F5 201 - BIG-IP TMOS Administration Exam Blueprint Review

Presented by:

August Winterstein (DISA)
Wade Huff (Federal Healthcare)
Stephen Ringo (Army)
Ivan Reyes Mendez (SI)

MARCH 19-20, 2024

The goal:

If you are almost ready, this is an opportunity for a final review and to ask questions. You should already be familiar with BIG-IP and TMOS Administration. We will be covering all blueprint objectives – not the test. We do not have knowledge of the test questions.

Housekeeping

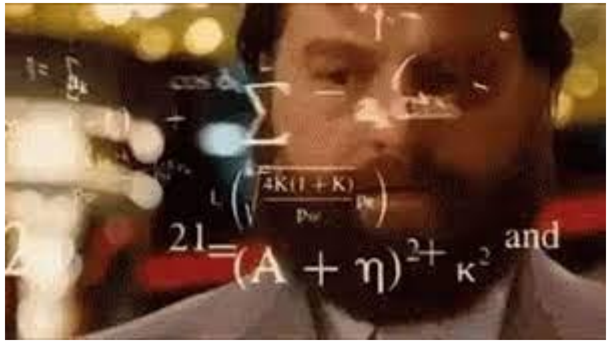
Unified Demonstration Framework (UDF)

F5 Candidate ID

Exam registration

Exam Structure

F5 201 exam – TMOS Administration



- The questions are all multiple choice.
  - There are no true/false questions.
  - There are no “all of the above/none of the above” questions.
- Questions are not adaptive – do not increase/decrease difficulty based on how you are doing
- 80 questions in 90 mins – only 70 scored
- 10 questions will be pilot/beta questions
- Passing score is 245 (70%) out of a range between 100 and 350
- Non-native English-speaking students have an additional 30 minutes!
- No command line engines (although you will have to know a few TMSH commands)

Exam Structure - continued

F5 201 exam – TMOS Administration

Advice:

- Flag long, complicated questions
- View whole exhibit before you close them (attachments)
- Manage Your Time!
- You can flag, review and re-answer questions (within the 90-minute test limit!)

F5 Exams: Multiple Attempt Rules!

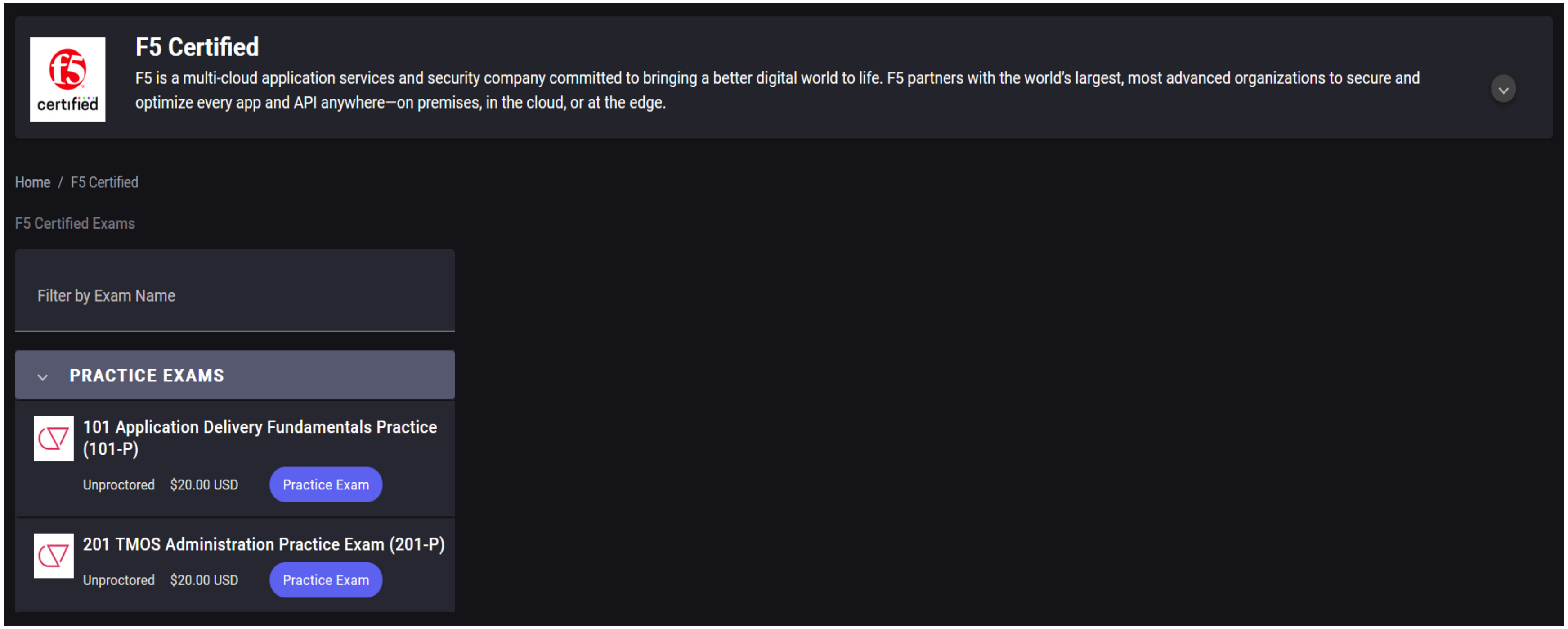
- After first failure, you must wait 15 days to re-test
- After second failure, you must wait 30 days to re-test
- After third failure, you must wait 45 days to re-test
- After fourth failure, you must wait 1 calendar year to re-test
- 5th and subsequent failed attempts, you must wait 90 days

Additional F5 Certification Resources

Exam Summaries and Blueprints: https://my.f5.com/manage/s/article/K29900360

Practice Exams - https://www.certiverse.com/#/store/f5

You will be able to setup account through Cert Program Enrollment Process



F5 Certified

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize every app and API anywhere—on premises, in the cloud, or at the edge.

Home / F5 Certified

F5 Certified Exams

Filter by Exam Name

PRACTICE EXAMS

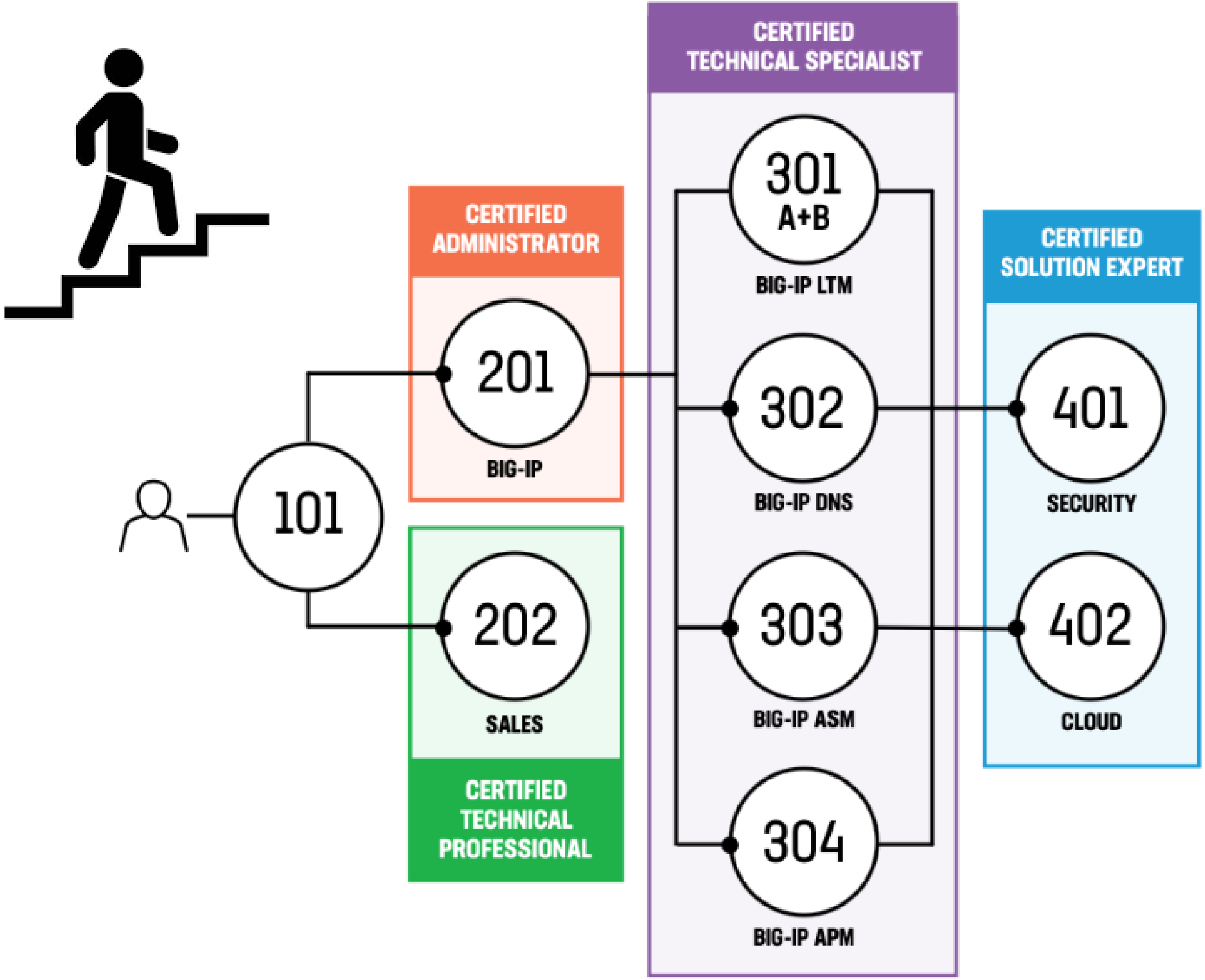
101 Application Delivery Fundamentals Practice (101-P)

Unproctored $20.00 USD

201 TMOS Administration Practice Exam (201-P)

Unproctored $20.00 USD

F5 Certifications & Exams



CERTIFIED ADMINISTRATOR

201 BIG-IP

101

202 SALES

CERTIFIED TECHNICAL PROFESSIONAL

CERTIFIED TECHNICAL SPECIALIST

301 A+B BIG-IP LTM

302 BIG-IP DNS

303 BIG-IP ASM

304 BIG-IP APM

CERTIFIED SOLUTION EXPERT

401 SECURITY

402 CLOUD

F5 offers four certification tracks covering different job roles—Administration, Sales, Product Specialization, and Solutions Engineering. Choose the path that suits your needs and the depth of expertise required for your career or industry.

Administrator Track

Completion of an Administrator track validates that you have the fundamental knowledge necessary to manage, maintain, and do basic fault isolation of previously installed and configured F5 products or solutions.

Technical Professional Track

Completion of a Technical Professional track validates that you have the skills, understanding, and specialized knowledge of F5 solutions, allowing you to more effectively contribute to the F5 ecosystem.

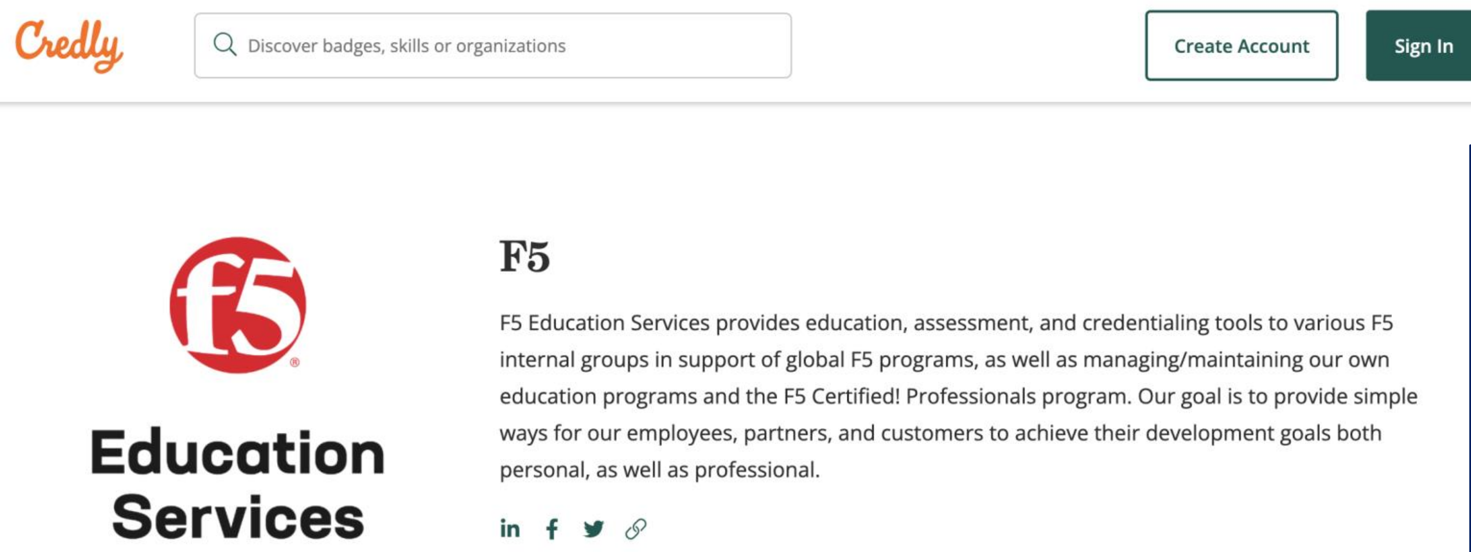
Technical Specialist Track

Completion of a Technical Specialist track validates that you have the expert-level knowledge needed to design, implement, and troubleshoot a specific F5 product as part of an overall solution.

Solution Expert Track

Completion of a Solution Expert track validates that you have the expert-level knowledge needed to architect and design complex, integrated solutions with multiple F5 products and industry standards aligned with business and technical requirements.

F5 Certification Badges



Credly

Discover badges, skills or organizations

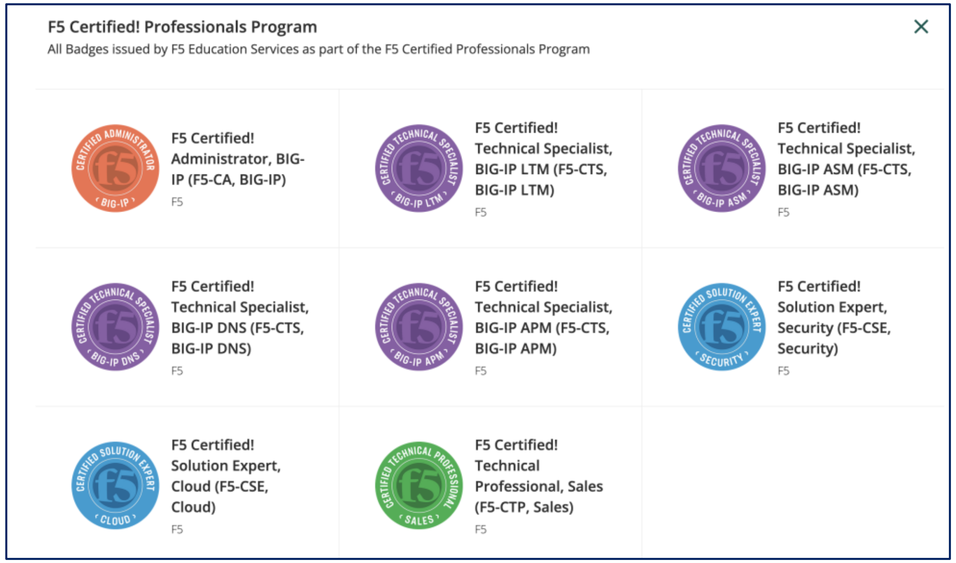
Create Account

Sign In

Education Services

F5

F5 Education Services provides education, assessment, and credentialing tools to various F5 internal groups in support of global F5 programs, as well as managing/maintaining our own education programs and the F5 Certified! Professionals program. Our goal is to provide simple ways for our employees, partners, and customers to achieve their development goals both personal, as well as professional.



F5 Certified! Professionals Program

All Badges issued by F5 Education Services as part of the F5 Certified Professionals Program

- F5 Certified! Administrator, BIG-IP (F5-CA, BIG-IP) — F5
- F5 Certified! Technical Specialist, BIG-IP LTM (F5-CTS, BIG-IP LTM) — F5
- F5 Certified! Technical Specialist, BIG-IP ASM (F5-CTS, BIG-IP ASM) — F5
- F5 Certified! Technical Specialist, BIG-IP DNS (F5-CTS, BIG-IP DNS) — F5
- F5 Certified! Technical Specialist, BIG-IP APM (F5-CTS, BIG-IP APM) — F5
- F5 Certified! Solution Expert, Security (F5-CSE, Security) — F5
- F5 Certified! Solution Expert, Cloud (F5-CSE, Cloud) — F5
- F5 Certified! Technical Professional, Sales (F5-CTP, Sales) — F5

Symposium Exam Info

- Exams on **Thursday 3/21**
- Complimentary practice exam vouchers – email s.lopatin@f5.com

1. Register for the F5 Certified™ program – (https://certification.f5.com/)
    - Must **register BEFORE 3/21** – no same day registrations
2. Create a Certiverse account (https://www.certiverse.com/#/store/F5)
3. Prepare and **bring your own device** (email below if you don't have one)
    - https://help.certiverse.com/portal/en/kb/articles/hardware-requirements
    - No Chromebooks, iPads, or tablets
4. Send an email to the F5 Certified team (support@mail.education.f5.com)

with your Candidate ID (ex. F500001234)

- you'll receive a follow-up email with a link to the Symposium scheduling portal.

Networking

Objectives 1.01 and 2.03

1.01

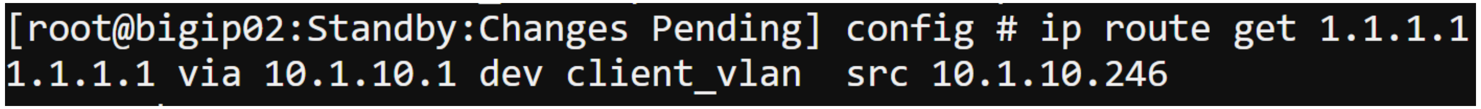
Explain the relationship between interfaces, trunks, VLANs, self-IPs, routes and their status/statistics

- Explain the dependencies of interfaces/trunks, VLANs, self-IPs
- Compare Interface status (Up/Down)
- Illustrate the use of a trunk in a BIG-IP solution
- Demonstrate ability to assign VLAN to interface and/or trunk
- Distinguish between tagged vs untagged VLAN
- Identify, based on traffic, which VLAN/route/egress IP would be used

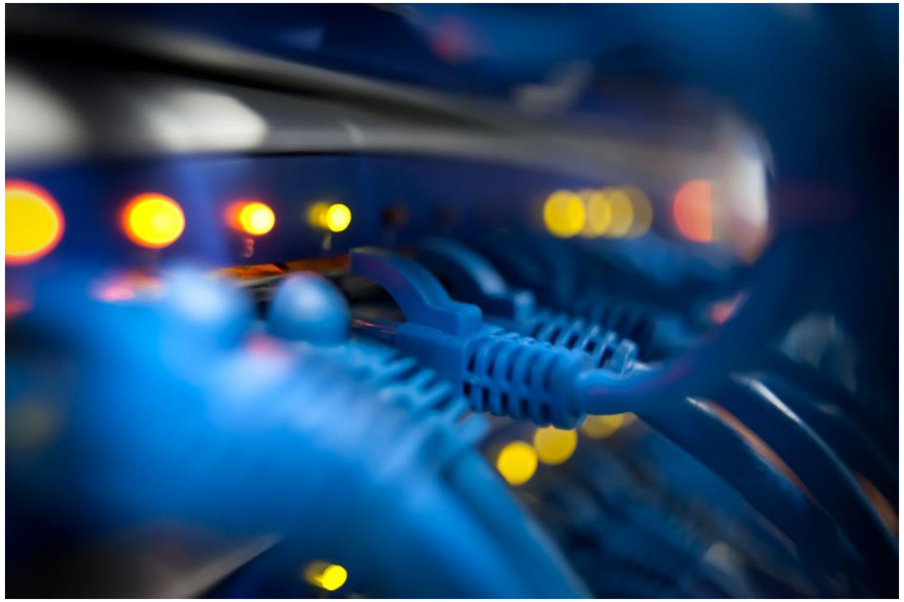
Configuring the network

https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-1-0.html

1. Configure the out-of-band management interface (eth0/mgmt) on the control plane
   - LCD panel (hardware)
   - config command
2. Set up Interfaces and Trunks (L1)
3. Assign interfaces and trunks to VLANs (L2)
4. Assign Self IPs to VLANs (L3)
5. Set up Default Gateway

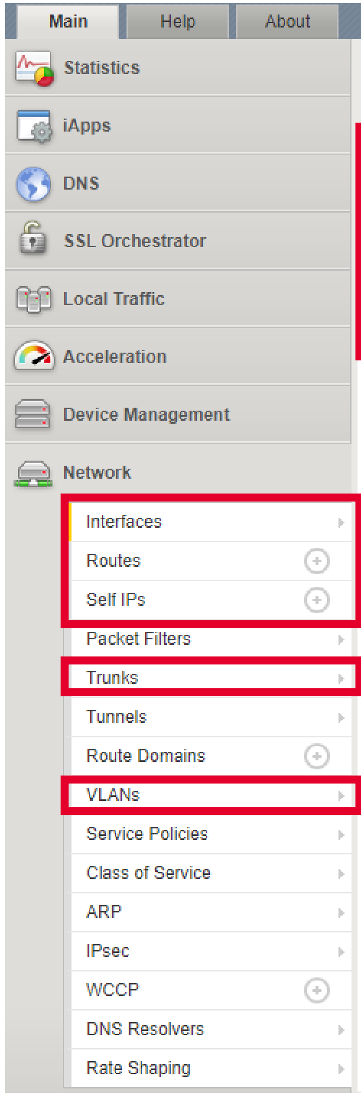


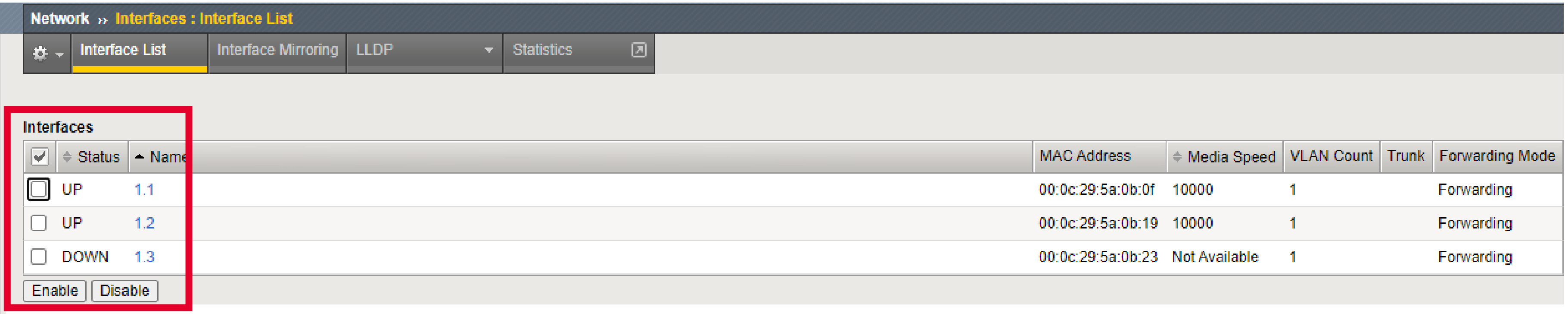
```
[root@bigip02:Standby:Changes Pending] config # ip route get 1.1.1.1
1.1.1.1 via 10.1.10.1 dev client_vlan  src 10.1.10.246
```



Interfaces

[Manual Chapter : Interfaces]



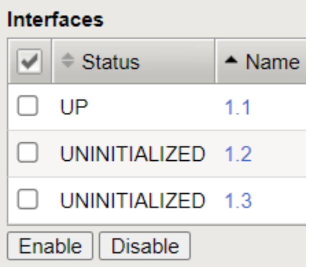


Interfaces

☑	Status	Name	MAC Address	Media Speed	VLAN Count	Trunk	Forwarding Mode
□	UP	1.1	00:0c:29:5a:0b:0f	10000	1		Forwarding
□	UP	1.2	00:0c:29:5a:0b:19	10000	1		Forwarding
□	DOWN	1.3	00:0c:29:5a:0b:23	Not Available	1		Forwarding

Enable Disable

- Control Plane Networking Elements are found on the sidebar
  - You should be familiar with the Interfaces, Routes, Self IPs, Trunks and VLANs selections
  - You can determine interface status and Enable/Disable (state) interfaces
  - Status: UP, DOWN, DISABLED, UNINTIALIZED *(VE Only)*
    - K12697: Initialization of a TMM interface on BIG-IP Virtual Edition
  - Interfaces can also be configured and enabled or disabled via TMSH, for example:
    - `tmsh modify net interface 1.3 { disabled }`



Interfaces

☑	Status	Name
□	UP	1.1
□	UNINITIALIZED	1.2
□	UNINITIALIZED	1.3

Enable Disable

Traffic Management Shell (TMSH)

https://clouddocs.f5.com/cli/tmsh-reference/v13/ with link to Full TMSH Reference Guide PDF

- When does the configuration get written to disk?
  - In the GUI the changes are made to the running configuration and written to disk immediately.
  - In TMSH configuration changes are made to the running configuration, but NOT written to disk
    - A TMSH command is required to save the configuration to disk, or a change made through the GUI will force a write to disk

```
(tmos)# save sys config
Saving running configuration...
  /config/bigip.conf
  /config/bigip_base.conf
  /config/bigip_user.conf
Saving Ethernet mapping...done
```

- Show vs List
  - **show** commands allow you to view runtime information, statistics and status
  - **list** commands allow you to view the running configuration and settings

tmsh vlan examples

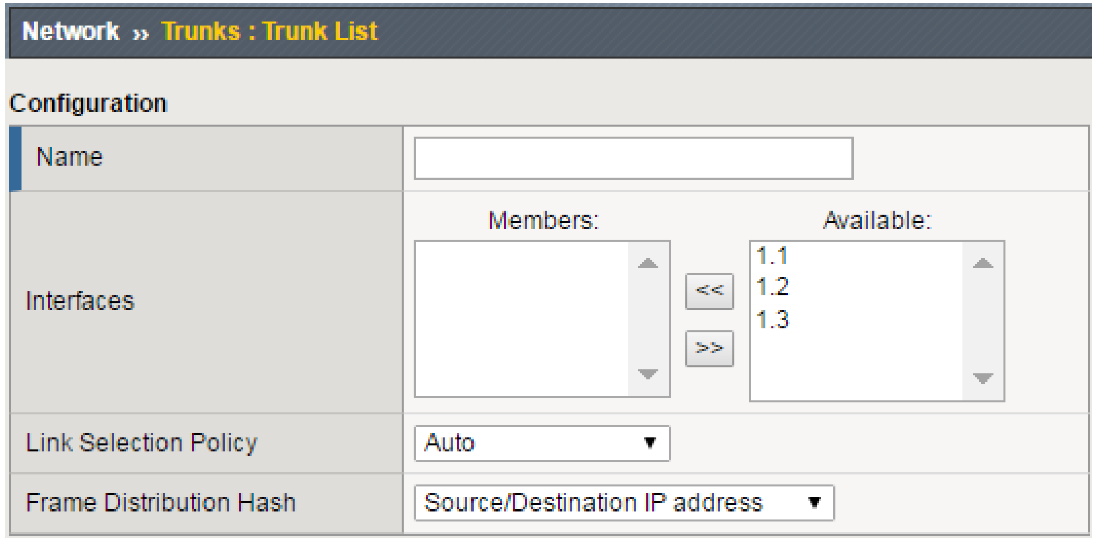
```
(tmos)# list net vlan

net vlan ha_vlan {
    fwd-mode l3
    interfaces {
        1.3 { }
    }
    tag 4092
}
net vlan new_vlan {
    fwd-mode l3
    interfaces {
        1.3 {
            tagged
        }
    }
    tag 30
}
```

```
(tmos)# show net vlan new_vlan

-------------------------------------
Net::Vlan: new_vlan
-------------------------------------
Interface Name      new_vlan
Mac Address (True)  00:0c:29:5a:0b:23
MTU                 1500
Tag                 30

  -----------------------
  | Net::Vlan-Member: 1.3
  -----------------------
  | Tagged     yes

     ----------------------------------------------------------------
     | Net::Interface
     | Name  Status     Bits  Bits  Pkts  Pkts  Drops  Errs      Media
     |                    In   Out    In   Out
     ----------------------------------------------------------------
     | 1.3        up  867.1K  1.1M   652  3.3K      0     0  10000T-FD
```

BIG-IP Trunks

- BIG-IP trunks can be set up as LACP (default) or Etherchannel (Cisco link aggregation)
  - IMPORTANT: A BIG-IP trunk (interface) is not equivalent to a Cisco trunk (VLAN tagging)
    - Cisco terminology uses Port Channel for link aggregation and trunk for 802.1q VLAN tagging

A trunk is created from the Network >> Trunks

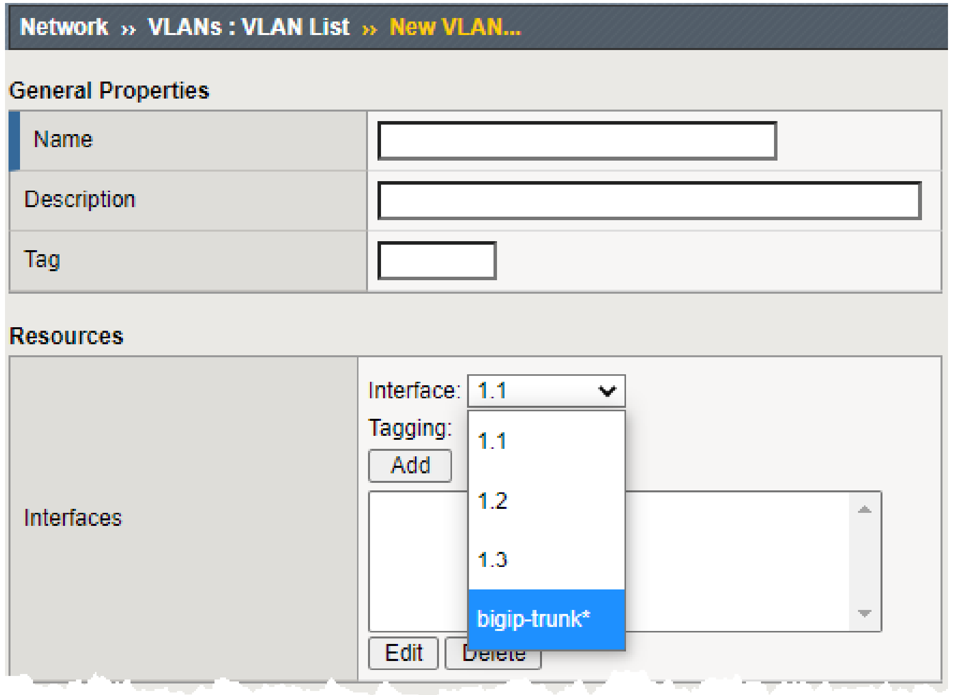


Network » Trunks : Trunk List

Configuration

Name	
Interfaces	Members: Available: 1.1, 1.2, 1.3
Link Selection Policy	Auto
Frame Distribution Hash	Source/Destination IP address

Once created the trunk shows up as an interface



Network » VLANs : VLAN List » New VLAN...

General Properties

Name	
Description	
Tag	

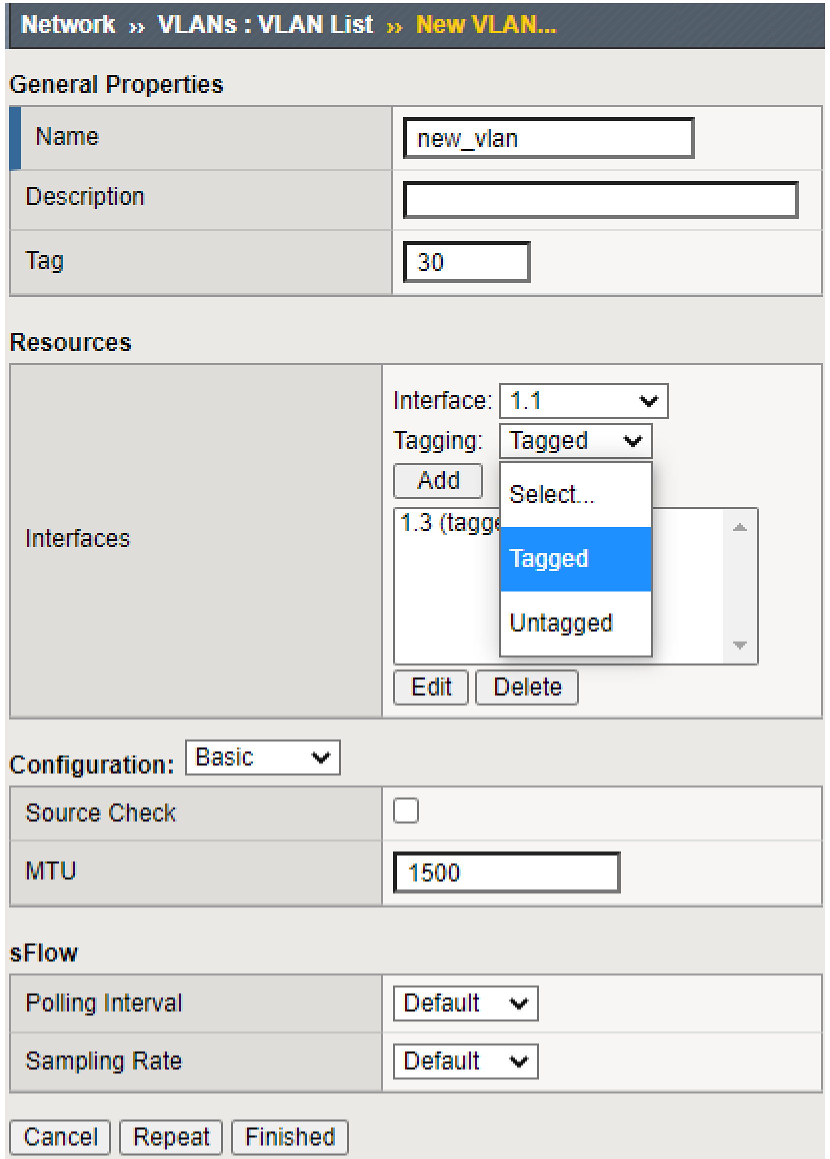
Resources

Interfaces	Interface: 1.1 Tagging:

Tagged vs Untagged VLANs

[Manual Chapter : VLANs VLAN Groups and VXLAN]

- If you wish to have more than one VLAN over the same physical interface or trunk
- Place interfaces and trunks into the Untagged or Tagged boxes
- **Untagged** interfaces do not require a Tag be entered
  - The BIG-IP will assign a Tag to logically separate internal traffic
- **Tagged** interfaces run 802.1q VLAN tagging
  - You need to manually enter the tag



General Properties

Name	new_vlan
Description	
Tag	30

Resources

Interfaces	Interface: 1.1 Tagging: Tagged Add Select... Tagged Untagged 1.3 (tagge Edit Delete

Configuration: Basic

Source Check	☐
MTU	1500

sFlow

Polling Interval	Default
Sampling Rate	Default

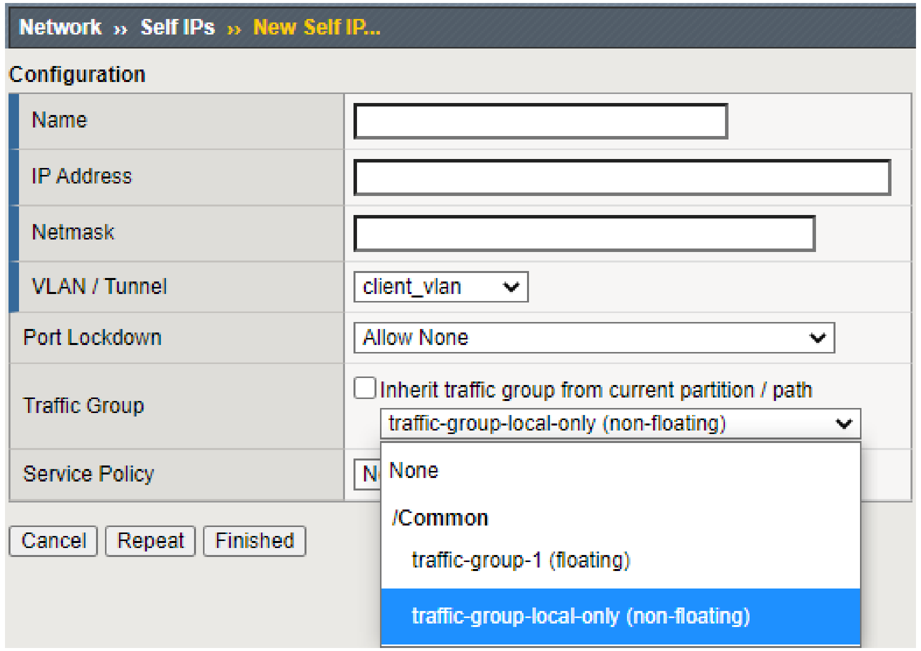
Types of Self IPs

Manual Chapter : Self IP Addresses

- Self IPs have **Port Lockdown (allow none)** configured by default and only respond to ICMP traffic.
- You should understand the difference between floating and non-floating self IPs.
- There are two types of self IP addresses that you can create:
    - A **static (non-floating) self IP** address is an IP address that the BIG-IP system does not share with another BIG-IP system.
        - Any self IP address that you assign to the default traffic group **traffic-group-local-only** is a static self IP address.
        - If the BIG-IP goes down, the static self IPs go down with it.
        - Used for monitoring based on route table
    - A **floating self IP** address is an IP address that two (or more) BIG-IP systems share.
        - Any self IP address that you assign to the default traffic group **traffic-group-1** is a floating self IP address.
        - Or any traffic group that is **NOT** traffic-group-local-only (all other traffic groups are floating)
        - A floating self IP only responds on the Active BIG-IP, if the Active BIG-IP goes down the floating self IP is activated on another BIG-IP in the Device Service Cluster (DSC)

Self IPs

Manual Chapter : Self IP Addresses

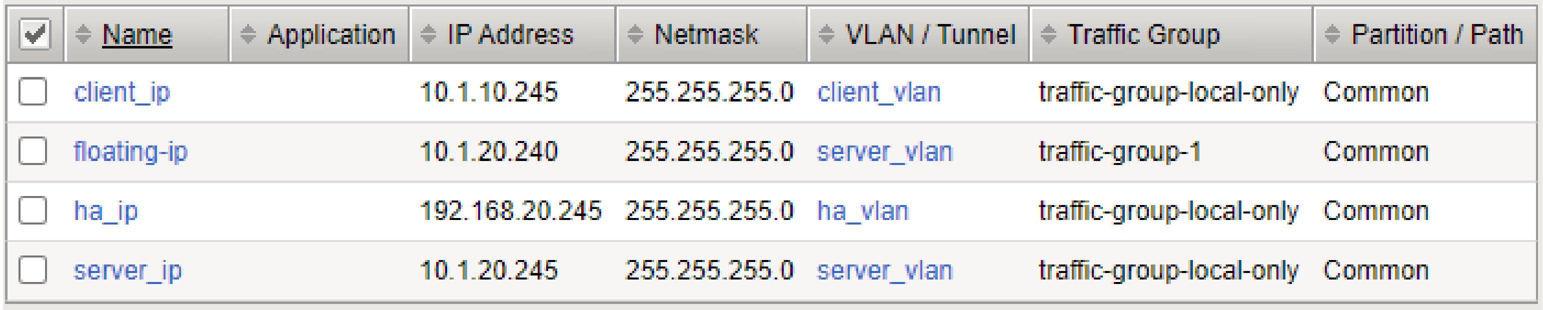


Network » Self IPs » New Self IP...

Configuration

Name	
IP Address	
Netmask	
VLAN / Tunnel	client_vlan
Port Lockdown	Allow None
Traffic Group	□ Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	N

None
/Common
traffic-group-1 (floating)
traffic-group-local-only (non-floating)
Cancel
Repeat
Finished



☑	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
□	client_ip		10.1.10.245	255.255.255.0	client_vlan	traffic-group-local-only	Common
□	floating-ip		10.1.20.240	255.255.255.0	server_vlan	traffic-group-1	Common
□	ha_ip		192.168.20.245	255.255.255.0	ha_vlan	traffic-group-local-only	Common
□	server_ip		10.1.20.245	255.255.255.0	server_vlan	traffic-group-local-only	Common

```
(tmos)# list net self
net self floating-ip {
    address 10.1.20.240/24
    floating enabled
    traffic-group traffic-group-1
    unit 1
    vlan server_vlan
}
net self ha_ip {
    address 192.168.20.245/24
    allow-service {
        default
    }
    traffic-group traffic-group-local-only
    vlan ha_vlan
}
net self server_ip {
    address 10.1.20.245/24
    traffic-group traffic-group-local-only
    vlan server_vlan
}
net self client_ip {
    address 10.1.10.245/24
    traffic-group traffic-group-local-only
    vlan client_vlan
}
```

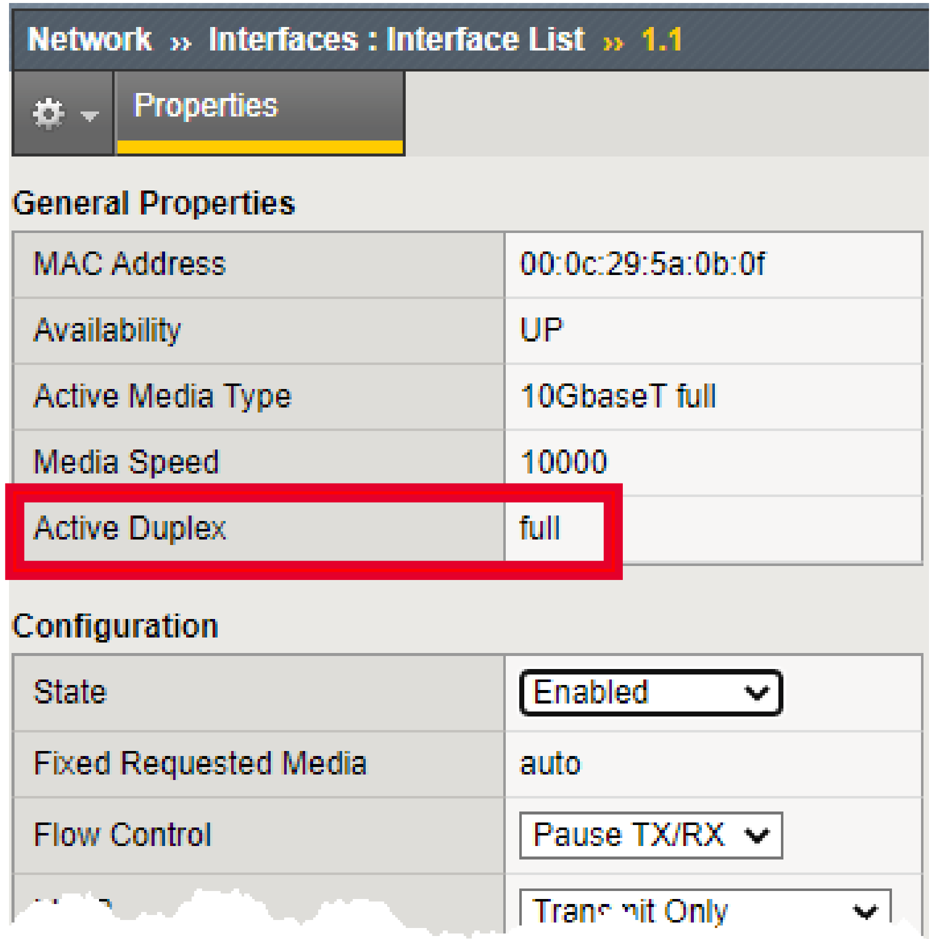
2.03

Identify network level performance issues

- Identify Speed and Duplex
- Distinguish TCP profiles (optimized profiles)
- Identify when a packet capture is needed within the context of a performance issue

2.03 Identify Speed and Duplex

```
(tmos)# list net interface
net interface 1.1 {
    if-index 48
    mac-address 00:0c:29:5a:0b:0f
    media-active 10000T-FD
    media-fixed 10000T-FD
    media-max auto
}
net interface 1.2 {
    if-index 64
    mac-address 00:0c:29:5a:0b:19
    media-active 10000T-FD
    media-fixed 10000T-FD
    media-max auto
}
net interface 1.3 {
    if-index 80
    mac-address 00:0c:29:5a:0b:23
    media-fixed 10000T-FD
    media-max auto
}
net interface mgmt {
    if-index 32
    mac-address 00:0c:29:5a:0b:05
    media-active 100TX-FD
```



Network » Interfaces : Interface List » 1.1

General Properties

MAC Address	00:0c:29:5a:0b:0f
Availability	UP
Active Media Type	10GbaseT full
Media Speed	10000
Active Duplex	full

Configuration

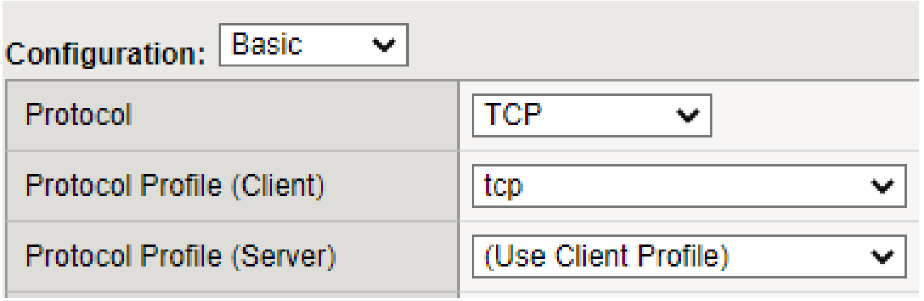
State	Enabled
Fixed Requested Media	auto
Flow Control	Pause TX/RX
	Transmit Only

Be familiar with where things are in the GUI.

2.03 Distinguish TCP profiles (optimized profiles)

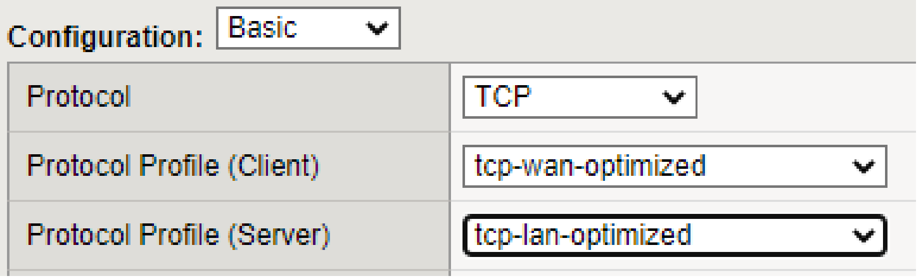
Manual Chapter : Protocol Profiles

K10711911: Overview of the TCP profile (13.x)



Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)



Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp-wan-optimized
Protocol Profile (Server)	tcp-lan-optimized

- tcp-lan-optimized and f5-tcp-lan profiles
  - pre-configured profiles for LAN-based or interactive traffic
- tcp-wan-optimized and f5-tcp-wan profiles
  - pre-configured profile types for traffic over a WAN link
- tcp-mobile-optimized profile
  - pre-configured with default values set to give better performance to service providers' 3G and 4G customers.
- mptcp-mobile-optimized profile (Multipath TCP)
  - pre-configured profile type for use in reverse proxy and enterprise environments for mobile applications that are front-ended by a BIG-IP system

2.03 Identify when a packet capture is needed within the context of a performance issue

K411: Overview of packet tracing with the tcpdump utility

- BIG-IP is a full proxy. Two *separate* tcpdumps (one on each side of the proxy) are often needed.
  - Can by done by opening two SSH sessions, or running the dumps in background (&)
  - Note - be very careful running tcpdumps in the background! (fg brings to foreground)
- When a tcpdump is required, always make it as specific as possible
  - Limit it to the appropriate interfaces/VLANs and hosts/ports
  - -i 0.0 captures on all ints except mgmt

```
system# tcpdump –i external –eX host 10.10.10.10 and port 80
```

```
system# tcpdump –i (1.1, f5_trunk1, external, 0.0) –eX –w /var/tmp/dump.cap
```

Troubleshooting Tools

- Curl Utility - http://curl.haxx.se/
  - ***curl*** *is a command line tool for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP.*
  - *It is supported on BIG-IP and is great for troubleshooting connectivity and monitors*

curl http://www.mysitename.com

curl http://10.128.20.11

```
[root@bigip249] config # curl -i 10.128.20.11
HTTP/1.1 200 OK
Date: Wed, 06 Aug 2014 20:05:13 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.4.9-4ubuntu2.2
Vary: Accept-Encoding
Content-Length: 3819
Connection: close
Content-Type: text/html

<html>
<head>
<TITLE>Using virtual server 10.128.20.11 and pool member 10.128.20.11 (Node
#1)</TITLE>
<meta http-equiv="Content-Type" content="text/html; charset=us-ascii" />
 <script language="javascript">
    …………………
 </script>
```

BIG-IP Traffic Flow

Objective 1.02

1.02

Determine expected traffic behavior based on configuration

- Determine the egress source IP based on configuration
- Consider the packet and/or virtual server processing order (wildcard vips)
- Identify traffic diverted due to status of traffic objects (vs, pool, pool member)
- Identify when connection/rate limits are reached
- Identify traffic diverted due to persistence

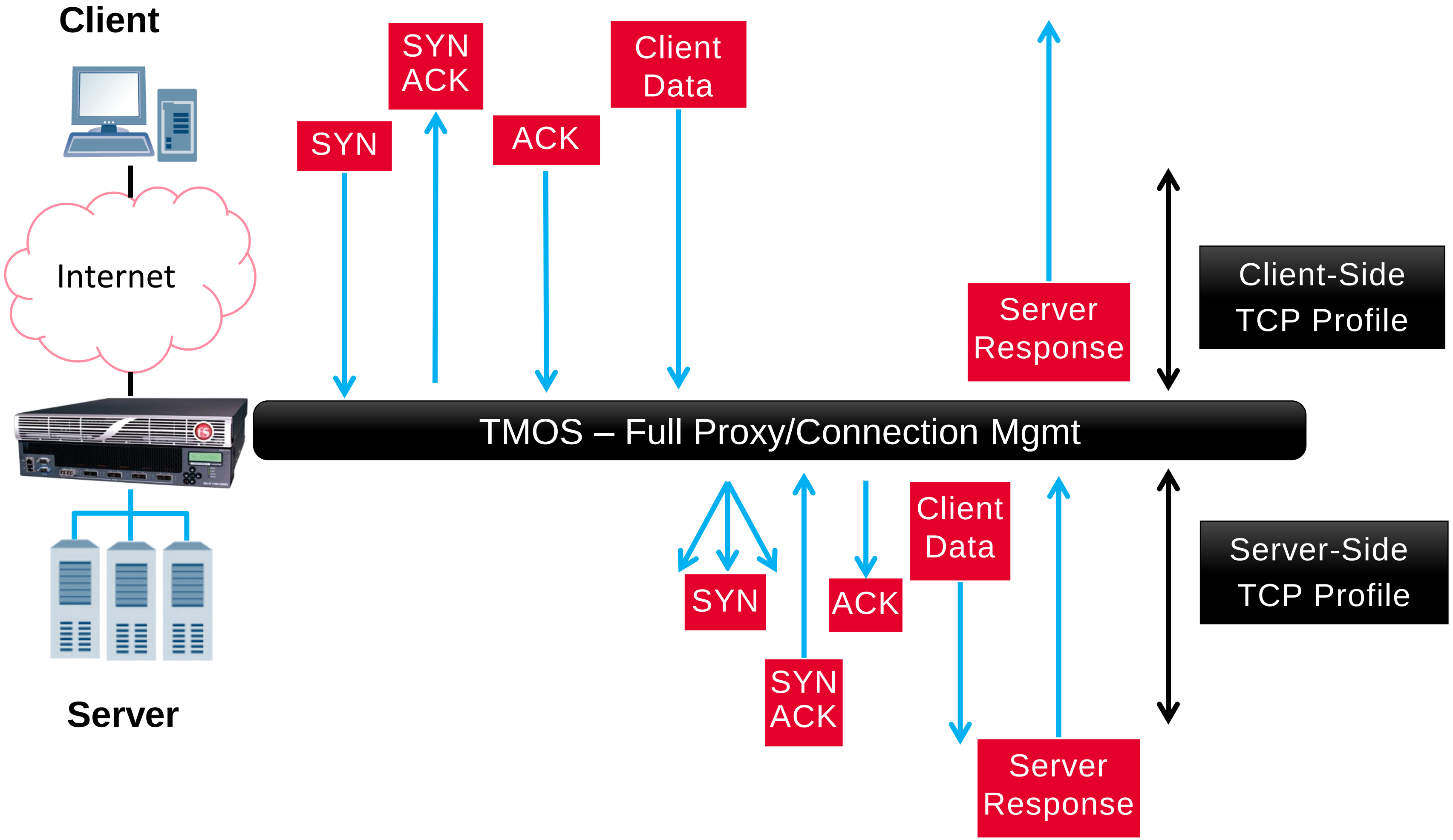
1.02 Determine the egress source IP based on configuration

Traffic Flow through the BIG-IP

- TMOS is a full proxy architecture
- **Routed mode** (recommended)
  - Servers are on an internal network behind the BIG-IP
  - The BIG-IP is the default gateway for the servers
- **Secure Network Address Translation (SNAT) Mode**
  - The BIG-IP translates the original source IP, to an IP address owned by the BIG-IP
  - Allows a BIG-IP to be inserted into existing networks without changing the existing IP address structure
  - Can be used to create One-Armed/Single-Network mode

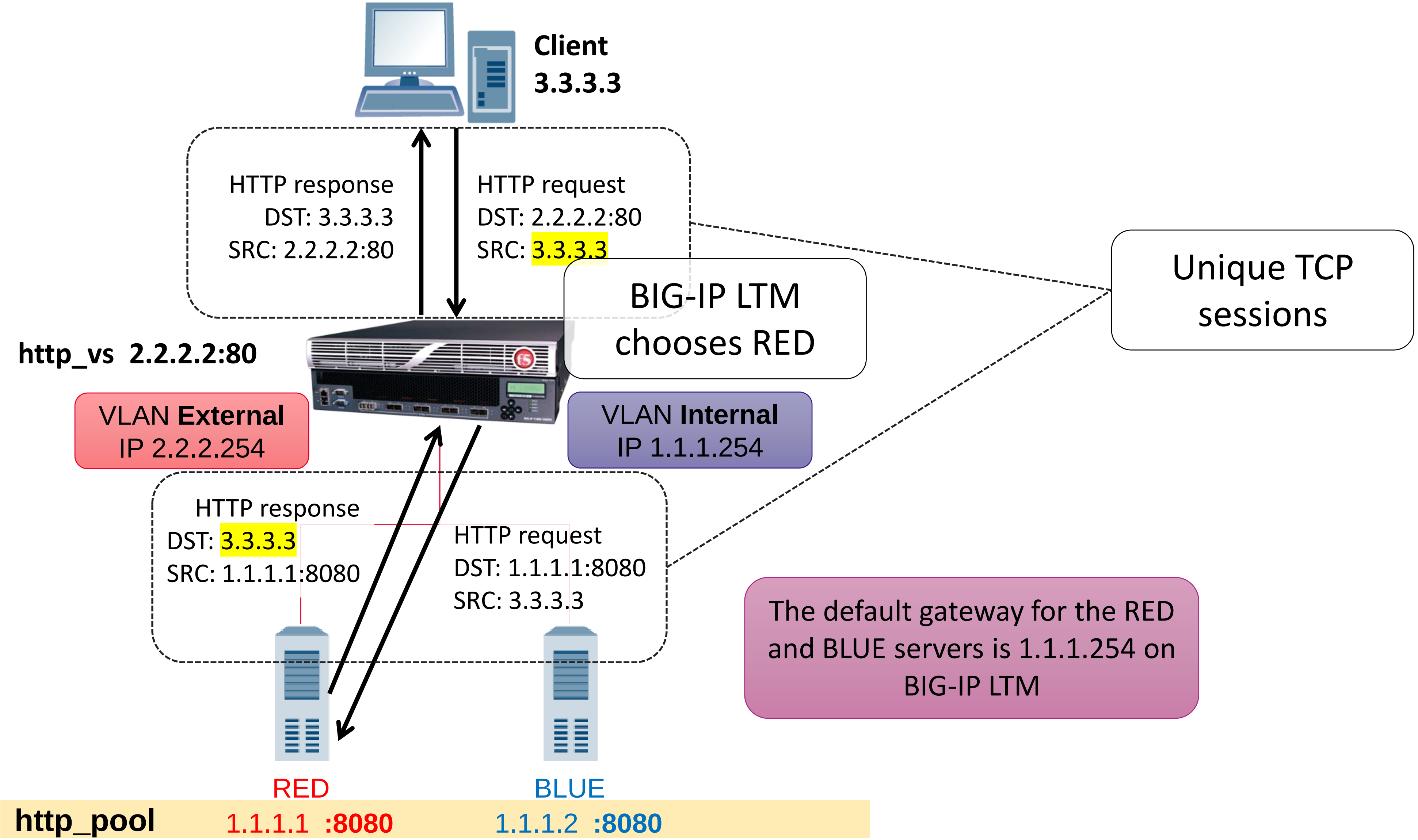
TMOS – Full proxy Architecture

- Remember there are always two connections to a transaction.
- The BIG-IP connection table contains information about all the sessions currently established on the BIG-IP system.
  - Can be displayed via TMSH
  - Shows client-side/server side connection pairs



Traffic flow through BIG-IP when BIG-IP is the default gateway

Routed mode



Client
3.3.3.3

HTTP response
DST: 3.3.3.3
SRC: 2.2.2.2:80

HTTP request
DST: 2.2.2.2:80
SRC: 3.3.3.3

Unique TCP sessions

BIG-IP LTM chooses RED

http_vs 2.2.2.2:80

VLAN **External**
IP 2.2.2.254

VLAN **Internal**
IP 1.1.1.254

HTTP response
DST: 3.3.3.3
SRC: 1.1.1.1:8080

HTTP request
DST: 1.1.1.1:8080
SRC: 3.3.3.3

The default gateway for the RED and BLUE servers is 1.1.1.254 on BIG-IP LTM

	RED	BLUE
http_pool	1.1.1.1 **:8080**	1.1.1.2 **:8080**

NATs and SNATs

Manual Chapter : NATS and SNATs

- You can create **NAT**s on a BIG-IP
  - NAT is an address translation object to translate one IP address in a packet header to another IP address.
    - Consists of a one-to-one mapping of a public IP address to an internal private class IP address.
    - All ports are open
- Much more common and important are **SNAT**s, **understanding how SNATs work is key**.
- A *secure network address translation (**SNAT**)* is a BIG-IP Local Traffic Manager™ feature that translates the source IP address within a connection to a BIG-IP system IP address that you define. The destination node then uses that new source address as its destination address when responding to the request.
  - Can map multiple original addresses to a single translation address
  - Only the source can use the translation to establish connections
  - Only supports TCP and UDP by default
    - This makes SNATs more secure than NATs

SNATs – How they are used

Manual Chapter : NATS and SNATs

- **When the default gateway of the server node is not the BIG-IP system**.
  - This is a very common scenario.
- **When clients and servers are on the same network.**
  - For example, web servers talking to applications or databases
- **SNATs for server-initiated (outbound) connections.**
  - Allow servers to access outside resources safely.

SNAT Automap and Self IP Selection

K7336: The SNAT Automap and self IP address selection

- SNAT Automap uses the Self-IPs already assigned to the BIG-IP VLANs for translation.
  - SNATs are almost always assigned at the virtual server level
- SNAT Automap selects a translation address from the available self IP address in the following order of preference:

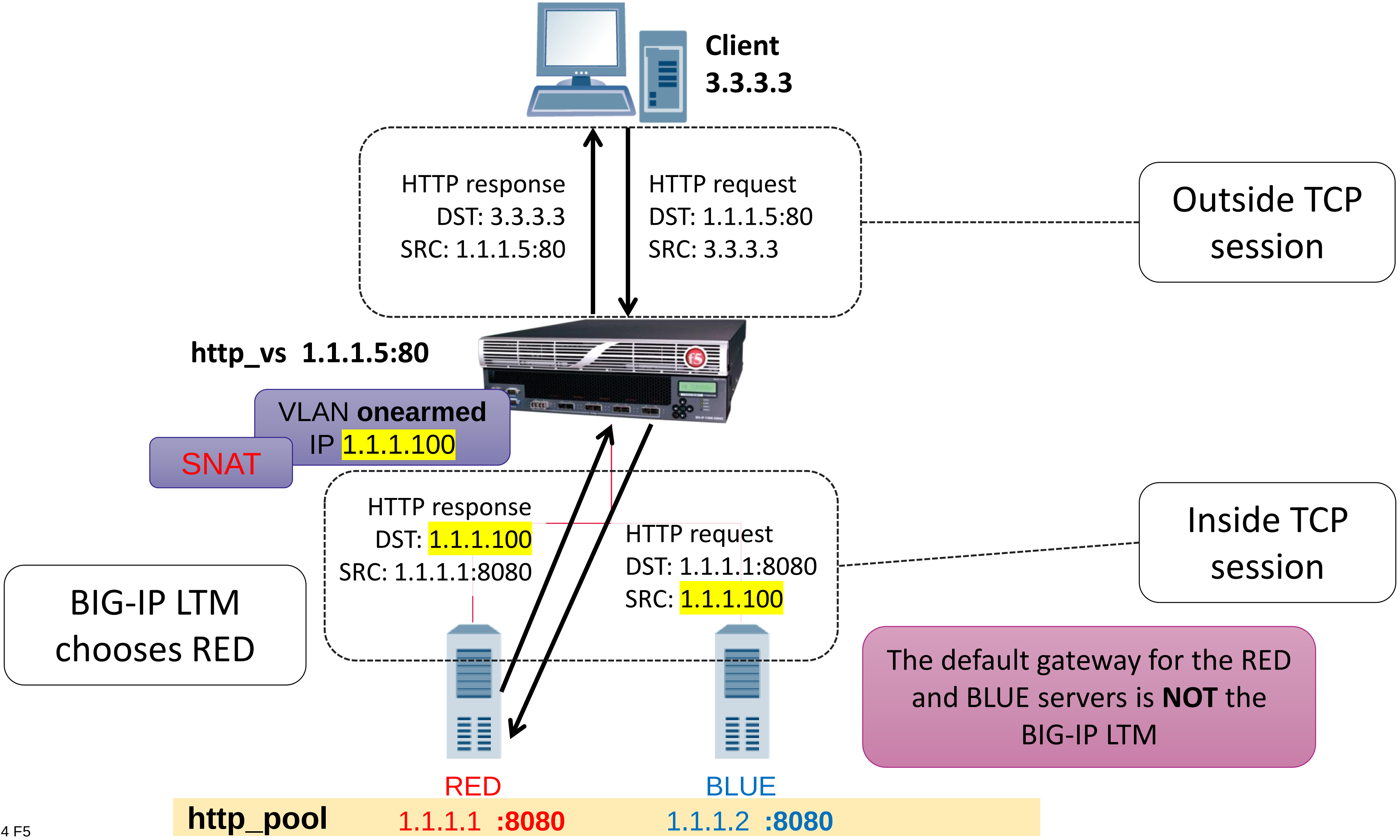
1. **Floating self IP addresses on the egress VLAN**
2. Floating self IP addresses on different VLANs
3. **Non-floating self IP addresses on the egress VLAN**
4. Non-floating self IP addresses on different VLANs

SNAT Pools

RECOMMENDED READING: K7820: Overview of SNAT features

- SNAT uses ports to separate client connections
  - More than roughly 65000 concurrent connections will exhaust the ports of a single SNAT'd IP
    - Note: BIG-IP Cluster Multiprocessing (CMP) can cause this limit to be exceeded, but always plan using this as the maximum
  - This is also known as port overload
  - Once the ports are exhausted connections will be dropped.
    - K8246: How the BIG-IP system handles SNAT port exhaustion
- SNAT Pools must be used if the concurrent connections will exceed this limit.
  - You will need enough IPs in the pool to handle the maximum number of concurrent connections.
- An additional benefit of SNAT pools is that they failover seamlessly if SNAT mirroring is selected.
  - SNAT mirroring mirrors the SNAT IP address and port utilized to the next active device in the cluster.

Traffic flow through BIG-IP when SNATs are used



Client
3.3.3.3

HTTP response
DST: 3.3.3.3
SRC: 1.1.1.5:80

HTTP request
DST: 1.1.1.5:80
SRC: 3.3.3.3

Outside TCP session

http_vs 1.1.1.5:80

VLAN **onearmed**
IP 1.1.1.100

SNAT

HTTP response
DST: 1.1.1.100
SRC: 1.1.1.1:8080

HTTP request
DST: 1.1.1.1:8080
SRC: 1.1.1.100

Inside TCP session

BIG-IP LTM chooses RED

The default gateway for the RED and BLUE servers is **NOT** the BIG-IP LTM

RED

BLUE

http_pool 1.1.1.1 **:8080** 1.1.1.2 **:8080**

1.02 Consider the packet and/or virtual server processing order (wildcard VIPs)

K9038: The order of precedence for local traffic object listeners

Packet Processing Priority

1. Existing connection in connection table
2. AFM/Packet filter rule
3. Virtual server
4. SNAT
5. NAT
6. Self-IP
7. Drop

Virtual Server Order of Precedence

K14800: Order of precedence for virtual server matching (11.3.0 and later)

- Understand how a virtual server processes a request
  - Precedence is from most specific to least specific
- The BIG-IP system uses an algorithm that places virtual server precedence in the following order:
  - Destination address
    - Which virtual address (IP) is most specific?
  - Source address
    - Is the source address permitted to access the virtual address?
  - Service port
    - What is the most specific port match?

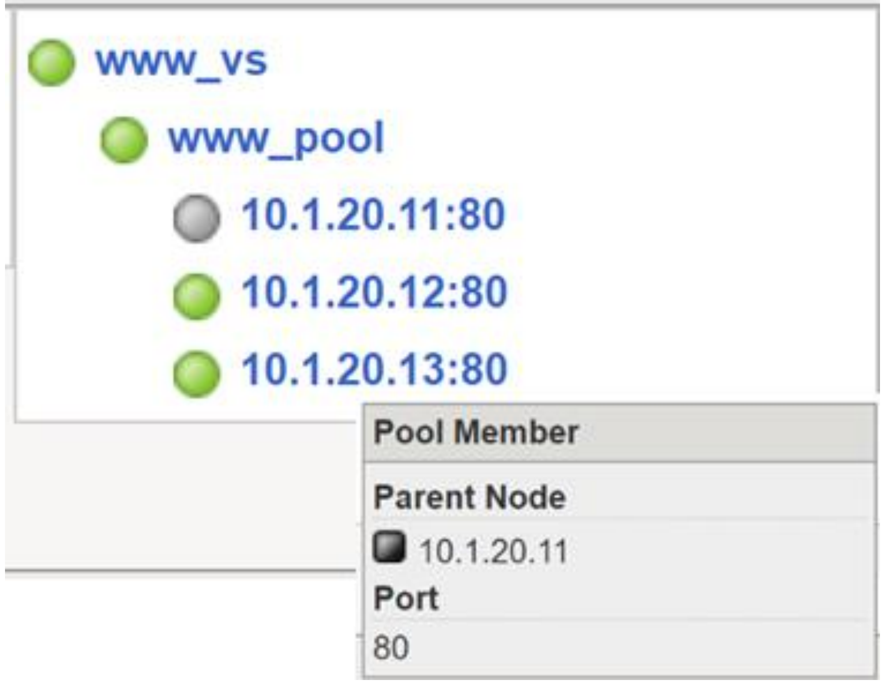
Order	Destination	Source	Service port
1	<host address>	<host address>	<port>
2	<host address>	<host address>	*
3	<host address>	<network address>	<port>
4	<host address>	<network address>	*
5	<host address>	*	<port>
6	<host address>	*	*
7	<network address>	<host address>	<port>
8	<network address>	<host address>	*
9	<network address>	<network address>	<port>
10	<network address>	<network address>	*
11	<network address>	*	<port>
12	<network address>	*	*
13	*	<host address>	<port>
14	*	<host address>	*
15	*	<network address>	<port>
16	*	<network address>	*
17	*	*	<port>
18	*	*	*

1.02 Identify traffic diverted due to status of traffic objects (VS, pool, pool member)

BIG-IP Object State and Status

How traffic is processed is affected by the state and status of an object.

- States are:
  - Enabled
  - Disabled
- Status is based on monitor responses and object hierarchy
  - The virtual server status is determined by the status of the pool
  - The pool status is determined by the status of pool members
  - A pool member is determined by the status of the node
    - Node is an IP address



● www_vs

● www_pool

○ 10.1.20.11:80

● 10.1.20.12:80

● 10.1.20.13:80

Pool Member

Parent Node

■ 10.1.20.11

Port

80

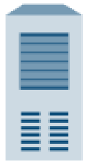
Load Balancing Components (Brief review)

- **Node**
  - IP address of the server supporting applications

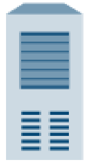
- **Pool Member**
  - A pool member is the IP Address:Port combination to access an application on the node (server)
  - Pool members are combined to form pools of applications
  - Since a single server may host multiple applications, a single node (server) may be a part of multiple pools

- **Pool**
  - A pool is a group of pool members supporting a particular application
  - Each pool has its own characteristics, such as monitor(s) and load balancing method

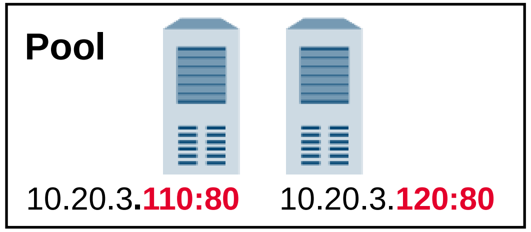
- **Virtual Server**
  - Is the IP Address:Port combination that represents a pool to the client side
  - Is a combination of a **virtual** IP address and **virtual** port
  - Access is limited to the defined port only
  - Multiple virtual servers can use the same servers or pools



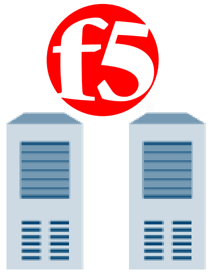
Node 10.20.3.110



Pool Member
10.20.3.110:**80 (http)**



Virtual Server
64.128.16.100:80



10.20.3.110:80 10.20.3.120:80

Monitor Status Reporting

Status	Status Definition	
🟢	Node	• Most recent monitor successful
	Pool Member	• Most recent monitor successful
	Pool	• **At least one pool member is available**
	Virtual Server	• Associated pool is available
🟦	Node	• No associated monitor (or timeout of first check not reached and not successful)
	Pool Member	• No associated monitor (or timeout of first check not reached and not successful)
	Pool	• All pool members are unknown/unmonitored (blue)
	Virtual Server	• Associated pool is unknown/unmonitored (blue)
♦	Node	• Most recent monitor failed (no successful checks within timeout period)
	Pool Member	• Most recent monitor failed (no successful checks within timeout period)
	Pool	• All members are offline and no members are available
	Virtual Server	• Associated pool is offline and no members available

Other Statuses and State

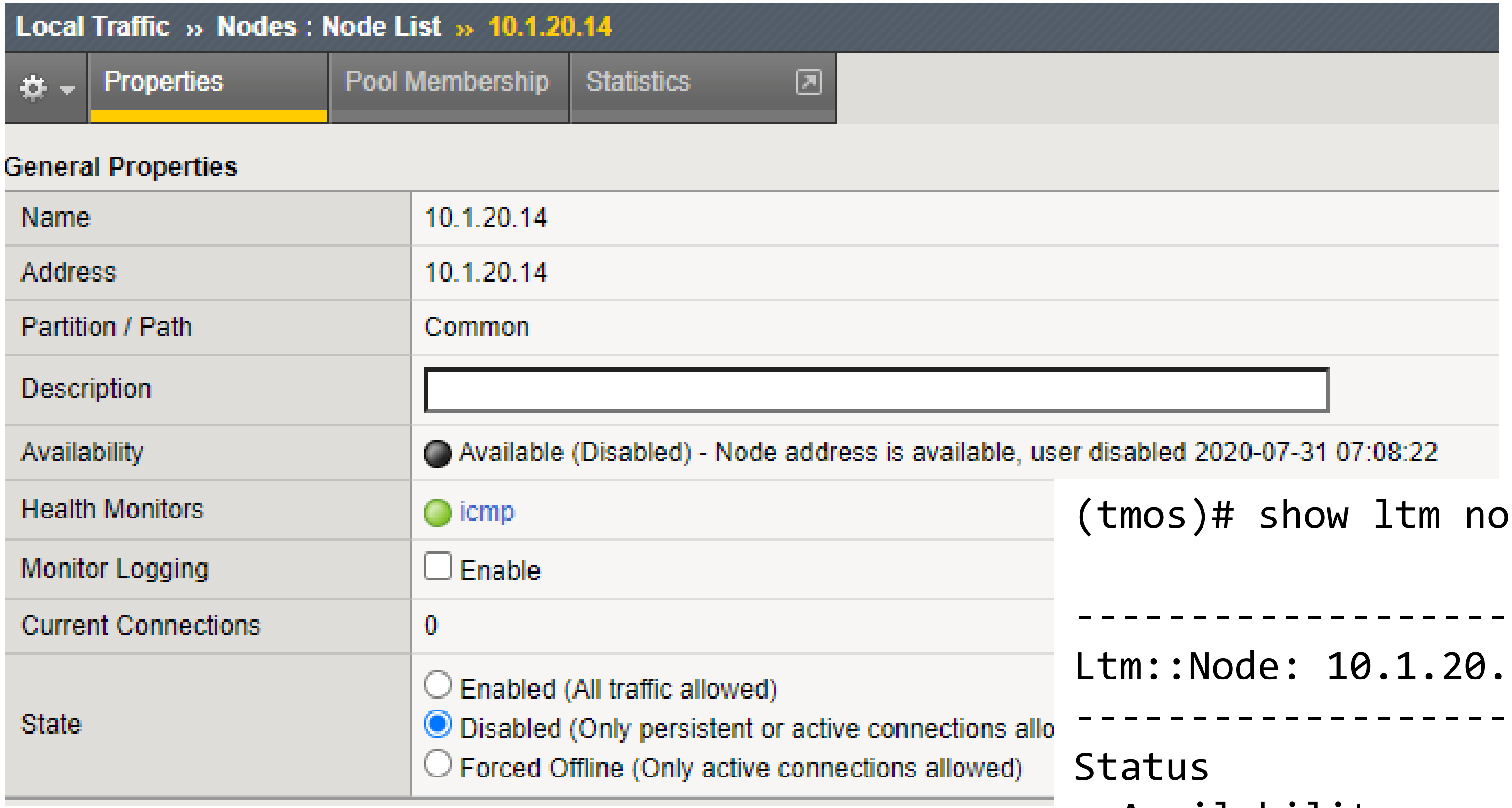
▲

- **Currently Unavailable**
  - The virtual server or all its resources have reached a connection limit that has been set by the administrator
  - A pool member has reached a connection limit that has been set by the administrator
  - The object has no further capacity for traffic until the current connections fall below the connection limit settings.

● ■ ◆ ▲

- **Disabled / Forced Offline**
  - The object has administratively been marked down and will not process traffic
  - The status icon will be a shape that represents the current monitor status of the object but will always be colored **black.**
  - A grey status shape ● would mean the child object has been disabled.
    - If you disable a node, the pool member associated with the node would go grey

Status and State



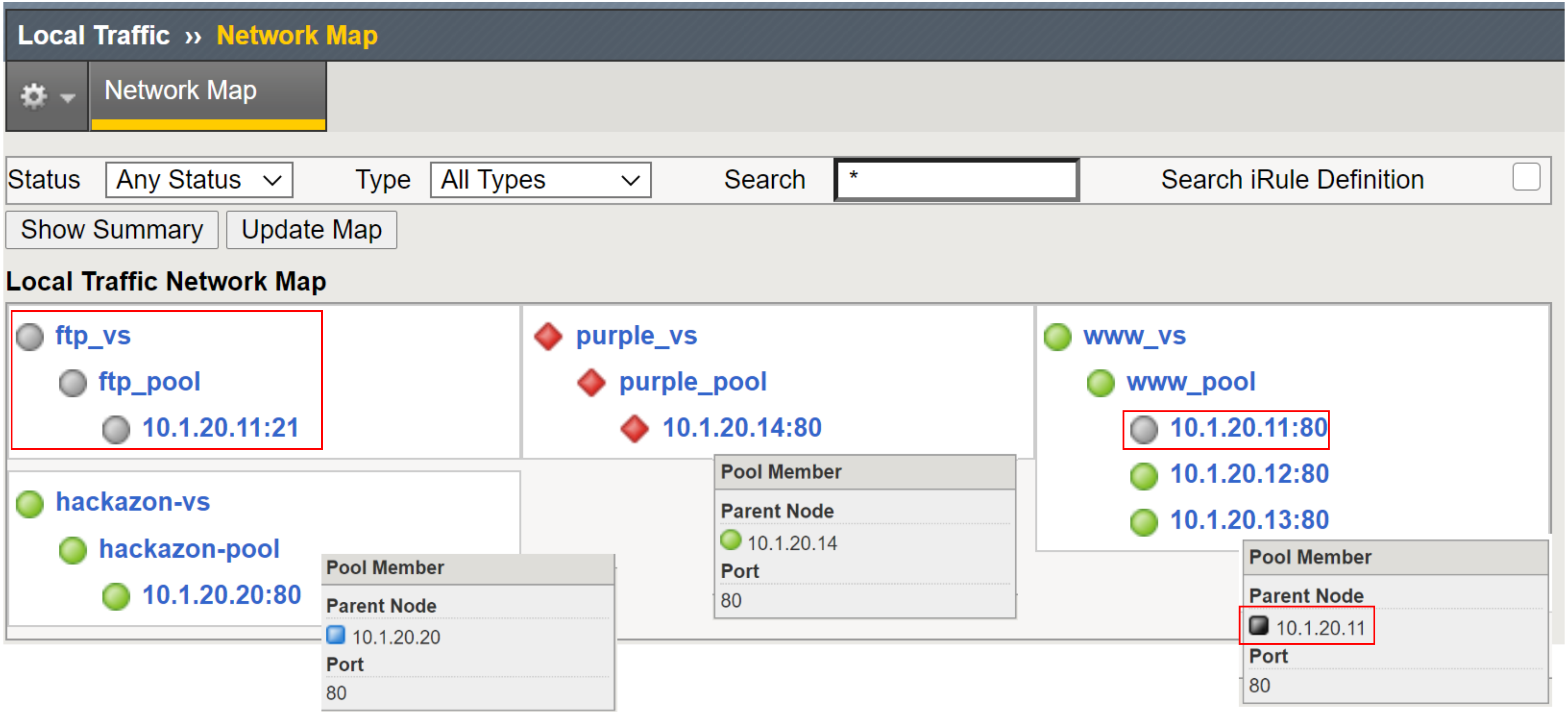
Local Traffic » Nodes : Node List » 10.1.20.14

General Properties

Name	10.1.20.14
Address	10.1.20.14
Partition / Path	Common
Description	
Availability	● Available (Disabled) - Node address is available, user disabled 2020-07-31 07:08:22
Health Monitors	● icmp
Monitor Logging	□ Enable
Current Connections	0
State	○ Enabled (All traffic allowed) ● Disabled (Only persistent or active connections allo ○ Forced Offline (Only active connections allowed)

```
(tmos)# show ltm node 10.1.20.14

------------------------------------------
Ltm::Node: 10.1.20.14 (10.1.20.14)
------------------------------------------
Status
  Availability   : available
  State          : disabled
  Reason         : Node address is available, user disabled
  Monitor        : icmp
  Monitor Status : up
  Session Status : user-disabled
```

Status and State – Network Map



Local Traffic ›› Network Map

Status: Any Status | Type: All Types | Search: * | Search iRule Definition □

Local Traffic Network Map

- ● ftp_vs
  - ● ftp_pool
    - ● 10.1.20.11:21
- ◆ purple_vs
  - ◆ purple_pool
    - ◆ 10.1.20.14:80
- ● www_vs
  - ● www_pool
    - ● 10.1.20.11:80
    - ● 10.1.20.12:80
    - ● 10.1.20.13:80
- ● hackazon-vs
  - ● hackazon-pool
    - ● 10.1.20.20:80

Pool Member
Parent Node
■ 10.1.20.20
Port
80

Pool Member
Parent Node
● 10.1.20.14
Port
80

Pool Member
Parent Node
■ 10.1.20.11
Port
80

Identify traffic diverted due to persistence

Manual Chapter : Session Persistence Profiles

- Directs a client back to the same server after the initial load balancing decision has been made
  - Is required for stateful applications
  - May skew load balancing statistics
- The persistence profile is assigned at the virtual server level.
- Persistence methods you should know
  - Source Address Affinity (aka Simple) Persistence (Based on source IP and network mask)
  - Cookie Persistence (Recommended for HTTP)
- Other persistence methods
  - SSL Session ID, Session Initiated Protocol (SIP), MSRDP
  - Universal Persistence
    - iRules can create persistence records based on anything in the client’s request, such as, jsessionid, username, etc.

Persistence Settings

Manual Chapter : Session Persistence Profiles

Match Across Services

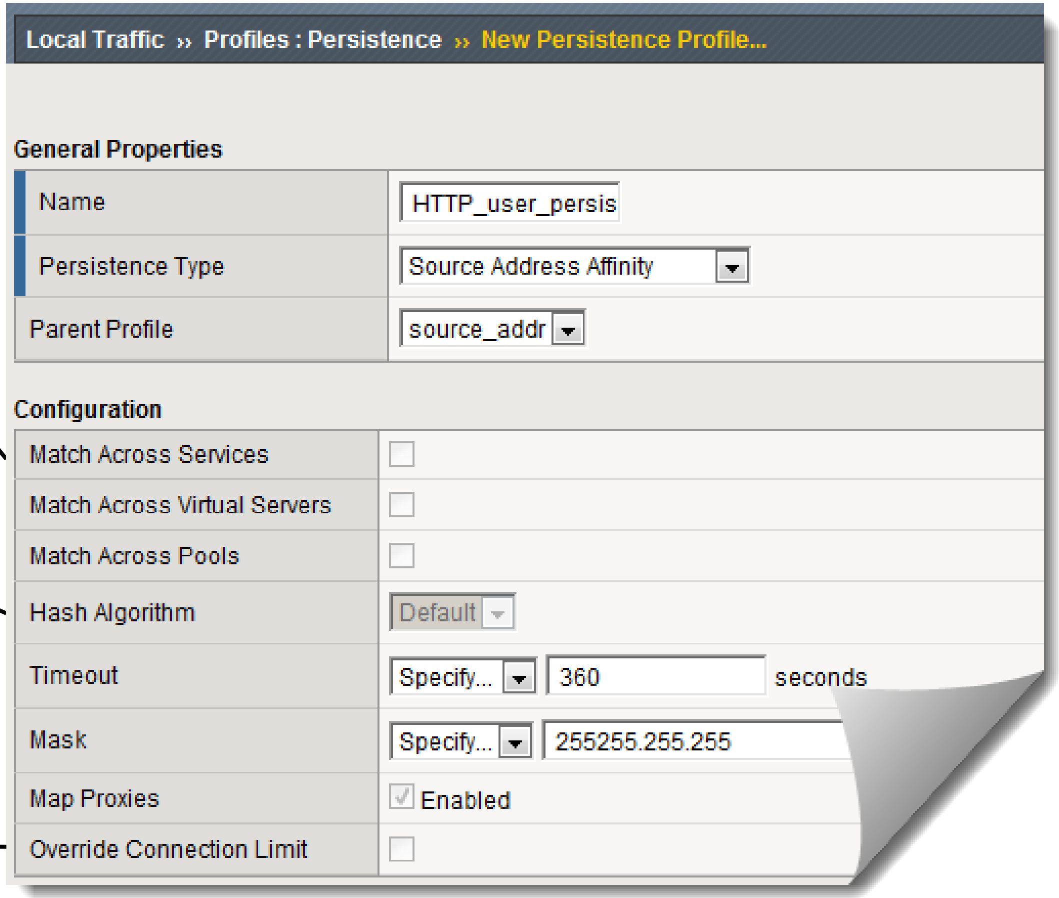
- When enabled, specifies that all persistent connections from a client IP address that go to the same virtual IP address also go to the same pool member

Timeout

- Specifies the duration of the persistence entries
- Resets on a new connection

Override Connection Limit

- Allows new connections to be established when the connection limit is reached, if there is an existing persistence record



Local Traffic ›› Profiles : Persistence ›› New Persistence Profile...

General Properties

Name	HTTP_user_persis
Persistence Type	Source Address Affinity
Parent Profile	source_addr

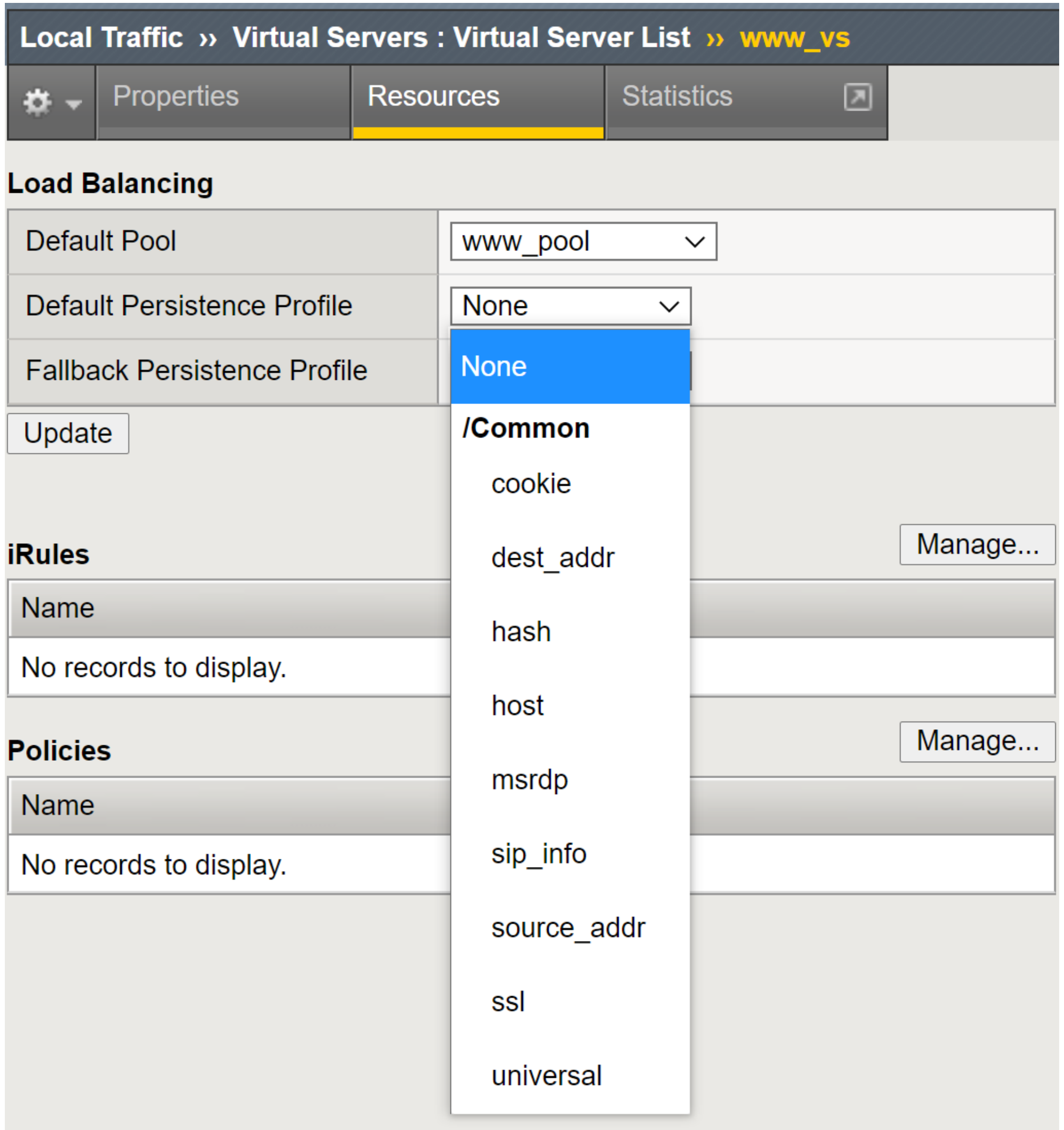
Configuration

Match Across Services	□
Match Across Virtual Servers	□
Match Across Pools	□
Hash Algorithm	Default
Timeout	Specify... 360 seconds
Mask	Specify... 255255.255.255
Map Proxies	☑ Enabled
Override Connection Limit	□

Persistence Methods

[Manual: Session Persistence Profiles]

- Configured under Resources tab in a Virtual Server
- Fallback persistence
  - If there is not a persistence record from the Default Persistence Profile
  - Check if a persistence record was created by the fallback and use that record
- Fallback example:
  - If users don't allow cookies fallback to source persistence.



Local Traffic ›› Virtual Servers : Virtual Server List ›› www_vs

Load Balancing

Default Pool	www_pool
Default Persistence Profile	None
Fallback Persistence Profile	

iRules

Name
No records to display.

Policies

Name
No records to display.

Virtual Servers

Objectives 4.01, 1.03, 2.02

4.01

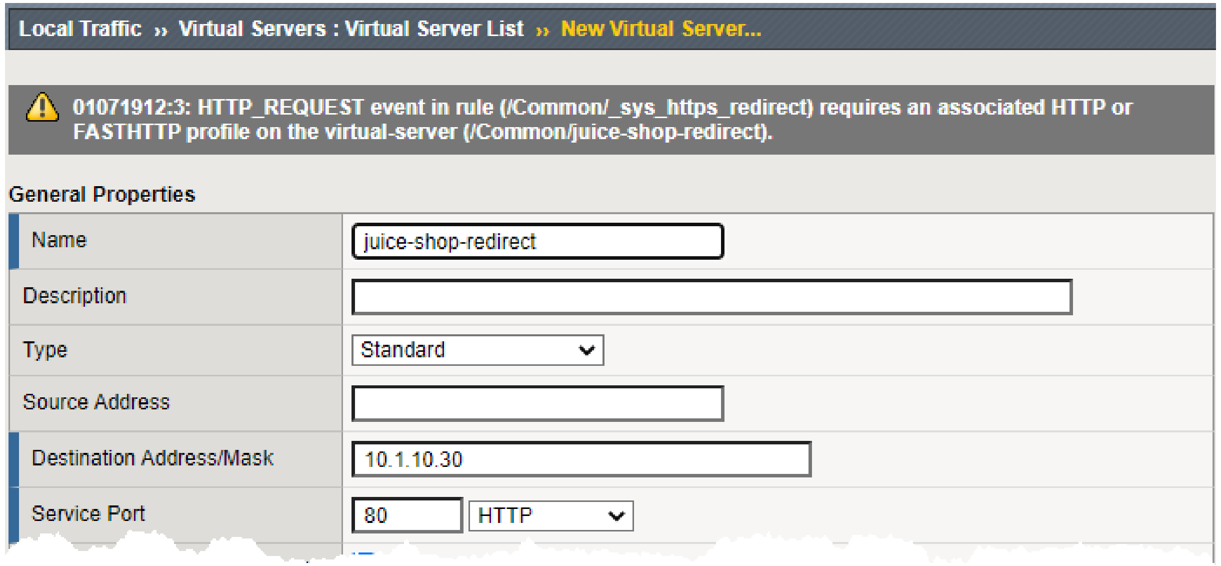
Apply procedural concepts required to modify and manage virtual servers

- Apply appropriate protocol specific profile
- Apply appropriate persistence profile
- Apply appropriate HTTPS encryption profile
- Identify iApp configured objects
- Report use of iRules
- Show default pool configuration

4.01 Apply appropriate protocol specific profile

MANUAL CHAPTER: VIRTUAL SERVERS

- All virtual servers must have a Protocol profile assigned
- If looking beyond L4 information is required, then the appropriate L7 profile needs to be assigned.
  - For example, FTP profile for FTP applications
  - For example, HTTP profile if the cookie or other information needs to be viewed or manipulated.

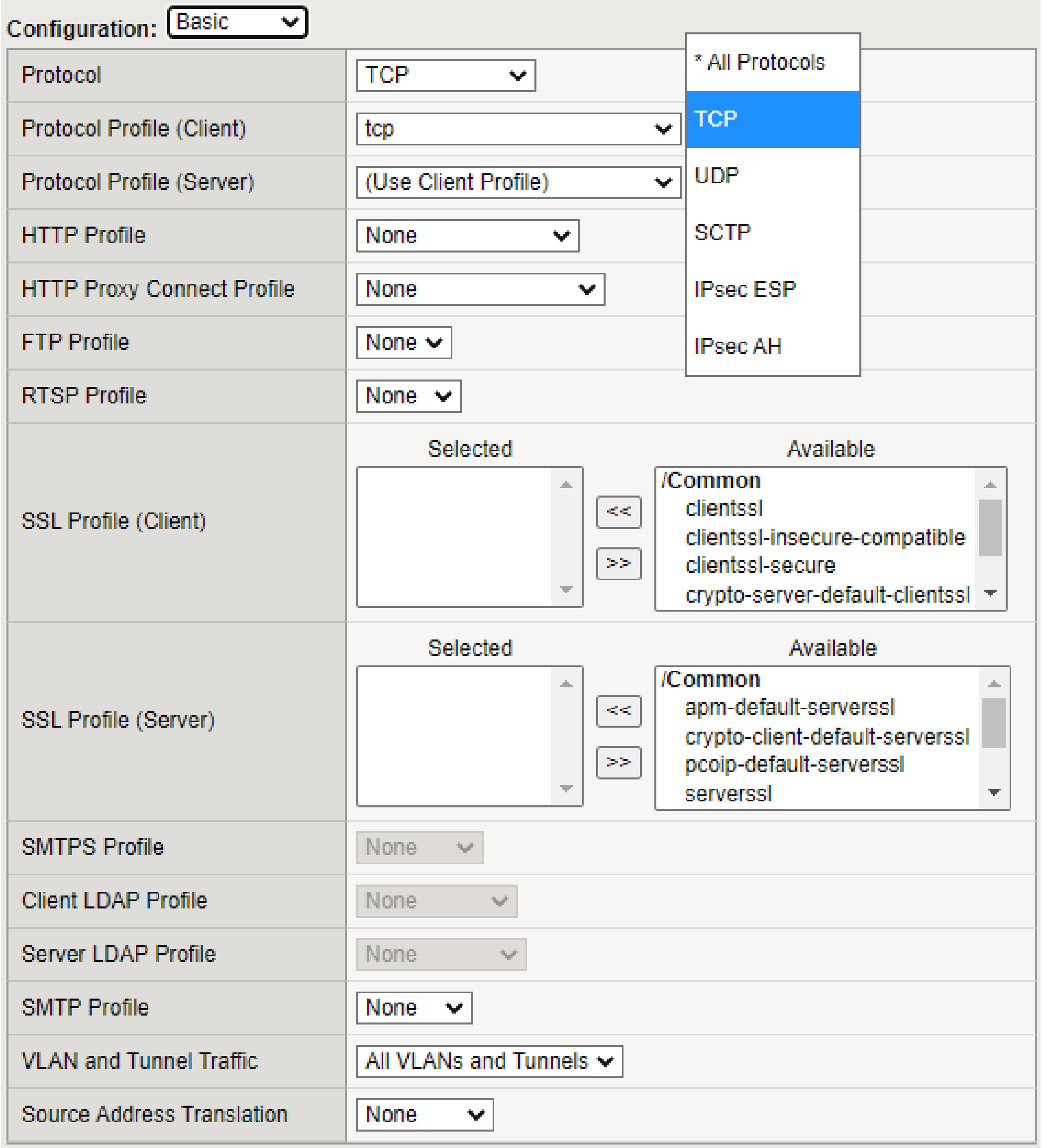


Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

⚠ 01071912:3: HTTP_REQUEST event in rule (/Common/_sys_https_redirect) requires an associated HTTP or FASTHTTP profile on the virtual-server (/Common/juice-shop-redirect).

General Properties

Name	juice-shop-redirect
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.1.10.30
Service Port	80 HTTP



Configuration: Basic

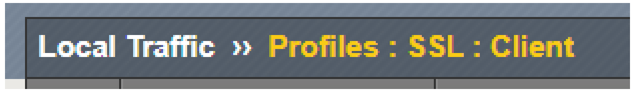
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: Available: /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	None

4.01 Apply appropriate HTTPS encryption profile

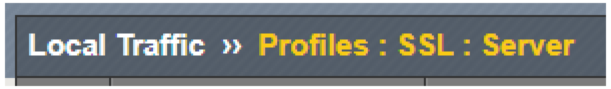
K14783: Overview of the Client SSL profile (11.x - 16.x)

K14806: Overview of the Server SSL profile (11.x - 16.x)

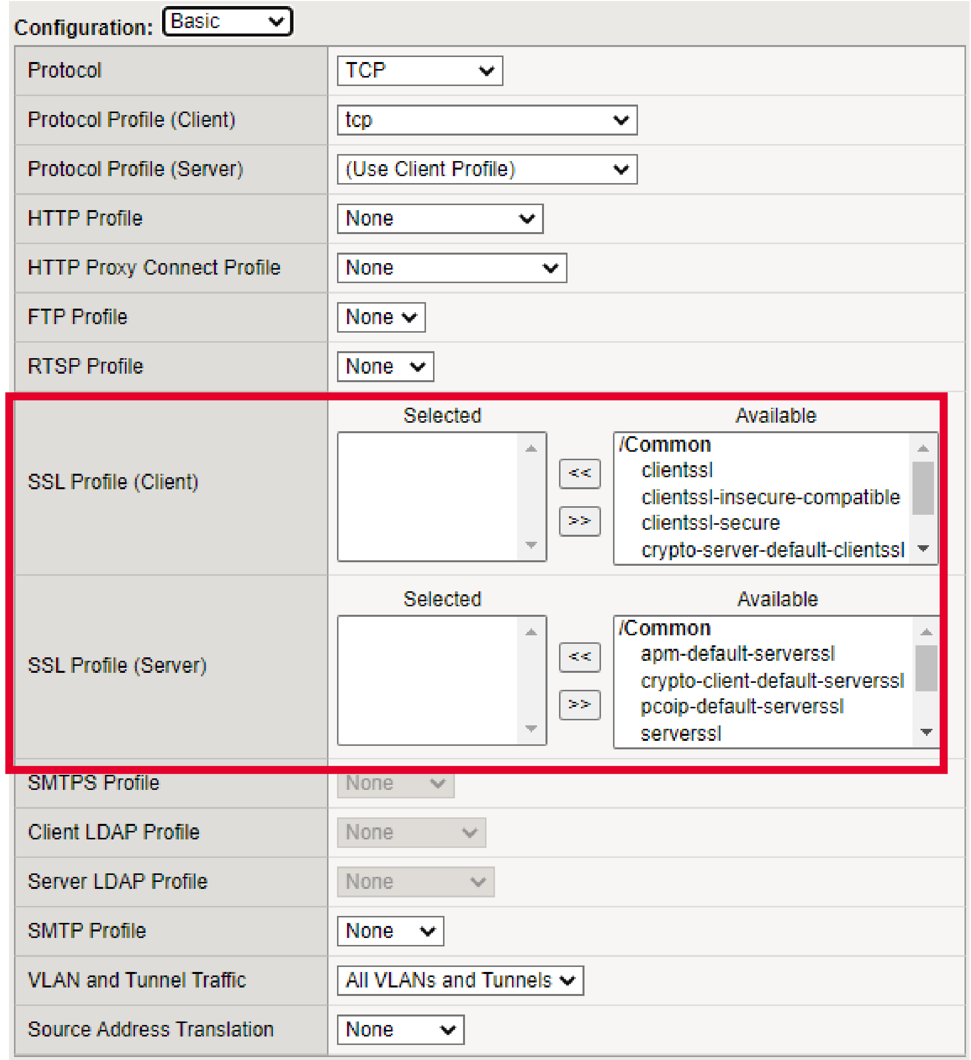
- SSL Profile requirements
  - SSL Client-Side profile, with the appropriate cert & key for SSL offload
  - SSL Server-Side profile, if the pool members service HTTPS traffic
- An HTTP profile is NOT required.



Local Traffic » Profiles : SSL : Client



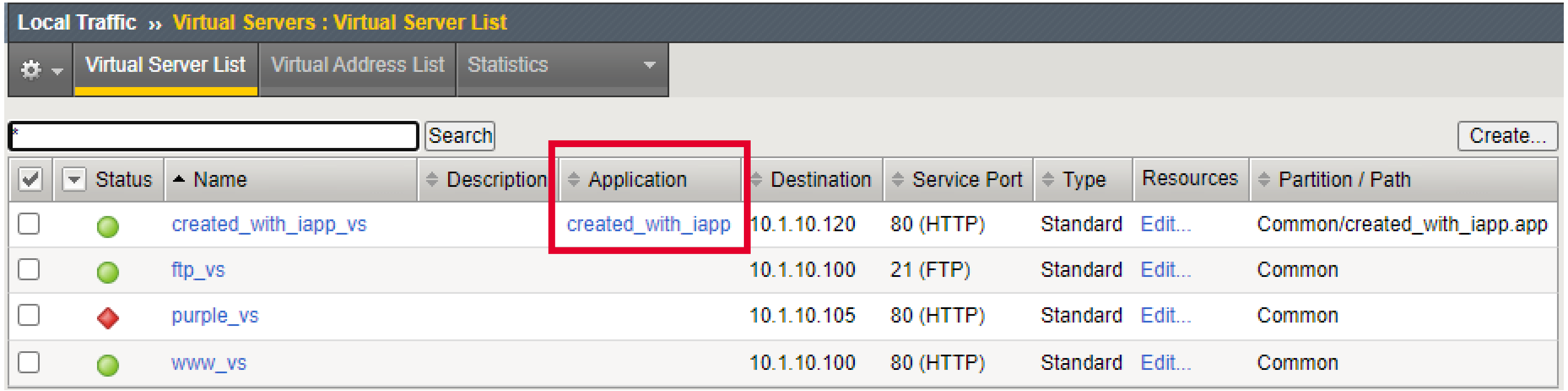
Local Traffic » Profiles : SSL : Server



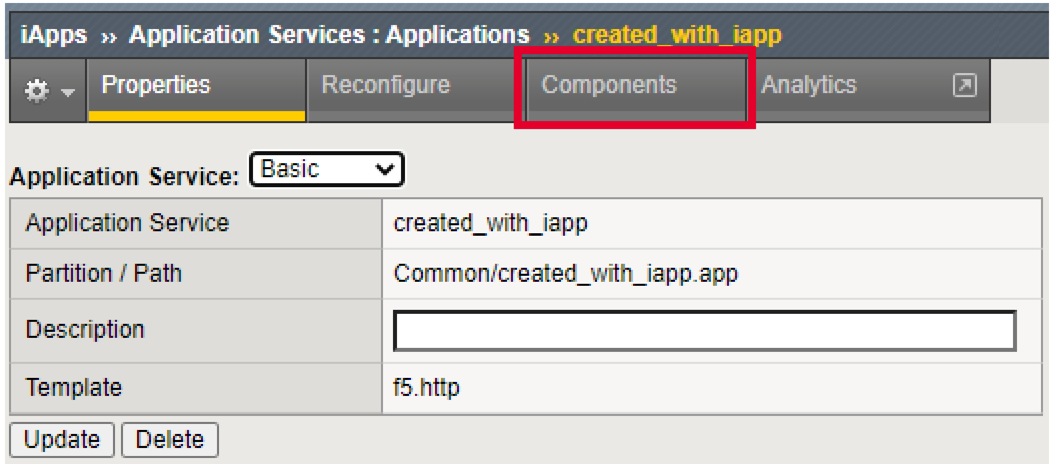
Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: Available: /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	None

4.01 Identify iApp configured objects



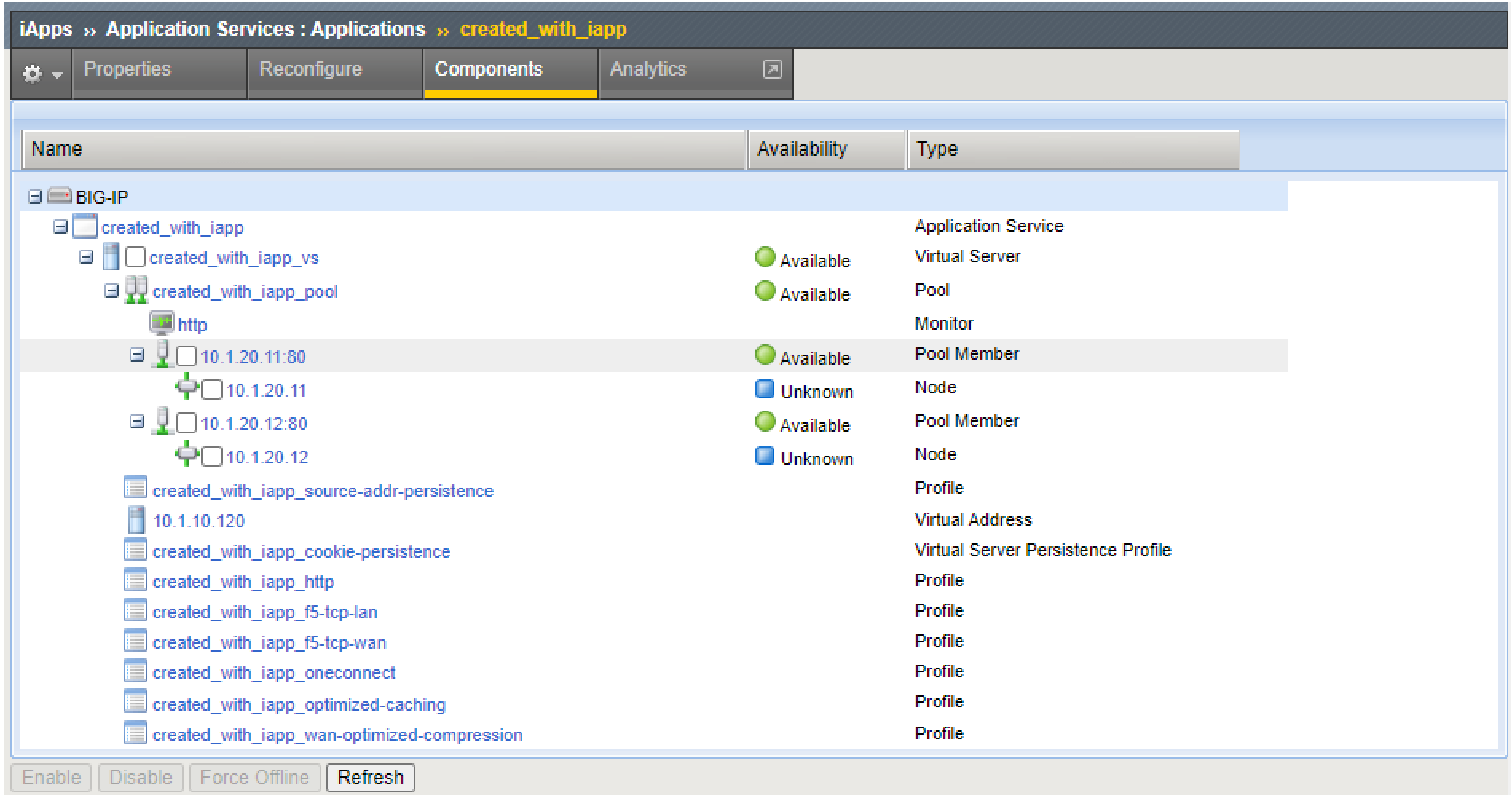
☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
□	●	created_with_iapp_vs		created_with_iapp	10.1.10.120	80 (HTTP)	Standard	Edit...	Common/created_with_iapp.app
□	●	ftp_vs			10.1.10.100	21 (FTP)	Standard	Edit...	Common
□	◆	purple_vs			10.1.10.105	80 (HTTP)	Standard	Edit...	Common
□	●	www_vs			10.1.10.100	80 (HTTP)	Standard	Edit...	Common


iApps ›› Application Services : Applications ›› created_with_iapp
Properties
Reconfigure
Components
Analytics
Update
Delete

Application Service: Basic

Application Service	created_with_iapp
Partition / Path	Common/created_with_iapp.app
Description	
Template	f5.http

4.01 Identify iApp configured objects



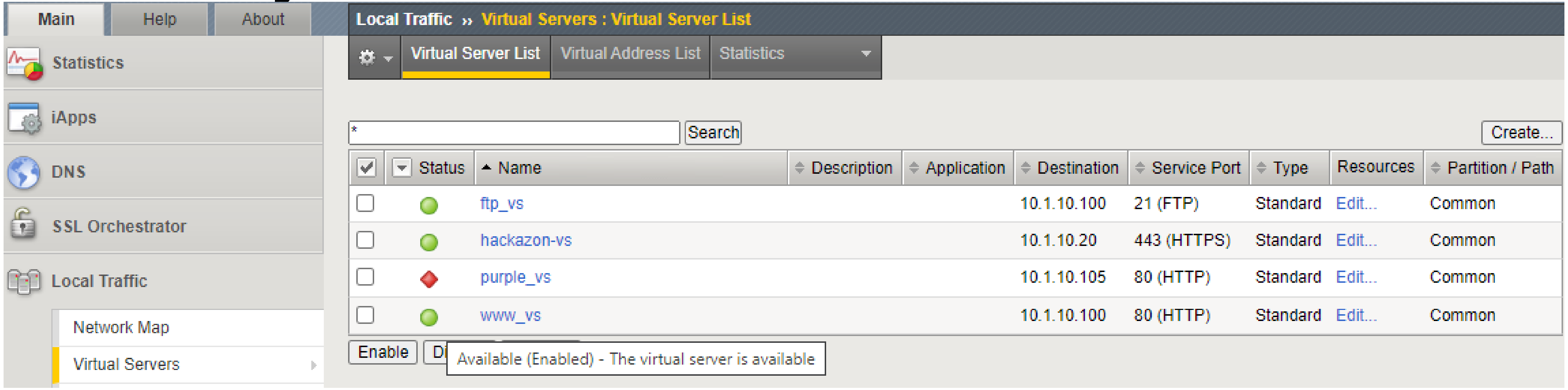
Name	Availability	Type
BIG-IP		
created_with_iapp		Application Service
created_with_iapp_vs	Available	Virtual Server
created_with_iapp_pool	Available	Pool
http		Monitor
10.1.20.11:80	Available	Pool Member
10.1.20.11	Unknown	Node
10.1.20.12:80	Available	Pool Member
10.1.20.12	Unknown	Node
created_with_iapp_source-addr-persistence		Profile
10.1.10.120		Virtual Address
created_with_iapp_cookie-persistence		Virtual Server Persistence Profile
created_with_iapp_http		Profile
created_with_iapp_f5-tcp-lan		Profile
created_with_iapp_f5-tcp-wan		Profile
created_with_iapp_oneconnect		Profile
created_with_iapp_optimized-caching		Profile
created_with_iapp_wan-optimized-compression		Profile

1.03

Identify the reason a virtual server is not working as expected

- Identify the current configured state of the virtual server
- Identify the current availability status of the virtual server
- Identify misconfigured IP address and/or Port
- Identify conflicting/misconfigured profiles

1.03 Identify the state and status of a virtual server



Local Traffic » Virtual Servers : Virtual Server List

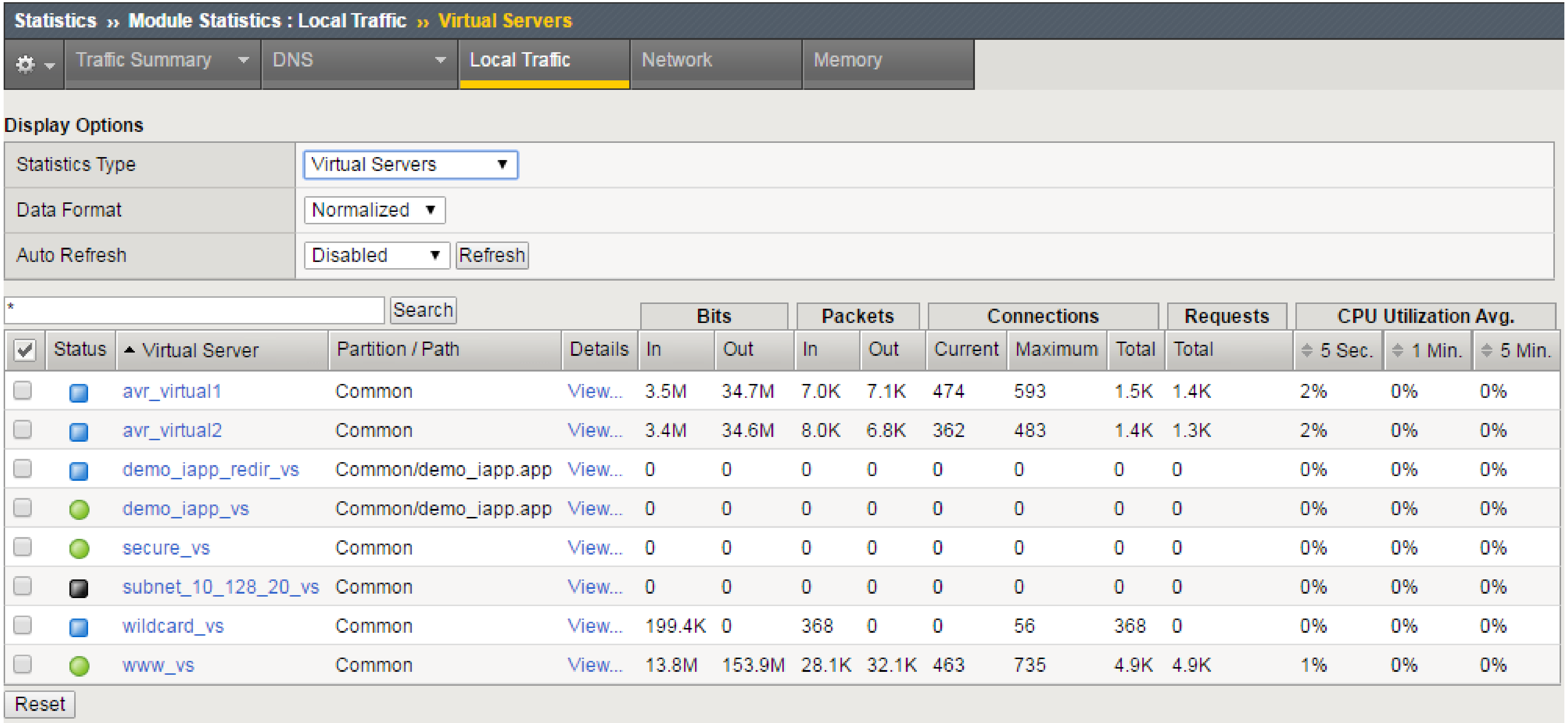
☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
☐	●	ftp_vs			10.1.10.100	21 (FTP)	Standard	Edit...	Common
☐	●	hackazon-vs			10.1.10.20	443 (HTTPS)	Standard	Edit...	Common
☐	◆	purple_vs			10.1.10.105	80 (HTTP)	Standard	Edit...	Common
☐	●	www_vs			10.1.10.100	80 (HTTP)	Standard	Edit...	Common

Available (Enabled) - The virtual server is available

```
# show ltm virtual www_vs
------------------------------------------------------------
Ltm::Virtual Server: www_vs
-----------------------------------------------------------
Status
  Availability     : available
  State            : enabled
  Reason           : The virtual server is available
  CMP              : enabled
  CMP Mode         : all-cpus
  Destination      : 10.1.10.100:80

Traffic                             ClientSide  Ephemeral  General
  Bits In                                577.1K          0        -
<cut>
```

Virtual Server Statistics

Manual Chapter: Virtual Servers



Statistics » Module Statistics : Local Traffic » Virtual Servers

Display Options

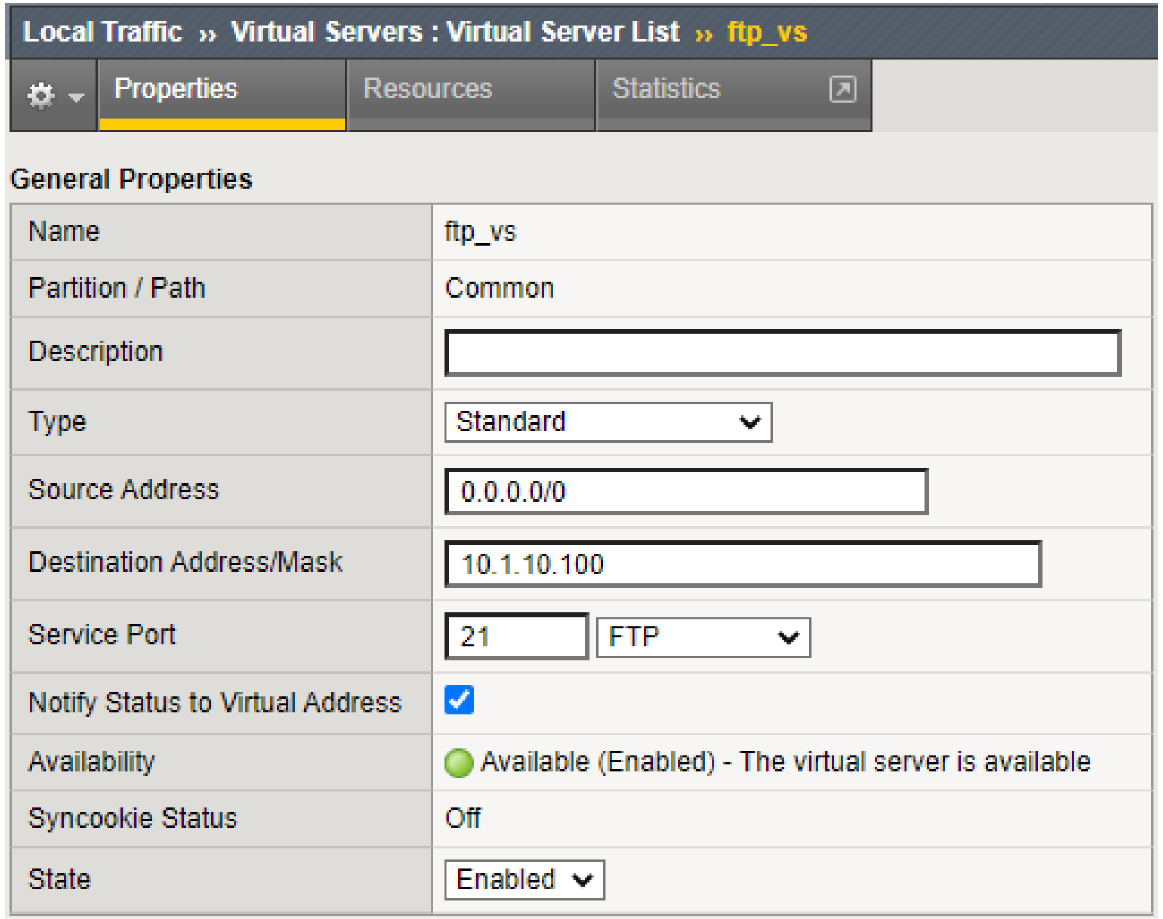
Statistics Type	Virtual Servers ▼
Data Format	Normalized ▼
Auto Refresh	Disabled ▼ Refresh

* Search

					Bits		Packets		Connections			Requests	CPU Utilization Avg.		
☑	Status	▲ Virtual Server	Partition / Path	Details	In	Out	In	Out	Current	Maximum	Total	Total	⇕ 5 Sec.	⇕ 1 Min.	⇕ 5 Min.
□	🟦	avr_virtual1	Common	View...	3.5M	34.7M	7.0K	7.1K	474	593	1.5K	1.4K	2%	0%	0%
□	🟦	avr_virtual2	Common	View...	3.4M	34.6M	8.0K	6.8K	362	483	1.4K	1.3K	2%	0%	0%
□	🟦	demo_iapp_redir_vs	Common/demo_iapp.app	View...	0	0	0	0	0	0	0	0	0%	0%	0%
□	🟢	demo_iapp_vs	Common/demo_iapp.app	View...	0	0	0	0	0	0	0	0	0%	0%	0%
□	🟢	secure_vs	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%
□	⬛	subnet_10_128_20_vs	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%
□	🟦	wildcard_vs	Common	View...	199.4K	0	368	0	0	56	368	0	0%	0%	0%
□	🟢	www_vs	Common	View...	13.8M	153.9M	28.1K	32.1K	463	735	4.9K	4.9K	1%	0%	0%

1.03 Identify misconfigured IP address and/or Port

Manual Chapter: Virtual Servers



Local Traffic » Virtual Servers : Virtual Server List » ftp_vs
Properties
Resources
Statistics

General Properties

Name	ftp_vs
Partition / Path	Common
Description	
Type	Standard
Source Address	0.0.0.0/0
Destination Address/Mask	10.1.10.100
Service Port	21 FTP
Notify Status to Virtual Address	☑
Availability	● Available (Enabled) - The virtual server is available
Syncookie Status	Off
State	Enabled

```
(tmos)# list ltm virtual ftp_vs
ltm virtual ftp_vs {
    destination 10.1.10.100:ftp
    ip-protocol tcp
    mask 255.255.255.255
    pool ftp_pool
    profiles {
        ftp { }
        tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        pool SNAT249_pool
        type snat
    }
    translate-address enabled
    translate-port enabled
    vs-index 2
}
```

Profile Types

Manual : BIG-IP Local Traffic Management: Profiles Reference (v13.1)

K23843660: BIG-IP LTM-DNS operations guide | Chapter 5: BIG-IP LTM profiles

Profile Type	Description
Protocol profiles	
Fast L4	Defines the behavior of Layer 4 IP traffic.
Fast HTTP	Improves the speed at which a virtual server processes HTTP requests.
TCP	Defines the behavior of TCP traffic.
UDP	Defines the behavior of UDP traffic.
SSL profiles	
Client	Defines the behavior of client-side SSL traffic. See also Persistence Profiles.
Server	Defines the behavior of server-side SSL traffic. See also Persistence Profiles.

Profile Types

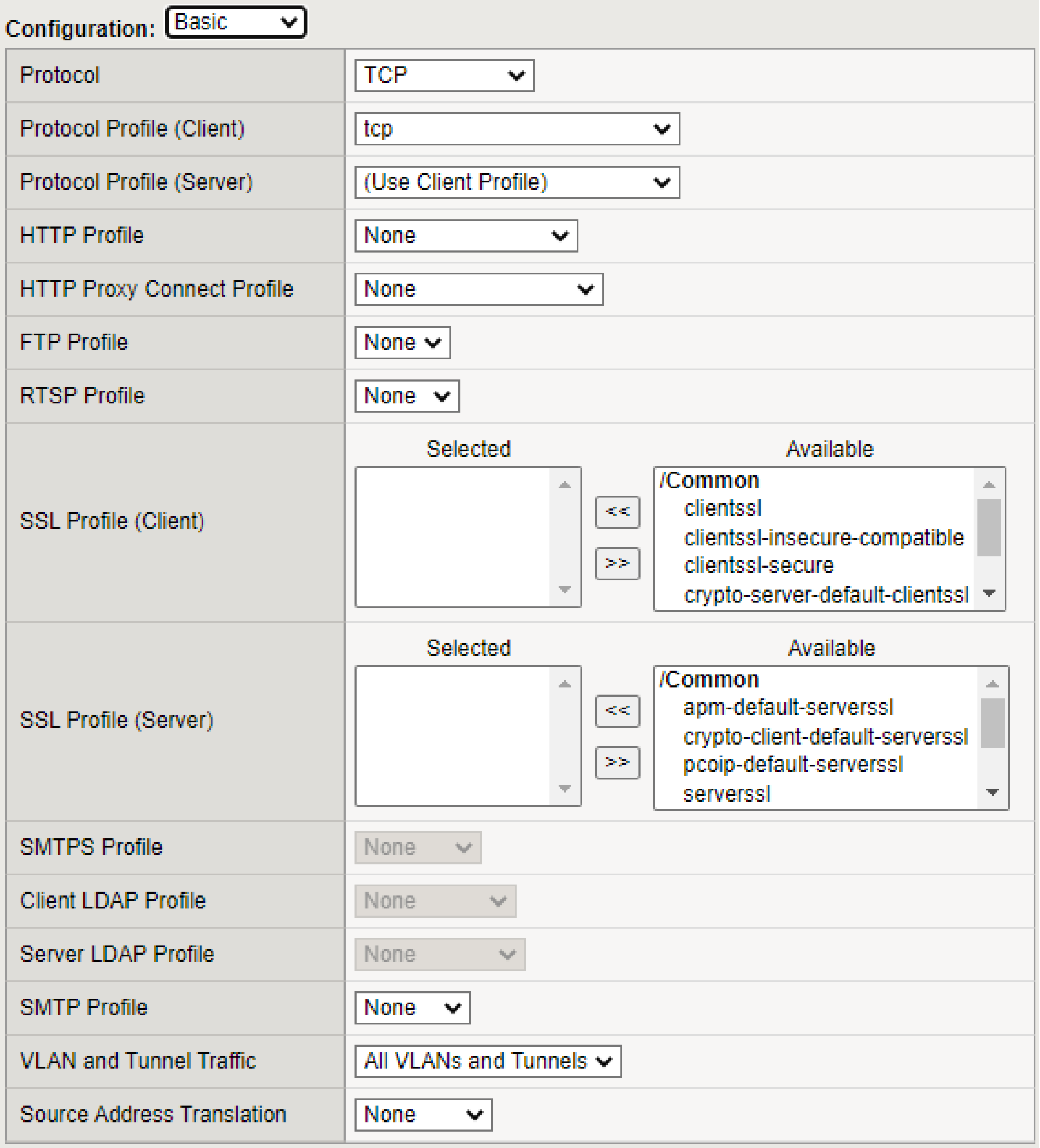
Manual : BIG-IP Local Traffic Management: Profiles Reference (v13.1)

Profile Type	Description
Services profiles	
HTTP	Defines the behavior of HTTP traffic.
FTP	Defines the behavior of FTP traffic.
Persistence profiles	
Cookie	Implements session persistence using HTTP cookies.
Destination Address Affinity	Implements session persistence based on the destination IP address specified in the header of a client request. Also known as sticky persistence.
Hash	Implements session persistence in a way similar to universal persistence, except that the BIG-IP system uses a hash for finding a persistence entry.
Microsoft® Remote Desktop	Implements session persistence for Microsoft® Remote Desktop Protocol sessions.
SIP	Implements session persistence for connections using Session Initiation Protocol Call-ID.
Source Address Affinity	Implements session persistence based on the source IP address specified in the header of a client request. Also known as simple persistence.
SSL	Implements session persistence for non-terminated SSL sessions, using the session ID.
Universal	Implements session persistence using the BIG-IP system's Universal Inspection Engine (UIE).

Misconfigured/Missing Profiles

Common mistakes/things to think about:

- The Protocol profile limits traffic to that protocol
  - i.e. Using the TCP profile, you can not ping through a virtual
- If looking into L4, L7, (ie HTTP), the appropriate protocol profile is needed
- SSL Profile requirements
  - HTTPS virtual, HTTPS pool members, where no HTTP profile is required, does NOT have to have SSL profiles, basically L4
  - SSL Offload, virtual HTTP, pool members HTTP will require a SSL Profile (Client)
  - HTTPS virtual, HTTPS pool members, where you need to look into the HTTP header (ie. Cookie persistence) and/or data require BOTH an SSL Profile (Client) and an SSL Profile (Server)



Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: (empty) Available: /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: (empty) Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	None

2.02 R

Identify the different virtual server types

- Standard, Forwarding, Stateless, Reject
- Performance (Layer 4) and Performance (HTTP)

Virtual Server Types

Virtual server type	Description of virtual server type
Standard	**A Standard virtual server directs client traffic to a load balancing pool and is the most basic type of virtual server. It is a general purpose virtual server that does everything not expressly provided by the other types of virtual servers.**
Forwarding (Layer 2)	A Forwarding (Layer 2) virtual server typically shares the same IP address as a node in an associated Virtual Local Area Network (VLAN). You use a Forwarding (Layer 2) virtual server in conjunction with a VLAN group.
Forwarding (IP)	*A Forwarding (IP) virtual server forwards packets directly to the destination IP address specified in the client request. A Forwarding (IP) virtual server has no pool members to load balance.*
Performance (Layer 4)	*A Performance (Layer 4) virtual server has a FastL4 profile associated with it. A Performance (Layer 4) virtual server increases the speed at which the virtual server processes packets.*
Performance (HTTP)	*A Performance (HTTP) virtual server has a FastHTTP profile associated with it. The Performance (HTTP) virtual server and related profile increase the speed at which the virtual server processes HTTP requests.*
Stateless	*A Stateless virtual server improves the performance of User Datagram Protocol (UDP) traffic in specific scenarios.*
Reject	*A Reject virtual server rejects any traffic destined for the virtual server IP address.*
DHCP Relay	A Dynamic Host Configuration Protocol (DHCP) relay virtual server relays DHCP client requests for an IP address to one or more DHCP servers, and provides DHCP server responses with an available IP address for the client. (BIG-IP 11.1.0 and later)
Internal	An Internal virtual server enables usage of Internet Content Adaptation Protocol (ICAP) servers to modify HTTP requests and responses by creating and applying an ICAP profile and adding Request Adapt or Response Adapt profiles to the virtual server. (BIG-IP 11.3.0 and later)
Message Routing	A Message Routing virtual server uses a Session Initiation Protocol (SIP) application protocol and functions in accordance with a SIP session profile and SIP router profile. (BIG-IP 11.6.0)

Pools

Objectives 4.02, 1.04, 2.04

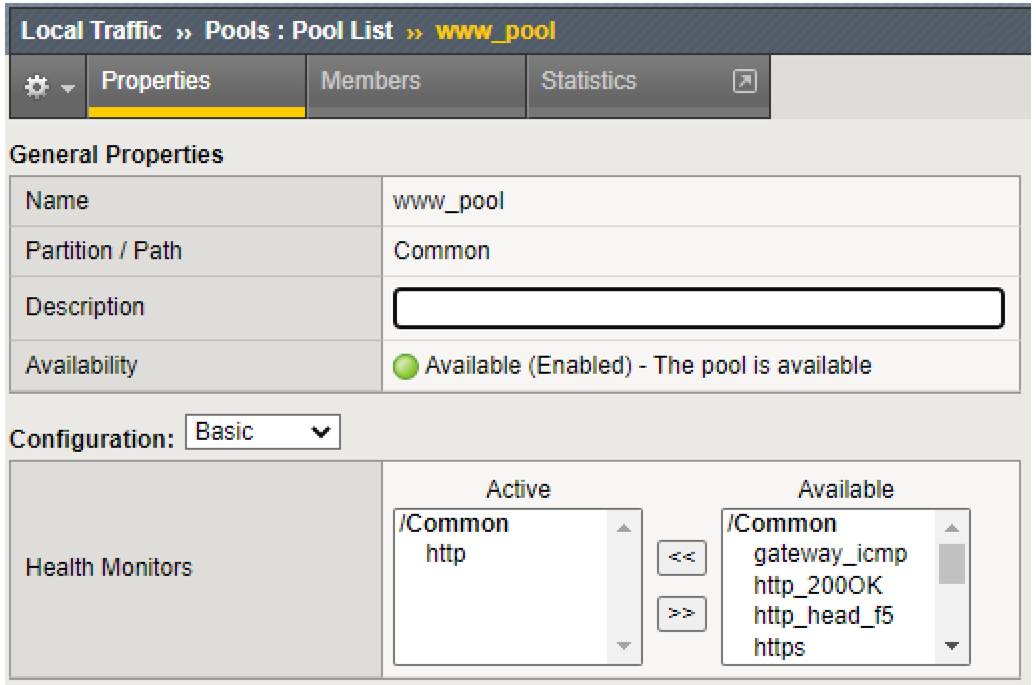
4.02

Apply procedural concepts required to modify and manage pools

- Determine configured health monitor
- Determine the load balancing method for a pool
- Determine pool member service port configuration
- Determine the active nodes in a priority group configuration
- Apply appropriate health monitor
- Apply load balancing method for a pool
- Apply pool member service port configuration

4.02 Determine configured health monitor

Manual : BIG-IP Local Traffic Manager: Monitors Reference



Local Traffic » Pools : Pool List » www_pool

General Properties

Name	www_pool
Partition / Path	Common
Description	
Availability	● Available (Enabled) - The pool is available

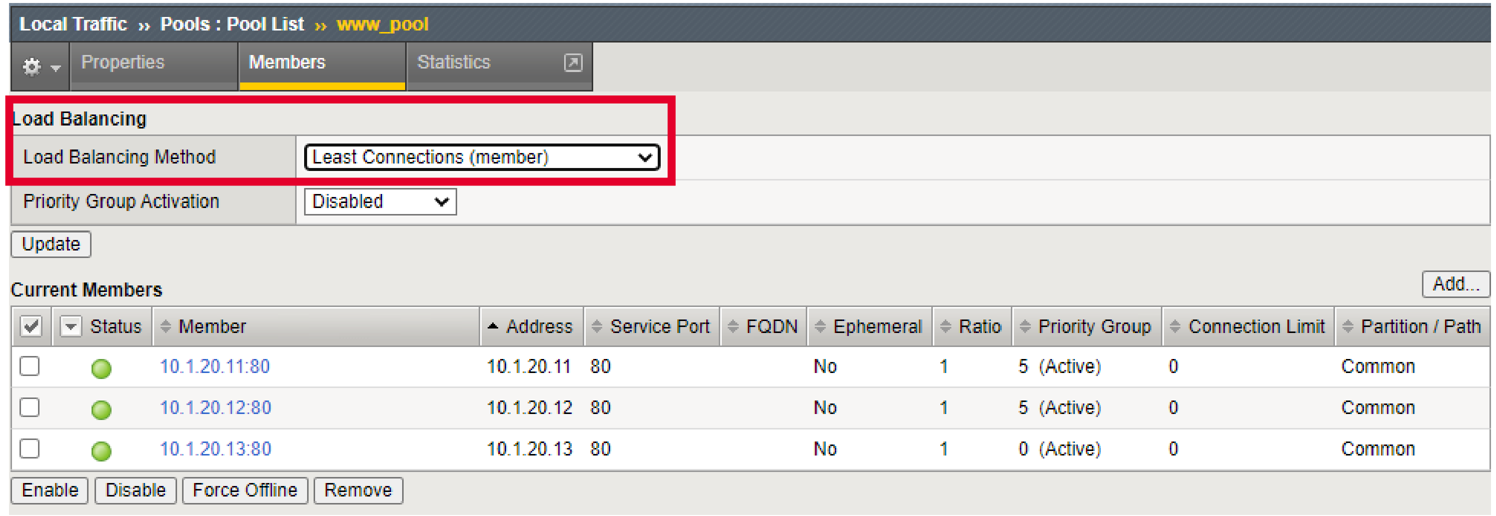
Configuration: Basic

	Active	Available
Health Monitors	/Common http	/Common gateway_icmp http_200OK http_head_f5 https

```
(tmos)# list ltm pool www_pool
ltm pool www_pool {
    members {
        10.1.20.11:http {
            address 10.1.20.11
            session monitor-enabled
            state up
        }
        10.1.20.12:http {
            address 10.1.20.12
            session monitor-enabled
            state up
        }
        10.1.20.13:http {
            address 10.1.20.13
            session monitor-enabled
            state up
        }
    }
    monitor http
}
```

4.02 Determine the load balancing method for a pool

[Manual Chapter : About Pools]



Load Balancing

Load Balancing Method	Least Connections (member)
Priority Group Activation	Disabled

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	10.1.20.11:80	10.1.20.11	80		No	1	5 (Active)	0	Common
□	●	10.1.20.12:80	10.1.20.12	80		No	1	5 (Active)	0	Common
□	●	10.1.20.13:80	10.1.20.13	80		No	1	0 (Active)	0	Common

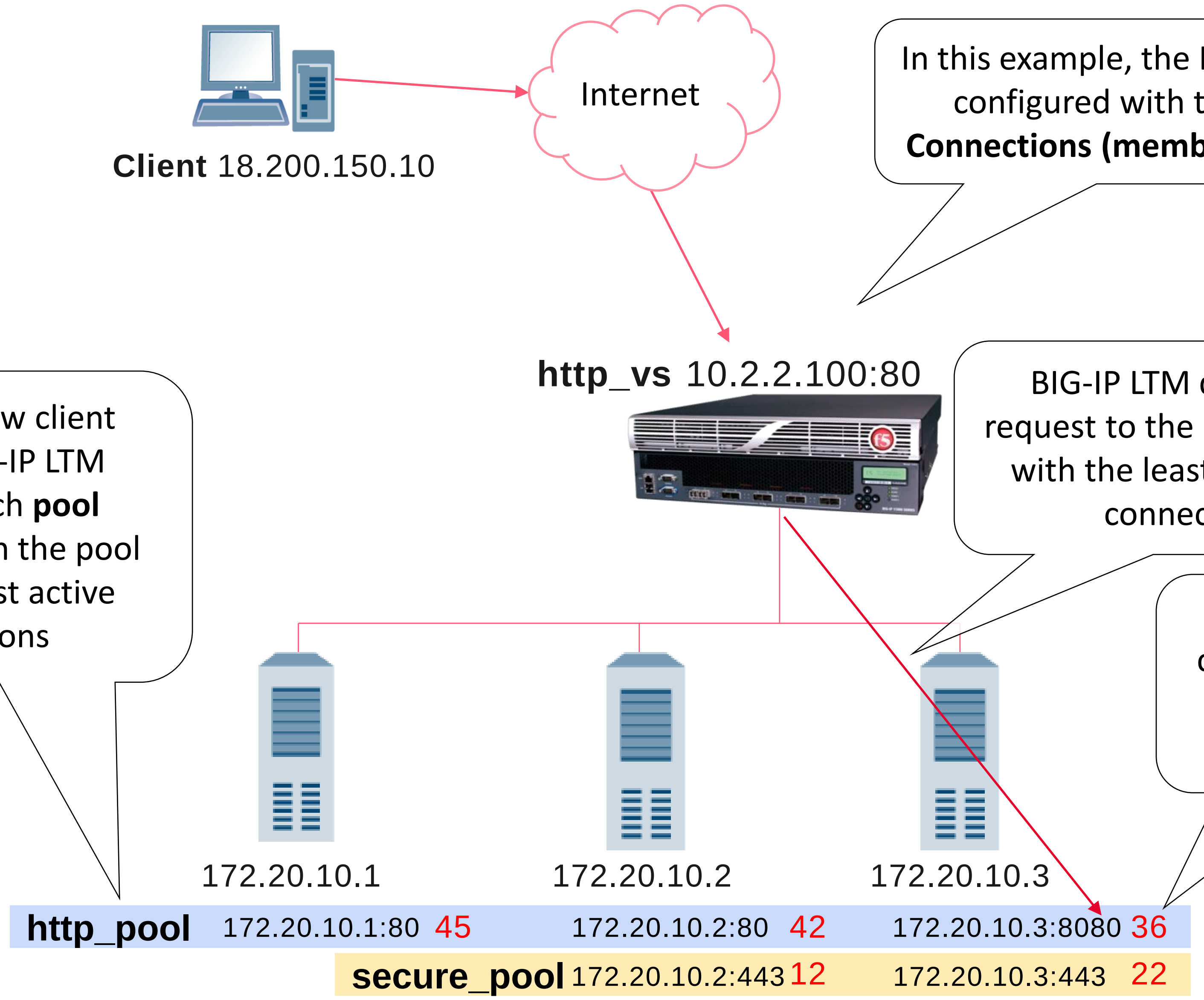
```
(tmos)# list ltm pool www_pool
ltm pool www_pool {
    load-balancing-mode least-connections-member
    members {
        10.1.20.11:http {
            address 10.1.20.11
            priority-group 5
            session monitor-enabled
            state up
        }
        10.1.20.12:http {
            address 10.1.20.12
            priority-group 5
            session monitor-enabled
            state up
        }
        10.1.20.13:http {
            address 10.1.20.13
            session monitor-enabled
            state up
        }
    }
    monitor http
}
```

Load Balancing methods

K6406: Overview of Least Connections, Fastest, Observed, and Predictive pool member load balancing

- A load balancing method is an algorithm used to determine which pool member to send traffic to
  - **Load balancing is connection based**
- Static load balancing methods distribute connections in a fixed manner
  - Round Robin (RR)
  - Ratio (Weighted Round Robin)
    - Distributes in a RR fashion for members/nodes whose ratio has not been met
- Dynamic load balancing looks at one or more factors, the most common method is:
  - Least Connections
    - Fewest L4 connections when load balancing decision is being made
    - Recommended when servers have similar capabilities
    - Very commonly used

Load Balancing a Service (Member)



In this example, the HTTP pool is configured with the **Least Connections (member)** method

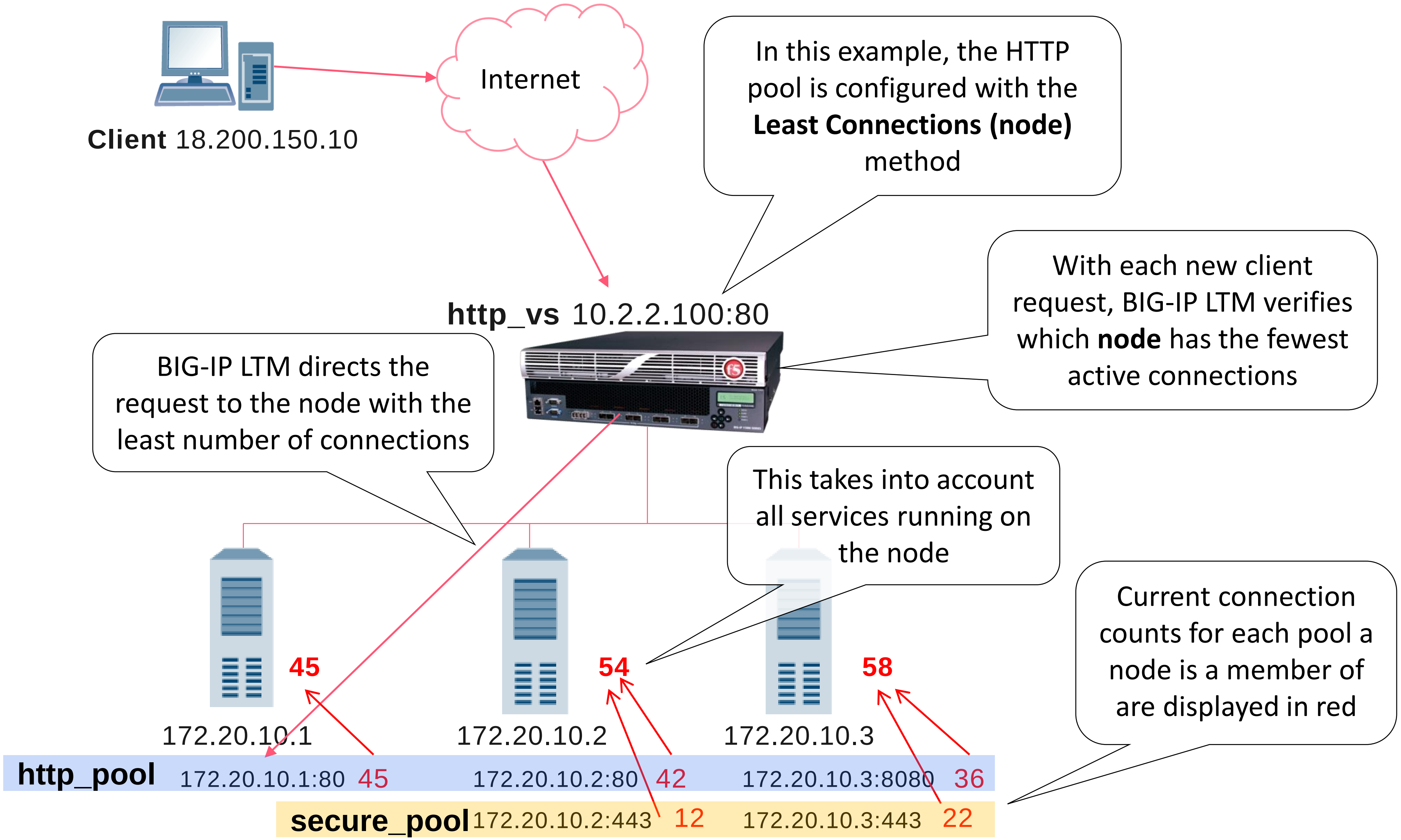
With each new client request, BIG-IP LTM verifies which **pool member** within the pool has the fewest active connections

BIG-IP LTM directs the request to the pool member with the least number of connections

Current connection counts for each pool member are displayed in red

http_pool	172.20.10.1:80	45	172.20.10.2:80	42	172.20.10.3:8080	36
secure_pool			172.20.10.2:443	12	172.20.10.3:443	22

Load Balancing an IP Address (Node)



Client 18.200.150.10
Internet
http_vs 10.2.2.100:80
45
54
58
172.20.10.1
172.20.10.2
172.20.10.3
http_pool 172.20.10.1:80 45 172.20.10.2:80 42 172.20.10.3:8080 36
secure_pool 172.20.10.2:443 12 172.20.10.3:443 22

In this example, the HTTP pool is configured with the **Least Connections (node)** method

With each new client request, BIG-IP LTM verifies which **node** has the fewest active connections

BIG-IP LTM directs the request to the node with the least number of connections

This takes into account all services running on the node

Current connection counts for each pool a node is a member of are displayed in red

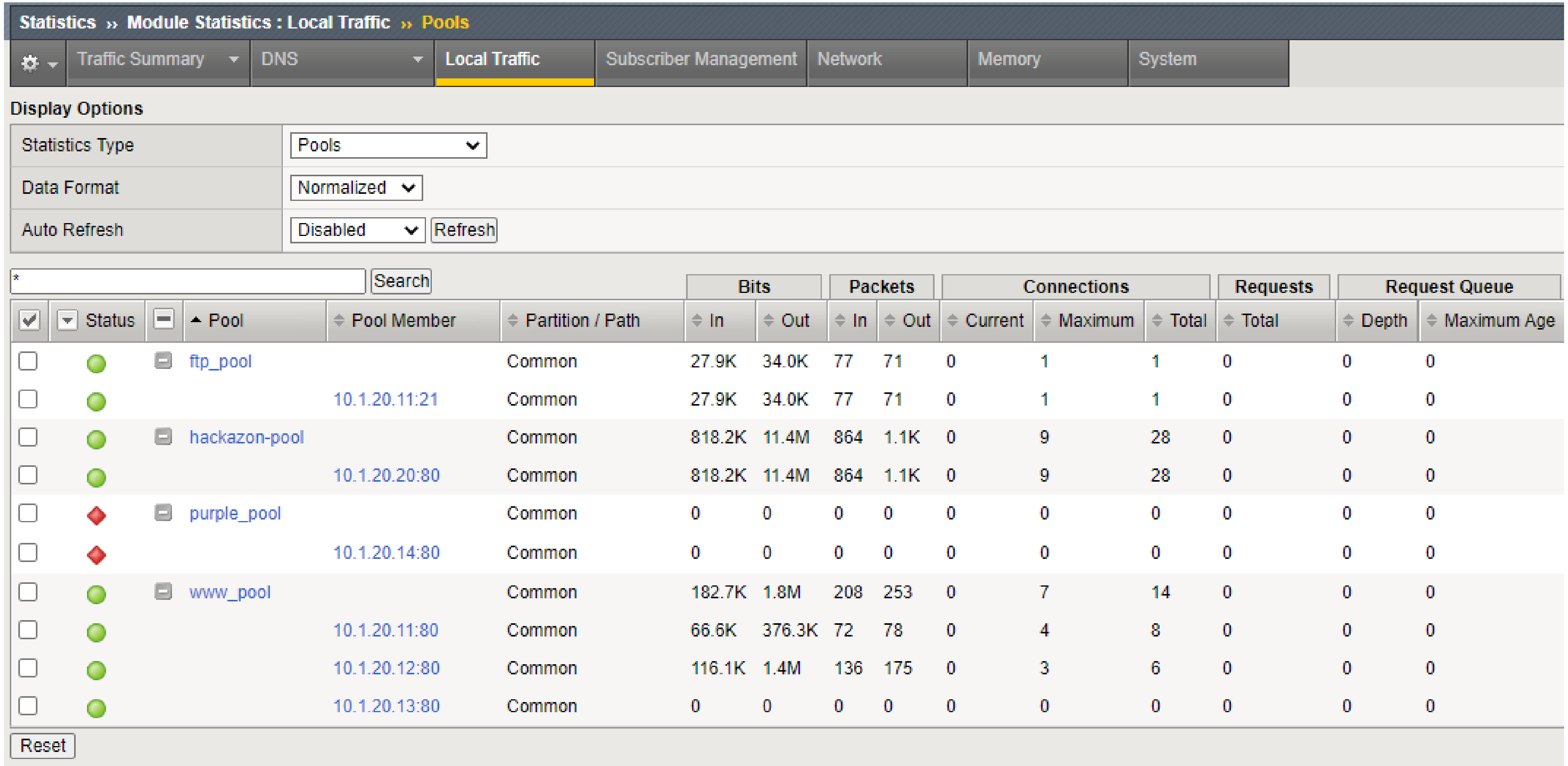
1.04

Identify the reason a pool is not working as expected

- Identify the current configured state of the pool/pool member
- Identify the current availability status of the pool/pool member
- Identify the reason a pool member has been marked down by health monitors
- Identify a pool member not in the active priority group

1.04 Identify the current configured state/status of the pool/pool member

Manual Chapter : About Pools



Statistics » Module Statistics : Local Traffic » Pools

Display Options

Statistics Type	Pools
Data Format	Normalized
Auto Refresh	Disabled [Refresh]

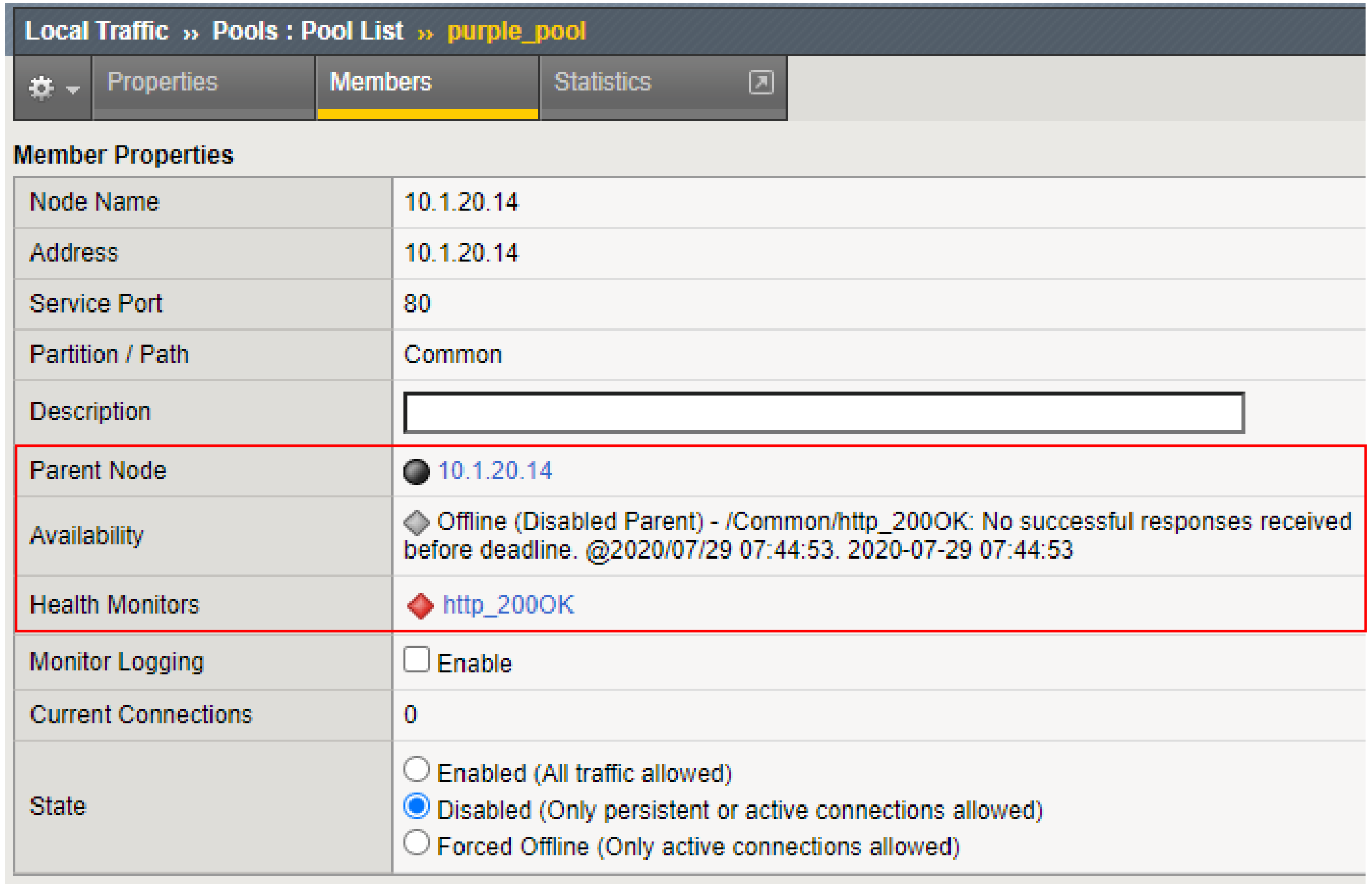
* [Search]

						Bits		Packets		Connections			Requests	Request Queue	
☑	Status	⊟	Pool	Pool Member	Partition / Path	In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age
□	🟢	⊟	ftp_pool		Common	27.9K	34.0K	77	71	0	1	1	0	0	0
□	🟢			10.1.20.11:21	Common	27.9K	34.0K	77	71	0	1	1	0	0	0
□	🟢	⊟	hackazon-pool		Common	818.2K	11.4M	864	1.1K	0	9	28	0	0	0
□	🟢			10.1.20.20:80	Common	818.2K	11.4M	864	1.1K	0	9	28	0	0	0
□	♦	⊟	purple_pool		Common	0	0	0	0	0	0	0	0	0	0
□	♦			10.1.20.14:80	Common	0	0	0	0	0	0	0	0	0	0
□	🟢	⊟	www_pool		Common	182.7K	1.8M	208	253	0	7	14	0	0	0
□	🟢			10.1.20.11:80	Common	66.6K	376.3K	72	78	0	4	8	0	0	0
□	🟢			10.1.20.12:80	Common	116.1K	1.4M	136	175	0	3	6	0	0	0
□	🟢			10.1.20.13:80	Common	0	0	0	0	0	0	0	0	0	0

[Reset]

1.04 Identify the current configured state/status of the pool/pool member

Manual Chapter : About Pools



Member Properties

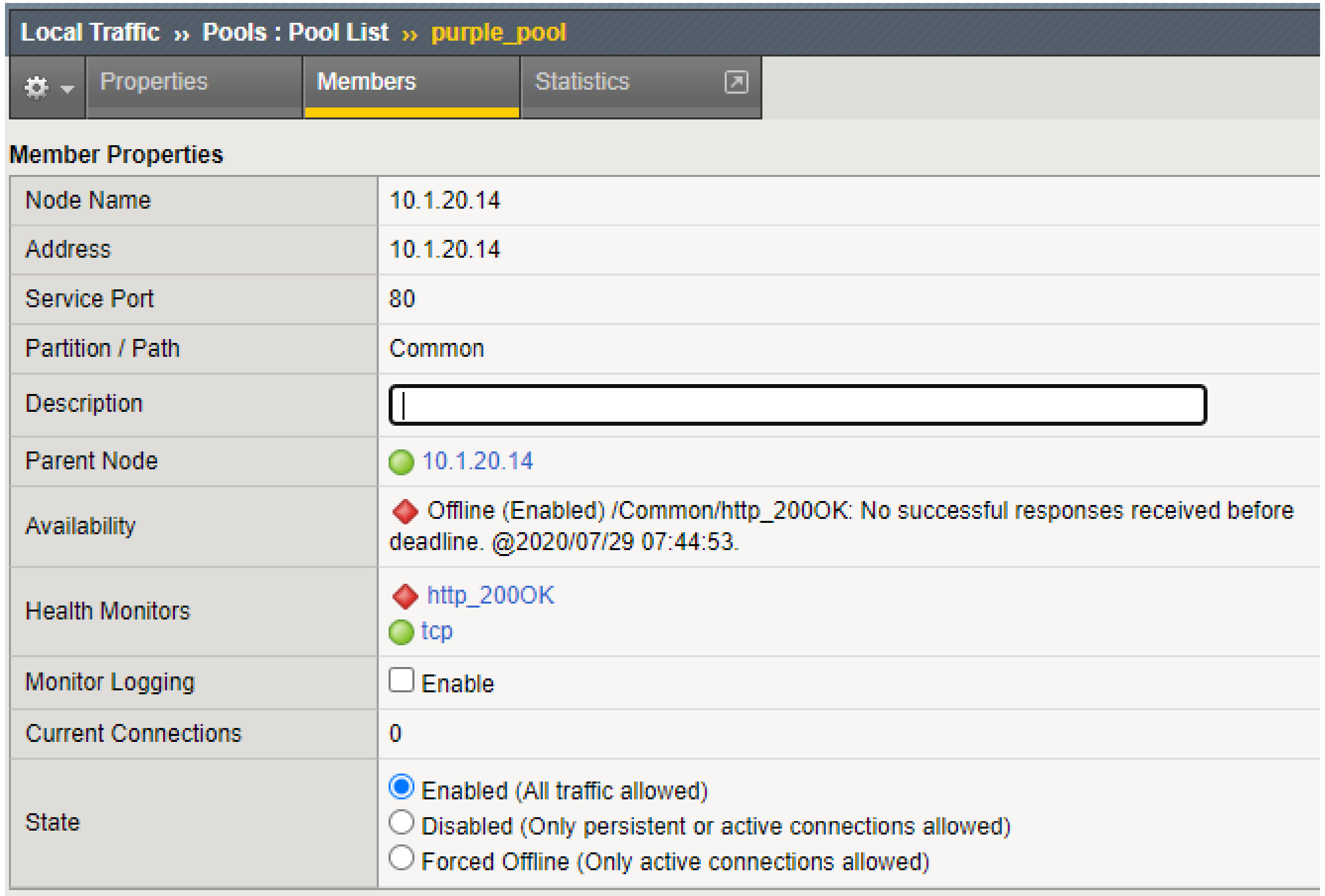
Node Name	10.1.20.14
Address	10.1.20.14
Service Port	80
Partition / Path	Common
Description	
Parent Node	● 10.1.20.14
Availability	◆ Offline (Disabled Parent) - /Common/http_200OK: No successful responses received before deadline. @2020/07/29 07:44:53. 2020-07-29 07:44:53
Health Monitors	◆ http_200OK
Monitor Logging	□ Enable
Current Connections	0
State	○ Enabled (All traffic allowed) ● Disabled (Only persistent or active connections allowed) ○ Forced Offline (Only active connections allowed)

```
(tmos)# show ltm pool purple_pool members
---------------------------------------------
Ltm::Pool: purple_pool
---------------------------------------------
Status
  Availability : offline
  State        : enabled
  Reason       : The children pool member(s) are down
  Monitor      : http_200OK
  Minimum Active Members : 0
  Current Active Members : 0
       Available Members : 0
       Total Members : 1
          Total Requests : 0
        Current Sessions : 0
<cut>
  -------------------------------------------
  | Ltm::Pool Member: 10.1.20.14:80
  -------------------------------------------
  | Status
  |   Availability   : offline
  |   State          : disabled-by-parent
  |   Reason         : http_200OK: No successful
responses received before deadline. @2020/07/29 07:44:53.
  |   Monitor        : http_200OK (pool monitor)
  |   Monitor Status : down
  |   Session Status : addr-disabled
  |   Pool Name      : purple_pool
  |   IP Address     : 10.1.20.14
```

1.04 Identify the reason a pool member has been marked down by health monitors

Manual Chapter : About Pools

- There are numerous reasons a pool member may be marked down.
  - Misconfigured monitor
  - Wrong monitor
  - Wrong port
  - Bad network path to servers
- IMPORTANT: Monitors are sourced from the **base** self IP on the outbound VLAN the BIG-IP uses to send traffic to the pool member being monitored.



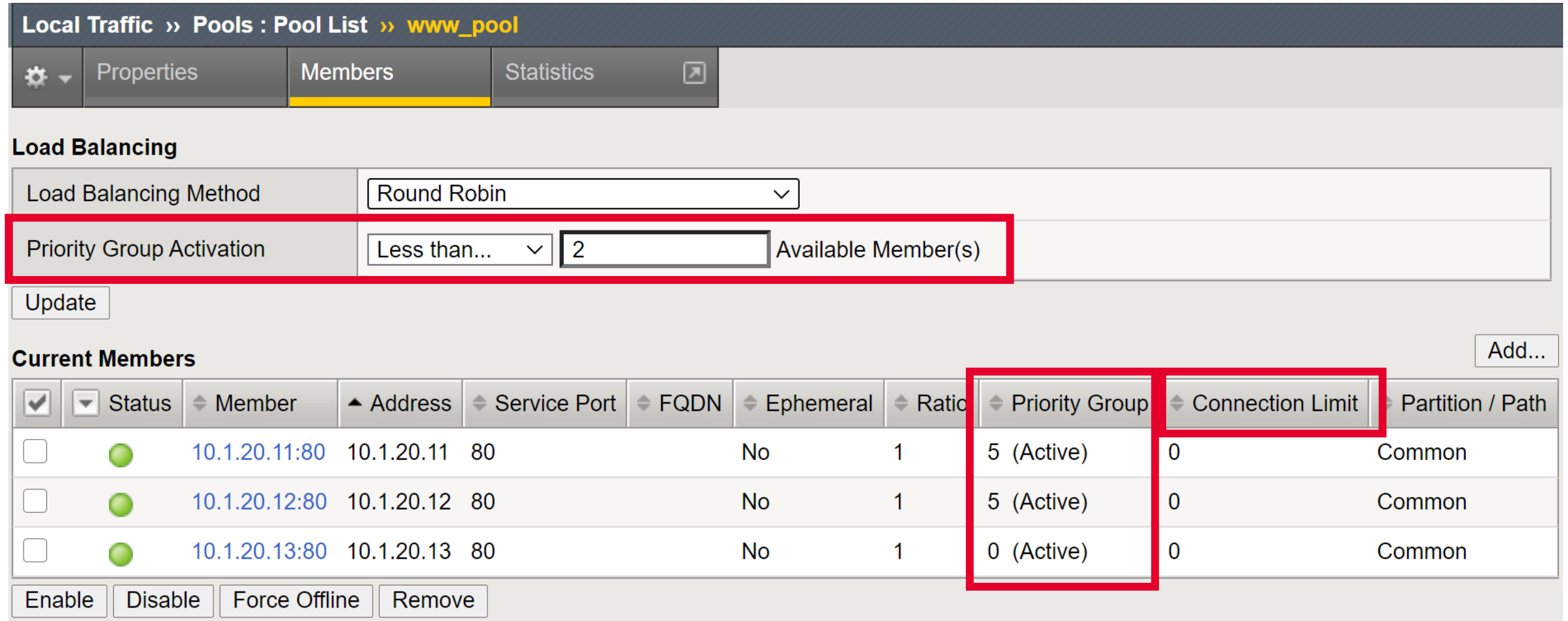
Member Properties

Node Name	10.1.20.14
Address	10.1.20.14
Service Port	80
Partition / Path	Common
Description	
Parent Node	● 10.1.20.14
Availability	◆ Offline (Enabled) /Common/http_200OK: No successful responses received before deadline. @2020/07/29 07:44:53.
Health Monitors	◆ http_200OK ● tcp
Monitor Logging	□ Enable
Current Connections	0
State	● Enabled (All traffic allowed) ○ Disabled (Only persistent or active connections allowed) ○ Forced Offline (Only active connections allowed)

1.04 Identify a pool member not in the active priority group

Priority Group Activation

- Priority Group Activation load balancing
  - Allows pool members to be used only if preferred pool members are unavailable.
  - Each pool member is assigned a priority
  - Connections are sent to the highest priority pool members first.
  - A minimum number of available members are assigned



Local Traffic ›› Pools : Pool List ›› www_pool

Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Less than... 2 Available Member(s)

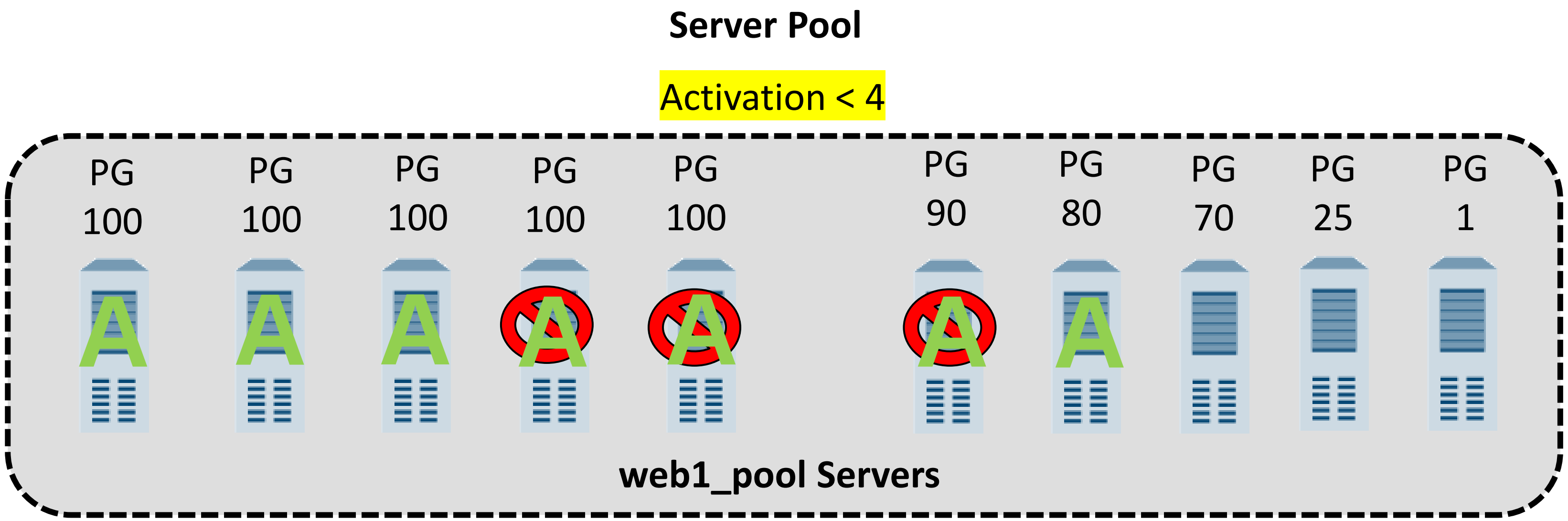
Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	10.1.20.11:80	10.1.20.11	80		No	1	5 (Active)	0	Common
□	●	10.1.20.12:80	10.1.20.12	80		No	1	5 (Active)	0	Common
□	●	10.1.20.13:80	10.1.20.13	80		No	1	0 (Active)	0	Common

1.04 Identify a pool member not in the active priority group

Priority Group Activation

- Priority Group Activation is a failure mechanism
  - Can dynamically pull in new members into the pool
  - Pulls lower priority groups into higher priority groups
  - Pulls in all members of a priority group together



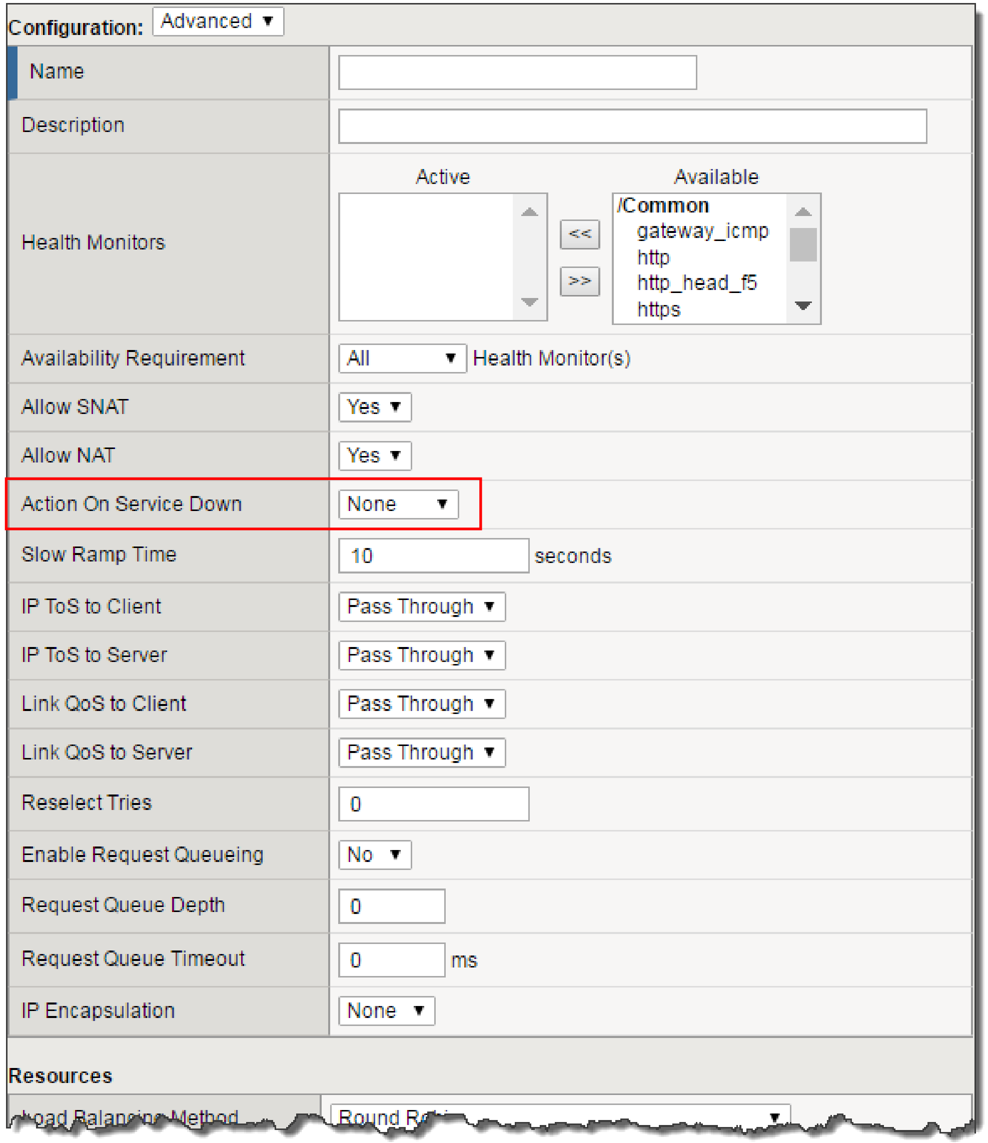
2.04

Identify the reason load balancing is not working as expected

- Identify current availability status
- Identify misconfigurations (incorrect health checks, action on service down, etc.)
- Consider persistence, priority group activation, rate/connection limits

2.04 Action on Service Down

- Action on Service Down
  - **None** – RST to client after idle timeout reached (Default)
  - **Reject** – sent RST to active client connections
  - **Drop** – silently remove the connection
  - **Reselect** – move connection to alternate pool member
- Slow Ramp Time
  - Set less traffic to newly established pool member



Configuration: Advanced

Name	
Description	
Health Monitors	Active: Available: /Common gateway_icmp http http_head_f5 https
Availability Requirement	All Health Monitor(s)
Allow SNAT	Yes
Allow NAT	Yes
Action On Service Down	None
Slow Ramp Time	10 seconds
IP ToS to Client	Pass Through
IP ToS to Server	Pass Through
Link QoS to Client	Pass Through
Link QoS to Server	Pass Through
Reselect Tries	0
Enable Request Queueing	No
Request Queue Depth	0
Request Queue Timeout	0 ms
IP Encapsulation	None

Resources

Load Balancing Method	Round R

Enabling/Disabling Nodes and Pool Members

State determines how persistence and connections are handled

Pool Member State	Interaction with Pool Member
Enabled All Traffic Allowed	Existing Connection – Maintained New Persistence Records – Can be Created New Connections – Can be Created
Disabled (Members or Nodes) Only persistent or active connections allowed.	Existing Connection – Maintained New Persistence Records – Not Created New Connections – Can be Created *only* for Client with an Existing Persistence record
Forced Offline (Members or Nodes) Only active connections allowed.	Existing Connection – Maintained New Persistence Records – Not Created New Connections – Not Created

2.04 Consider persistence, priority group activation, rate/connection limits

REVIEW

- Persistence
  - Check records
  - Object state
  - Understand the difference in behavior of
    - Pools and Nodes which are Disabled or Forced Offline
    - Persistence Override Connection limits

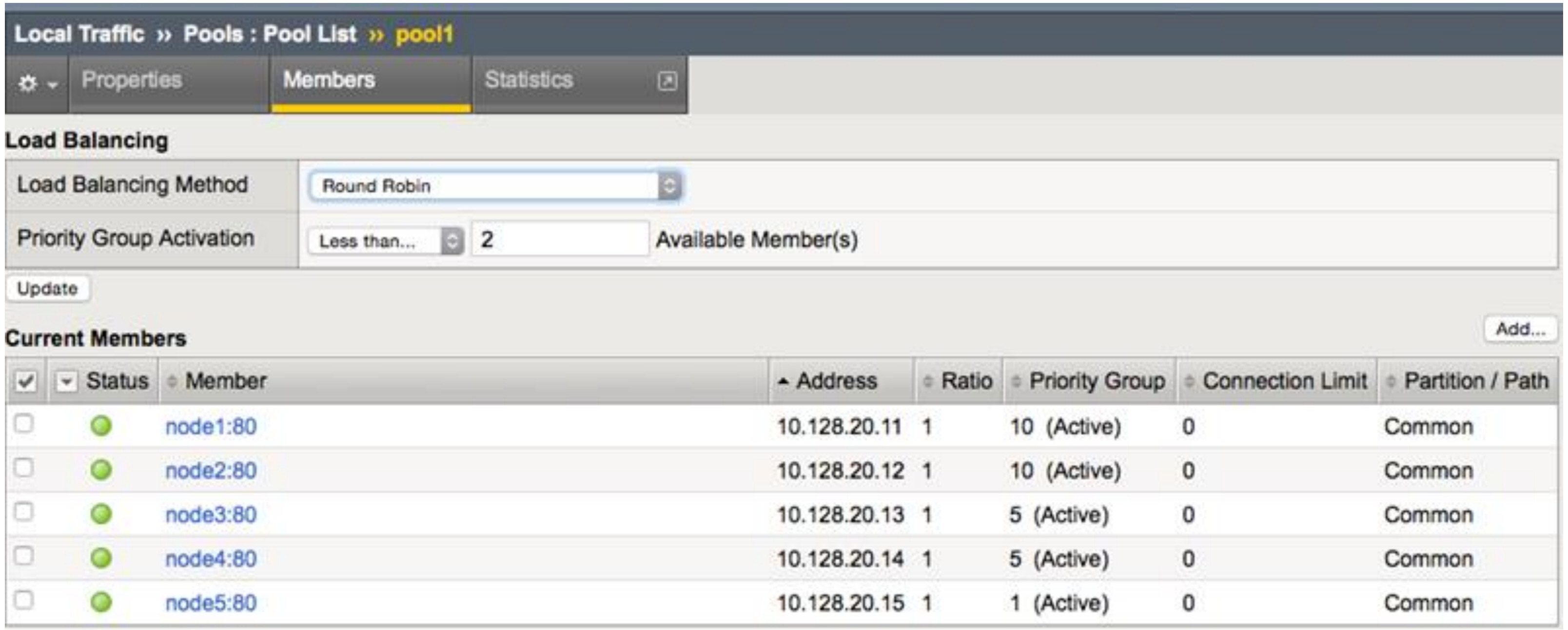
Review

Is there something wrong with this pool?

If all members are up why aren't all members taking traffic?

If **node1** fails, which members will take traffic?

If all members are up, but you see traffic statistics on node3 and node4 what does that tell you?



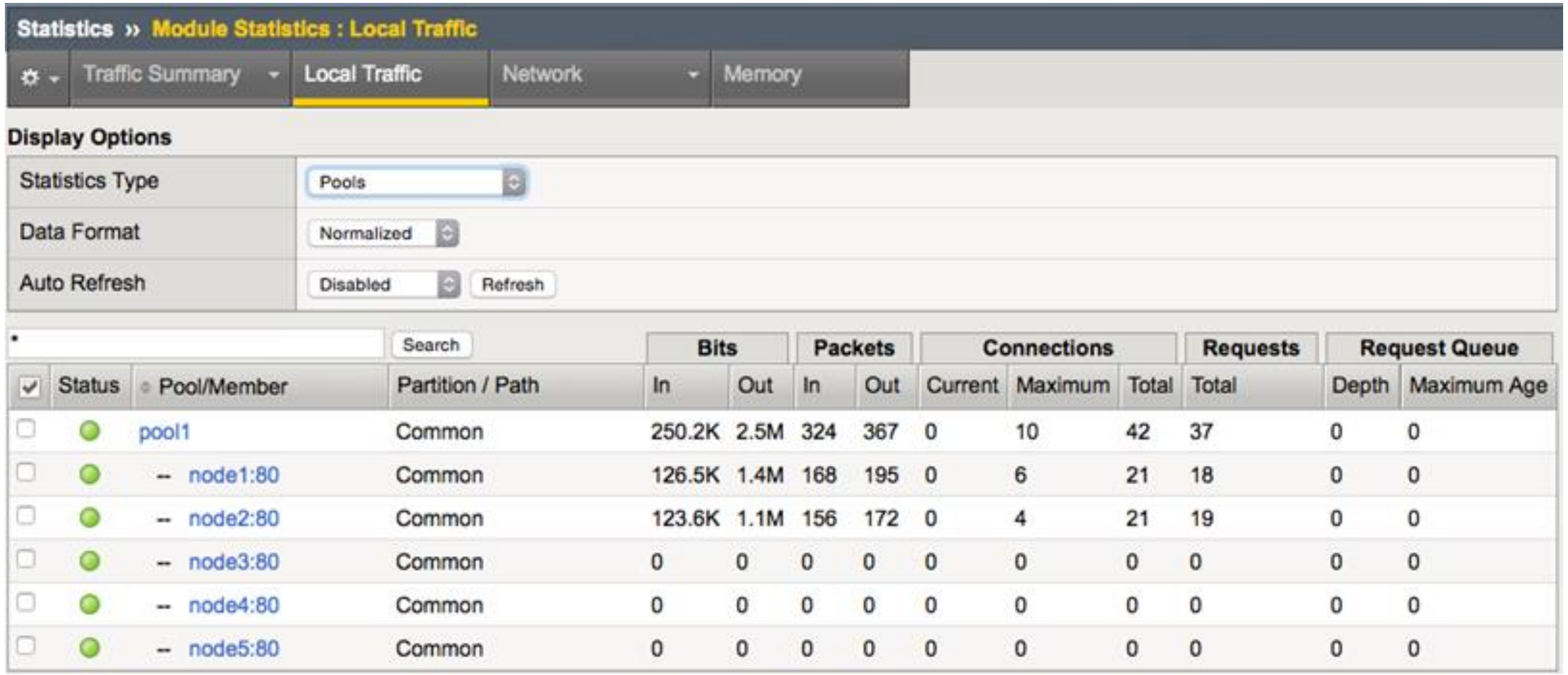
Local Traffic » Pools : Pool List » pool1

Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Less than... 2 Available Member(s)

Current Members

☑	Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	node1:80	10.128.20.11	1	10 (Active)	0	Common
□	●	node2:80	10.128.20.12	1	10 (Active)	0	Common
□	●	node3:80	10.128.20.13	1	5 (Active)	0	Common
□	●	node4:80	10.128.20.14	1	5 (Active)	0	Common
□	●	node5:80	10.128.20.15	1	1 (Active)	0	Common

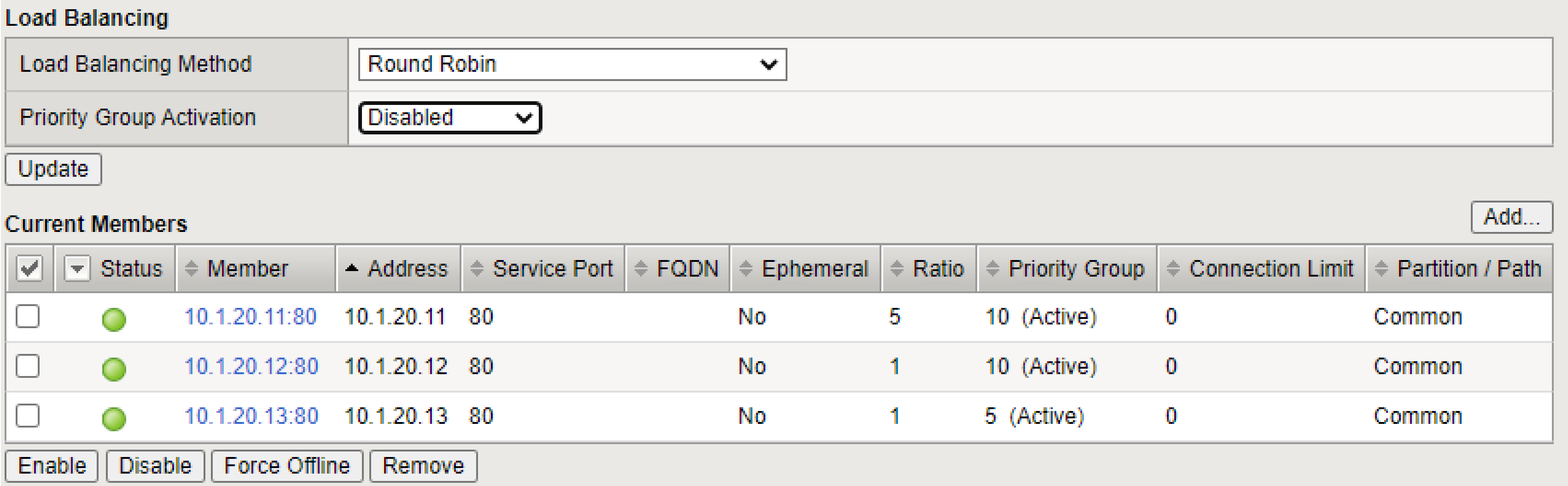


Statistics » Module Statistics : Local Traffic

Display Options

Statistics Type	Pools
Data Format	Normalized
Auto Refresh	Disabled

				Bits		Packets		Connections			Requests	Request Queue	
☑	Status	Pool/Member	Partition / Path	In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age
□	●	pool1	Common	250.2K	2.5M	324	367	0	10	42	37	0	0
□	●	-- node1:80	Common	126.5K	1.4M	168	195	0	6	21	18	0	0
□	●	-- node2:80	Common	123.6K	1.1M	156	172	0	4	21	19	0	0
□	●	-- node3:80	Common	0	0	0	0	0	0	0	0	0	0
□	●	-- node4:80	Common	0	0	0	0	0	0	0	0	0	0
□	●	-- node5:80	Common	0	0	0	0	0	0	0	0	0	0



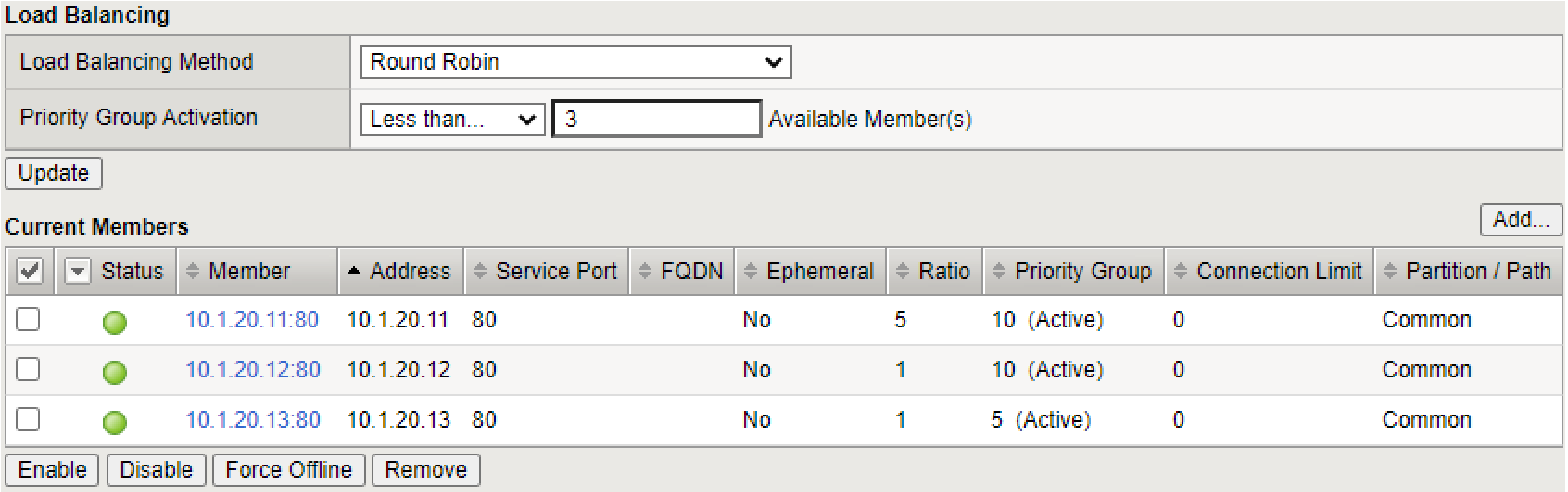
Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Disabled

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	10.1.20.11:80	10.1.20.11	80		No	5	10 (Active)	0	Common
□	●	10.1.20.12:80	10.1.20.12	80		No	1	10 (Active)	0	Common
□	●	10.1.20.13:80	10.1.20.13	80		No	1	5 (Active)	0	Common

Given the configuration what pool member will take the most connections?



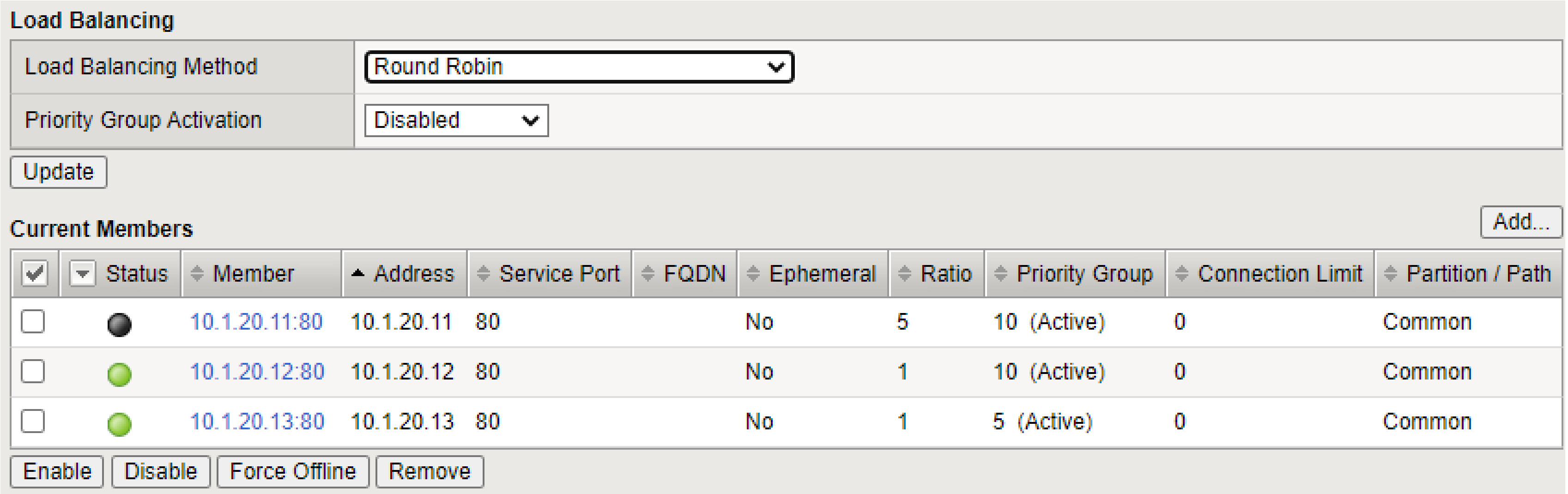
Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Less than... 3 Available Member(s)

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	10.1.20.11:80	10.1.20.11	80		No	5	10 (Active)	0	Common
□	●	10.1.20.12:80	10.1.20.12	80		No	1	10 (Active)	0	Common
□	●	10.1.20.13:80	10.1.20.13	80		No	1	5 (Active)	0	Common

Given the configuration which pool members will process traffic?



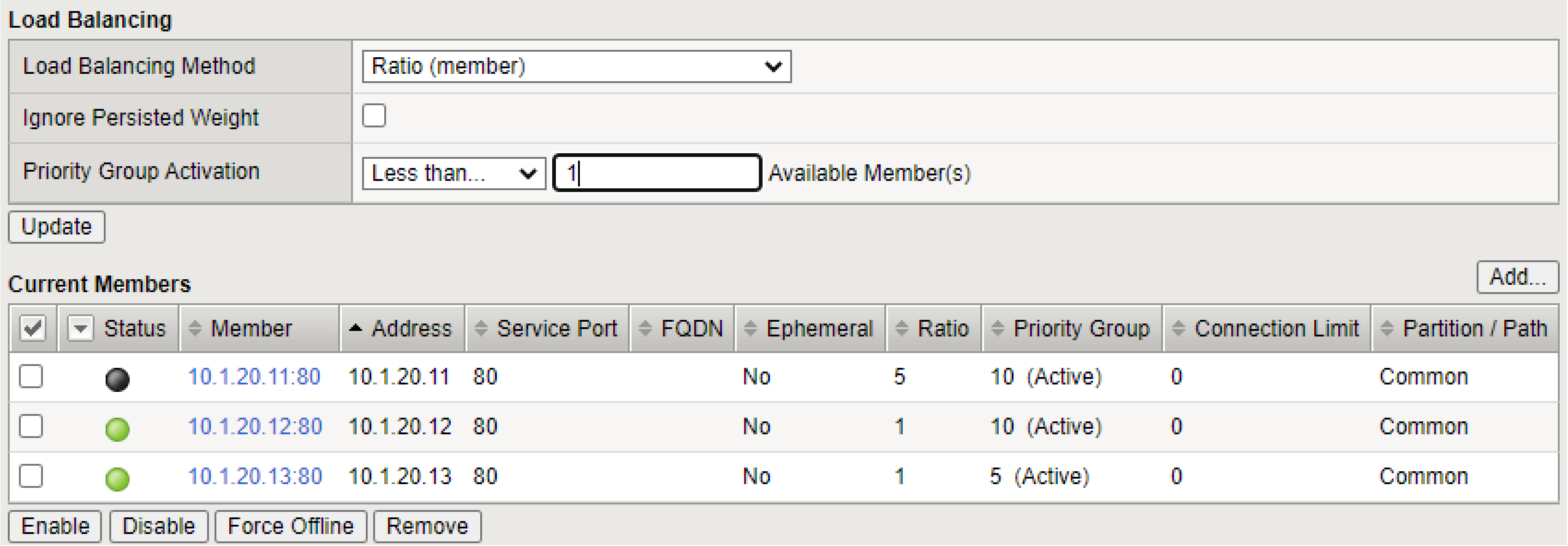
Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Disabled

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
☐	●	10.1.20.11:80	10.1.20.11	80		No	5	10 (Active)	0	Common
☐	🟢	10.1.20.12:80	10.1.20.12	80		No	1	10 (Active)	0	Common
☐	🟢	10.1.20.13:80	10.1.20.13	80		No	1	5 (Active)	0	Common

You have disabled 10.1.20.11:80, but the pool member continues to receive new connections. What does this tell you?



Load Balancing

Load Balancing Method	Ratio (member)
Ignore Persisted Weight	☐
Priority Group Activation	Less than... 1 Available Member(s)

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
☐	●	10.1.20.11:80	10.1.20.11	80		No	5	10 (Active)	0	Common
☐	🟢	10.1.20.12:80	10.1.20.12	80		No	1	10 (Active)	0	Common
☐	🟢	10.1.20.13:80	10.1.20.13	80		No	1	5 (Active)	0	Common

Given the configuration what pool member will take the most connection?

System Configuration

Objectives 3.01, 3.02, 3.04 - 3.09, 5.02

3.01

Identify and report current device status

- Interpret the LCD panel warning messages
- Use the dashboard to gauge the current running status of the system
- Review the Network Map in order to determine the status of objects
- Interpret current systems status via GUI or TMSH
- Interpret high availability and device trust status

3.01 Interpret the LCD panel warning messages

K15521451: BIG-IP TMOS operations guide | Chapter 12: Log files and alerts

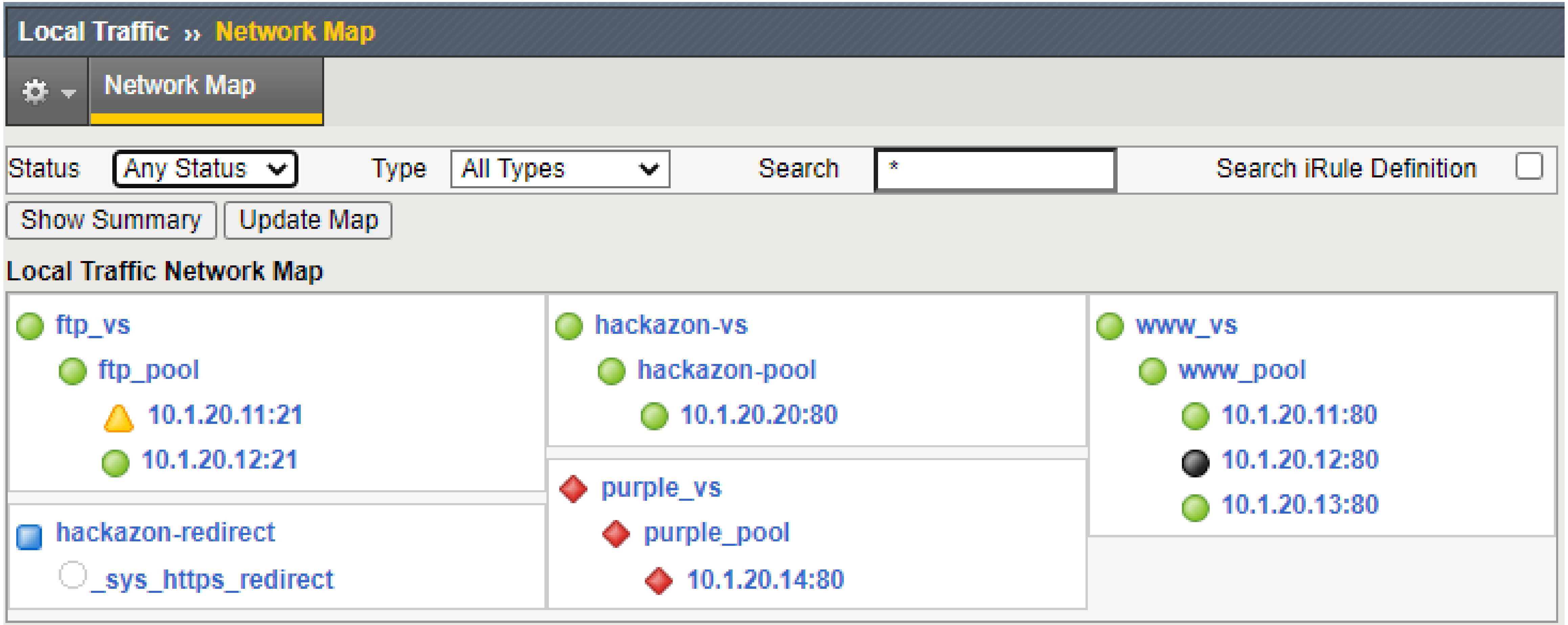
- /etc/alertd/alert.conf – contains the LCD error message

```
LCD Warning:  Critical: 9d Blocking Dos Attack

Local Traffic Log: sweeper_update: aggressive
mode activated. 372313/438016 pages
```

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/platform-b5000/2.html?sr=54998935

3.01 Review the Network Map in order to determine the status of objects

REVIEW



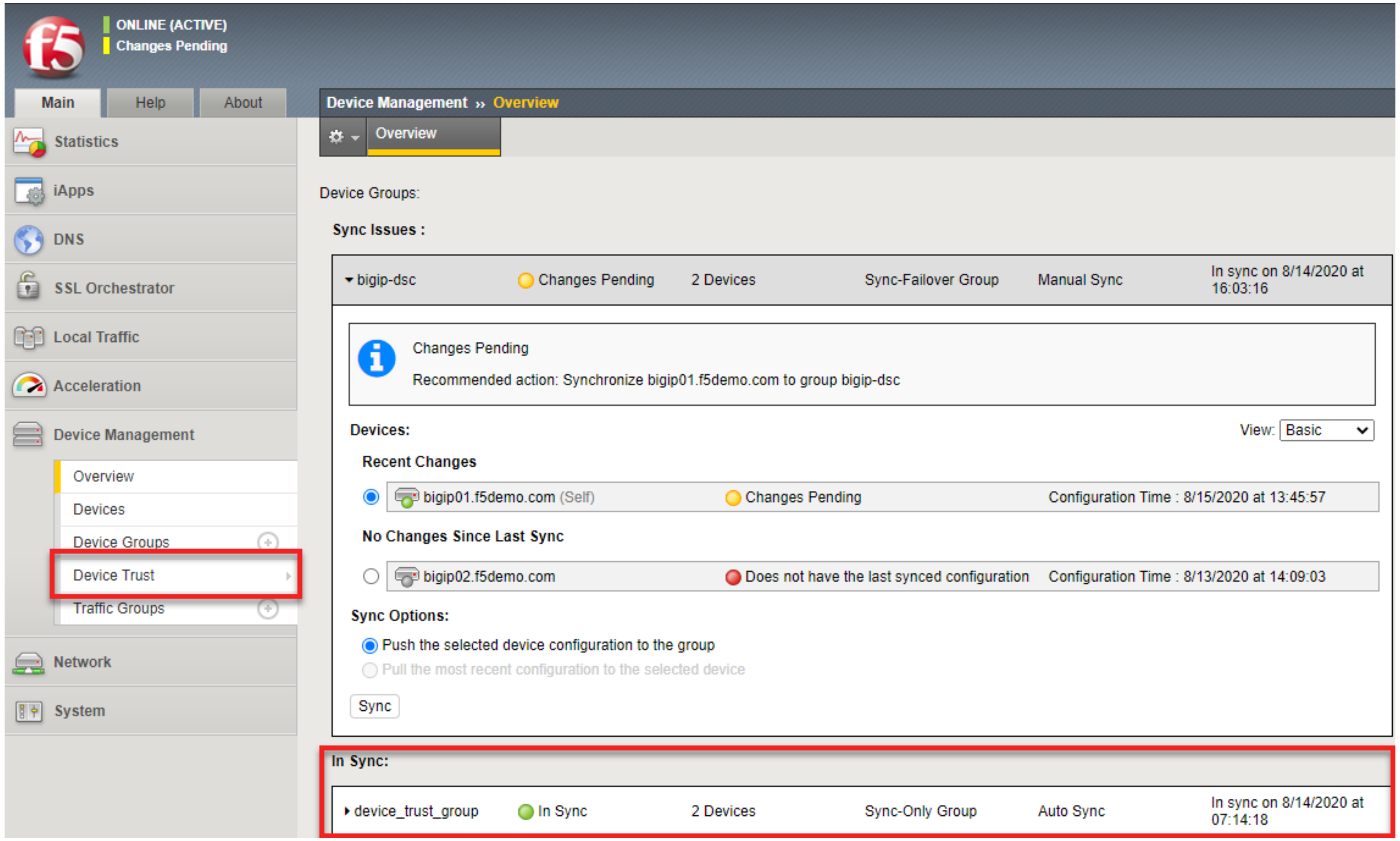
Local Traffic Network Map

- ● ftp_vs
  - ● ftp_pool
    - △ 10.1.20.11:21
    - ● 10.1.20.12:21
- ■ hackazon-redirect
  - ○ _sys_https_redirect
- ● hackazon-vs
  - ● hackazon-pool
    - ● 10.1.20.20:80
- ◆ purple_vs
  - ◆ purple_pool
    - ◆ 10.1.20.14:80
- ● www_vs
  - ● www_pool
    - ● 10.1.20.11:80
    - ● 10.1.20.12:80
    - ● 10.1.20.13:80

3.01 Interpret high availability and device trust status

[Manual : BIG-IP Device Service Clustering: Administration](#)

- To create secure communications between BIG-IPs in a HA configuration (Device Service Cluster – DSC) they are place into a Device Trust Group:
  - BIG-IP exchanges device certificates
  - If a certificate expires the trust is broken
  - The device_trust_group must be in sync for configsync, mirroring and network failover to be available.
- More on HA later…



Device Groups:

Sync Issues :

▾ bigip-dsc	Changes Pending	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/14/2020 at 16:03:16

Changes Pending

Recommended action: Synchronize bigip01.f5demo.com to group bigip-dsc

Devices:

View: Basic

Recent Changes

●	bigip01.f5demo.com (Self)	Changes Pending	Configuration Time : 8/15/2020 at 13:45:57

No Changes Since Last Sync

○	bigip02.f5demo.com	Does not have the last synced configuration	Configuration Time : 8/13/2020 at 14:09:03

Sync Options:

● Push the selected device configuration to the group

○ Pull the most recent configuration to the selected device

Sync

In Sync:

▸ device_trust_group	In Sync	2 Devices	Sync-Only Group	Auto Sync	In sync on 8/14/2020 at 07:14:18

3.03

Identify management connectivity configurations

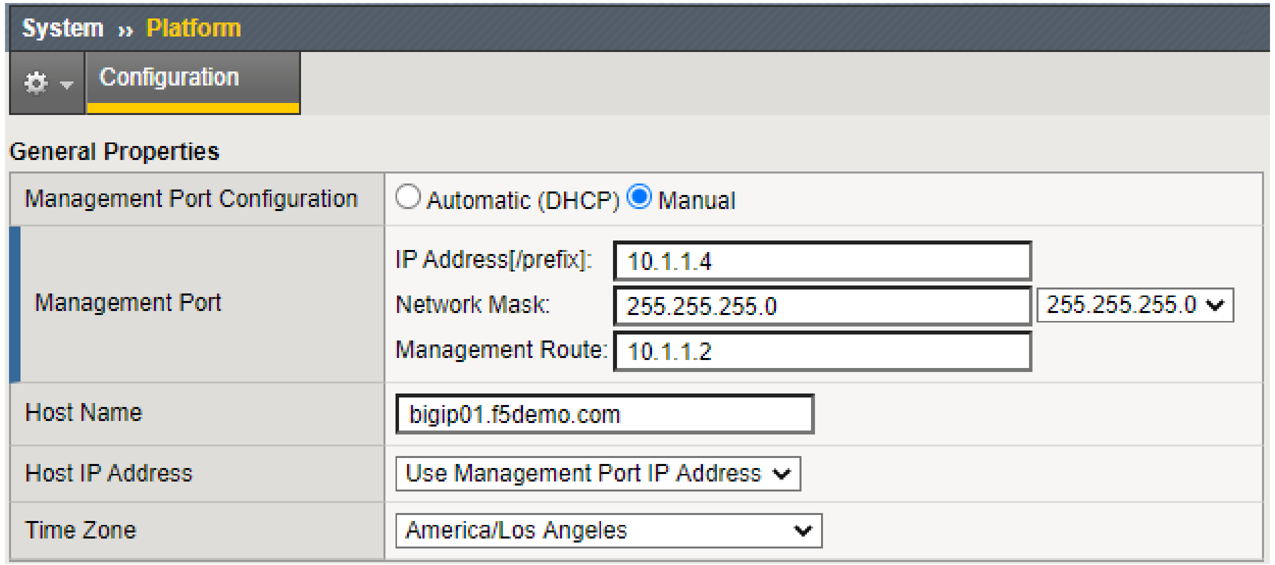
- Identify the configured management-IP address
- Show remote connectivity to the BIG-IP Management interface
- Explain management IP connectivity issue
- Interpret port lockdown settings to Self-IP
- Identify HTTP/SSH access list to management-IP address

3.03 Identify the configured management-IP address

K15040: Configuring and displaying the management IP address for the BIG-IP system

K7312: Overview of the management interface (port)

GUI


System » Platform

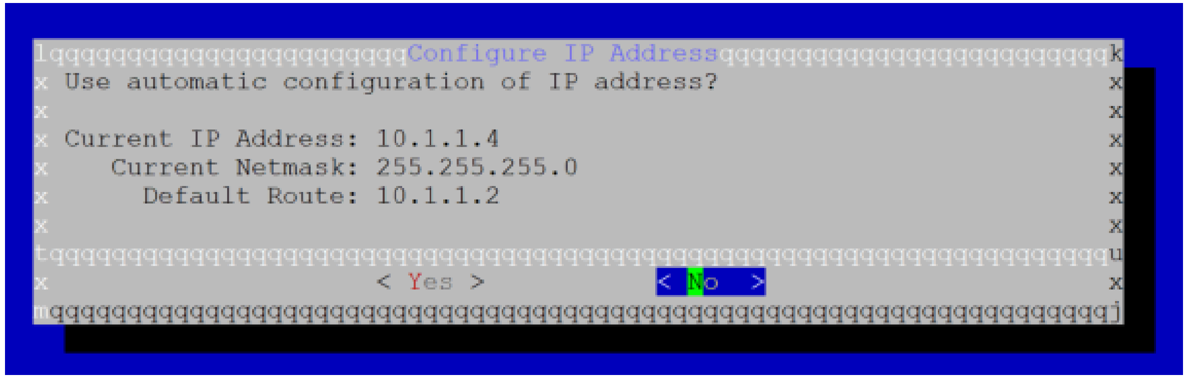
Configuration

General Properties

Management Port Configuration	○ Automatic (DHCP) ● Manual
Management Port	IP Address[/prefix]: 10.1.1.4 Network Mask: 255.255.255.0 (255.255.255.0) Management Route: 10.1.1.2
Host Name	bigip01.f5demo.com
Host IP Address	Use Management Port IP Address
Time Zone	America/Los Angeles

TMSH

```
tmos)# list sys management-ip
sys management-ip 10.1.1.4/24 {
    description configured-statically
}
```

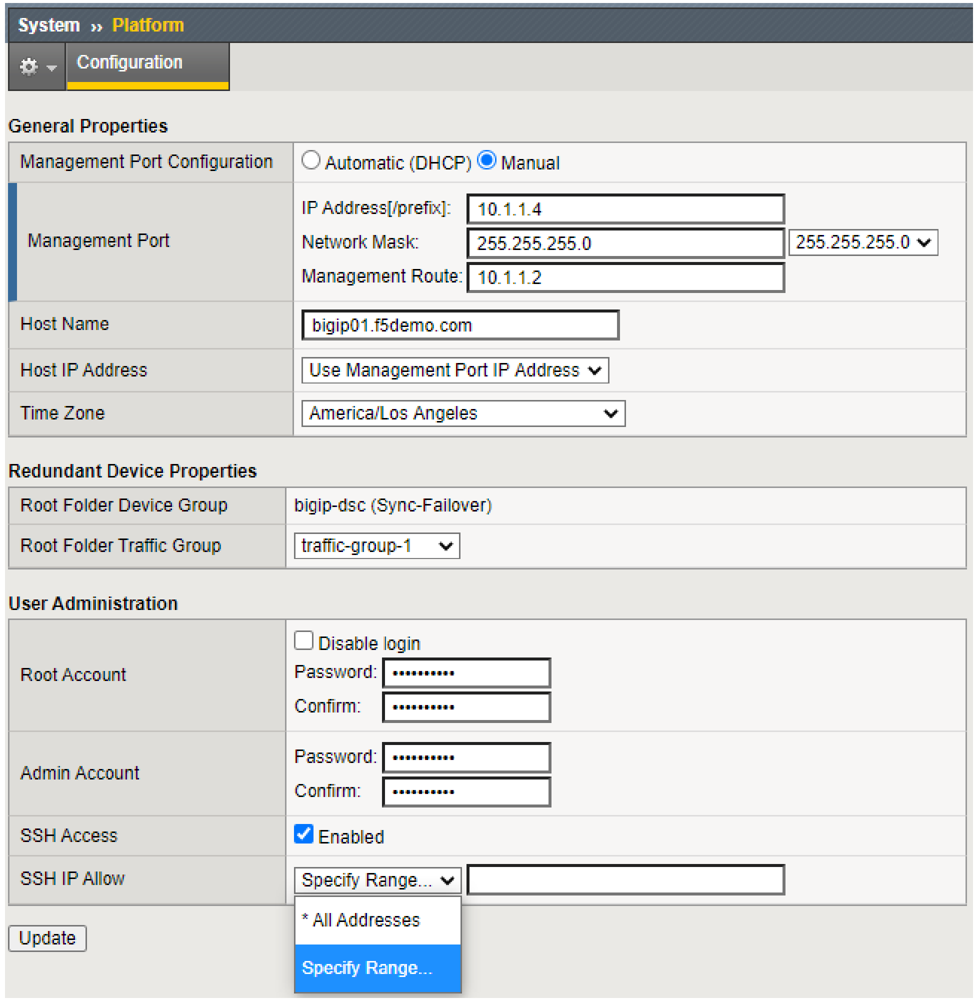


```
lqqqqqqqqqqqqqqqqqqqqqqqConfigure IP Addressqqqqqqqqqqqqqqqqqqqqqqqqqk
x Use automatic configuration of IP address?                          x
x                                                                     x
x Current IP Address: 10.1.1.4                                        x
x    Current Netmask: 255.255.255.0                                   x
x      Default Route: 10.1.1.2                                        x
x                                                                     x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                      < Yes >              < No  >                   x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

“config” utility at the linux prompt

3.03 Identify SSH access list to management-IP address

K13309: Restricting access to the Configuration utility by source IP address (11.x - 16.x)



General Properties

Management Port Configuration	○ Automatic (DHCP) ● Manual
Management Port	IP Address[/prefix]: 10.1.1.4 Network Mask: 255.255.255.0 255.255.255.0 Management Route: 10.1.1.2
Host Name	bigip01.f5demo.com
Host IP Address	Use Management Port IP Address
Time Zone	America/Los Angeles

Redundant Device Properties

Root Folder Device Group	bigip-dsc (Sync-Failover)
Root Folder Traffic Group	traffic-group-1

User Administration

Root Account	□ Disable login Password: •••••••••• Confirm: ••••••••••
Admin Account	Password: •••••••••• Confirm: ••••••••••
SSH Access	☑ Enabled
SSH IP Allow	Specify Range...

- To add to the allow list:
  - modify /sys sshd allow add { <IP address or IP address range> }
- To replace the list
  - modify /sys sshd replace-all-with {<IP address or IP address range>}
- Default is:

```
(tmos)# list sys sshd allow
sys sshd {
    allow { All }
}
```

- Save the change by entering the following command:
  - save /sys config

3.03 Identify HTTP access list to management-IP address

K13309: Restricting access to the Configuration utility by source IP address (11.x - 16.x)

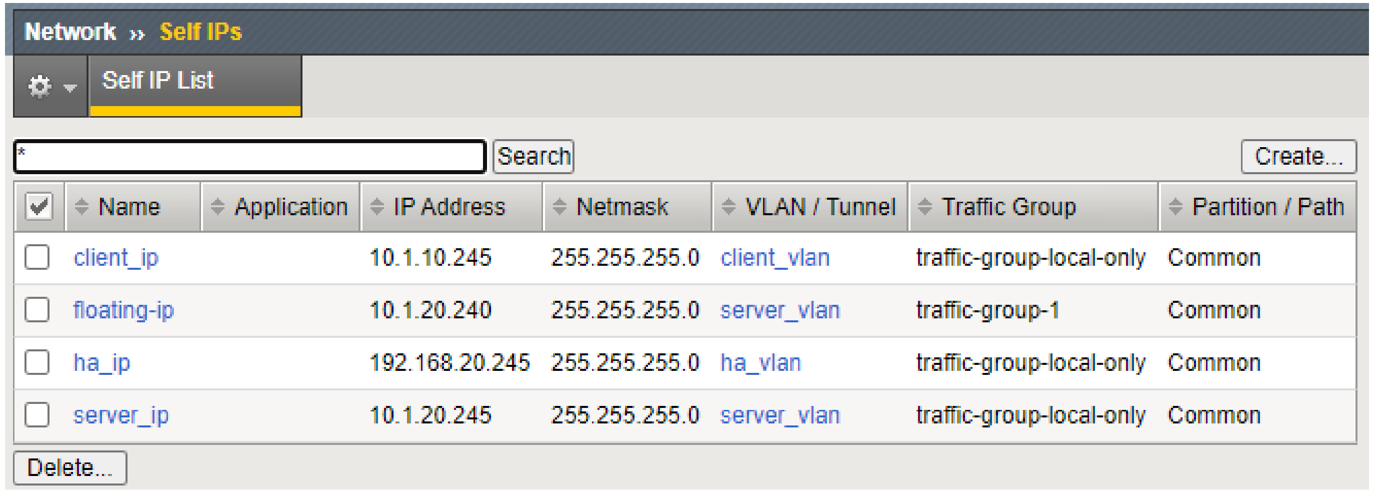
- To add to the allow list:
  - modify /sys httpd allow add { <IP address or IP address range> }
- To replace the list
  - modify /sys httpd replace-all-with {<IP address or IP address range>}
- Default is:

```
(tmos)# list sys httpd
allow
sys httpd {
    allow { All }
}
```

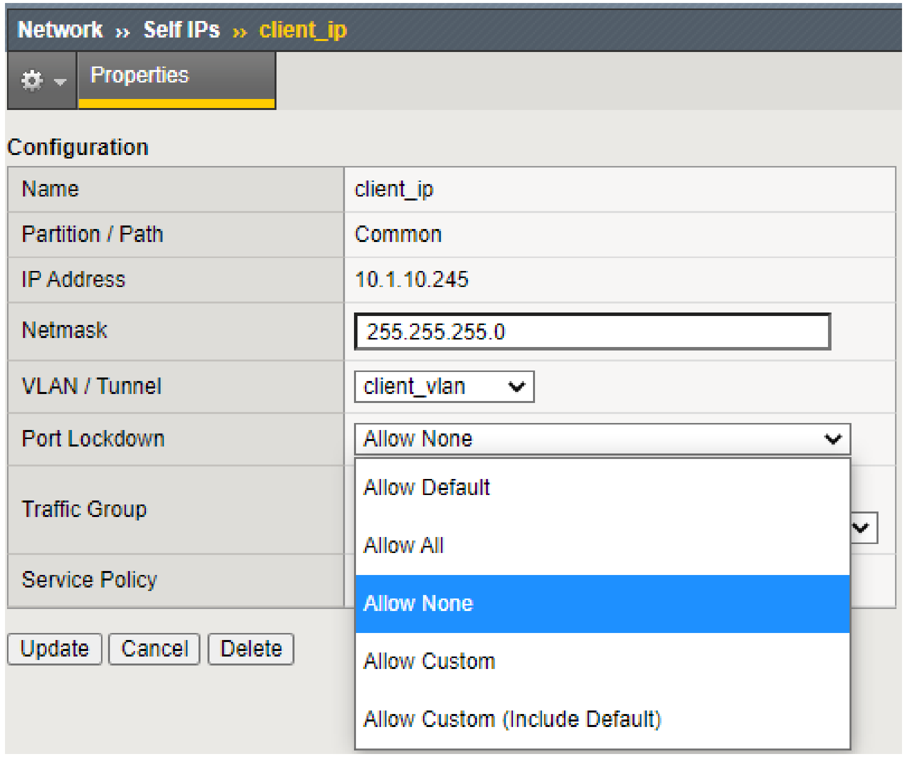
- Save the change by entering the following command:
  - save /sys config

3.03 Interpret port lockdown settings to Self-IP

- Port Lockdown determines which ports a self IP address will respond to
  - By default Port Lockdown is none, and the self IP only responds to ICMP
- Port Lockdown settings can be modified to allow other traffic, such as, port 443 or 22 for management



☑	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
□	client_ip		10.1.10.245	255.255.255.0	client_vlan	traffic-group-local-only	Common
□	floating-ip		10.1.20.240	255.255.255.0	server_vlan	traffic-group-1	Common
□	ha_ip		192.168.20.245	255.255.255.0	ha_vlan	traffic-group-local-only	Common
□	server_ip		10.1.20.245	255.255.255.0	server_vlan	traffic-group-local-only	Common

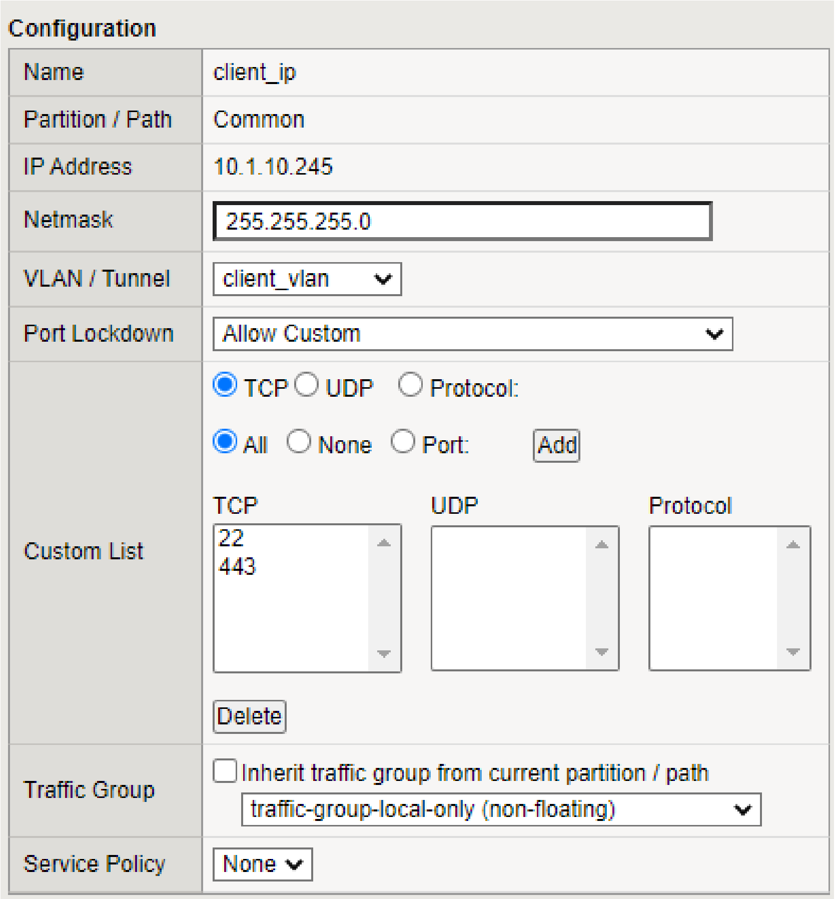


Configuration

Name	client_ip
Partition / Path	Common
IP Address	10.1.10.245
Netmask	255.255.255.0
VLAN / Tunnel	client_vlan
Port Lockdown	Allow None
Traffic Group	
Service Policy	

3.03 Interpret port lockdown settings to Self-IP

- You can select “Allow Default” which opens the following:
  - ospf:any
  - tcp:domain (53)
  - tcp:f5-iquery (4353)
  - tcp:https (443)
  - tcp:snmp (161)
  - tcp:ssh (22)
  - udp:520
  - udp:cap (1026 - for network failover)
  - udp:domain (53)
  - udp:f5-iquery (4353)
  - udp:snmp (161)
- Or you can select custom ports to open



Configuration

Name	client_ip
Partition / Path	Common
IP Address	10.1.10.245
Netmask	255.255.255.0
VLAN / Tunnel	client_vlan
Port Lockdown	Allow Custom
Custom List	● TCP ○ UDP ○ Protocol: ● All ○ None ○ Port: Add TCP: 22, 443 UDP: Protocol: Delete
Traffic Group	□ Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

```
list net self
net self client_ip {
    address
10.1.10.245/24
    allow-service {
        tcp:ssh
        tcp:https
    }
```

3.03 Explain management IP connectivity issue

- If using OOB Management
  - Is the IP, netmask and default gateway configured correctly
  - Is the interface up
    - At the Linux prompt: **ifconfig -a mgmt**
- If using a Self IP
  - Is the IP and netmask configured correctly
    - Are they routable
  - Are the appropriate ports open, 22 for SSH and/or 443 for the GUI interface
  - Are the any packet filters blocking traffic

5.02

Explain the processes of licensing, license reactivation, and license modification

- Show where to license (activate.F5.com)
- Identify license issues
- Identify Service Check Date (upgrade)

5.02 Identify Service Check Date (upgrade)

In the license file /config/bigip.license

```
#
#       Licensing Information
#
Licensed date :                   20160617
License start :                   20160616
License end :                     20160802
Service check date :              20160522
#
#       Platform Information
#
Registration Key :                NHQRP-YWHGO-WFQJK-YAZTM-FHJYBFE
Licensed version :                11.5.3
```

```
(tmos)# show sys license
Sys::License
Licensed Version    10.0.1
Registration key    W8521-87284-29591-40029-4630899
Licensed On         2009/06/19
License Start Date  2009/06/18
License End Date    2011/07/06
Service Check Date  2011/06/06
Platform ID C62
Appliance Serial Number bip055932s

Active Modules
Global Traffic Manager Module (C270772-7443956)
ADD IPV6 GATEWAY
STP Feature Module
Link Controller Module (D336898-2457178)
ADD IPV6 GATEWAY
ADD RATE SHAPING
ADD ROUTING BGP
ADD ROUTING OSPF
ADD ROUTING RIP
Local Traffic Manager Module (Z235635-4592979)
ADD IPV6 GATEWAY
ADD RATE SHAPING
ADD 5 MBPS COMPRESSION
ADD RAMCACHE
ADD ROUTING BGP
ADD ROUTING OSPF
ADD ROUTING RIP
Message Security Manager
ADD CLIENT AUTHENTICATION
ADD SSL 100
```

3.07

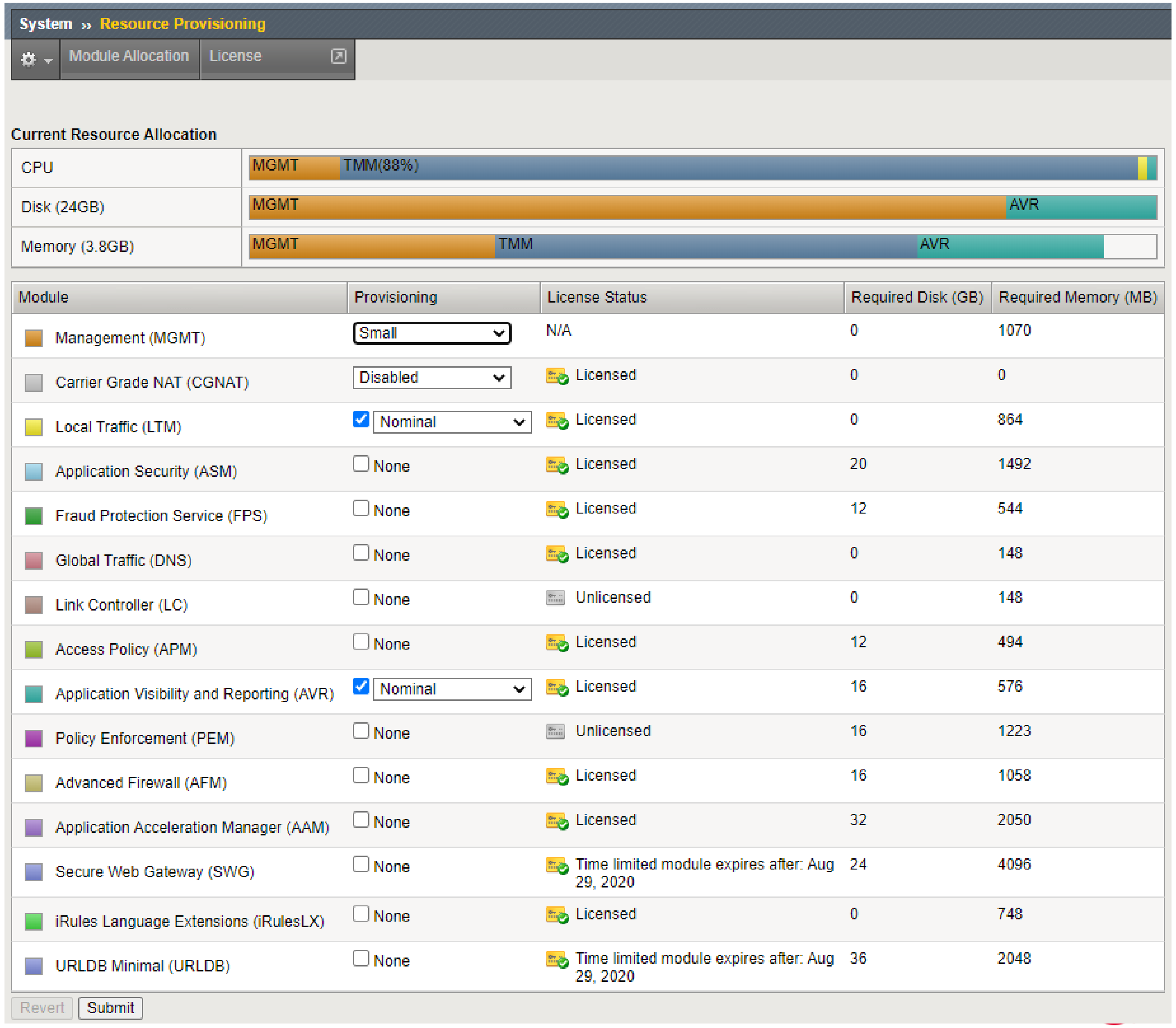
Identify which modules are licensed and/or provisioned

- Show provisioned modules
- Report modules which are licensed
- Report modules which are provisioned but not licensed
- Show resource utilization of provisioned modules

3.07 Show provisioned modules

- The Resource Provisioning page
  - Shows licensed modules
  - Show subscriptions license and expiration
  - Show provisioned modules

A module must be Licensed and Provisioned to process traffic.



System » Resource Provisioning

Current Resource Allocation

CPU	MGMT TMM(88%)
Disk (24GB)	MGMT AVR
Memory (3.8GB)	MGMT TMM AVR

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
🟧 Management (MGMT)	Small	N/A	0	1070
⬜ Carrier Grade NAT (CGNAT)	Disabled	Licensed	0	0
🟨 Local Traffic (LTM)	☑ Nominal	Licensed	0	864
🟦 Application Security (ASM)	☐ None	Licensed	20	1492
🟩 Fraud Protection Service (FPS)	☐ None	Licensed	12	544
🟥 Global Traffic (DNS)	☐ None	Licensed	0	148
🟫 Link Controller (LC)	☐ None	Unlicensed	0	148
🟩 Access Policy (APM)	☐ None	Licensed	12	494
🟦 Application Visibility and Reporting (AVR)	☑ Nominal	Licensed	16	576
🟪 Policy Enforcement (PEM)	☐ None	Unlicensed	16	1223
🟨 Advanced Firewall (AFM)	☐ None	Licensed	16	1058
🟪 Application Acceleration Manager (AAM)	☐ None	Licensed	32	2050
🟦 Secure Web Gateway (SWG)	☐ None	Time limited module expires after: Aug 29, 2020	24	4096
🟩 iRules Language Extensions (iRulesLX)	☐ None	Licensed	0	748
🟦 URLDB Minimal (URLDB)	☐ None	Time limited module expires after: Aug 29, 2020	36	2048

3.09

Identify configured system services

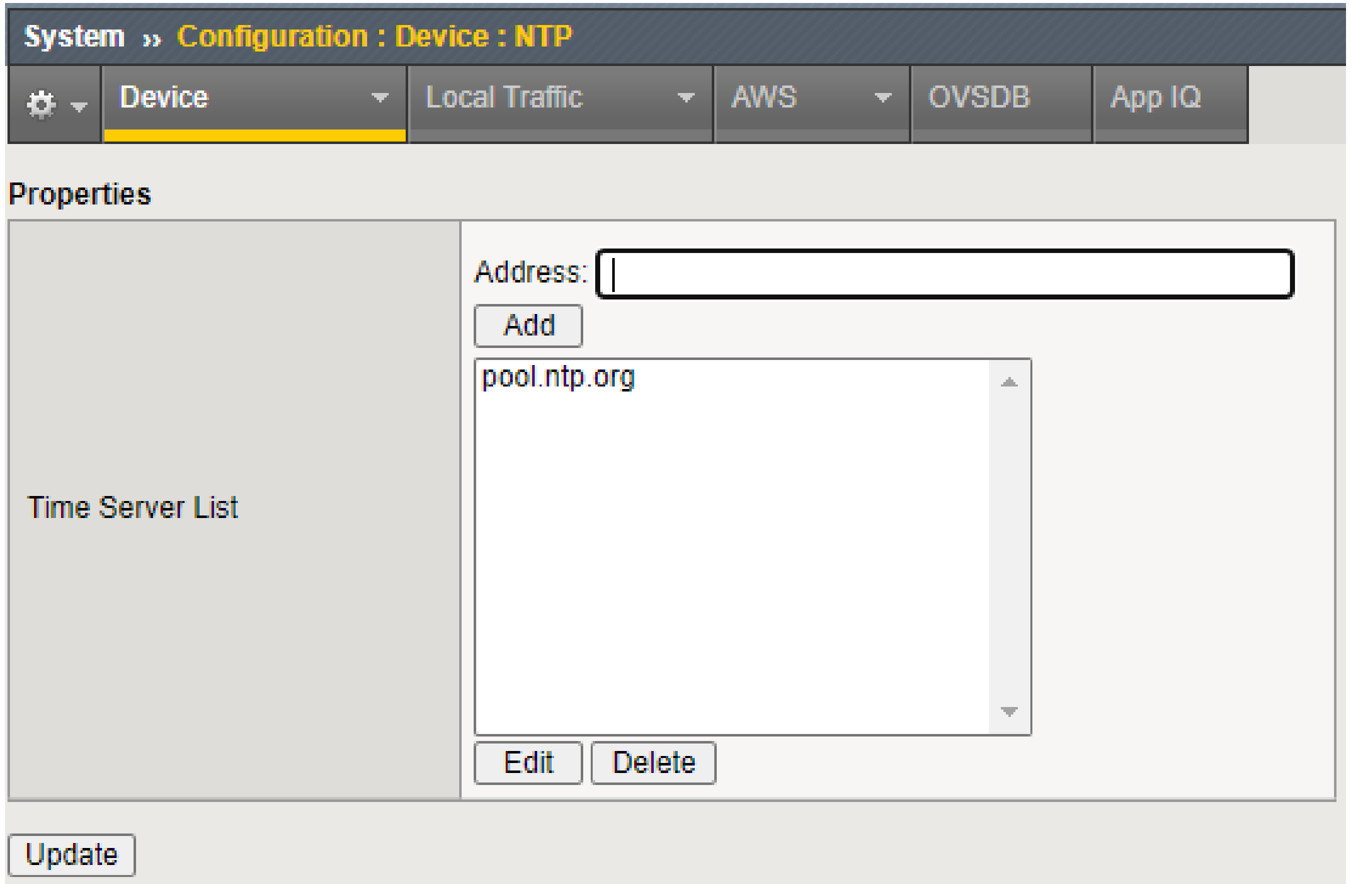
- Show proper configuration for: DNS, NTP, SNMP, syslog

3.09 Show proper configuration for: DNS, NTP, SNMP, syslog

Manual Chapter : General Configuration Properties

K13380: Configuring the BIG-IP system to use an NTP server from the command line (11.x - 13.x)

- NTP is essential for:
  - Device Service Clusters
  - Configsync
  - Logging



Time Server List

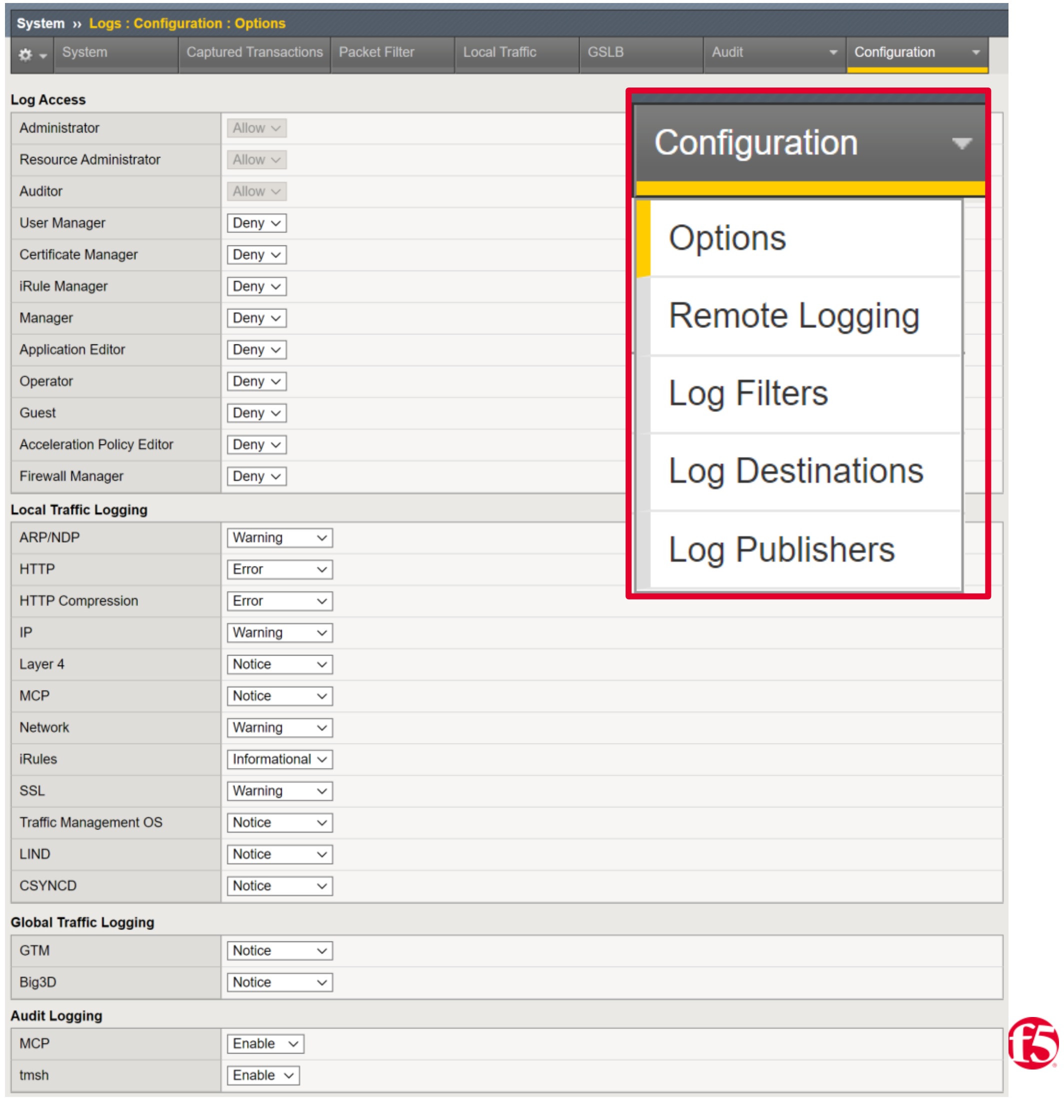
Address:

pool.ntp.org

3.09 Show proper configuration for: DNS, NTP, SNMP, syslog

[Manual Chapter : About Logging]

- Log Destinations
  - The High-Speed Logging (HSL) or Unformatted destination
  - Defines the protocol to use (UDP or TCP)
  - Defines the server pool the log message will go too
- The Formatted destination defines the format of the messages being sent
  - There are two parts to a Destination
    - Where a message is going : HSL Destination
    - What the message looks like: Formatted Destination
- Publisher
  - A Publisher is a collection of Formatted Destinations



Log Access

Administrator	Allow
Resource Administrator	Allow
Auditor	Allow
User Manager	Deny
Certificate Manager	Deny
iRule Manager	Deny
Manager	Deny
Application Editor	Deny
Operator	Deny
Guest	Deny
Acceleration Policy Editor	Deny
Firewall Manager	Deny

Local Traffic Logging

ARP/NDP	Warning
HTTP	Error
HTTP Compression	Error
IP	Warning
Layer 4	Notice
MCP	Notice
Network	Warning
iRules	Informational
SSL	Warning
Traffic Management OS	Notice
LIND	Notice
CSYNCD	Notice

Global Traffic Logging

GTM	Notice
Big3D	Notice

Audit Logging

MCP	Enable
tmsh	Enable

Tools for Testing – DNS, NTP, SNMP, SYSLOG

- DNS
  - You should know to use and interpret the results of the `dig` utility
- NTP
  - K10240: Verifying NTP peer server communications
- SNMP
  - There is a test snmp button on the configuration page
- Good old tcpdump
- Show services
  - `tmsh show service <service>` or `tmsh show service` (shows all services)
  - From the linux prompt: **bigstart status**
    - This will show you the status of the various daemons the BIG-IP uses.

3.08

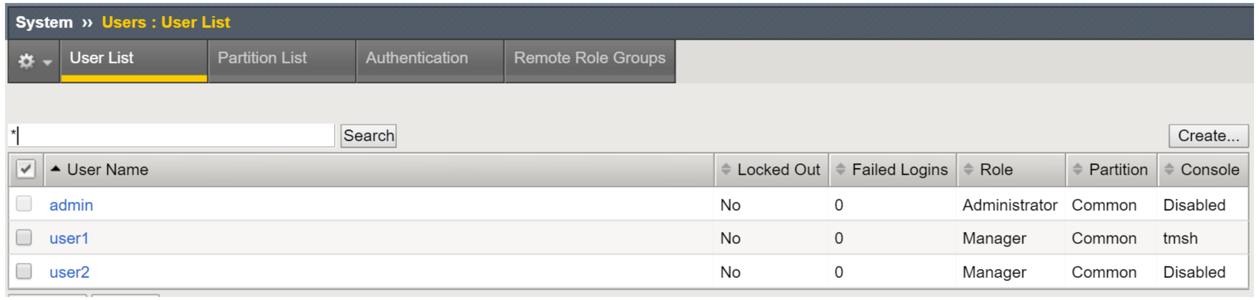
Explain authentication methods

- Explain how to create a user
- Explain how to modify user properties
- Explain options for remote authentication provider
- Explain use of groups using remote authentication provider

3.08 Explain how to create a user

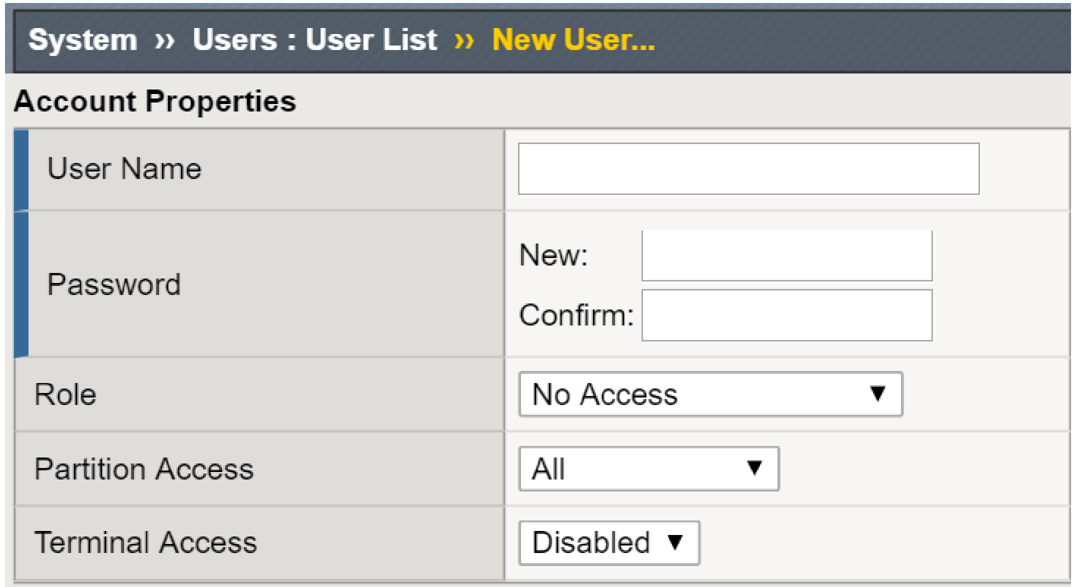
[Manual : BIG-IP Systems: User Account Administration]

- User and Password are required
- Assign a role
- Assign partition access
  - A user may be assigned to one partition or All partitions
- Assign the type of terminal access (Specify the type of CLI access)
  - Disabled
    - The user may access only the GUI interface
  - TMSH
    - Permits the user access to the TMOS CLI shell via SSH
  - Advanced Shell
    - Permits user access to the Linux prompt
    - Administrator and Resource Administrator only



System » Users : User List

☑	User Name	Locked Out	Failed Logins	Role	Partition	Console
□	admin	No	0	Administrator	Common	Disabled
□	user1	No	0	Manager	Common	tmsh
□	user2	No	0	Manager	Common	Disabled



System » Users : User List » New User...

Account Properties

User Name	
Password	New: Confirm:
Role	No Access ▼
Partition Access	All ▼
Terminal Access	Disabled ▼

User Roles (most common)

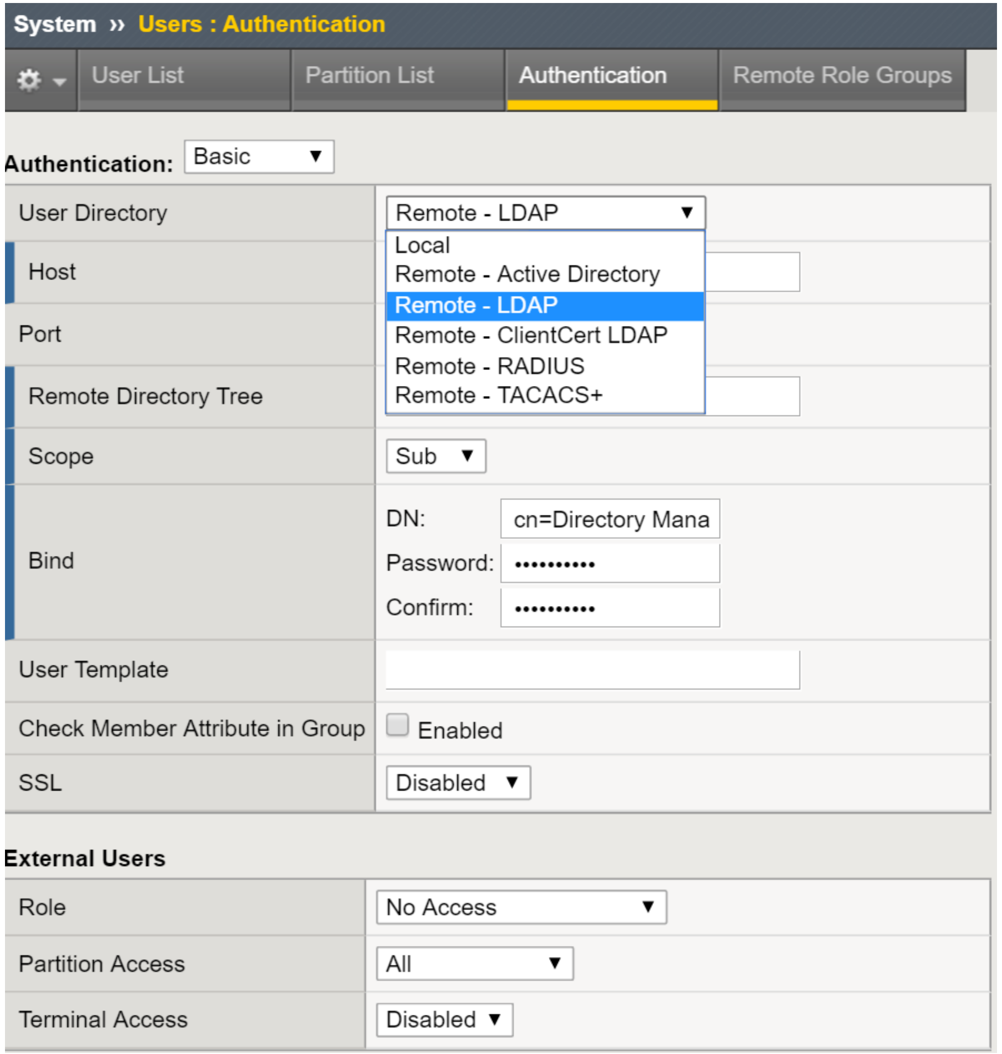
Manual : BIG-IP Systems: User Account Administration

- **No Access**
  - Prevents users from accessing the system. Basically turns off the account without deleting the account.
- **Guest**
  - Grants users limited, view-only access to a specific set of objects.
- **Operator**
  - Grants users permission to enable or disable existing nodes and pool members. Cannot enable/disable virtual servers.
- **Application Editor**
  - Grants users permission to modify existing nodes, pools, pool members, and monitors.
- **Manager**
  - Permission to create, modify, and delete virtual servers, pools, pool members, nodes, custom profiles, custom monitors, and iRules.
- **Resource Administrator**
  - Grants users complete access to all objects on the system, except access to create/modify users (except for themselves)
- **Administrator**
  - Grants users complete access to all objects on the system.

3.08 Explain options for remote authentication provider

Manual : BIG-IP Systems: User Account Administration

- Still will always need a least one admin local account
  - For config sync functionality
  - In case you lose access to authentication server
- Supports AD, LDAP, TACACS+ and RADIUS



Authentication: Basic

User Directory	Remote - LDAP Local Remote - Active Directory Remote - LDAP Remote - ClientCert LDAP Remote - RADIUS Remote - TACACS+
Host	
Port	
Remote Directory Tree	
Scope	Sub
Bind	DN: cn=Directory Mana Password: •••••••••• Confirm: ••••••••••
User Template	
Check Member Attribute in Group	□ Enabled
SSL	Disabled

External Users

Role	No Access
Partition Access	All
Terminal Access	Disabled

3.05

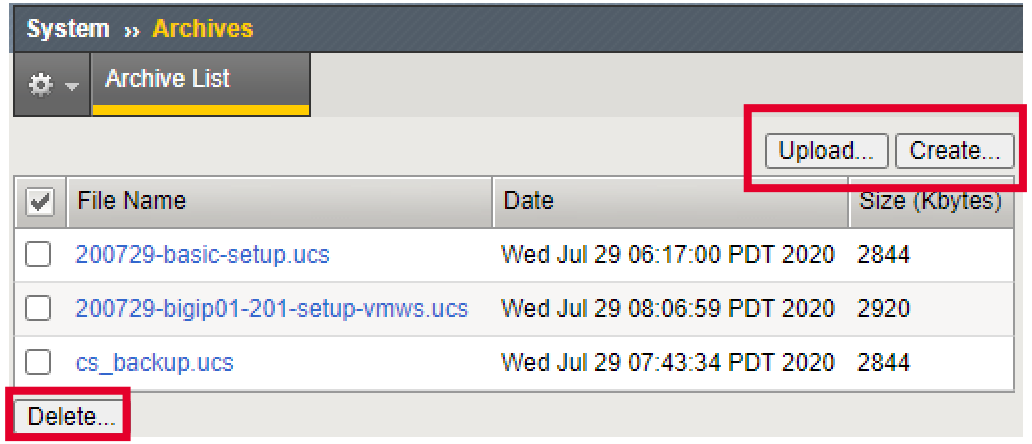
Apply procedural concepts required to create, manage, and restore a UCS archive

- Summarize the use case of a UCS backup
- Execute UCS backup procedure
- Execute UCS restore procedure
- Explain proper long-term storage of UCS backup file
- Explain the contents of the UCS file (private keys)

3.05 Execute UCS backup and restore procedure

K13132: BACKING UP AND RESTORING BIG-IP CONFIGURATION FILES WITH A UCS ARCHIVE

You can create, delete, restore, upload and download UCS archives from the GUI interface:



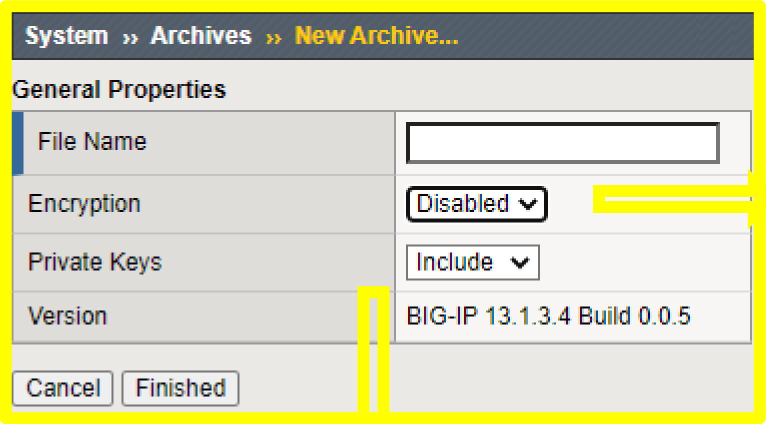
System » Archives

Archive List

Upload... Create...

☑	File Name	Date	Size (Kbytes)
□	200729-basic-setup.ucs	Wed Jul 29 06:17:00 PDT 2020	2844
□	200729-bigip01-201-setup-vmws.ucs	Wed Jul 29 08:06:59 PDT 2020	2920
□	cs_backup.ucs	Wed Jul 29 07:43:34 PDT 2020	2844

Delete...

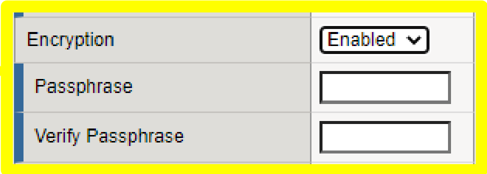


System » Archives » New Archive...

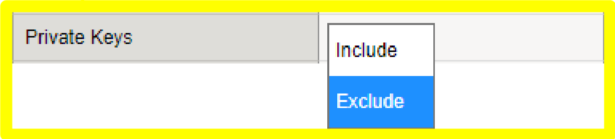
General Properties

File Name	
Encryption	Disabled
Private Keys	Include
Version	BIG-IP 13.1.3.4 Build 0.0.5

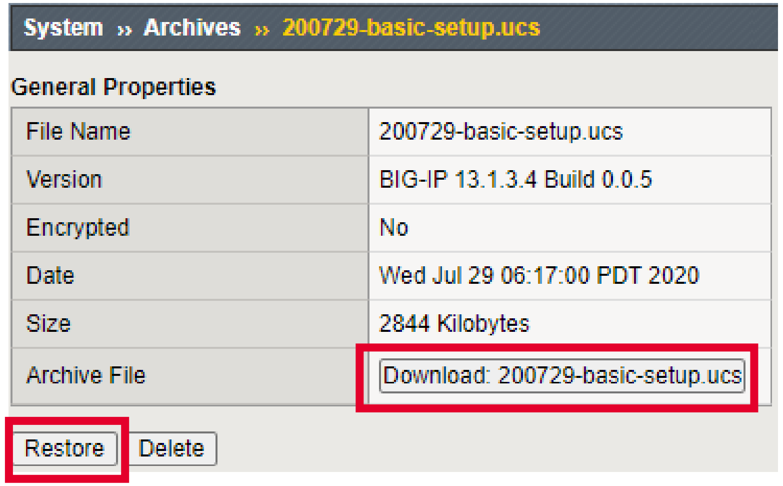
Cancel Finished



Encryption	Enabled
Passphrase	
Verify Passphrase	



Private Keys	Include Exclude



System » Archives » 200729-basic-setup.ucs

General Properties

File Name	200729-basic-setup.ucs
Version	BIG-IP 13.1.3.4 Build 0.0.5
Encrypted	No
Date	Wed Jul 29 06:17:00 PDT 2020
Size	2844 Kilobytes
Archive File	Download: 200729-basic-setup.ucs

Restore Delete

3.05 Execute UCS backup and restore procedure

Manual Chapter : Archives

- You can also create, delete and restore UCS backups using TMSH, but TMSH has options the GUI doesn’t.
  - Backup the BIG-IP: save sys ucs <ucs filename>
  - Restore the BIG-IP: load sys ucs <ucs filename>
- If you are restoring an RMA or migrating to a new platform you do NOT want to restore the license.
  - load sys ucs <filename> **no-license**
  - If you are migrating platforms you may not want to restore the base configurations as interfaces may be different.
  - On the system you are restoring you would build the base first, interfaces, VLANs, self IPs, etc
  - load sys ucs **platform-migrate** <filename> **no-license**
- Other TMSH options
  - no-platform-check Bypass platform check.
  - passphrase Passphrase for (un)encrypting UCS.
  - reset-trust Reset device and trust domain certificates and keys when loading a UCS.

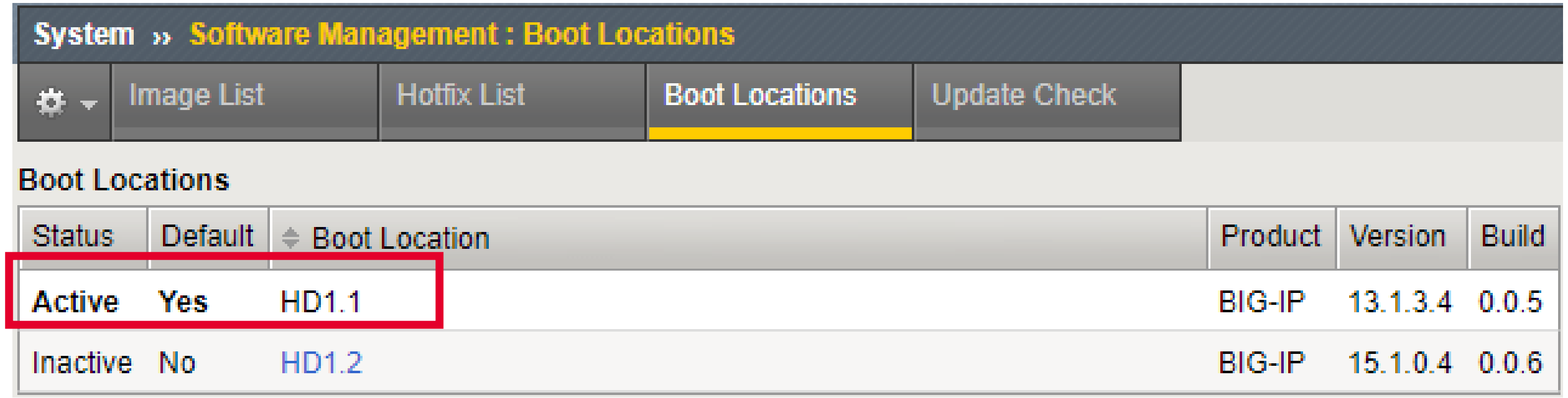
3.06

Apply procedural concepts required to manage software images

- Given an HA pair, describe the appropriate strategy for deploying a new software image
- Perform procedure to upload new software image
- Show currently configured boot location
- Demonstrate creating new volume for software images

3.06 Show currently configured boot location

```
(tmos)# show sys software
--------------------------------------------------
Sys::Software Status
Volume  Product   Version  Build  Active    Status
--------------------------------------------------
HD1.1    BIG-IP  13.1.3.4  0.0.5     yes  complete

----------------------------
Sys::Software Update Check
----------------------------
  Check Enabled          true
  Phonehome Enabled      true
  Frequency            weekly
  Status              failure
  Errors                    8
```

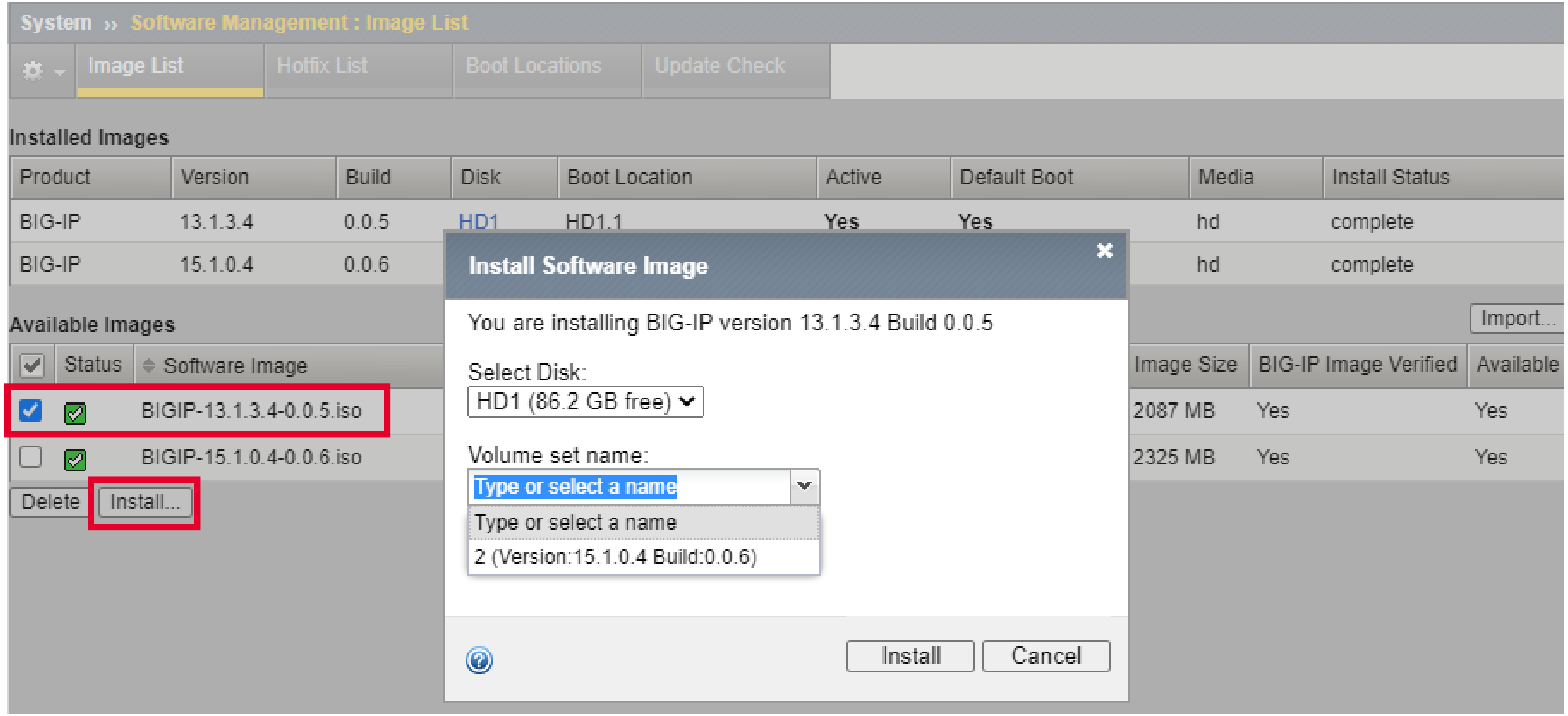


Boot Locations

Status	Default	Boot Location	Product	Version	Build
Active	**Yes**	HD1.1	BIG-IP	13.1.3.4	0.0.5
Inactive	No	HD1.2	BIG-IP	15.1.0.4	0.0.6

3.06 Demonstrate creating new volume for software images

install sys software image <iso> volume <name>



Installed Images

Product	Version	Build	Disk	Boot Location	Active	Default Boot	Media	Install Status
BIG-IP	13.1.3.4	0.0.5	HD1	HD1.1	Yes	Yes	hd	complete
BIG-IP	15.1.0.4	0.0.6					hd	complete

Available Images

☑	Status	Software Image	Image Size	BIG-IP Image Verified	Available
☑	✓	BIGIP-13.1.3.4-0.0.5.iso	2087 MB	Yes	Yes
□	✓	BIGIP-15.1.0.4-0.0.6.iso	2325 MB	Yes	Yes

Install Software Image

You are installing BIG-IP version 13.1.3.4 Build 0.0.5

Select Disk: HD1 (86.2 GB free)

Volume set name: Type or select a name

- Type or select a name
- 2 (Version:15.1.0.4 Build:0.0.6)

3.04 (R)

List which log files could be used to find events and/or hardware issues

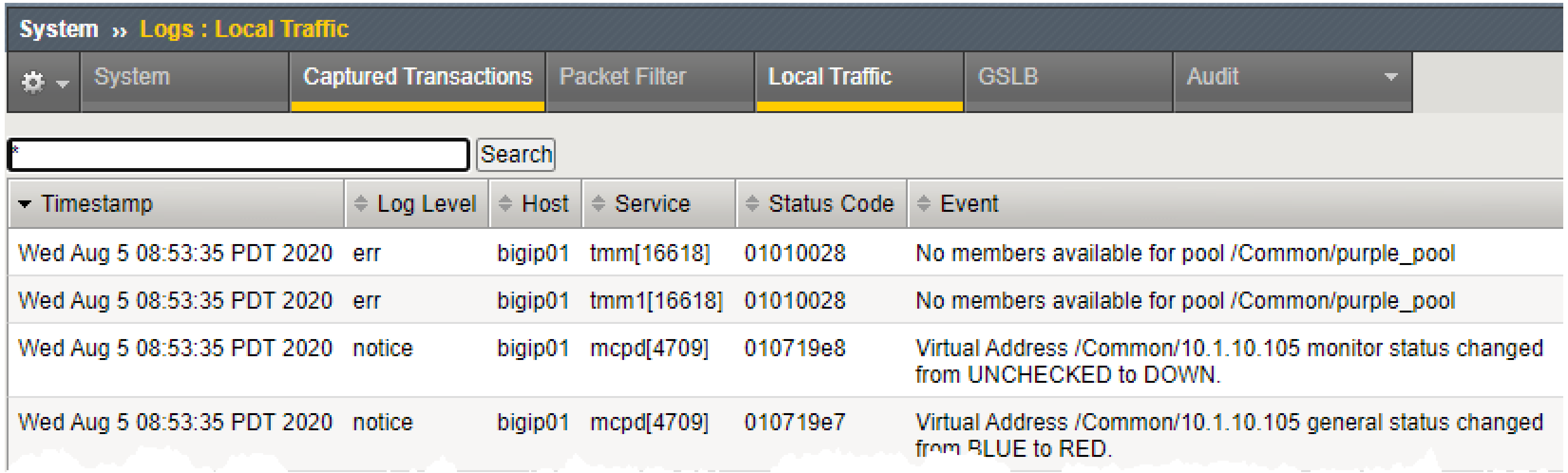
- Identify use of /var/log/ltm, var/log/secure, /var/log/audit
- Identify severity log level of an event
- Identify event from a log message

3.04 Identify use of /var/log/ltm, var/log/secure, /var/log/audit

Manual Chapter : About Logging

K16197: Reviewing BIG-IP log files

- /var/log/ltm
  - The local traffic messages pertain specifically to the BIG-IP local traffic management events
  - Can be found in the GUI under System >> Logs >> Local Traffic
  - In TMSH: `show sys log ltm`
  - In bash: `cat /var/log/ltm`

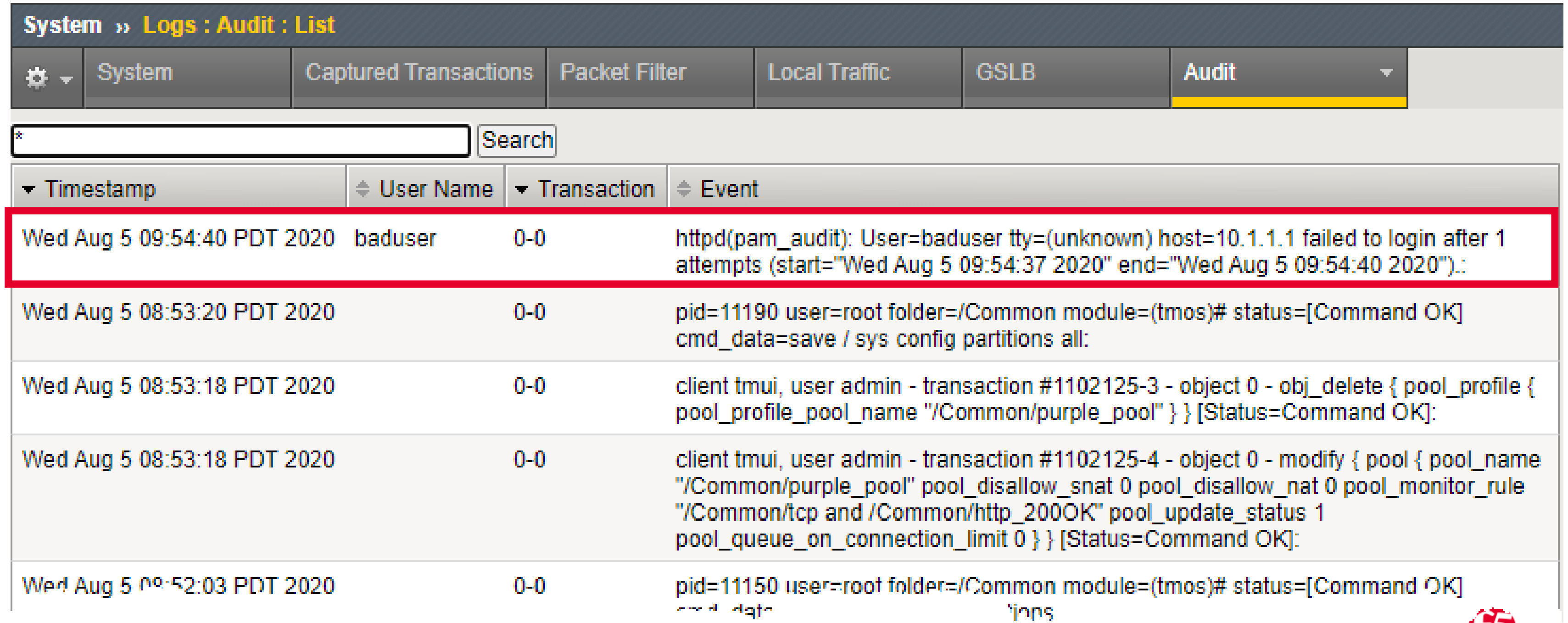


Timestamp	Log Level	Host	Service	Status Code	Event
Wed Aug 5 08:53:35 PDT 2020	err	bigip01	tmm[16618]	01010028	No members available for pool /Common/purple_pool
Wed Aug 5 08:53:35 PDT 2020	err	bigip01	tmm1[16618]	01010028	No members available for pool /Common/purple_pool
Wed Aug 5 08:53:35 PDT 2020	notice	bigip01	mcpd[4709]	010719e8	Virtual Address /Common/10.1.10.105 monitor status changed from UNCHECKED to DOWN.
Wed Aug 5 08:53:35 PDT 2020	notice	bigip01	mcpd[4709]	010719e7	Virtual Address /Common/10.1.10.105 general status changed from BLUE to RED.

3.04 Identify use of /var/log/ltm, var/log/secure, /var/log/audit

Auditing User Access

- /var/log/secure
  - Log information related to authentication and authorization privileges.
  - Can be found in the GUI under System >> Logs >> Audit
  - In TMSH, `show sys log secure`
  - In Bash, `cat /var/log/secure`



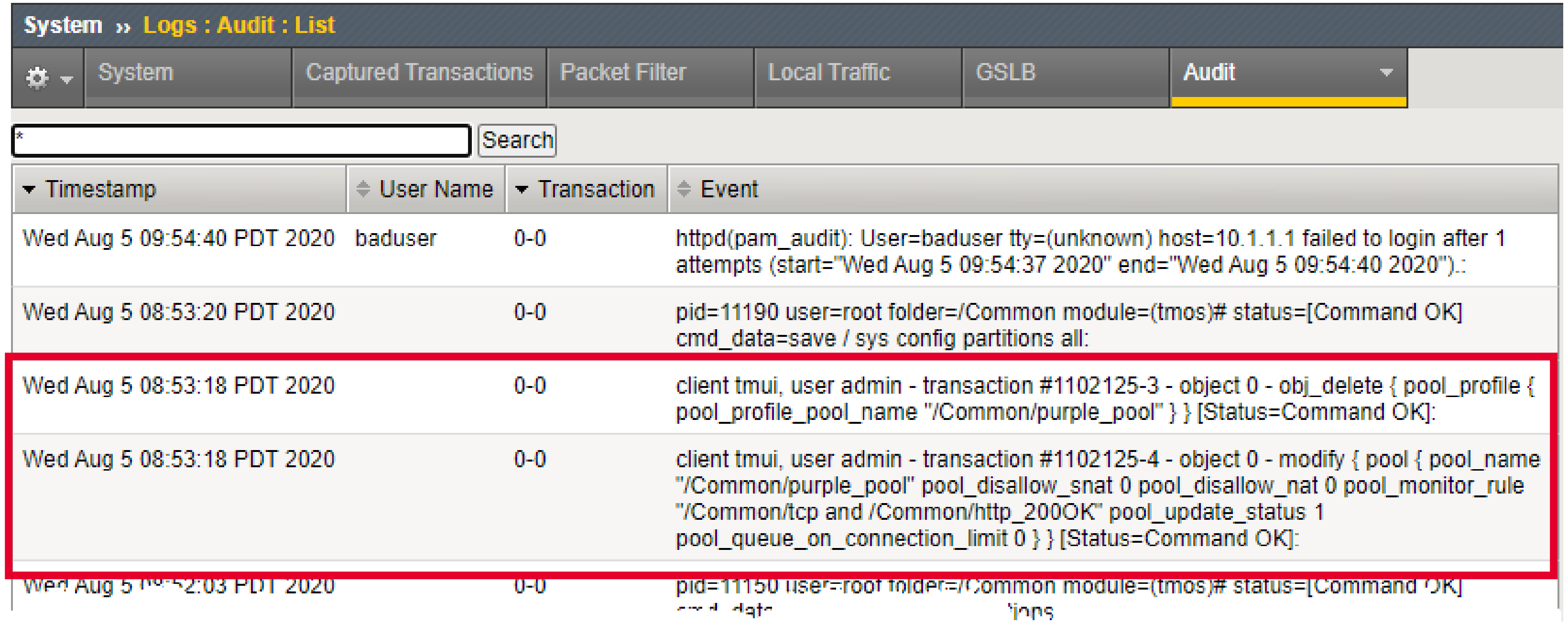
Timestamp	User Name	Transaction	Event
Wed Aug 5 09:54:40 PDT 2020	baduser	0-0	httpd(pam_audit): User=baduser tty=(unknown) host=10.1.1.1 failed to login after 1 attempts (start="Wed Aug 5 09:54:37 2020" end="Wed Aug 5 09:54:40 2020").:
Wed Aug 5 08:53:20 PDT 2020		0-0	pid=11190 user=root folder=/Common module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all:
Wed Aug 5 08:53:18 PDT 2020		0-0	client tmui, user admin - transaction #1102125-3 - object 0 - obj_delete { pool_profile { pool_profile_pool_name "/Common/purple_pool" } } [Status=Command OK]:
Wed Aug 5 08:53:18 PDT 2020		0-0	client tmui, user admin - transaction #1102125-4 - object 0 - modify { pool { pool_name "/Common/purple_pool" pool_disallow_snat 0 pool_disallow_nat 0 pool_monitor_rule "/Common/tcp and /Common/http_200OK" pool_update_status 1 pool_queue_on_connection_limit 0 } } [Status=Command OK]:
Wed Aug 5 08:52:03 PDT 2020		0-0	pid=11150 user=root folder=/Common module=(tmos)# status=[Command OK] cmd_data

3.04 Identify use of /var/log/ltm, var/log/secure, /var/log/audit

[Manual Chapter : About Logging](#)

[K16197: Reviewing BIG-IP log files](#)

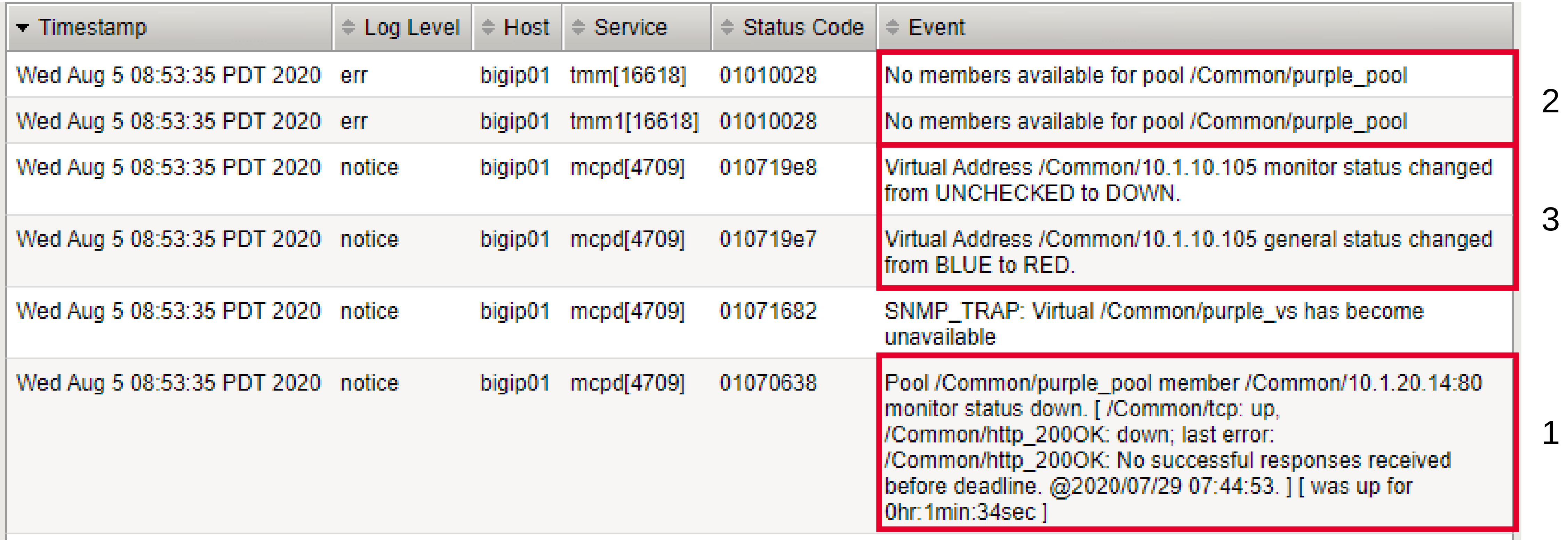
- /var/log/audit
  - Log changes to the BIG-IP system configuration. Logging audit events is optional.
  - Can be found in the GUI under System >> Logs >> Audit
    - In TMSH, `show sys log audit`
    - In Bash, `cat /var/log/audit`



Timestamp	User Name	Transaction	Event
Wed Aug 5 09:54:40 PDT 2020	baduser	0-0	httpd(pam_audit): User=baduser tty=(unknown) host=10.1.1.1 failed to login after 1 attempts (start="Wed Aug 5 09:54:37 2020" end="Wed Aug 5 09:54:40 2020").:
Wed Aug 5 08:53:20 PDT 2020		0-0	pid=11190 user=root folder=/Common module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all:
Wed Aug 5 08:53:18 PDT 2020		0-0	client tmui, user admin - transaction #1102125-3 - object 0 - obj_delete { pool_profile { pool_profile_pool_name "/Common/purple_pool" } } [Status=Command OK]:
Wed Aug 5 08:53:18 PDT 2020		0-0	client tmui, user admin - transaction #1102125-4 - object 0 - modify { pool { pool_name "/Common/purple_pool" pool_disallow_snat 0 pool_disallow_nat 0 pool_monitor_rule "/Common/tcp and /Common/http_200OK" pool_update_status 1 pool_queue_on_connection_limit 0 } } [Status=Command OK]:
Wed Aug 5 [illegible]:52:03 PDT 2020		0-0	pid=11150 user=root folder=/Common module=(tmos)# status=[Command OK] [illegible]

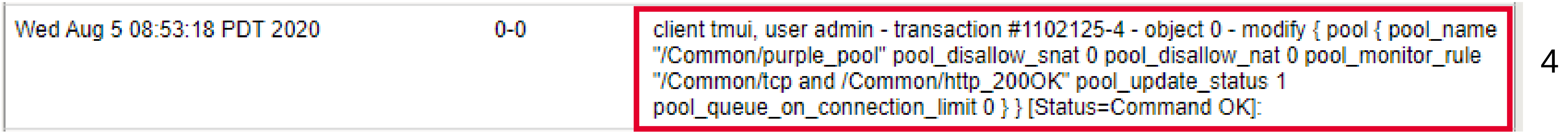
3.04 Identify event from a log message

Local Traffic



Timestamp	Log Level	Host	Service	Status Code	Event
Wed Aug 5 08:53:35 PDT 2020	err	bigip01	tmm[16618]	01010028	No members available for pool /Common/purple_pool
Wed Aug 5 08:53:35 PDT 2020	err	bigip01	tmm1[16618]	01010028	No members available for pool /Common/purple_pool
Wed Aug 5 08:53:35 PDT 2020	notice	bigip01	mcpd[4709]	010719e8	Virtual Address /Common/10.1.10.105 monitor status changed from UNCHECKED to DOWN.
Wed Aug 5 08:53:35 PDT 2020	notice	bigip01	mcpd[4709]	010719e7	Virtual Address /Common/10.1.10.105 general status changed from BLUE to RED.
Wed Aug 5 08:53:35 PDT 2020	notice	bigip01	mcpd[4709]	01071682	SNMP_TRAP: Virtual /Common/purple_vs has become unavailable
Wed Aug 5 08:53:35 PDT 2020	notice	bigip01	mcpd[4709]	01070638	Pool /Common/purple_pool member /Common/10.1.20.14:80 monitor status down. [/Common/tcp: up, /Common/http_200OK: down; last error: /Common/http_200OK: No successful responses received before deadline. @2020/07/29 07:44:53.] [was up for 0hr:1min:34sec]

Audit



Wed Aug 5 08:53:18 PDT 2020	0-0	client tmui, user admin - transaction #1102125-4 - object 0 - modify { pool { pool_name "/Common/purple_pool" pool_disallow_snat 0 pool_disallow_nat 0 pool_monitor_rule "/Common/tcp and /Common/http_200OK" pool_update_status 1 pool_queue_on_connection_limit 0 } } [Status=Command OK]:

HA and System State

Objectives 3.10, 3.02, 2.01

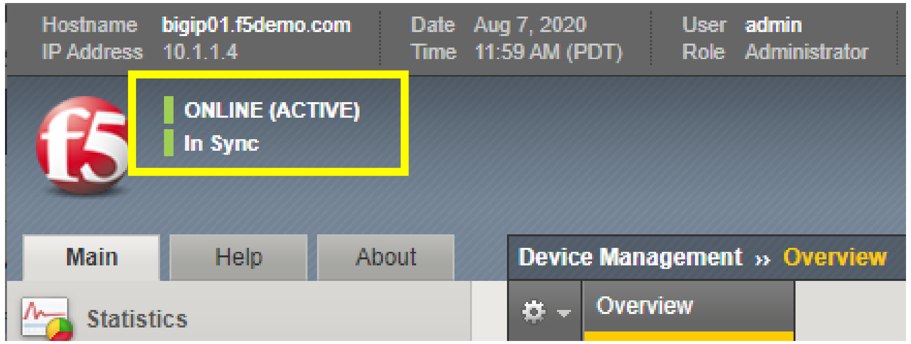
3.10

Explain config sync

- Show config sync status
- Explain when a config sync is necessary
- Compare configuration timestamp
- Demonstrate config sync procedure
- Report errors which occur during config sync

3.10 Show config sync status

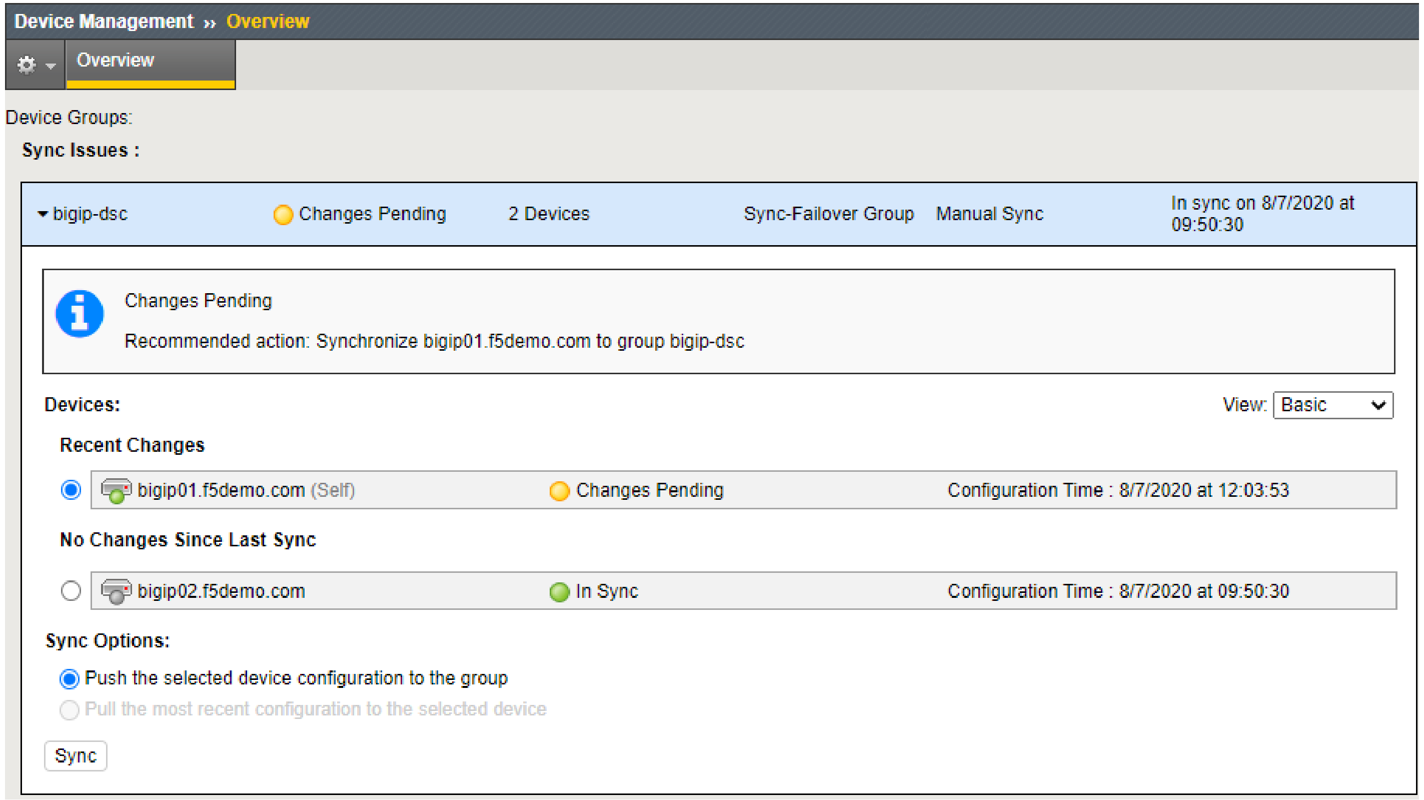
Manual Chapter : Managing Configuration Synchronization



Hostname bigip01.f5demo.com
IP Address 10.1.1.4
Date Aug 7, 2020
Time 11:59 AM (PDT)
User admin
Role Administrator

ONLINE (ACTIVE)
In Sync

- By default, syncing a configuration is a manual process



Device Groups:

Sync Issues :

bigip-dsc	Changes Pending	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/7/2020 at 09:50:30

Changes Pending

Recommended action: Synchronize bigip01.f5demo.com to group bigip-dsc

Devices:

View: Basic

Recent Changes

●	bigip01.f5demo.com (Self)	Changes Pending	Configuration Time : 8/7/2020 at 12:03:53

No Changes Since Last Sync

○	bigip02.f5demo.com	In Sync	Configuration Time : 8/7/2020 at 09:50:30

Sync Options:

● Push the selected device configuration to the group

○ Pull the most recent configuration to the selected device

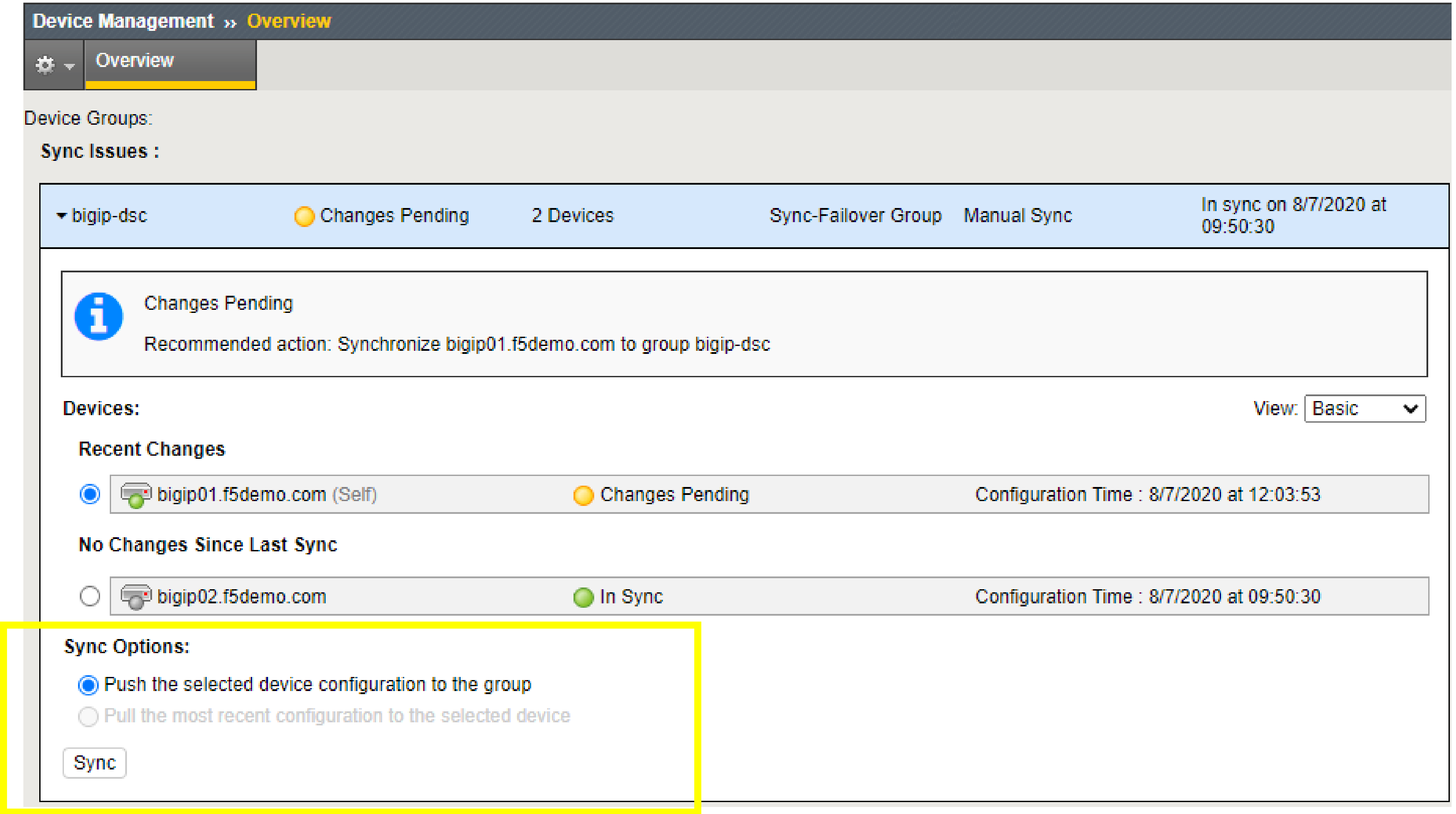
Sync

```
[root@bigip01:Active:Changes Pending] config #
```

3.10 Demonstrate config sync procedure (GUI)

Manual Chapter : Managing Configuration Synchronization

- F5 YouTube: Performing a ConfigSync using the Configuration utility ~2 min
- You can Push or Pull a configsync
  - You may want a pull if you make changes you regret



Device Groups:

Sync Issues :

▾ bigip-dsc	● Changes Pending	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/7/2020 at 09:50:30

Changes Pending

Recommended action: Synchronize bigip01.f5demo.com to group bigip-dsc

Devices:

View: Basic

Recent Changes

●	bigip01.f5demo.com (Self)	● Changes Pending	Configuration Time : 8/7/2020 at 12:03:53

No Changes Since Last Sync

○	bigip02.f5demo.com	● In Sync	Configuration Time : 8/7/2020 at 09:50:30

Sync Options:

● Push the selected device configuration to the group

○ Pull the most recent configuration to the selected device

3.10 Demonstrate config sync procedure (TMSH)

K14856: Performing a ConfigSync using tmsh

- F5 YouTube: Performing a ConfigSync using tmsh ~1min
- run /cm config-sync <sync_direction> <sync_group>
- <sync_direction>

```
 force-full-load-push    Sync configuration to the specified device group even if
                         the system would deem this unsafe. This may result in
                         loss of configuration on other devices.

  from-group             Sync configuration from specified device group.

  recover-sync           Resets the local device configuration and restores trust
                         domain, device, and device-group information to default
                         settings.

  to-group               Sync configuration to specified device group.
```

3.02

Apply procedural concepts required to manage the state of a high availability pair

- Report current active/standby failover state
- Show device trust status
- Execute force to standby procedure
- Execute force to offline procedure

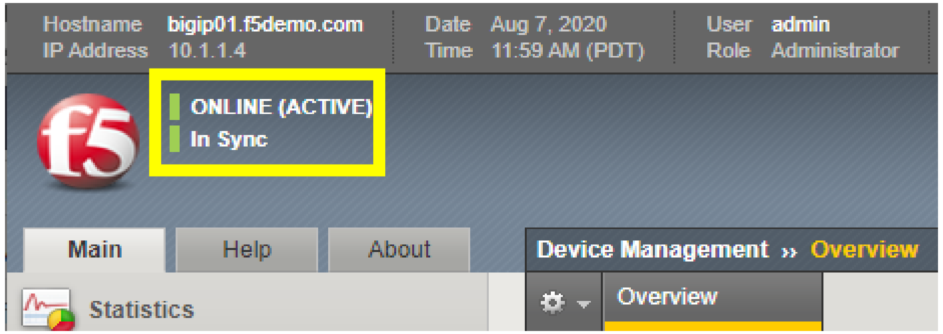
Before we begin: A little more on Device Service Clusters.

Manual : BIG-IP Device Service Clustering: Administration

- For BIG-IPs to be combined into clusters for high availability, certain things must configured:
  - BIG-IPs must have a valid device certificate
  - On the device, IP addressing must be defined for failover
  - Devices must be place into a trust group
  - Devices in a trust group and then be place into a failover group

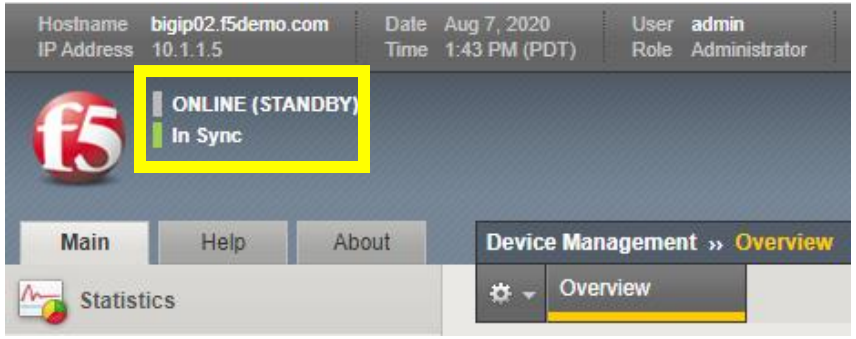
3.02 Report current active/standby failover state

Manual : BIG-IP Device Service Clustering: Administration



Hostname bigip01.f5demo.com
IP Address 10.1.1.4
Date Aug 7, 2020
Time 11:59 AM (PDT)
User admin
Role Administrator

ONLINE (ACTIVE)
In Sync



Hostname bigip02.f5demo.com
IP Address 10.1.1.5
Date Aug 7, 2020
Time 1:43 PM (PDT)
User admin
Role Administrator

ONLINE (STANDBY)
In Sync

```
[root@bigip01:Active:In Sync] config #
```

```
[root@bigip02:Standby:In Sync] config #
```

Active – there are one of more active traffic groups that can failover

Standby – there are no active traffic groups that can failover

Have a working knowledge of mirroring.

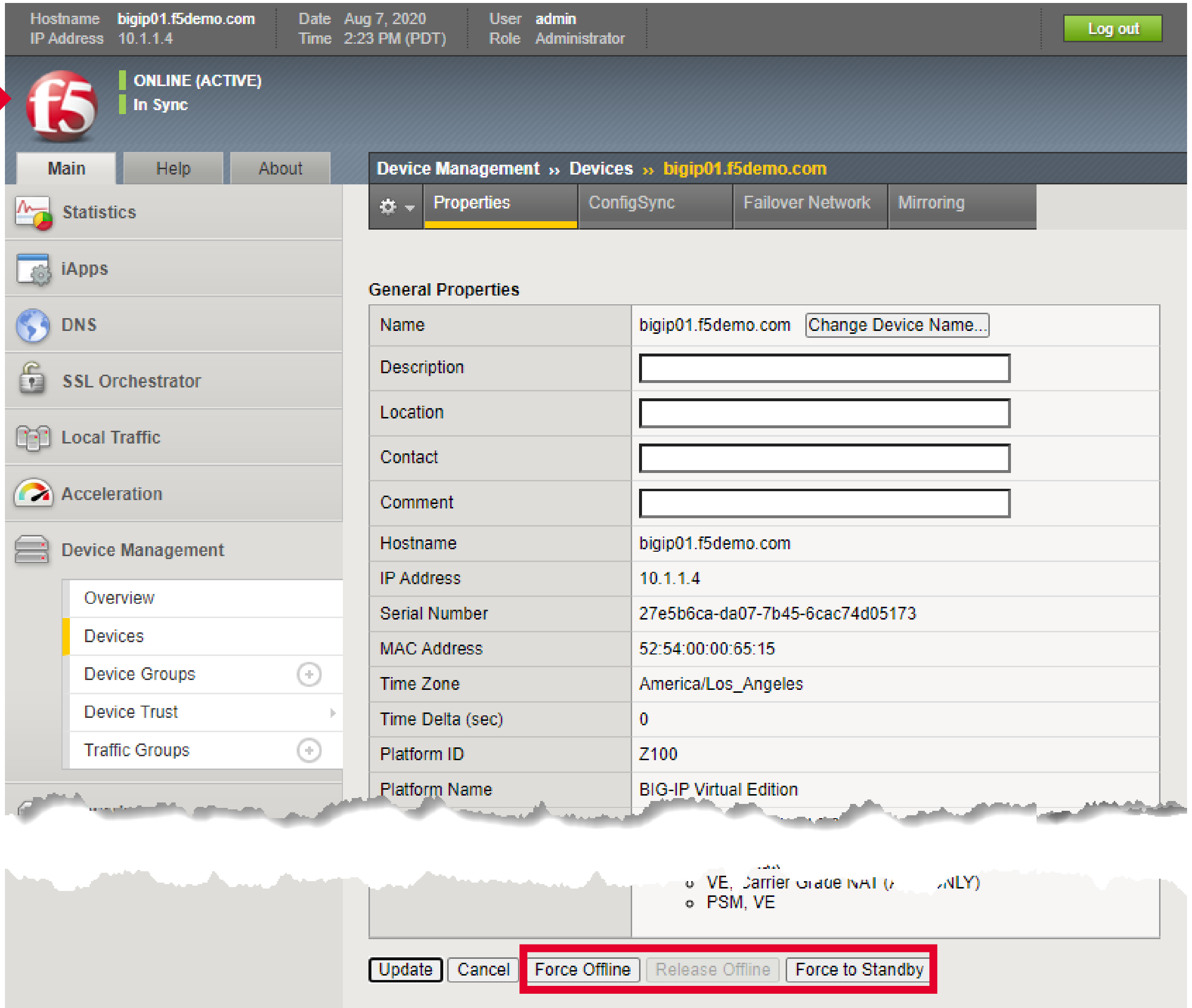
- SNAT
- Persistence
  - Only if persistence records are kept locally on the BIG-IP, not necessary for Cookie persistence.
- Connection Table
  - Only for long term connections, ie. FTP, resource intensive

3.02 Execute force to standby or offline procedure

[Manual : BIG-IP Device Service Clustering: Administration](#)

```
(tmos)# run sys failover
```

```
offline  Changes the status of a unit or cluster to
         Forced Offline. If persist or no-persist are
         not specified, the change in status will be
         persisted in-between system restarts.

online   Changes the status of a unit or cluster from
         Forced Offline to either Active or Standby,
         depending upon the status of the other unit
         or cluster in a redundant pair.

standby Specifies that the active unit or cluster
         fails over to a Standby state, causing the
         standby unit or cluster to become Active.
```



Hostname bigip01.f5demo.com
IP Address 10.1.1.4
Date Aug 7, 2020
Time 2:23 PM (PDT)
User admin
Role Administrator

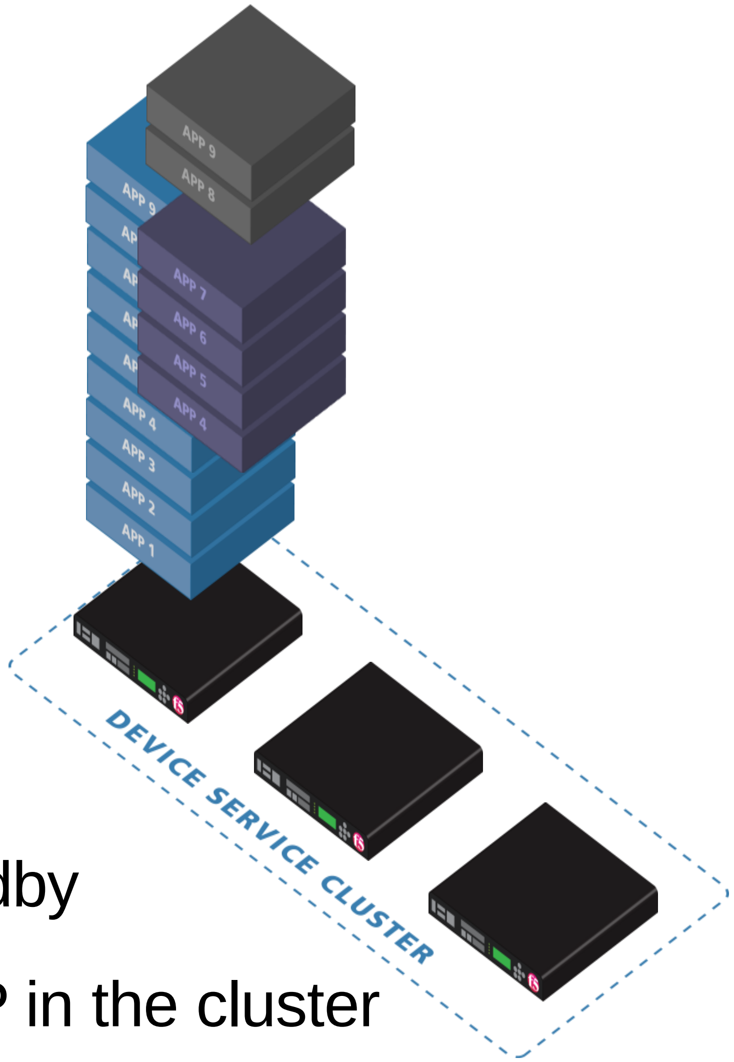
ONLINE (ACTIVE)
In Sync

Device Management » Devices » bigip01.f5demo.com

General Properties

Name	bigip01.f5demo.com
Description	
Location	
Contact	
Comment	
Hostname	bigip01.f5demo.com
IP Address	10.1.1.4
Serial Number	27e5b6ca-da07-7b45-6cac74d05173
MAC Address	52:54:00:00:65:15
Time Zone	America/Los_Angeles
Time Delta (sec)	0
Platform ID	Z100
Platform Name	BIG-IP Virtual Edition
	◦ VE, Carrier Grade NAT (ONLY) ◦ PSM, VE

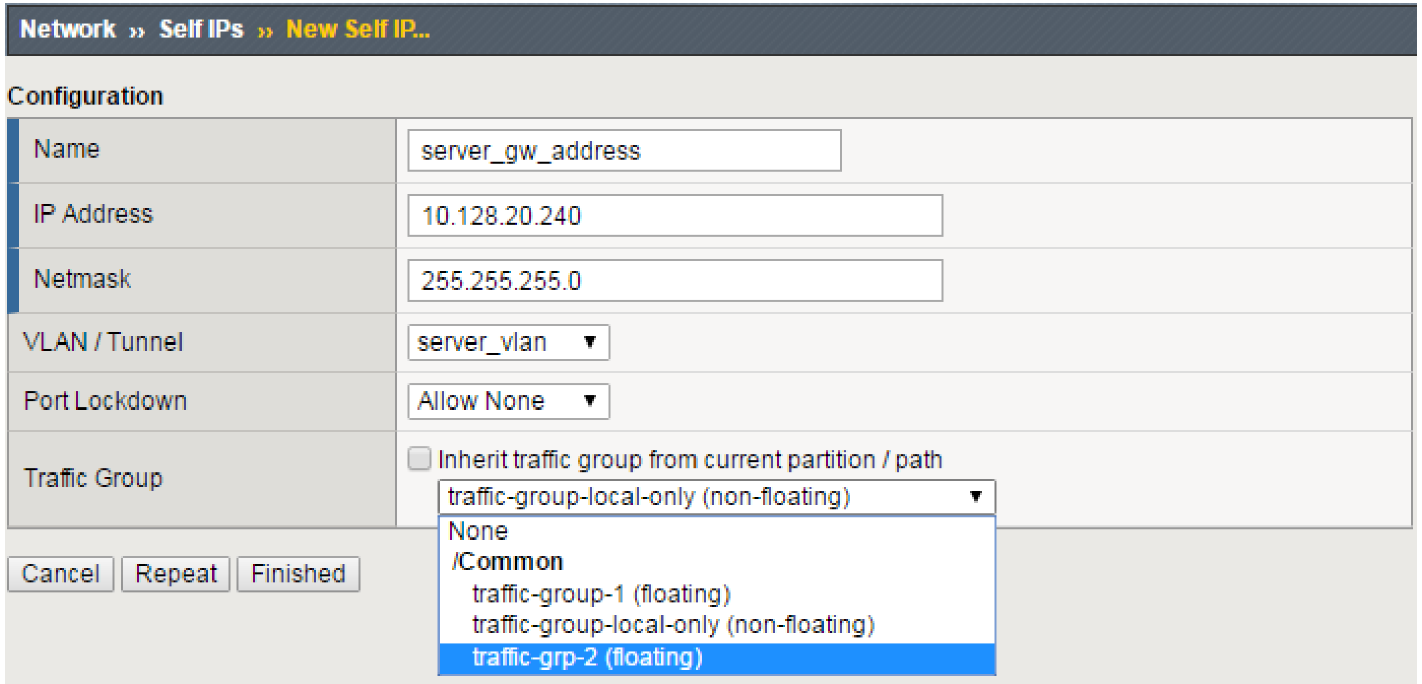
Traffic Groups



- A collection of listeners to failover
- Create traffic groups and assign applications to the group
- Activate traffic groups on cluster members
- If a cluster member has no active traffic groups it is in standby
- If a device fails, the traffic group migrates to another BIG-IP in the cluster

The all important Floating Self IP

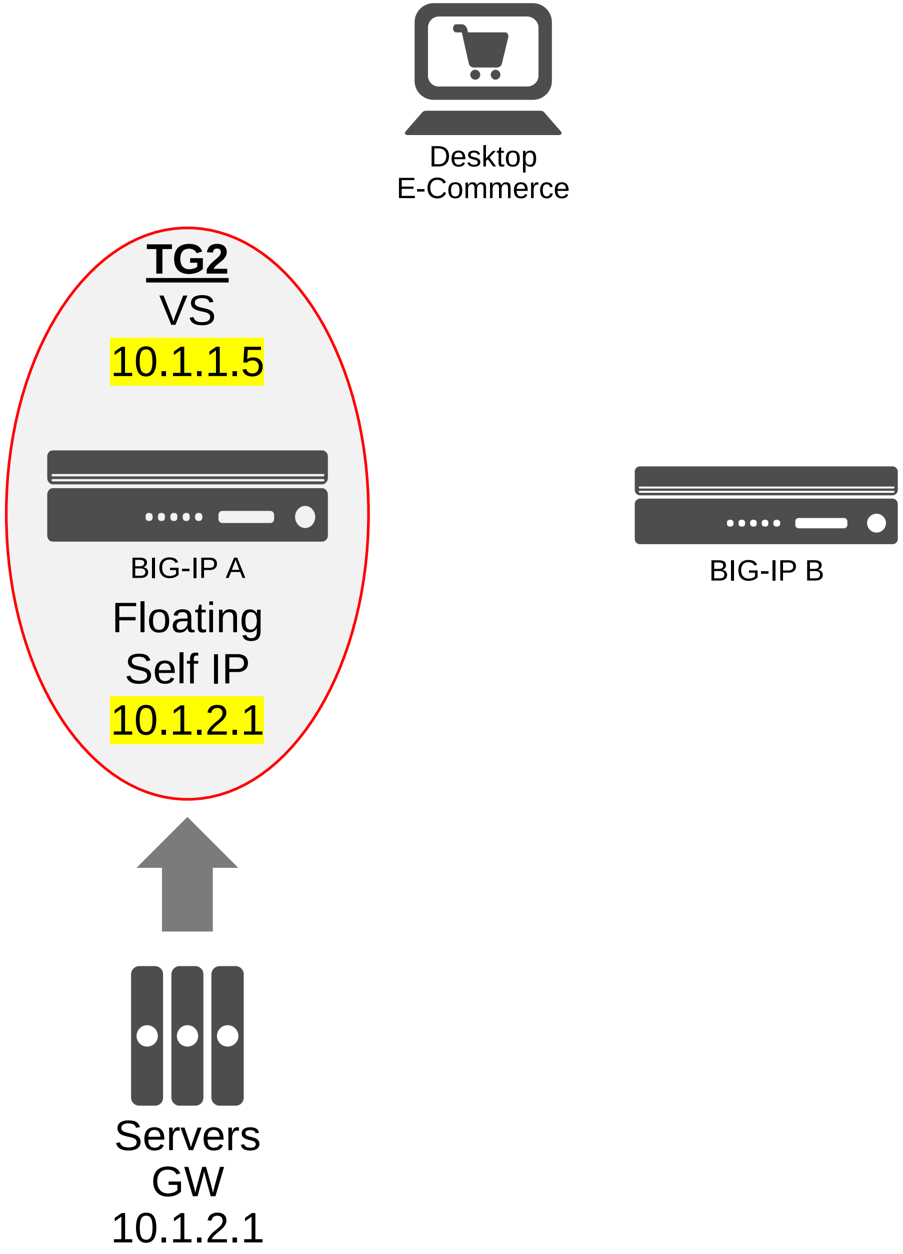
- Self IP addresses that need to move on failover to ensure application access
  - The server’s default gateway is the BIG-IP



Network » Self IPs » New Self IP...

Configuration

Name	server_gw_address
IP Address	10.128.20.240
Netmask	255.255.255.0
VLAN / Tunnel	server_vlan ▼
Port Lockdown	Allow None ▼
Traffic Group	□ Inherit traffic group from current partition / path traffic-group-local-only (non-floating) ▼ None /Common traffic-group-1 (floating) traffic-group-local-only (non-floating) traffic-grp-2 (floating)



2.01

Determine resource utilization

- Distinguish between control plane and data plane resources
- Identify CPU statistics per virtual server
- Interpret Statistics for interfaces
- Determine Disk utilization and Memory utilization

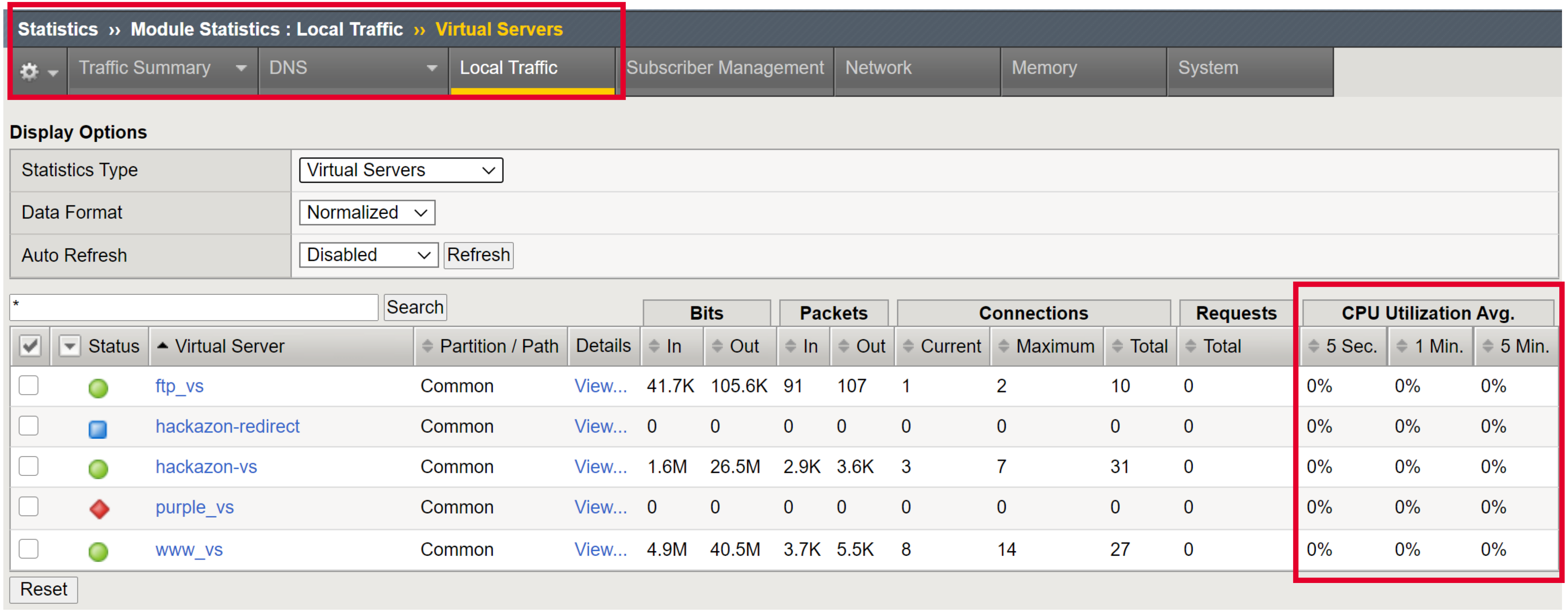
2.01 Distinguish between control plane and data plane resources

https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-1-0.html

- Control Plane
- Linux OS
  - Hardened CentOS
  - Use to boot HW/SW
  - Runs TMSH CLI and APIs
  - Runs Out-of-Band Management
    - By default uses DHCP
    - IP address can be assigned manually
    - Unique IP subnet and default gateway

- Data Plane
- TMOS (Traffic Management OS)
  - aka TMM
  - Runs TMM switch interface
  - L3 Switching and Routing
    - VLANs, Self IPs, Routing for TMM
  - Pools and Virtual Servers
  - Monitors
  - And basically all things basic to Local Traffic Management and application security.

2.01 Identify CPU statistics per virtual server



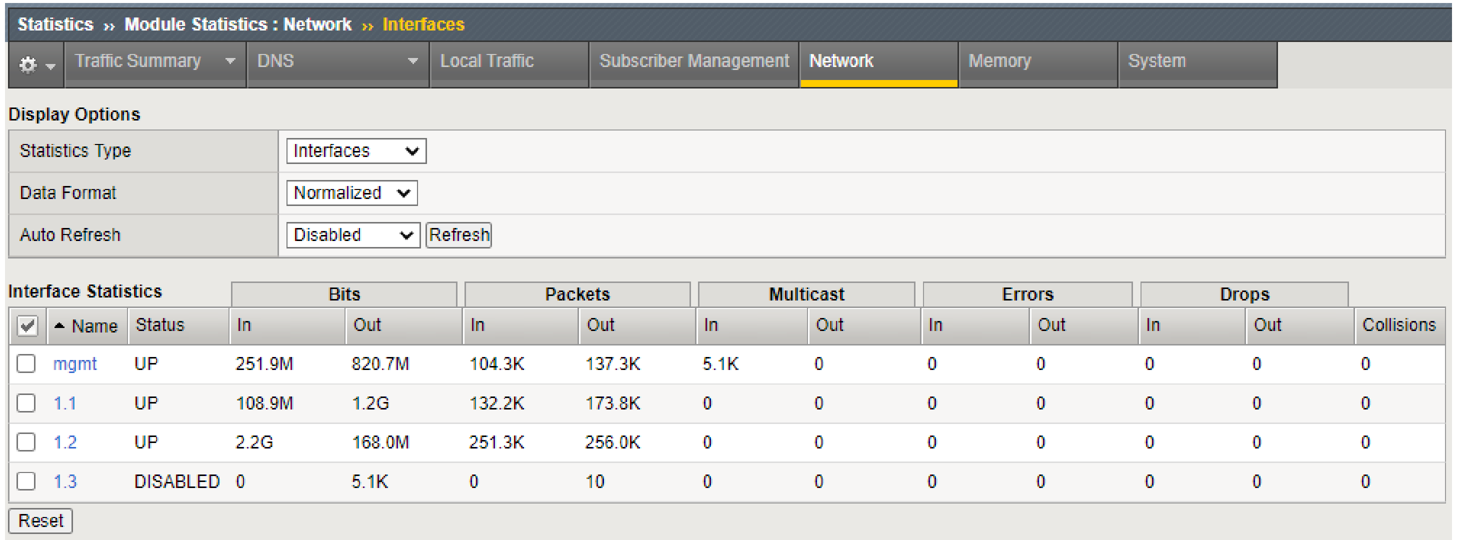
Statistics ›› Module Statistics : Local Traffic ›› Virtual Servers

Display Options

Statistics Type	Virtual Servers
Data Format	Normalized
Auto Refresh	Disabled Refresh

					Bits		Packets		Connections			Requests	CPU Utilization Avg.		
☑	Status	▲ Virtual Server	Partition / Path	Details	In	Out	In	Out	Current	Maximum	Total	Total	5 Sec.	1 Min.	5 Min.
□	●	ftp_vs	Common	View...	41.7K	105.6K	91	107	1	2	10	0	0%	0%	0%
□	■	hackazon-redirect	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%
□	●	hackazon-vs	Common	View...	1.6M	26.5M	2.9K	3.6K	3	7	31	0	0%	0%	0%
□	◆	purple_vs	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%
□	●	www_vs	Common	View...	4.9M	40.5M	3.7K	5.5K	8	14	27	0	0%	0%	0%

2.01 Interpret Statistics for interfaces



Display Options

Statistics Type	Interfaces
Data Format	Normalized
Auto Refresh	Disabled

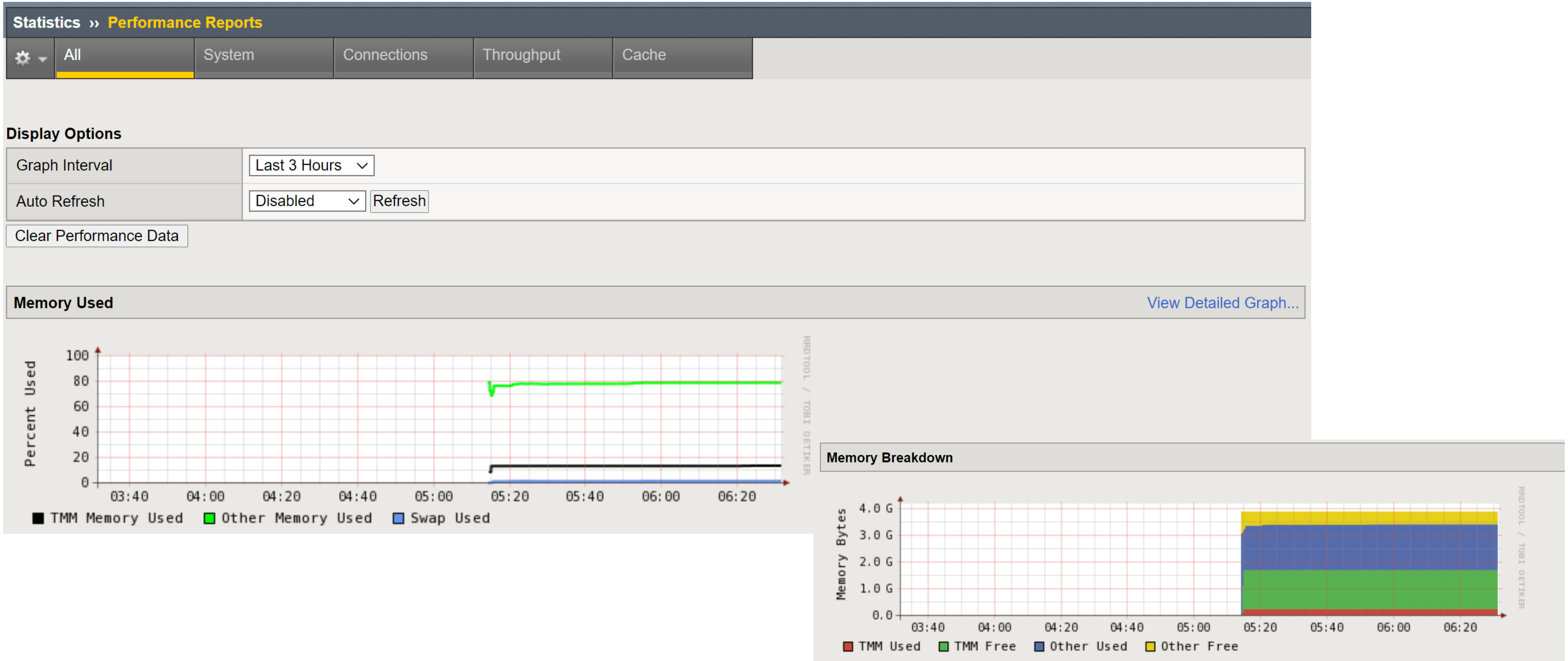
Interface Statistics

			Bits		Packets		Multicast		Errors		Drops		
☑	▲ Name	Status	In	Out	In	Out	In	Out	In	Out	In	Out	Collisions
□	mgmt	UP	251.9M	820.7M	104.3K	137.3K	5.1K	0	0	0	0	0	0
□	1.1	UP	108.9M	1.2G	132.2K	173.8K	0	0	0	0	0	0	0
□	1.2	UP	2.2G	168.0M	251.3K	256.0K	0	0	0	0	0	0	0
□	1.3	DISABLED	0	5.1K	0	10	0	0	0	0	0	0	0

```
(tmos)# show net interface
----------------------------------------------------------------------
Net::Interface
Name     Status     Bits     Bits     Pkts     Pkts  Drops  Errs     Media
                      In      Out       In      Out
----------------------------------------------------------------------
1.1          up   111.4M     1.3G   136.1K   178.7K      0     0  10000T-FD
1.2          up     2.2G   170.3M   256.0K   260.3K      0     0  10000T-FD
1.3    disabled        0     5.1K        0       10      0     0       none
mgmt         up   254.3M   831.2M   105.4K   139.0K      0     0   100TX-FD
```

- Errors – number of packets containing errors
- Drops – number of packets drop for processing or packet errors
- Collisions – should only occur on half-duplex links (not common)

2.01 Determine Disk utilization and Memory utilization



Statistics ›› Performance Reports

Display Options

Graph Interval	Last 3 Hours
Auto Refresh	Disabled Refresh

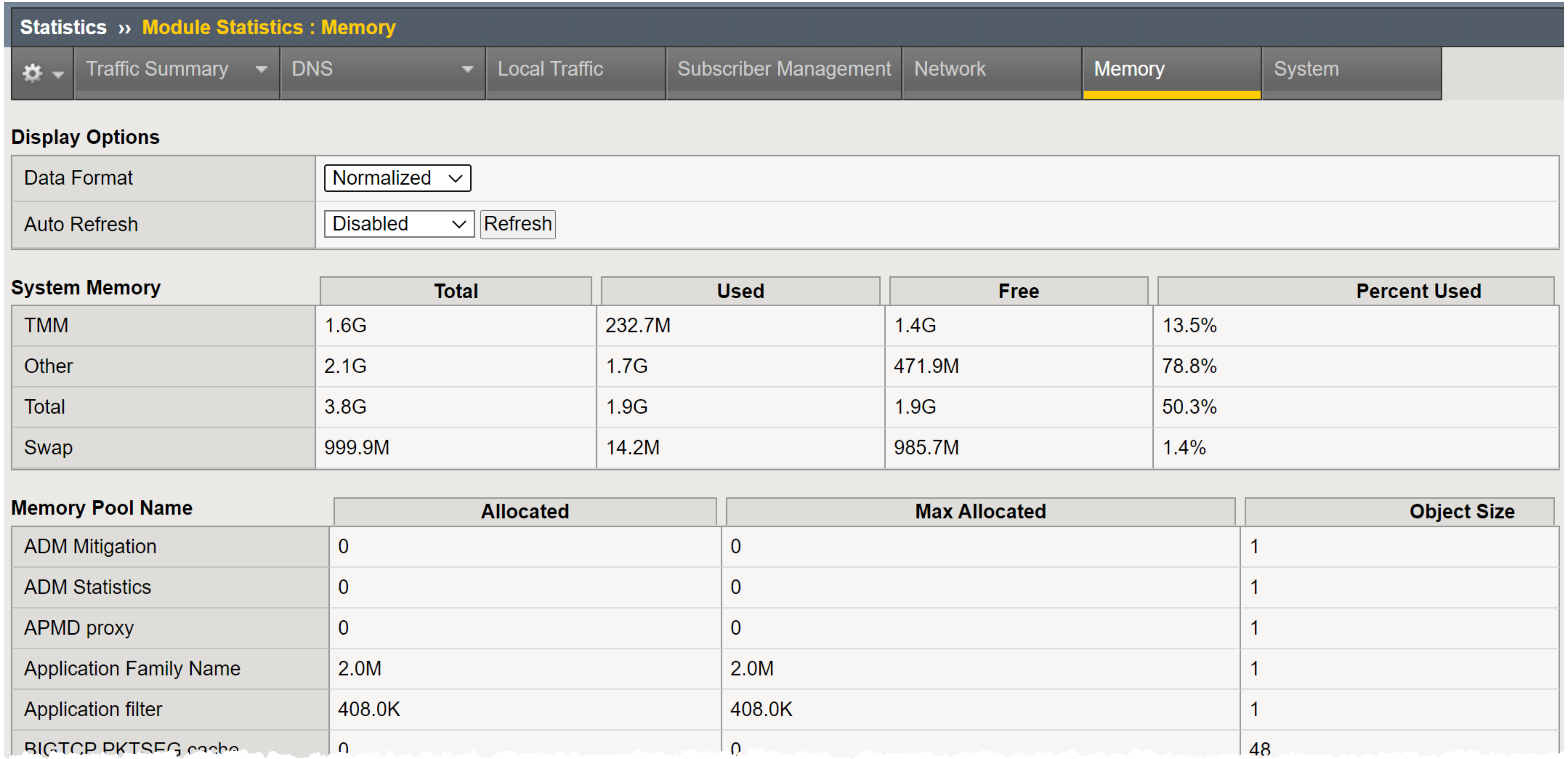
Clear Performance Data

Memory Used

View Detailed Graph...

Memory Breakdown

2.01 Determine Disk utilization and Memory utilization



Display Options

Data Format	Normalized
Auto Refresh	Disabled Refresh

System Memory	Total	Used	Free	Percent Used
TMM	1.6G	232.7M	1.4G	13.5%
Other	2.1G	1.7G	471.9M	78.8%
Total	3.8G	1.9G	1.9G	50.3%
Swap	999.9M	14.2M	985.7M	1.4%

Memory Pool Name	Allocated	Max Allocated	Object Size
ADM Mitigation	0	0	1
ADM Statistics	0	0	1
APMD proxy	0	0	1
Application Family Name	2.0M	2.0M	1
Application filter	408.0K	408.0K	1
BIGTCP PKTSEG cache	0	0	48

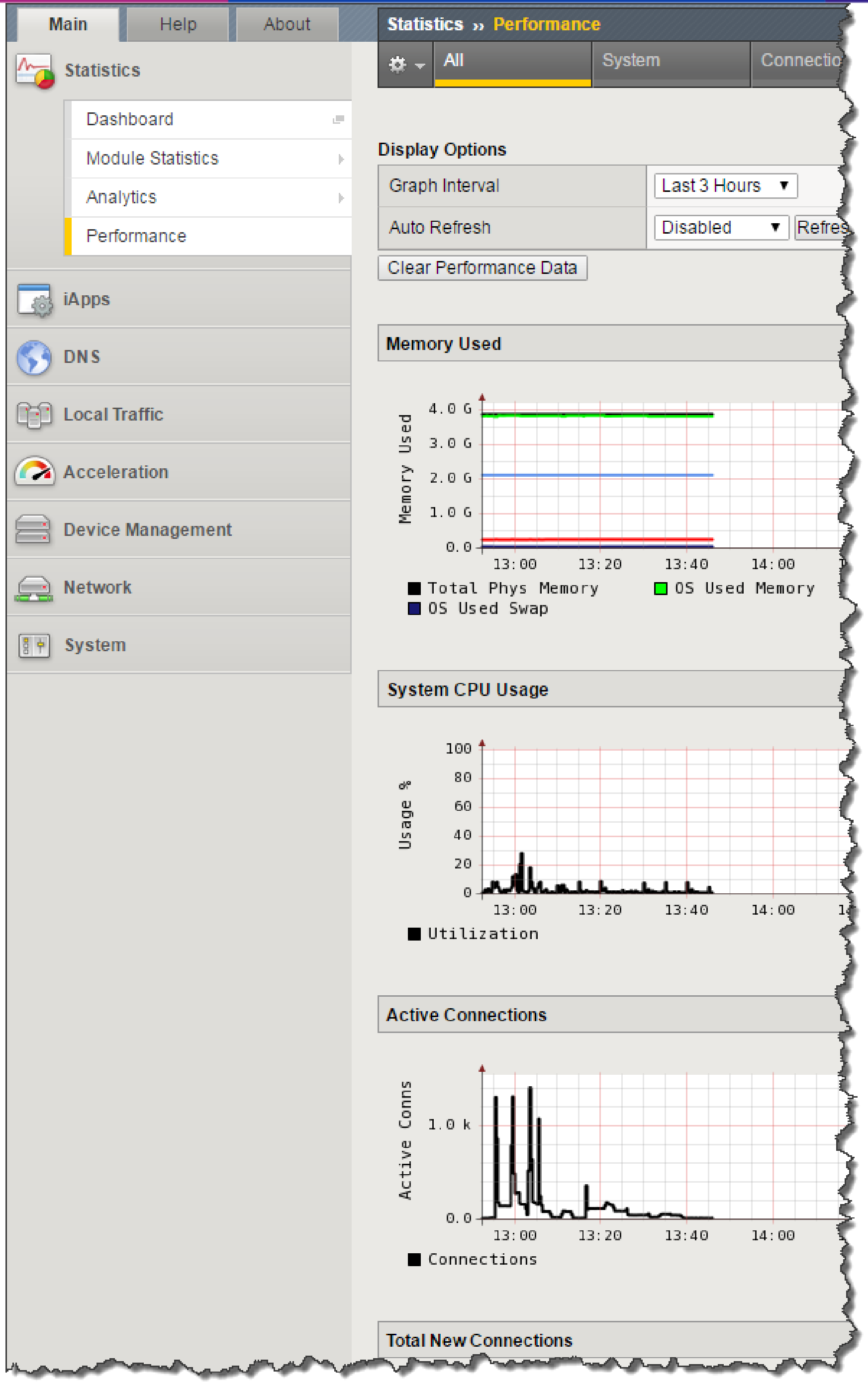
Determine Disk utilization and Memory utilization

K14403: Maintaining disk space on the BIG-IP system

```
[root@bigip01:Active:Disconnected] config # df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg--db--vda-set.1.root
                      427M  274M  131M  68% /
none                  3.9G  2.3M  3.9G   1% /dev/shm
/dev/mapper/vg--db--vda-set.1._config
                      3.2G   87M  2.9G   3% /config
/dev/mapper/vg--db--vda-set.1._usr
                      4.0G  3.2G  655M  83% /usr
/dev/mapper/vg--db--vda-set.1._var
                      3.0G  792M  2.1G  28% /var
/dev/mapper/vg--db--vda-dat.share
                       20G  306M   19G   2% /shared
/dev/mapper/vg--db--vda-dat.log
                      2.9G  106M  2.7G   4% /var/log
/dev/mapper/vg--db--vda-dat.appdata
                       25G  190M   24G   1% /appdata
none                  3.9G   35M  3.9G   1% /shared/rrd.1.2
none                  3.9G   16M  3.9G   1% /var/tmstat
none                  3.9G  1.6M  3.9G   1% /var/run
prompt                4.0M   28K  4.0M   1% /var/prompt
none                  3.9G     0  3.9G   0% /var/loipc
```

Performance Statistics

- On the Statistics >> Performance page you can find:
  - Memory Used
  - System CPU Usage
  - Active Connections and Total New Connections
  - Throughput - (bits) and (packets)
  - TMM Client-side and Server-side Throughput
  - HTTP Requests
  - RAM Cache Utilization
  - SSL Transactions
  - And more ……….
- In TMSH, `show /sys performance all-stats`



Graph Interval: Last 3 Hours

Auto Refresh: Disabled

Use support resources

Objectives 5.01 - 5.05

5.01

Define characteristics of a support ticket with F5

- List severity levels of a support ticket with F5
- List what to include in a support ticket with F5
- List ways to open support ticket with F5
- List where to open a support ticket with F5

The following slides are based* on v13.1 for more current support procedures see:

K2633: Instructions for submitting a support case to F5

* To the best of my knowledge and research.   Though most things have remained the same (ie. what to include in a support case), some things have changed slightly (ie. The web site for opening and viewing cases).

5.01 List severity levels of a support ticket with F5

K2633: Instructions for submitting a support case to F5

Sev1 –Site Down

- Software or hardware conditions on your F5 device are preventing the execution of critical business activities. The device will not power up or is not passing traffic
- **1 hour Initial Response**

Sev2 – Site at Risk

- Software or hardware conditions on your F5 device are preventing or significantly impairing high level commerce or business activities. The device is in degraded state that places your network or commerce at risk.
- **2 hour Initial Response**

Sev3 – Performance Degraded

- Software or hardware conditions on your F5 device have degraded service or functionality for normal business or commerce activities. Network traffic through the device is causing some applications to be unreachable, or operate in a diminished capacity.
- **4 Business Hours Initial Response****

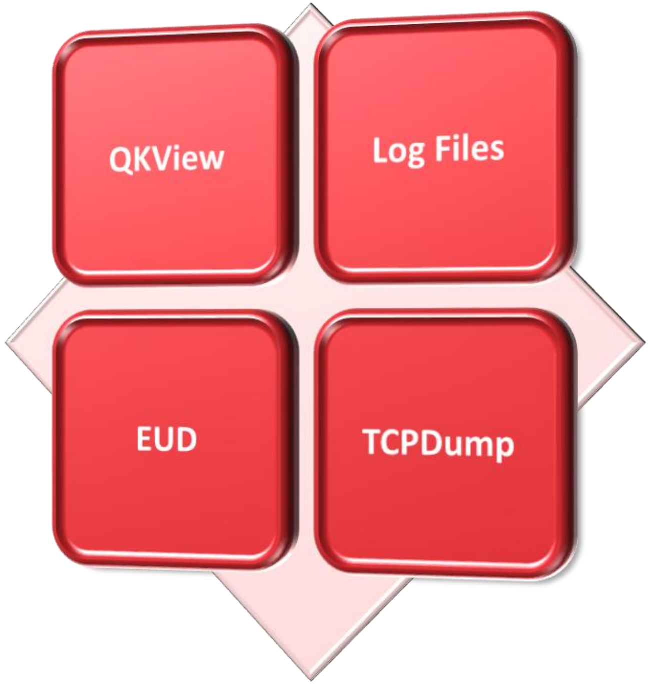
Sev4 - General Assistance

- Questions regarding configurations “how to”. Troubleshooting non-critical issue or requests for product functionality that is not currently part of the current product feature set.
- **Next Business Day Initial Response**

5.01 List what to include in a support ticket with F5

K2633: Instructions for submitting a support case to F5

Field	Data Required
Name	**The technical contact for this case**
Contact	**Cell (Mobile) phone or Desk phone**
F5 Serial #	**Required to obtain assistance**
F5 Product	**Platform – i.e., 1600, 3600, 8900, VE, BIGIQ, etc**
F5 Version	**Version (and any hot fixes already applied)**
Business Impact	**The criticality of this issue on your business**
Description	**Provide as complete a problem statement as possible:** • **What has happened?** • **Are there error messages? What are they?** • **When did the issue happen, where did it happen?** • **What changes have occurred in the configuration?** • **What changes have occurred in the network?** • **Is the issue happening on other F5 appliances?**
Instructions to replicate	**If you are able to replicate, please provide step-by-step instructions**
Remote Access Information	**Is it possible to access this unit directly?** **Is it possible to access this unit via a WebEX session?**



QKView

Log Files

EUD

TCPDump

K2486: Providing files to F5 Support

5.01 List ways and where to open a support ticket with F5

K2633: Instructions for submitting a support case to F5

- You can open a case by phone.
- You can open a case by going to https://my.f5.com
- You must meet the following prerequisites:
  - You have a serial number with an active support contract.
  - You have a support account with permissions for the affected device.
  - You have a problem or question that was not resolved when searching MyF5

F5 WebSu

Welcom

Welcome to F5 W

- Create and update
- Review your past cases
- Search AskF5 during cas
- Provide feedback dire

The AskF5 Knowle s about F5 products and services. Simply type a question

To learn m eatures the Guidelines and Policies online documentati

You do not have any cases.

*All dates and times shown in GMT-0500 (Central Daylight Time), based on your local system time.

Proactive Cases

Use for upgrade and major maintenance work

- Notification requested one week in advance
- Open by contacting the support center
- Available during contracted support hours

Required information

- Serial number(s) affected
- Date and time of the change window
- Complete description of the change activity including roll-back plan
- Diagnostics (QKView and logs)

If during the maintenance window you run into an issue you can call to support and reference the proactive case ID.

5.03

Apply procedural concepts required to perform an End User Diagnostic (EUD)

- Understand requirements of EUD
- Understand impact of running EUD
- Identify methods of booting the EUD
- Understand how to collect EUD output (console/log)

5.03 Identify methods of booting the EUD

Manual Chapter : Verifying Installing and Loading the EUD Files

- Boot the EUD from a USB flash drive
  - Plug your EUD USB flash drive into the system, and boot to the EUD.
- Boot the EUD from a USB DVD drive
  - Plug your USB DVD drive into the system, and boot to the EUD.
- Run the EUD from the system boot menu
  - As the system is booting, select the EUD option from the boot menu.
  - As the unit boots, it pauses briefly on the boot menu. Use the arrow keys to highlight End User Diagnostics.

5.03 Understand impact of running EUD

Manual Chapter : The End-User Diagnostic EUD

CAUTION:

- You should not run these test tools on a system that is actively processing traffic in a production environment. **These tests stop the unit and prevent it from processing traffic.**
- Run this tool **only** if you are instructed to by an F5® Support representative or if you are verifying a hardware issue with a unit that is already removed from production.
- You **WILL** have to reboot the unit.
- You may have to power cycle the unit

5.04

Apply procedural concepts required to generate a qkview and collect results from iHealth

- Identify methods of running qkview
- Identify method of retrieving qkview
- Understand information contained in qkview
- Identify when appropriate to run qkview
- Understand where to upload qkview (iHealth)

5.04 Identify methods of running and retrieving qkview

K12878: Generating diagnostic data using the qkview utility

- Go to the Getting Started training
  - F5 Free Training: Getting Started with BIG-IP iHealth
    - Running the qkview utility from the Configuration utility (BIG-IP)
    - Running the qkview utility from the command line (BIG-IP or BIG-IQ)

5.04 Understand information contained in qkview

- In general a qkview contains everything support might need for diagnosing issues:
  - Statistics
  - Log files
  - /config directory
  - /etc directory
  - Performance graph rrd data
  - Other miscellaneous configurations files
- Potential sensitive data is excluded

5.05

Identify which online support resource/tool to use

- DevCentral
- MyF5.com
- iHealth
- Support Portal

5.05 DevCentral

K20452352: F5 operations guides | Optimizing the support experience

- DevCentral (~~devcentral.f5.com~~ community.f5.com) is an online forum of F5 employees and customers that provides technical documentation, discussion forums, blogs, media and more, related to application delivery networking. DevCentral is a resource for education and advice on F5 technologies and is especially helpful for iRules, iApps, Automation and Orchestration Toolchain, etc.
- If you become a DevCentral member, you can do the following:
  - Ask forum questions
  - Rate and comment on content
  - Contribute to wikis
  - Download lab projects
  - Join community interest groups
  - Solve problems and search for information
  - Attend online community events
  - View educational videos

5.05 ~~AskF5.com~~ My.F5.com

K20452352: F5 operations guides | Optimizing the support experience

- ~~AskF5 (support.f5.com~~) MyF5 (myf5.com) is a great resource for thousands of articles and other documents to help you manage your F5 products more effectively. Step-by-step instructions, downloads, and links to additional resources give you the means to solve known issues quickly and without delay, and to address potential issues before they become reality.
- Whether you want to search the knowledge base to research an issue, or you need the most recent news on your F5 products, ~~AskF5~~ MyF5 is your source for product manuals, operations guides, and release notes, including the following:
  - F5 announcements
  - Known issues
  - Security advisories
  - Recommended practices
  - Troubleshooting tips
  - How-to documents
  - Changes in behavior
  - Diagnostic and firmware upgrades
  - Hotfix information
  - Product life cycle information

5.05 Support Portal

K20452352: F5 operations guides | Optimizing the support experience

- Cases are managed through the support portal ~~(support.f5.com)~~ (my.f5.com).

Lab tomorrow!

Tomorrow we will be using F5 UDF to complete labs to help prepare you for the certification. Please be sure to bring a non-GFE laptop! Disable corporate VPN. Chrome works best.

Additional Resources

F5 Certified! Professionals

Listed group

Study groups on LinkedIn

F5 Certified Professionals	https://www.linkedin.com/groups/85832
LinkedIn – F5 Certified! – 101	https://www.linkedin.com/groups/6711359/profile
LinkedIn – F5 Certified! – 201	https://www.linkedin.com/groups/6709915/profile

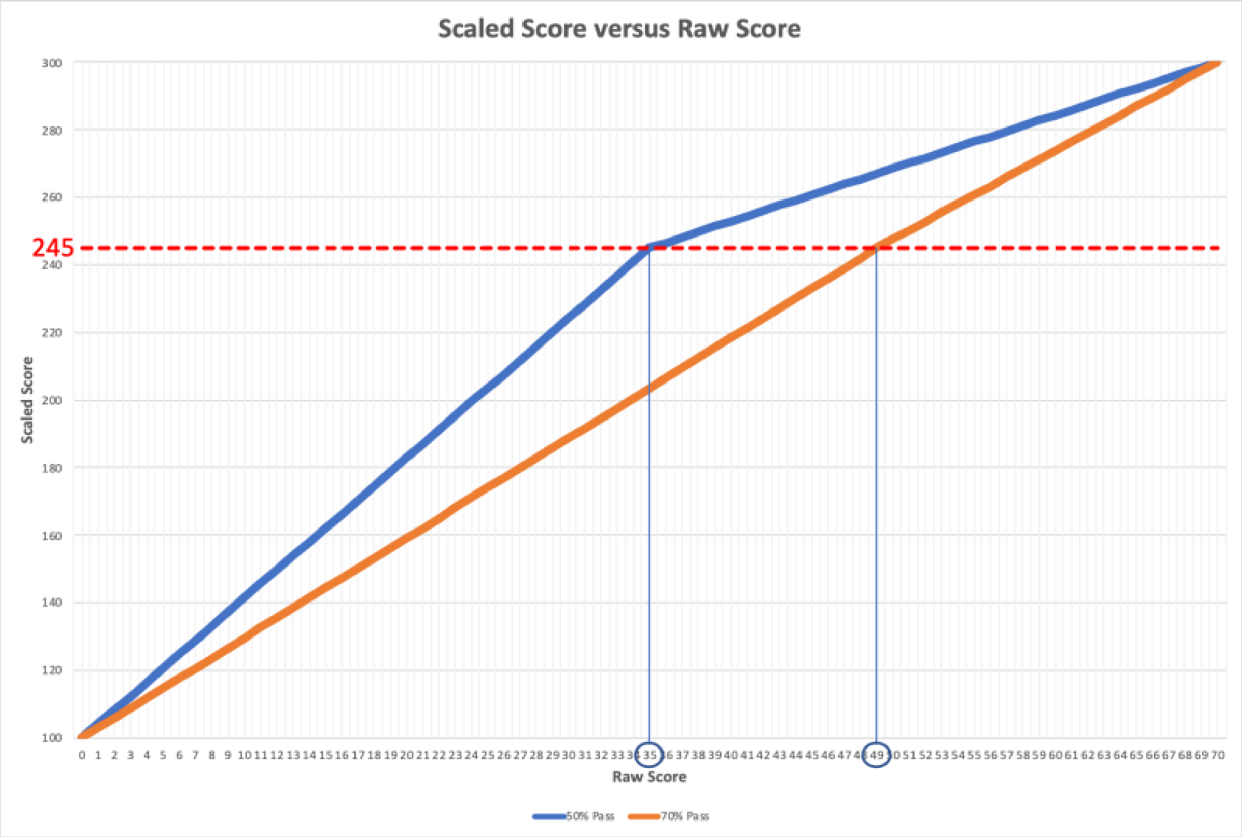
F5 Certification Exams – Scaled Scoring

PASS = 245

How does scaled-scoring work?

Scaled-scoring is a method of score reporting that standardizes scores across exams, different exam forms, and exam versions.

Instead of reporting exam results as a percentage of total items answered correctly and having different required passing percentages for each exam, all F5 exams are scored on a scaled-score basis, where your score will range from a possible 100-350 points; all F5 exams are calibrated for a passing score of 245 on that scale.



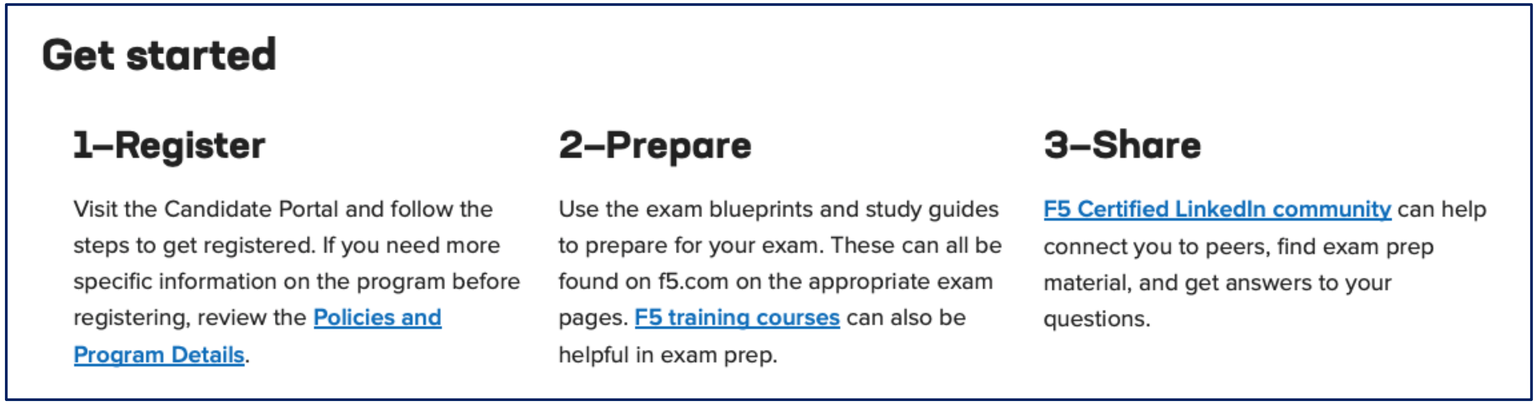
https://education.f5.com/hc/en-us/articles/4403992805019-How-does-Scaled-Scoring-work-

Questions? Email support@mail.education.f5.com

f5

F5 Certification Candidate Registration

- https://www.f5.com/learn/certification
- Scroll to the Candidate Portal link to register and create an account
- Fill out the form information
- Receive email with F5 Candidate ID
- Follow email instructions
- Register for exam today!



Get started

1–Register

Visit the Candidate Portal and follow the steps to get registered. If you need more specific information on the program before registering, review the Policies and Program Details.

2–Prepare

Use the exam blueprints and study guides to prepare for your exam. These can all be found on f5.com on the appropriate exam pages. F5 training courses can also be helpful in exam prep.

3–Share

F5 Certified LinkedIn community can help connect you to peers, find exam prep material, and get answers to your questions.

Virtual Server Match Examples

Match the connections on the right to the virtual server configurations on the left

1. Destination IP 10.0.33.199:80 with IP source of 10.30.1.0/24
2. Destination IP 10.0.33.199:80 with network source of 0.0.0.0/0
3. Destination IP 10.0.33.199:* with network source 10.30.1.0/24
4. Destination IP 10.0.33.199:* with network source 0.0.0.0/0
5. Destination Net 10.0.33.0/24:443 with network source 0.0.0.0/0
6. Destination Net 10.0.33.0/24:* with network source 0.0.0.0/0
7. Destination Net 0.0.0.0/0:80 with network source 10.128.20.0/24
8. Destination Net 0.0.0.0/0:* with network source 0.0.0.0/0

Connect to:	Source IP
10.1.33.199:80	10.30.1.120
10.0.33.199:80	10.30.2.120
10.0.33.199:443	17.64.223.120
10.0.33.196:443	10.30.1.120
74.125.21.106:80	10.128.20.100