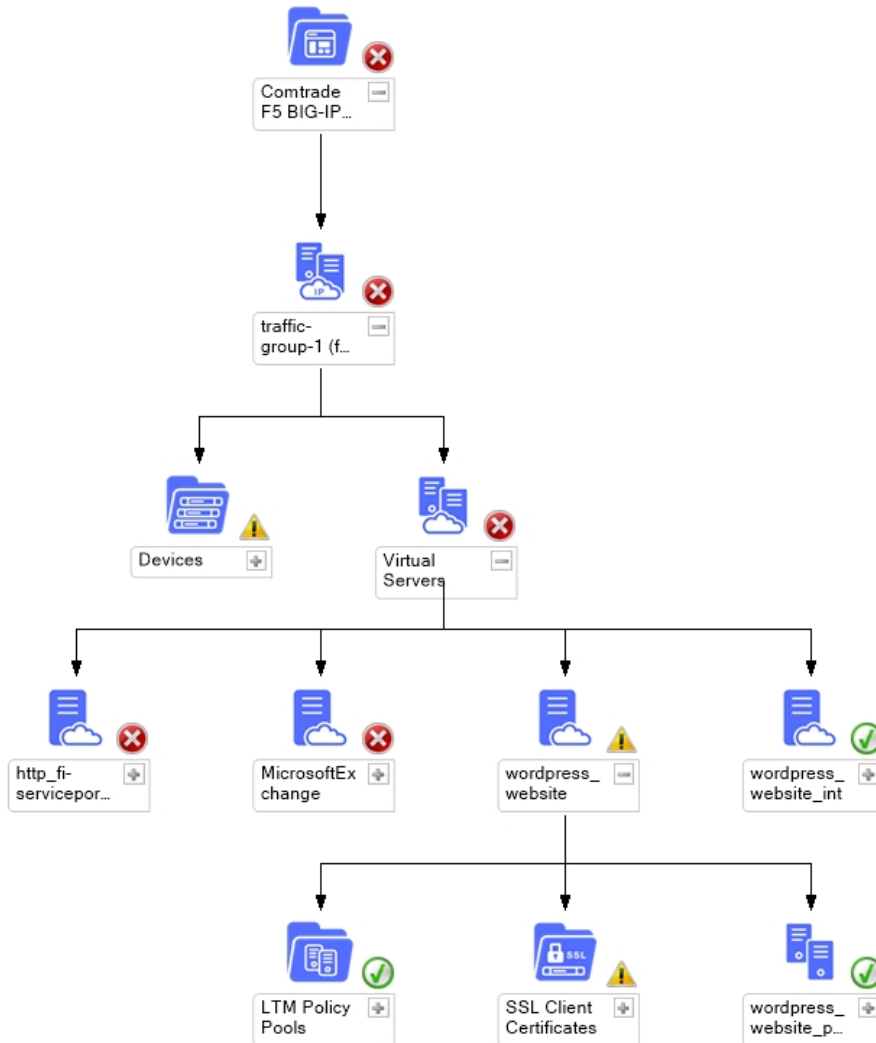


Figure 5-1: Topology LTM diagram shows Traffic Groups, Active and Passive Devices, Virtual servers, Pools and Pool members, SSL Certificates

HYCU SCOM Management Pack for F5 BIG-IP actively monitors availability and status of virtual servers, pools, pool members and generates an alert in case any of them is not available. Alerts are also generated in case SSL certificates expiration in days is below the warning or critical threshold.

Alert Description

Local Traffic Virtual server ~Common~TESTABSERVER on device bigipv1154ha1.hermes.sl (10.81.40.20) is in status unknown because The children pool member(s) either don't have service checking enabled, or service check results are not available yet.

Figure 5-2: Local Traffic Virtual Server Health Alert details

Alert Description

Local Traffic pool member /Common/192.168.64.4:80 part of ~Common~ws2012perf_Pool traffic is below or equal to the threshold.

Figure 5-3: F5 Local Traffic Pool Member traffic is below or equal to the threshold Alert details

Alert Description

Local Traffic pool ~Common~ws2012perf_Pool traffic is below or equal to the threshold.

Figure 5-4: F5 Local Traffic Pool traffic is below or equal to the threshold Alert details

On the virtual server level, the following metrics are collected:

- Current Client-Side Connections
- Total Requests Delta
- Client-Side Bits Out Delta (disabled by default starting with product version 4.1)
- Client-Side Bits In Delta (disabled by default starting with product version 4.1)
- Software Syncookies
- Hardware Syncookies
- Rejected Syncookies
- Issued Syncookies
- Accepted Syncookies
- Client-Side Inbound Traffic (in Mbps)
- Client-Side Outbound Traffic (in Mbps)
- Client-Side Overall Traffic (in Mbps)

Virtual Server Performance graphs can be found in the **Monitoring > F5 BIG-IP (by HYCU) > LTM > Local Traffic Virtual Server Performance** view.

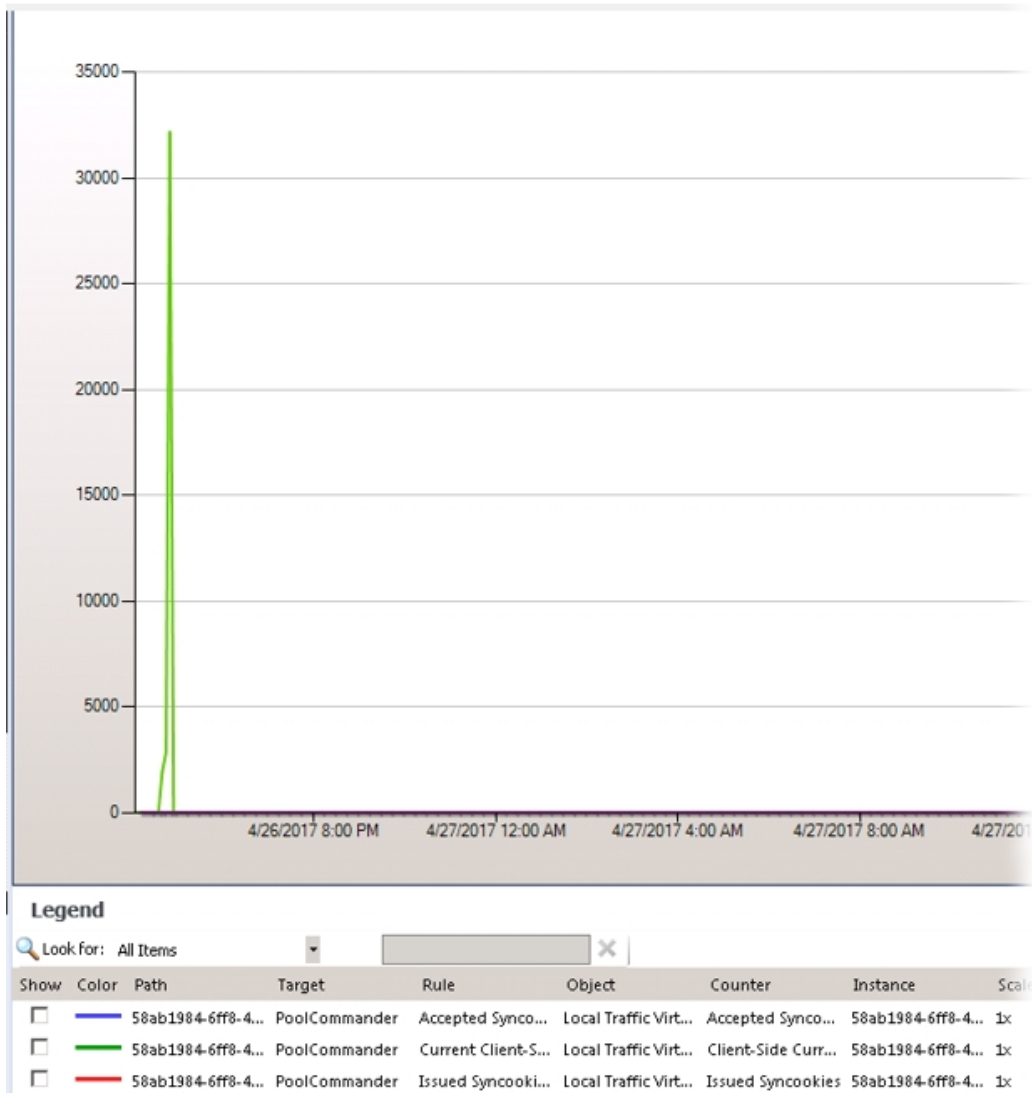


Figure 5-5: Virtual Server Performance Graph

On the pool level, the following metrics are collected:

- Server-Side Current Connections
- Server-Side Max Connections
- Server-Side Total Connections
- Server-Side Bits In Delta (disabled by default starting with product version 4.1)
- Server-Side Bits Out Delta (disabled by default starting with product version 4.1)
- Server-Side Packets In Delta
- Server-Side Packets Out Delta
- Server-Side Inbound Traffic for Local Traffic Pool (in Mbps)
- Server-Side Outbound Traffic for Local Traffic Pool (in Mbps)

Pool Performance graphs can be found in the **Monitoring > F5 BIG-IP (by HYCU) > LTM > Local Traffic Pool Performance** view.

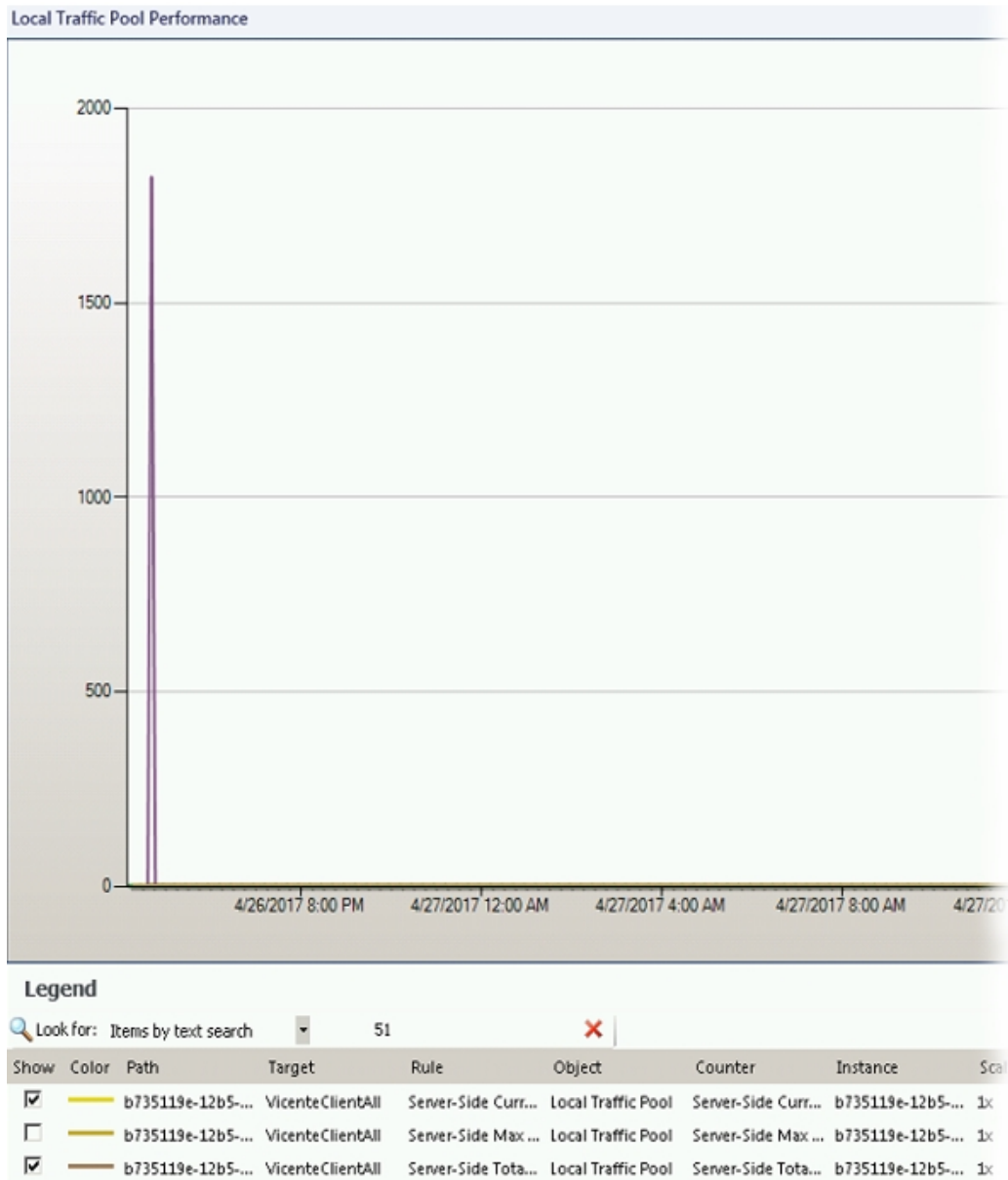


Figure 5–6: Pool Performance Graph

On the pool member level, the following metrics are collected:

- Server-Side Current Connections
- Server-Side Max Connections
- Server-Side Total Connections
- Server-Side Bits In Delta (disabled by default starting with product version 4.1)
- Server-Side Bits Out Delta (disabled by default starting with product version 4.1)
- Server-Side Packets In Delta
- Server-Side Packets Out Delta
- Server-Side Inbound Traffic for Local Traffic Pool Member (in Mbps)
- Server-Side Outbound Traffic for Local Traffic Pool Member (in Mbps)

Pool Member Performance graphs can be found in the **Monitoring > F5 BIG-IP (by HYCU) > LTM > Local Traffic Pool Member Performance** view.

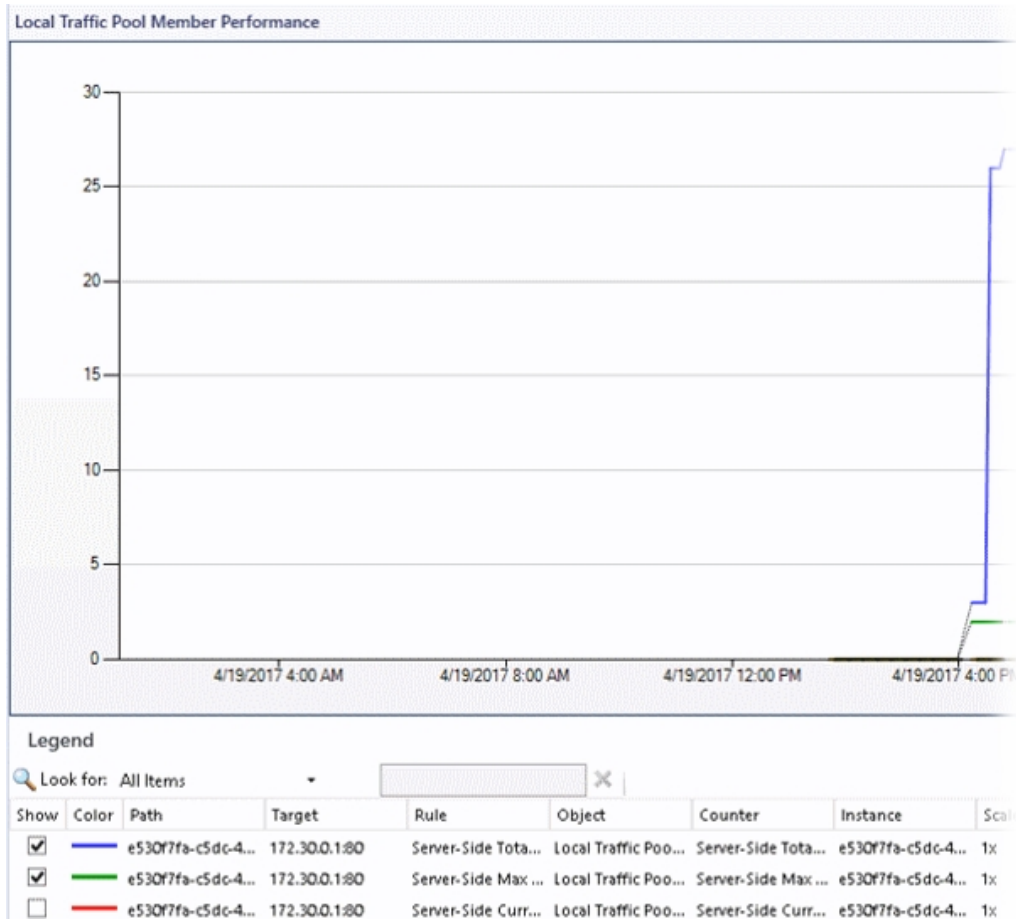


Figure 5-7: Pool Member Performance Graph

HYCU SCOM Management Pack for F5 BIG-IP also monitors health of a sync failover group:

- Number of available devices in Sync Failover Group is below threshold monitor
- Inconsistent states are reported for devices in Sync Failover Group monitor
- Sync Failover Group is not available for monitoring monitor
- Trust between F5 BIG-IP devices might be broken monitor
- F5 Sync Failover Group Configuration monitor
- Alert on Multiple F5 BIG-IP Failover Events rule
- Alert on F5 BIG-IP Failover Event rule

Alert Description

Number of devices that are available in Sync Failover group SFG2 is below predefined threshold.

Currently unavailable devices are:
big-ip11-6-0_supp04.hermes.si (10.49.14.129) is in status 'offline'
f5supp-bgp1160.hermes.si (10.49.39.124) is in status 'offline'

Currently available devices are:
big-ip11-6-0_supp03.hermes.si (10.49.14.128) is in status 'active'

Figure 5–8: Number of available devices in Sync Failover Group is below threshold Alert details

Alert Description

Devices states in Sync Failover Group are inconsistent. This means that devices are reporting different states for each other.

The following devices are members of SFG2 Sync Failover Group:
big-ip11-6-0_supp03.hermes.si (10.49.14.128)
big-ip11-6-0_supp04.hermes.si (10.49.14.129)
f5supp-bgp1160.hermes.si (10.49.39.124)

Figure 5–9: Inconsistent device states in Sync Failover Group Alert details

Alert Description

Sync Failover Group my-sync-failover is unavailable for monitoring.
This means that none of the devices from this sync failover group could be reached by Comtrade F5 BIG-IP MP. Please see Causes section for more details.

The following devices are members of this Sync Failover Group:
bigipv121ha1.hermes.si (10.49.39.147)
bigipv121ha2.hermes.si (10.49.39.146)
bigipv121ha3.hermes.si (10.49.39.145)

Figure 5–10: Sync Failover Group is not available for monitoring Alert details

Alert Description

Following list contains devices that may have broken trust:

Trust broken on:
* bigip1212ha2.hermes.si (10.49.38.120)
Devices reporting to be in trust with device above:
* bigip1212ha1.hermes.si (10.49.38.121)
* bigip1212ha3.hermes.si (10.49.38.118)
* bigip1212sa.hermes.si (10.49.38.117)

Broken trust might cause unexpected behavior such as configuration not being synced among all devices or devices not being able to fail over to one another after the trust is broken.

Figure 5–11: Trust between F5 BIG-IP devices might be broken Alert details



Figure 5–12: F5 BIG-IP Failover Event alert



Figure 5–13: Multiple F5 BIG-IP Failover Events alert



Figure 5–14: F5 Sync Failover Group is not in sync alert

Filtering virtual servers, pools, and pool members

1. In the Authoring pane, navigate to **Management Pack Objects > Object Discoveries**.
2. Locate and right-click **F5 Sync Failover Group Discovery** and select **Overrides >**

Override the Object Discovery > For all objects of class: HYCU F5 BIG-IP Applications.

3. Locate Ignore Pattern and select its **Override** option.

Fill the Override Value text field with one or more regular expressions separated with logical OR.

Example

Regular expression in the Override Value text field

```
^test_|Test12
```

This pattern excludes all virtual servers, pools, and pool members which names begin with test_ or contain Test12. The Ignore Pattern parameter is case sensitive. Identified objects are not discovered and monitored. All objects that are under the excluded object (that is, Pool, and Pool Members for Virtual Server, or Pool Members for Pool) are excluded as well. SSL certificates which belong only to excluded virtual servers are excluded as well. The ASM Statistics dashboard does not show statistics for this object. The ASM Security Policies view and custom state views do not show these objects. HYCU Management Pack for F5 BIG-IP ASM (Reports) filters these objects from the moment you entered a value for the Ignore Pattern parameter.

4. Locate Include Pattern and select its **Override** option.

Fill the Override Value text field with one or more regular expressions separated with logical OR.

Example

Regular expression in the Override Value text field

```
^test_|Test12
```

This pattern causes discovery of only virtual servers, pools, and pool members which names begin with test_ OR contain Test12 are discovered. If the name of virtual server, pool, or pool member matches Include Pattern, but does not match the Ignore Pattern, the object is discovered in SCOM. If the name of Virtual Server, Pool, or Pool Member matches both Include Pattern and Ignore Pattern, the object is not discovered in SCOM. SSL Certificates that are being used by excluded Virtual Servers are not discovered by HYCU SCOM Management Pack for F5 BIG-IP. ASM Statistics Data is not collected for excluded Virtual Servers.

Possibility to choose F5 monitor states which can create alerts

Virtual servers, pools, and pool members can have different states on the F5 BIG-IP device. In HYCU SCOM Management Pack for F5 BIG-IP, choose states which should generate alerts.

1. Navigate to **Authoring > Management Pack Objects > Monitors**.
2. Choose and right-click the Virtual Server, Pool, or Pool Member monitor.
3. Navigate to **Overrides > Override the Monitor**.
4. Choose the objects for which the override should be applied.

Monitor name: F5 LTM Virtual Server Availability State Monitor
 Category: Availability Health
 Overrides target: Class: F5 LTM Virtual Server

Show Monitor Properties...

	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
	<input type="checkbox"/>	Enabled	Boolean	True	True	True	[No change]
	<input type="checkbox"/>	Generates Alert	Boolean	True	True	True	[No change]
▶	<input checked="" type="checkbox"/>	Monitor Black State	Boolean	False	False	False	[Added]
	<input type="checkbox"/>	Monitor Blue State	Boolean	False	False	False	[No change]
	<input type="checkbox"/>	Monitor Red State	Boolean	True	True	True	[No change]
	<input type="checkbox"/>	Monitor Yellow State	Boolean	True	True	True	[No change]
	<input type="checkbox"/>	Synchronization Time	String				[No change]
	<input type="checkbox"/>	Timeout Seconds	Integer	270	270	270	[No change]

Details:

Monitor Black State	Description
The new custom override will be created in the '[Not available]'. Click apply to view the new effective value for this parameter.	Parameter Description: In case that this parameter is set to true, the alert will be created if the virtual server is in state Black. BLACK state means that the virtual server has been disabled.

Management pack

Select destination management pack:

<Select Management Pack> New...

Help OK Apply Cancel

Figure 5-15: Virtual Server Availability State Monitor Override Properties

HYCU Management Pack for F5 BIG-IP LTM (Reports)

To access HYCU Management Pack for F5 BIG-IP LTM (Reports), do the following:

1. In the Monitoring pane, expand **Monitoring** and select **F5 BIG-IP (by HYCU) > LTM**.
2. Select a virtual server in one of the following views:
 - **LTM Diagram View**

- **Device - Local Traffic Virtual Server Dashboard**

- In **Task pane > Report Tasks** choose **Virtual Server Traffic Report**.

This report shows traffic details on a specific virtual server. You can choose to show traffic only during business hours, and select time and days of the week of your business cycle.

Reports contain the following information:

- Sample Count
- Min Value
- Max Value
- Average Value
- Standard Deviation

 Actions

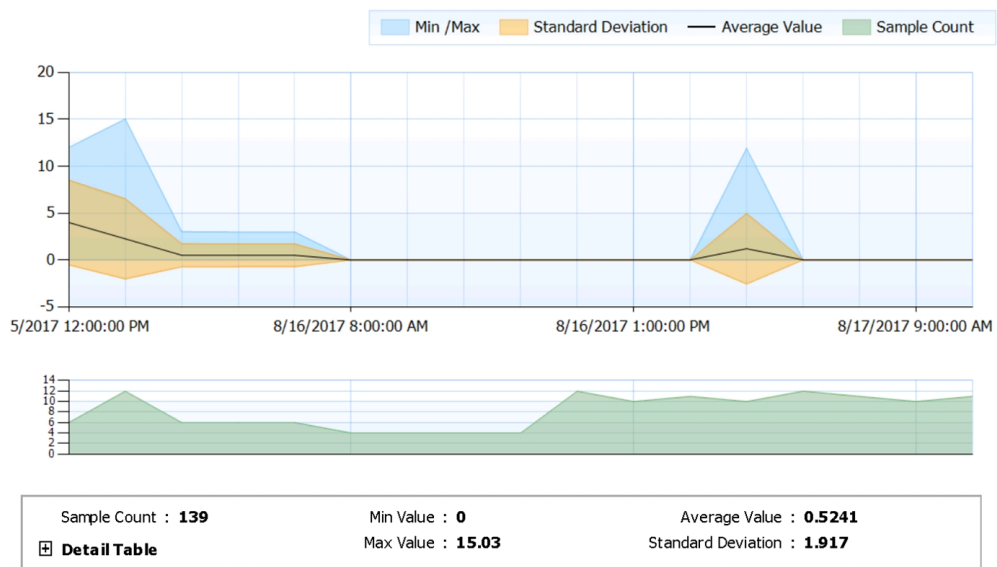


Figure 5-16: Virtual Server Traffic Report

Chapter 6

Monitoring ASM module

ASM Statistics dashboard

F5 BIG-IP Application Security Manager (ASM) protects against OWASP top 10 threats, application vulnerabilities, and zero-day attacks. Choose a device from device list which have ASM module, and then choose all virtual servers configured on that device or a specific virtual server identified by its full name.

Charts contain the following statistical information:

- Number of blocked sessions
- Number of alarmed sessions
- Number of transactions
- Top 5 attack types
- Top 5 requested URL
- Top 5 requesting IP addresses
- Top 5 requesting countries

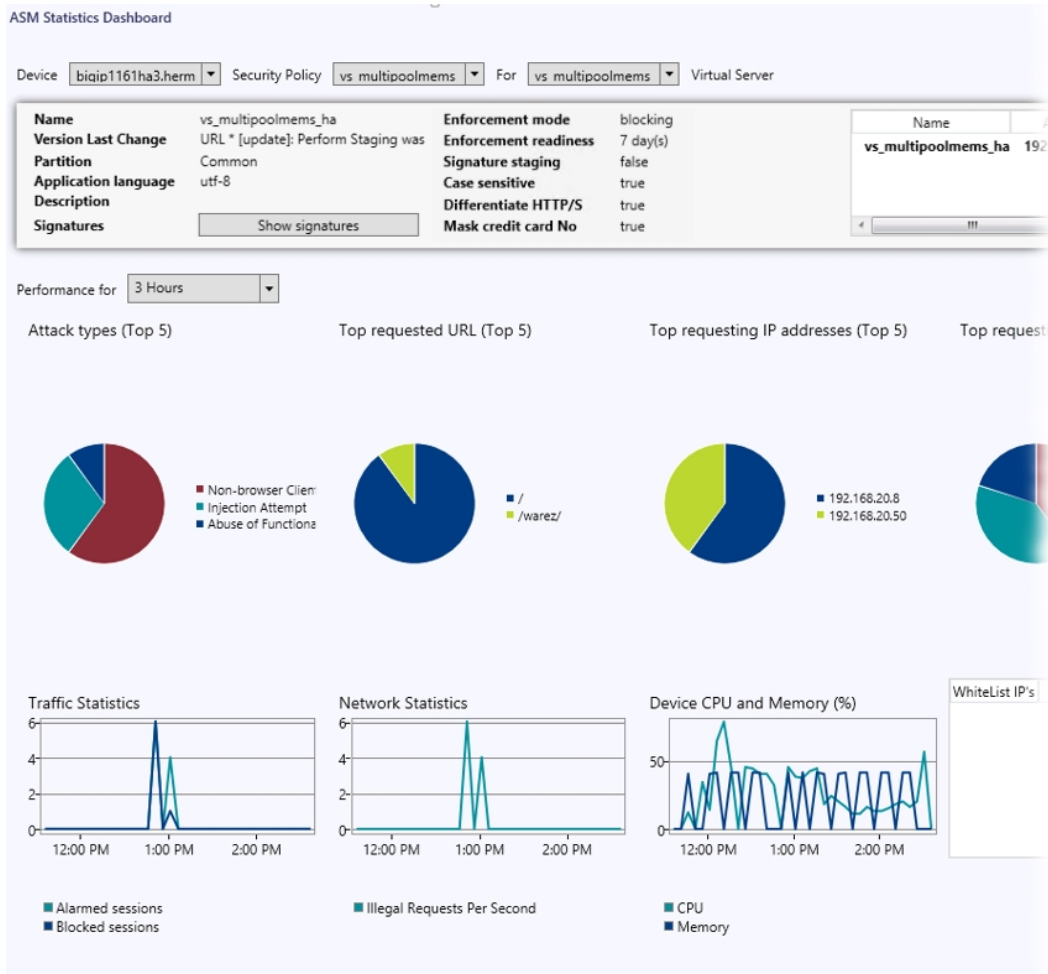


Figure 6–1: ASM Statistics dashboard

ASM Security Policies view

ASM Security Policies view shows all ASM Policies.

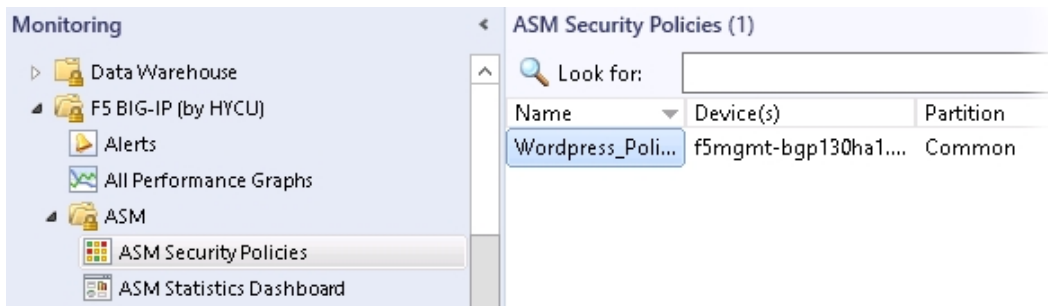


Figure 6–2: ASM Security policies

In the Report Tasks section, select **Configuration Changes** to create the Policies configuration changes report.

Note The following properties are not available in F5 BIG-IP versions earlier than

11.6.0:

- Login Enforcement
- Brute Force Attack Prevention Reference
- Geolocation Enforcement
- Session Tracking Statuses
- Login Pages
- IP Intelligence
- CSRF Settings

HYCU Management Pack for F5 BIG-IP ASM (Reports)

In the Reporting view, click **HYCU Management Pack for F5 BIG-IP ASM (Reports)**.

Available reports are as follows:

- ASM Attacks

This report summarizes ASM attack attempts that occurred in the selected period of time. It presents charts with five most frequent attack types, requested URLs, and request origins (countries, IP addresses). The report also includes tables with a complete list of attack attempts, grouped by attack type. Details about the following are available for each attack attempt: attacked target, attack origin, and attack characteristics.

Columns contain the following information:

- Date and Time
- Device Host Name
- Virtual Server Name
- Virtual Server Endpoint
- Virtual Server Partition
- Requested URL
- Request Origin (Country)
- Request Origin (IP Address)
- Security Policy
- Attack Severity
- Violation Type

Report Time : 5/24/2018 3:09 PM
 Analysis Based on Period : From 4/24/2018 12:53 PM to 5/24/2018 12:53 PM
 Device Host Name : All
 Virtual Server IP Address : All
 Virtual Server Port : All
 Request Origin (Country) : All
 Request Origin (IP Address) : All
 Attack Type : All

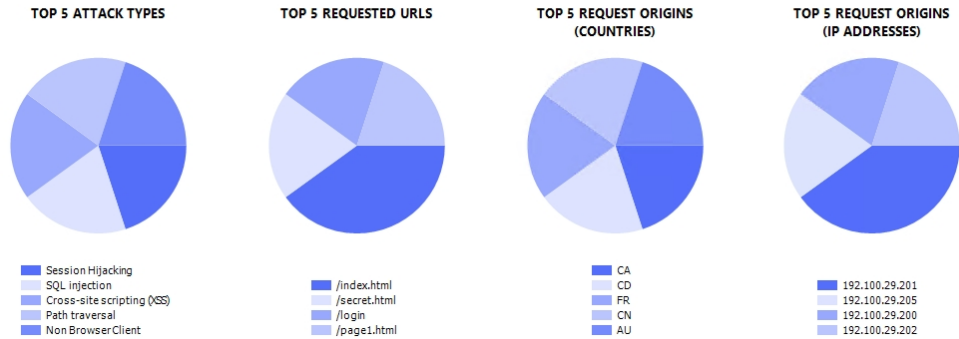


Figure 6-3: Attack report charts

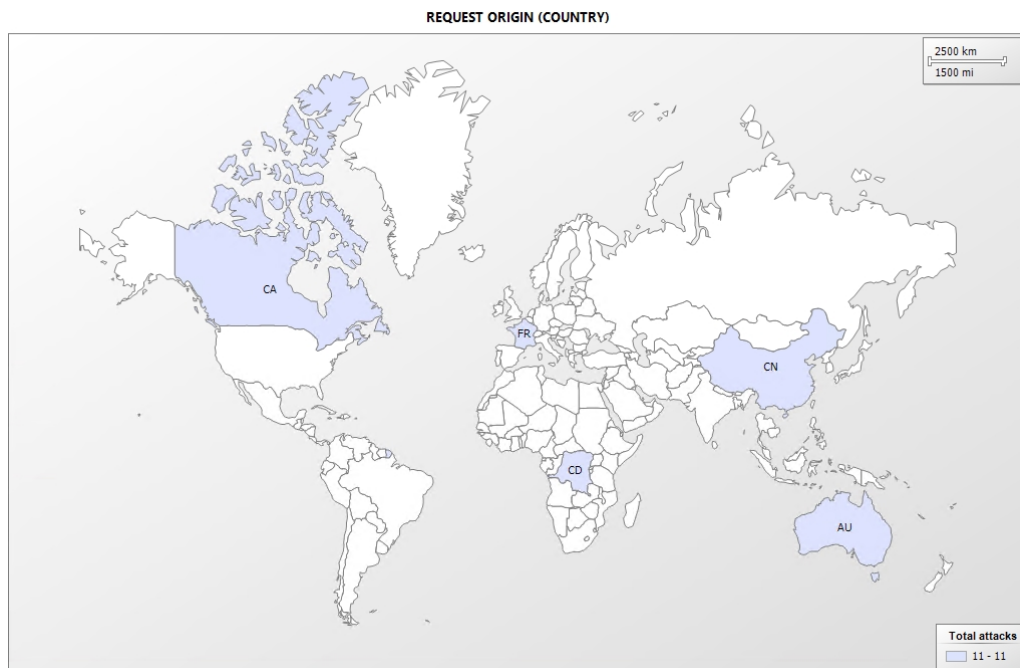


Figure 6-4: Map of attack origins

- ASM User Sessions

This report shows details about all user sessions marked as illegal by ASM on a selected F5 BIG-IP device, filtered by a specific support ID, attack type, and request origin (country and IP address).

Columns contain the following information:

- Date and Time
- Support ID
- Attack Type

- Requested URL
- Request Origin (Country)
- Request Origin (IP Address)
- Enforcement Mode
- Attack Severity
- Violation Type

Chapter 7

Monitoring DNS module

Monitoring wide IPs

HYCU SCOM Management Pack for F5 BIG-IP monitors the availability of F5 DNS Wide IPs. Wide IPs can have different states on the F5 BIG-IP device. In HYCU SCOM Management Pack for F5 BIG-IP, choose states which should generate alerts.

1. Navigate to **Authoring > Management Pack Objects > Monitors**.
2. Choose and right-click the F5 DNS Wide IP Availability State Monitor.
3. Navigate to **Overrides > Override the Monitor**.

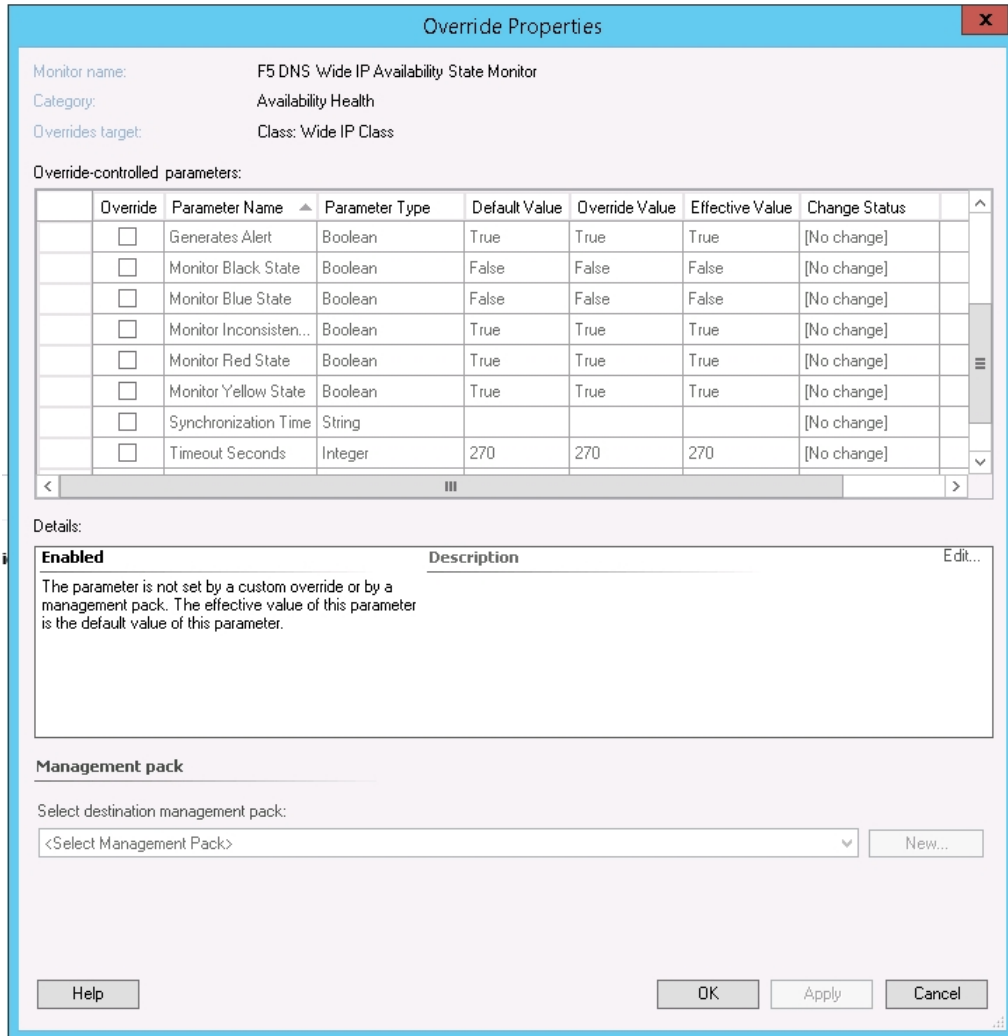


Figure 7-1: F5 DNS Wide IP Availability State Monitor Override Properties



Figure 7-2: Wide IP is in RED state alert

Alert Description

DNS Wide IP /Common/wideip.inconsistent has inconsistent states on some of the devices. Reported states are:

* bigip1161ha3.hermes.si (10.49.39.236): Black because 'No enabled pools available: disabled directly'

* bigip1161ha2.hermes.si (10.49.38.146): Red because 'No enabled pools available'

* bigip1161ha1.hermes.si (10.49.39.240): Black because 'No enabled pools available: disabled directly'

Figure 7-3: Wide IP has different states on some of the devices alert

Wide IP Performance graphs can be found in the **Monitoring > F5 BIG-IP Monitoring > DNS > Wide IP Performance graphs** view.

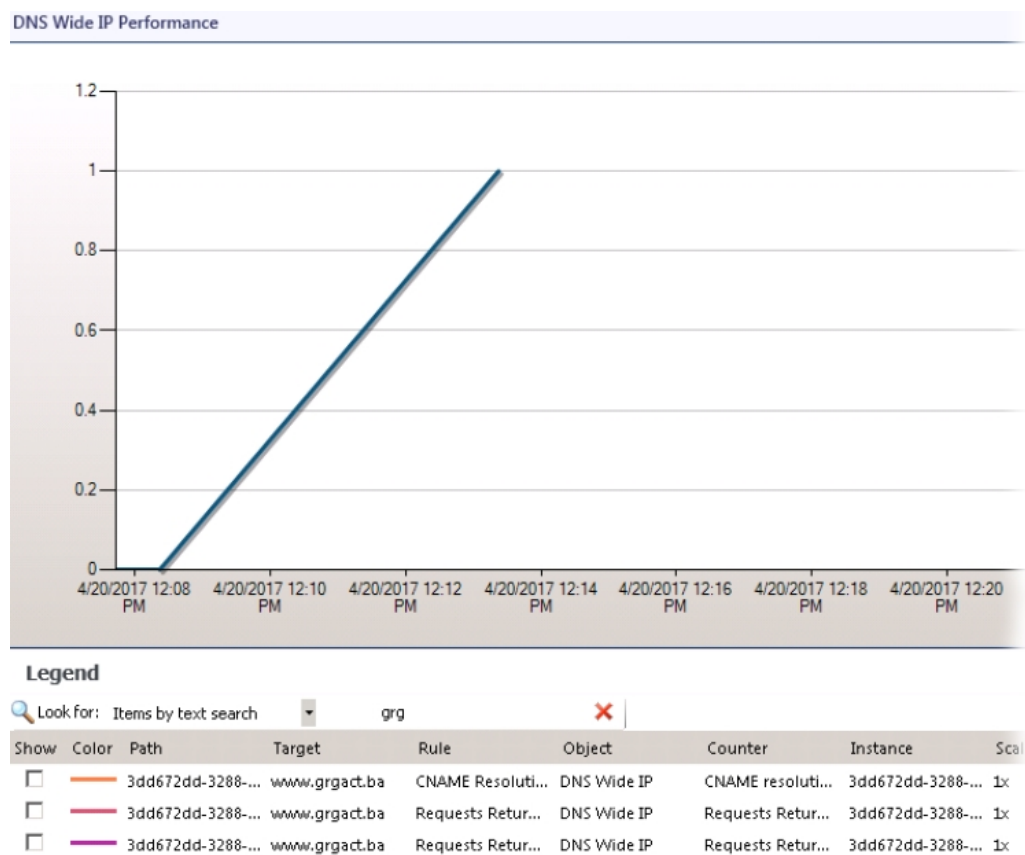


Figure 7-4: DNS Wide IP Performance graphs

Wide IPs view

Wide IPs view shows all Wide IPs and their health states. Wide IPs can be found in the **Monitoring > F5 BIG-IP (by HYCU) > DNS > Wide IPs** view.

Wide IPs (22)

Look for: Find Now Clear

State	Name	Partition	Pool Load Balan...	Ttl Persistence
Critical	marketing.com	Common	round-robin	3600
Critical	marketing.com	Common	round-robin	3600
Critical	BlueWideIp.test...	Common	round-robin	3600
Critical	marketing.com	Common	round-robin	3600
Critical	www.unavailab...	Common	round-robin	3600
Healthy	www.grgact.ba	Common	round-robin	3600
Healthy	www.???-bigip1...	Common	round-robin	3600
Healthy	*.dwa-bigip130....	Common	round-robin	3600
Healthy	cname.ct1.com	Common	round-robin	3600
Healthy	www.dwa-bigi...	Common	round-robin	3600
Healthy	www.???-bigip1...	Common	round-robin	3600
Healthy	www.???-bigip1...	Common	round-robin	3600
Healthy	www.dwa-ct.com	Common	round-robin	3600
Healthy	*.dwa-bigip130....	Common	round-robin	3600
Healthy	Blue.ba	Common	round-robin	3600
Healthy	www.dwa-bigi...	Common	round-robin	3600
Healthy	Blue.ba	Common	round-robin	3600
Healthy	www.dwa-bigi...	Common	round-robin	3600
Healthy	www.grgact.ba	Common	round-robin	3600
Healthy	*dwa?ct.com	Common	round-robin	3600
Healthy	Blue.ba	Common	round-robin	3600
Healthy	*.dwa-bigip130....	Common	round-robin	3600

Detail View

Wide IP properties of marketing.com

Display Name	marketing.com
Full Path Name	bigip130ha1.comtrade.com_default\marketing.com
Name	marketing.com
Partition	Common
Full Path	/Common/marketing.com
Description	
Pool Load Balancing Mode	round-robin
Ttl Persistence	3600

Figure 7-5: Wide IPs view

Some of the F5 BIG-IP Devices in F5 DNS Sync Group are not in sync monitor

Monitors if all F5 BIG-IP Devices in F5 DNS Sync Group are in sync.

Alert Description

Some of the F5 BIG-IP Devices in F5 DNS Sync Group DNSbigip130group are not in sync. The following devices are members of F5 DNS Sync Group:

- * bigip130sa.comtrade.com (10.49.38.27)
- * bigip130ha4.comtrade.com (10.49.37.249)
- * bigip130ha1.comtrade.com (10.49.38.37)
- * bigip130ha2.comtrade.com (10.49.38.36)

Figure 7-6: Some of the F5 BIG-IP Devices in F5 DNS Sync Group are not in sync alert

Chapter 8

Using dedicated Squared Up dashboard pack

General on Squared Up

Squared Up is a Microsoft System Center Operations Manager (SCOM) extension that provides rich operational dashboards. Within a few minutes after the download, your SCOM environment can be transformed with a web console that provides fast HTML5 dashboards, including the Total Dashboard Architecture (TDA) feature. Squared Up dashboard packs transform your management pack (monitoring) data into a set of specialized views. The power of SCOM is then accessible to the entire IT team: application engineering, F5 BIG-IP administrators, and SCOM administrators. To start your free evaluation of Squared Up, go to the [Squared Up Free Trial | Squared Up](#) webpage.

F5 BIG-IP (Comtrade) dashboard pack

The F5 BIG-IP (Comtrade) dashboard pack for Squared Up is a set of dashboards and perspectives of the F5 infrastructure. Squared Up platform gives you the ability to drill down through SCOM objects, interpret performance data, and—in case of alerts—identify their root cause quickly. Dashboards can be easily customized and scoped to a specific health state or object group. F5 BIG-IP (Comtrade) dashboard pack is available free of charge.

F5 Infrastructure

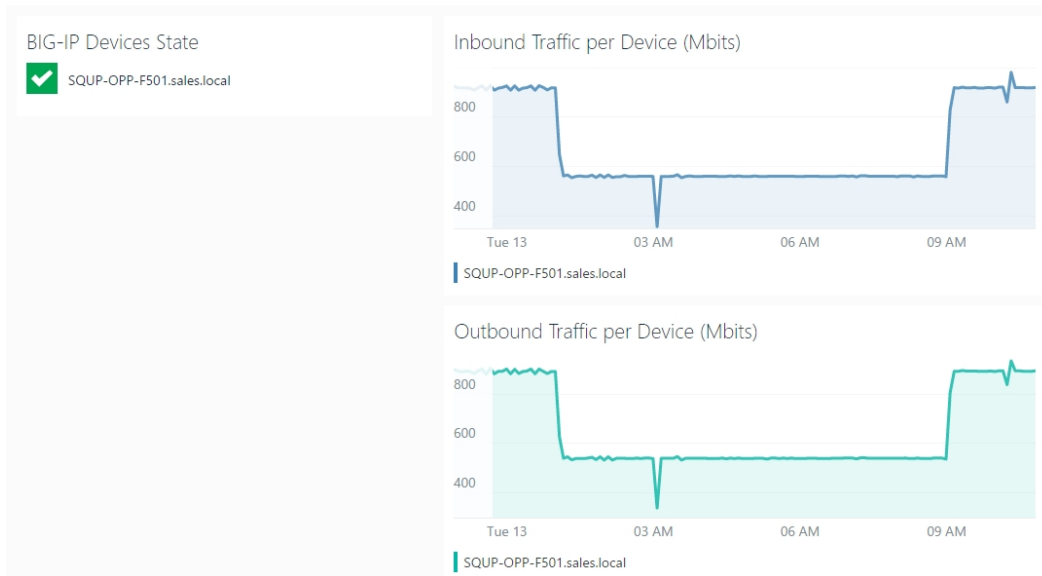


Figure 8-1: Infrastructure Overview dashboard (part 1)

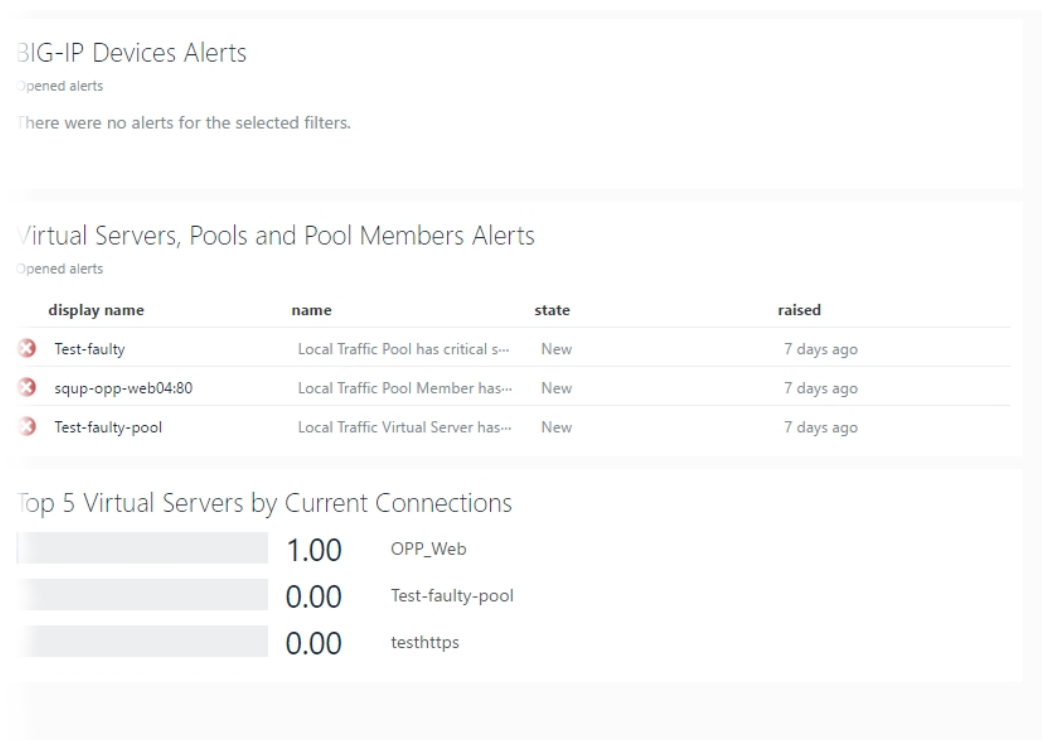
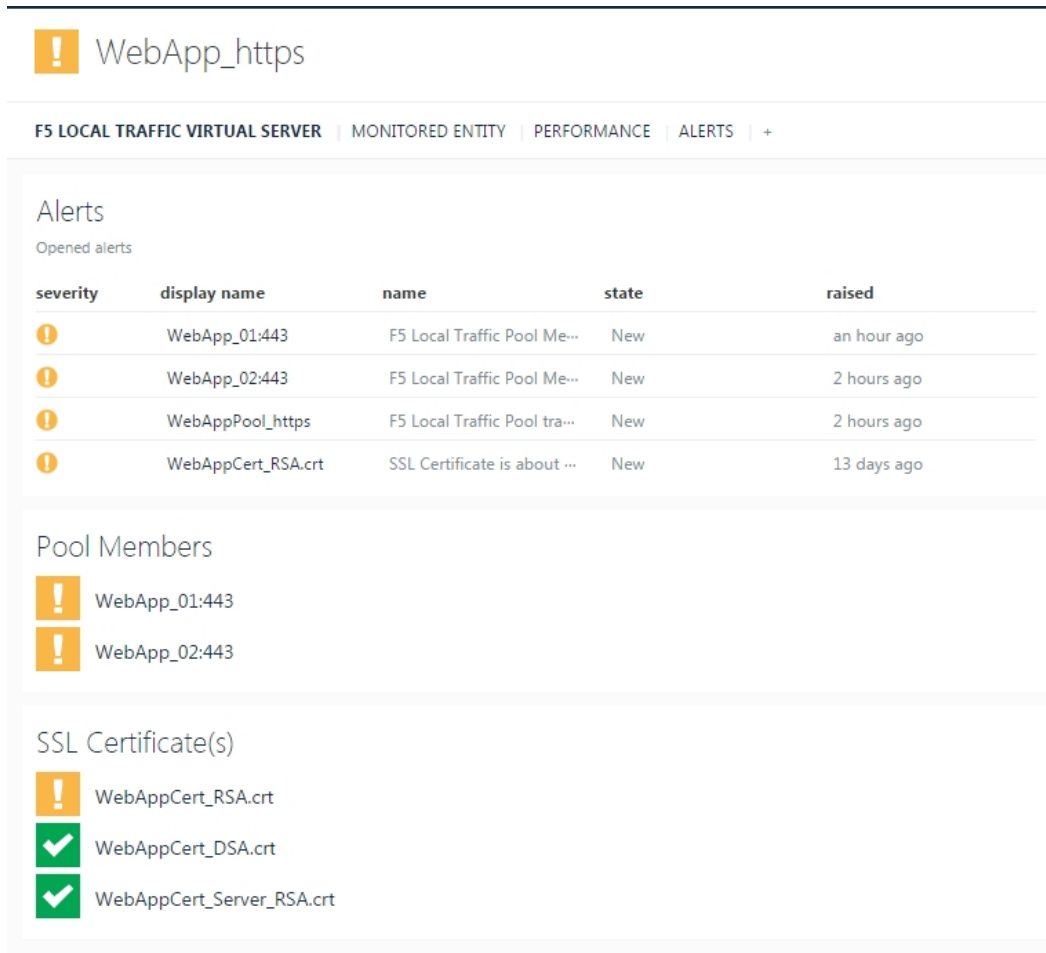


Figure 8-2: Infrastructure Overview dashboard (part 2)







WebApp_https



F5 LOCAL TRAFFIC VIRTUAL SERVER | MONITORED ENTITY | PERFORMANCE | ALERTS | +

Alerts

Opened alerts

severity	display name	name	state	raised
	WebApp_01:443	F5 Local Traffic Pool Me...	New	an hour ago
	WebApp_02:443	F5 Local Traffic Pool Me...	New	2 hours ago
	WebAppPool_https	F5 Local Traffic Pool tra...	New	2 hours ago
	WebAppCert_RSA.crt	SSL Certificate is about ...	New	13 days ago

Pool Members

-  WebApp_01:443
-  WebApp_02:443

SSL Certificate(s)




-  WebAppCert_RSA.crt
-  WebAppCert_DSA.crt
-  WebAppCert_Server_RSA.crt

Figure 8-3: Virtual Server perspective (part 1)

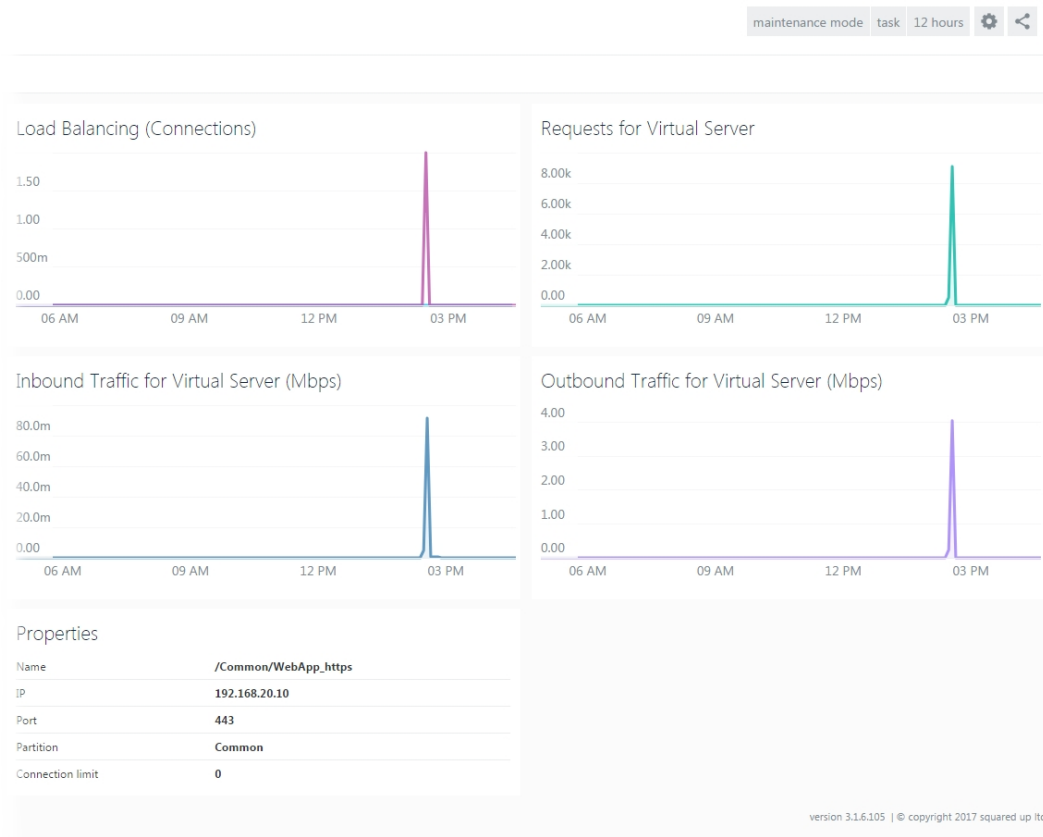


Figure 8–4: Virtual Server perspective (part 2)

Top-level standalone dashboards

F5 Application Delivery Health

F5 Infrastructure Overview

F5 LTM Pool Members Overview

Perspectives

F5 BIG-IP Device

F5 BIG-IP Failover Group or Standalone Device

F5 BIG-IP LTM Pool

F5 BIG-IP LTM Pool Member

F5 BIG-IP LTM Virtual Server

F5 BIG-IP SSL Certificate

Installation prerequisites

The F5 BIG-IP (Comtrade) dashboard pack has the following dependencies on the management packs included in Comtrade SCOM Management Pack for F5 BIG-IP¹:

Management pack	Version
Comtrade Management Pack for F5 BIG-IP ASM (Core)	4.1.4802.0
Comtrade Management Pack for F5 BIG-IP ASM (Reports)	4.1.4802.0
Comtrade Management Pack for F5 BIG-IP Device (Core)	4.1.4802.0
Comtrade Management pack for F5 BIG-IP DNS (Core)	4.1.4802.0
Comtrade Management pack for F5 BIG-IP LTM (Core)	4.1.4802.0

¹ Starting with version 5.3, the product is released under the name HYCU SCOM Management Pack for F5 BIG-IP. Product name is reflected in the names of the included management packs.

Acquiring the dashboard pack

To acquire the F5 BIG-IP (Comtrade) dashboard pack, do one of the following:

- Go to the [F5 BIG-IP \(Comtrade\) - SCOM Dashboard | Squared Up - Community Dashboards](#) webpage.
- If you are already logged in to the Squared Up interface, do the following:
 1. In the top toolbar, click the rightmost icon and select **import dashboard pack** from the menu.
 2. In the Community Section, pause mouse pointer on the **F5 BIG-IP (Comtrade)** entry and click **Install**.

Upon successful installation, the F5 BIG-IP (Comtrade) menu appears in the top toolbar.

For a detailed demo of the F5 BIG-IP (Comtrade) dashboard pack features, watch the [Webinar: F5 BIG-IP Monitoring with Comtrade Software](#) video on YouTube.

Chapter 9

Product information and latest updates

For additional information about SCOM MP for F5 BIG-IP, visit the [SCOM MP for F5 BIG-IP | HYCU](#) webpage.

For the latest product version and most up-to-date documentation, go to the [F5 Monitoring - HYCU](#) webpage.

HYCU Customer Support and information

Use the communication channels listed in this section if you need:

- Help with the product licensing process
- Assistance while using the product
- Additional information about this product
- Information about other HYCU products

Customer Support

Should you require additional information or assistance while using the product, contact the vendor that shipped it.

If you have purchased the product directly from HYCU, and are experiencing a problem, search for a solution on the following webpage:

support.hycu.com

In the absence of an article addressing your problem, ask HYCU Customer Support for assistance: on the webpage, click **Submit a request** and fill in the request form. You must be signed in with a valid account prior to submission. Apply for an account at the following email address:

support@hycu.com

Important: Before submitting a request to the Customer Support department, perform a health check on all systems that are in failed (critical, red) state and have the following information ready:

- Symptoms
- Sequence of events leading to the problem
- Commands and options that you used
- Messages you have received (a description with the date and time)

For a complete list of pieces of required support information, check troubleshooting sections in the product documentation.

Company website and video channel

For more information about our company and other products we offer, visit HYCU website at:

www.hycu.com

For additional product-related information, watch videos on the HYCU channel on YouTube:
www.youtube.com/c/HYCUInc

General information

For questions related to product business or purchase of this or other HYCU products, send an email to:
info@hycu.com

Feedback

For comments or suggestions about this product, including its documentation, send an email to:
info@hycu.com

We will be glad to hear from you!

