F5 301a v14.1 Certification Prep

Paul Deakin, Melisa Wentz, Hachul Jun and David Larsen

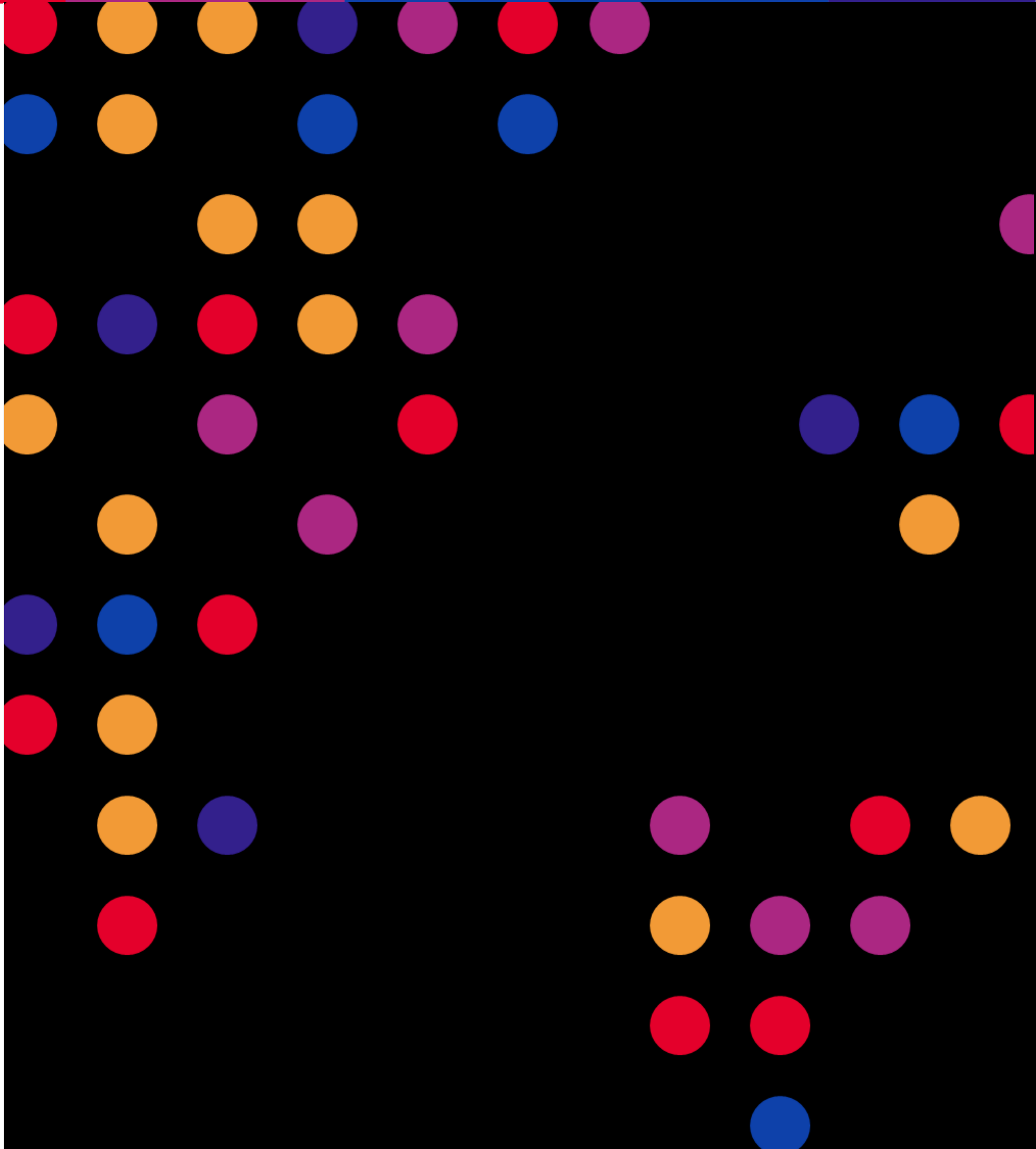
Systems Engineers, F5

March 2024

The goal

If you are just starting your study, this prep will hopefully help you determine strengths and weaknesses.

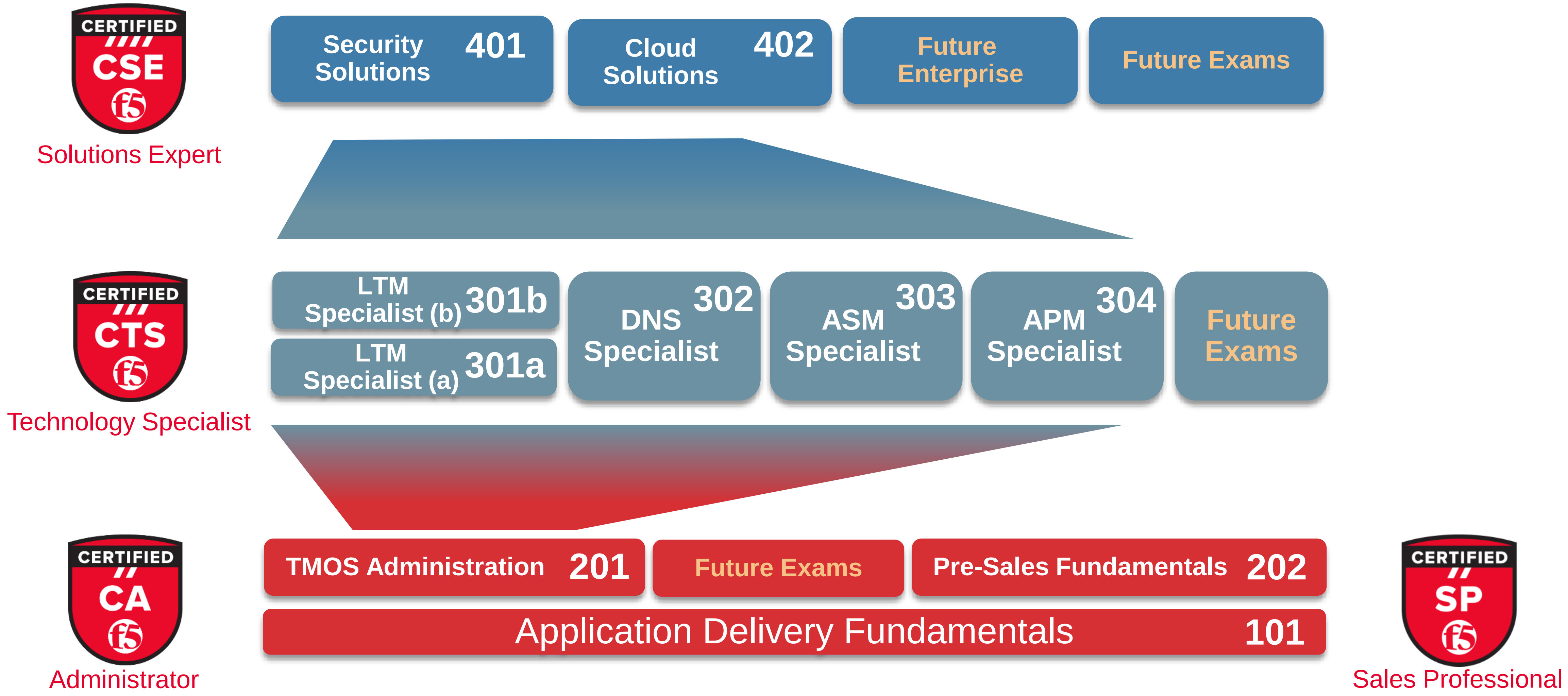
If you are almost ready, then this prep is an opportunity for a final review and to ask questions.



Setting expectations

- This course is not designed to have you take the 301 exam after completion.
- Understand, I have no more idea what is actually on the exam than you do.
  - The material is based off the blueprint and my experience having taken prior F5 exams and practice exams.
- We will not cover every topic in depth:
  - There is simply not enough time.
  - We will focus on the topics I think you need to know more deeply.
  - There are many links to additional information.
- This isn’t a course to teach you how to configure a BIG-IP
  - If you need basic Local Traffic Management training, though, that can be arranged :).

F5 Certification Exams



CERTIFIED CSE

Solutions Expert

Security Solutions 401

Cloud Solutions 402

Future Enterprise

Future Exams

CERTIFIED CTS

Technology Specialist

LTM Specialist (b) 301b

LTM Specialist (a) 301a

DNS Specialist 302

ASM Specialist 303

APM Specialist 304

Future Exams

CERTIFIED CA

Administrator

TMOS Administration 201

Future Exams

Pre-Sales Fundamentals 202

Application Delivery Fundamentals 101

CERTIFIED SP

Sales Professional

101—Application Delivery Fundamental Exam Blueprint

LEARNING

Certification

Get ahead with F5 Certifications

Becoming an F5 Certified professional validates your technical skills and expertise in application delivery networking. F5 certifications give you a high-quality, credible way to showcase and leverage your advanced knowledge with customers.

Learn more about the F5 Certification Program

https://partners.f5.com/learning/certification

101 - Application Delivery Fundamental

EXAM BLUEPRINT

ABOUT THE 101-APPLICATION DELIVERY FUNDAMENTALS EXAM.
The 101-Application Delivery Fundamentals exam is the first exam required to achieve Certified F5 BIG-IP Administrator status.

Successful completion of the 101-Application Delivery Fundamentals exam acknowledges the skills and understanding necessary for day-to-day management of Application Delivery Networks (ADNs).

WHAT IS THE 101-APPLICATION DELIVERY FUNDAMENTALS EXAM BLUEPRINT?
F5 Certified! exam blueprints list all the objectives an exam has to measure, much like a syllabus for the exam itself. Blueprints provide a detailed breakdown of the skills and knowledge a candidate should have to pass the exam. Blueprints can be used to identify areas for additional study, and are best used in conjunction with the Exam Study Guides.

PREREQUISITES:
None

CREDENTIAL AWARDED:
None (prerequisite to the TMOS Administration exam)

THIS EXAM IS BASED ON V13.1

V3_2019

Exam Structure

F5 301a exam—LTM Architect, Setup, and Deploy

- TMOS 14.1
- Multiple choice (there are NO true/false questions!)
- Not adaptive
- 80 questions in 90 mins
  - Non-native English-speaking students can have an additional 30 minutes if they request it
- No command line engines (although you will have to know a few TMSH commands)
- View whole exhibit before you close it (attachments)
- Manage your time!
- You can flag, review, and re-answer questions (within the 90-minute test limit!)
- *Secure Sauce (exam tips) at the end of the presentation!

F5 exams: multiple-attempt rules

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

Additional certification resources

- **Practice exams through Zoomorphix at www.examstudio.com**

  You will be able to set up account through Cert Program Enrollment Process

  (see next slide for list of exams)

- **Online exam study guides found here:**

  https://clouddocs.f5.com/training/community/f5cert/html/

  (NOTE: supporting K-Doc for each objective is listed—very helpful!)

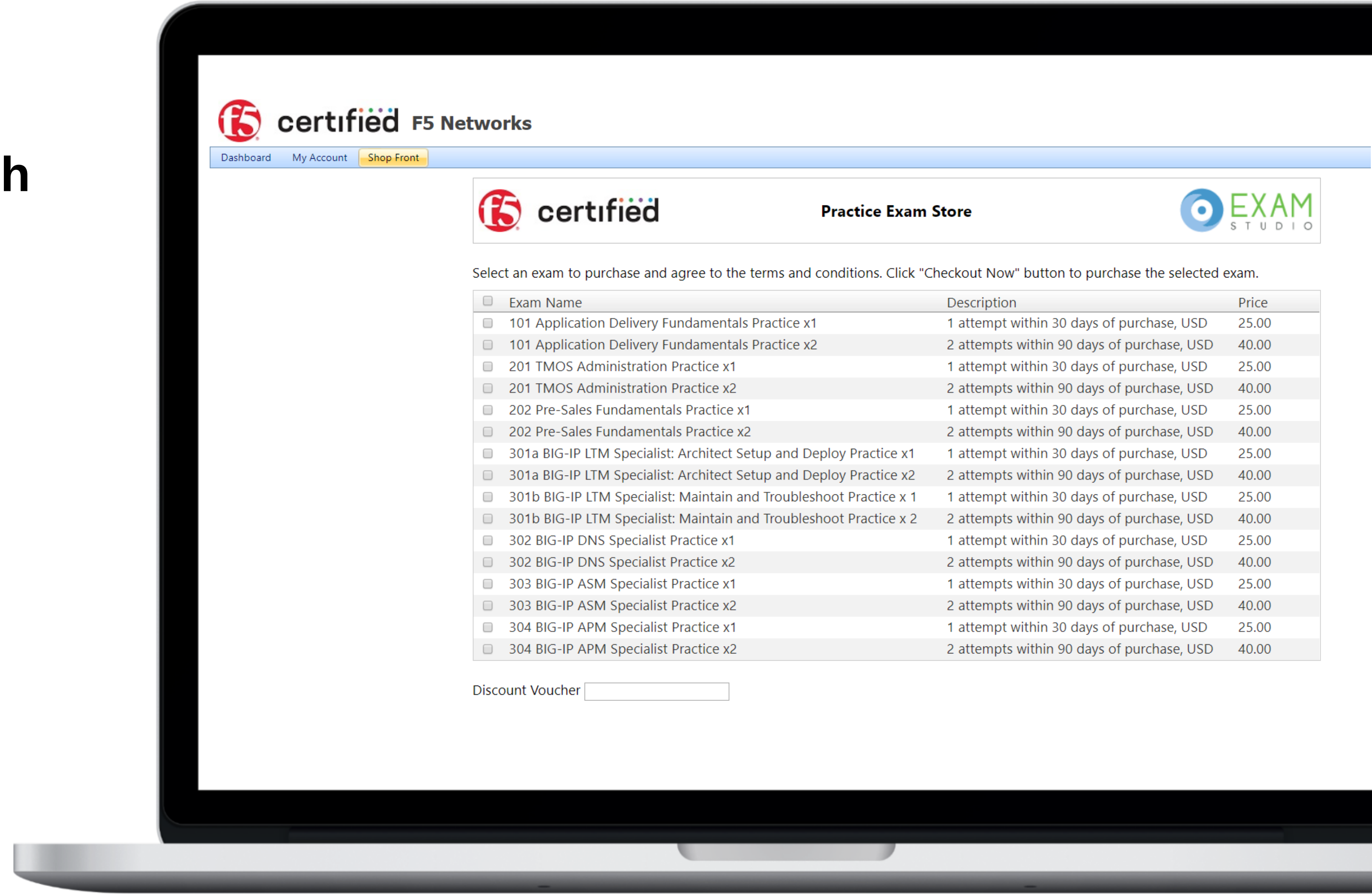
- **LinkedIn**

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

Available F5 practice exams

Practice exams through Zoomorphix at www.examstudio.com

You will be able to set up account through Cert Program Enrollment Process



certified F5 Networks

certified Practice Exam Store EXAM STUDIO

Select an exam to purchase and agree to the terms and conditions. Click "Checkout Now" button to purchase the selected exam.

□	Exam Name	Description	Price
□	101 Application Delivery Fundamentals Practice x1	1 attempt within 30 days of purchase, USD	25.00
□	101 Application Delivery Fundamentals Practice x2	2 attempts within 90 days of purchase, USD	40.00
□	201 TMOS Administration Practice x1	1 attempt within 30 days of purchase, USD	25.00
□	201 TMOS Administration Practice x2	2 attempts within 90 days of purchase, USD	40.00
□	202 Pre-Sales Fundamentals Practice x1	1 attempt within 30 days of purchase, USD	25.00
□	202 Pre-Sales Fundamentals Practice x2	2 attempts within 90 days of purchase, USD	40.00
□	301a BIG-IP LTM Specialist: Architect Setup and Deploy Practice x1	1 attempt within 30 days of purchase, USD	25.00
□	301a BIG-IP LTM Specialist: Architect Setup and Deploy Practice x2	2 attempts within 90 days of purchase, USD	40.00
□	301b BIG-IP LTM Specialist: Maintain and Troubleshoot Practice x 1	1 attempt within 30 days of purchase, USD	25.00
□	301b BIG-IP LTM Specialist: Maintain and Troubleshoot Practice x 2	2 attempts within 90 days of purchase, USD	40.00
□	302 BIG-IP DNS Specialist Practice x1	1 attempt within 30 days of purchase, USD	25.00
□	302 BIG-IP DNS Specialist Practice x2	2 attempts within 90 days of purchase, USD	40.00
□	303 BIG-IP ASM Specialist Practice x1	1 attempts within 30 days of purchase, USD	25.00
□	303 BIG-IP ASM Specialist Practice x2	2 attempts within 90 days of purchase, USD	40.00
□	304 BIG-IP APM Specialist Practice x1	1 attempt within 30 days of purchase, USD	25.00
□	304 BIG-IP APM Specialist Practice x2	2 attempts within 90 days of purchase, USD	40.00

Discount Voucher

F5 301a v14.1 certification prep

Before you ask. Yes, the slides are available for you to review.

A PDF copy of this slide deck with notes can be found on Partner Central in the Technical Hub under Technical Certification:

This is a direct link to the PDF

K70671013: BIG-IP LTM-DNS operations guide

- The current study guide for the 301a is based on v11.4 and has not been updated, though most of the information remains the same. But I strongly recommend you review the above article. You will also see many links from the following manuals:
- Manual: BIG-IP Local Traffic Management: Basics

https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0.html

- Manual: BIG-IP TMOS: Routing Administration

https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0.html

Architect and Deploy Applications

1.01

Determine which configuration objects are necessary to optimally deploy an application

- Determine least amount of configuration objects needed to deploy application
- Understand dependencies of configuration objects
- Understand needed LTM profiles to deploy an application
- Identify unnecessary configurations objects
- Understand the differences between virtual servers and virtual addresses

Topic Resources

- https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-1-0.html
- Manual Chapter: Interfaces
- https://clouddocs.f5.com/cli/tmsh-reference/v13/ with link to Full TMSH Reference Guide PDF
- Manual Chapter: Trunks
- Manual Chapter: VLANs VLAN Groups and VXLAN
- Manual Chapter: Self IP Addresses

1.02

Determine whether an application can be deployed with only the LTM module provisioned

- Identify the functionality of LTM configuration objects
- Identify LTM profile settings to deploy an application
- Determine capabilities of LTM configuration objects

Topic Resources

- https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-13-1-0.html
- Manual Chapter: Interfaces
- https://clouddocs.f5.com/cli/tmsh-reference/v13/ with link to Full TMSH Reference Guide PDF
- Manual Chapter: Trunks
- Manual Chapter: VLANs VLAN Groups and VXLAN
- Manual Chapter: Self IP Addresses

1.03

Identify the difference between deployments (e.g., one arm, two arm, npath, Direct Server Return (DSR)

- Identify configuration objects needed for L2/L3 nPath routing
- Determine how the IP address changes when using DSR
- Determine how IP addresses change when using a full proxy deployment
- Plan the network considerations for one arm and two arm deployments
- Understand the importance of auto last-hop

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits

  -K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.04

Choose correct profiles and settings to fit application requirements

- Identify LTM profile settings to deploy OneConnect
- Determine which profiles are needed to deploy an application
- Compare and contrast different communication protocols (TCP, UDP, FastL4)
- Compare performance impact of LTM profile settings

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
    - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.05

Choose virtual server type and load balancing type to fit application requirements

- Determine the difference between L2-L3 virtual servers
- Compare and contrast standard and Fast L4 virtual server types
- Compare and contrast different load balancing methods
- Identify different load balancing method use cases

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
  - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.06

Determine how to architect and deploy multi-tier applications using LTM technology

- Understand connection-based architecture and when/how to apply SNAT/persistence/SSL settings in a multi-tiered environment
- Identify which device handles specific configuration objects in a multi-tiered deployment

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
    - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.07

Distinguish between packet-based versus connection-based load balancing

- Demonstrate when to use packet-based load balancing
- Demonstrate when to use connection-based load balancing

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
  - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.08

Determine which configuration objects are necessary for applications that need the original client IP address

- Determine when SNAT is required
- Determine the required SNAT type
- Identify functions of X-forwarded-for
- Outline the steps needed to return the traffic to LTM without SNAT

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
  - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.09

Identify the matching order of multiple virtual servers

- Identify which virtual server would process particular traffic
- Identify why the virtual server fails to receive traffic

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
    - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.10

Given a basic iRule's functionality, determine the profiles and configuration options necessary to implement the iRule

- Determine what virtual server profile is necessary
- Determine when persistence profile is necessary

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
    - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

1.11

Describe how to deploy applications using iApp templates

- Identify when an iApp is appropriate
- Recognize how to modify an application deployed with an iApp
- Identify objects created by an iApp

Topic Resources

- Manual Chapter: NATS and SNATs
- K7336: The SNAT Automap and self IP address selection
- K7820: Overview of SNAT features
- K8246: How the BIG-IP system handles SNAT port exhaustion
- K9038: The order of precedence for local traffic object listeners
- K14800: Order of precedence for virtual server matching (11.3.0 and later)
- Manual Chapter: Setting Connection Limits
  - K8457: Connection limits for a CMP system are enforced per TMM instance
- Manual: Session Persistence Profiles

Set Up, Administer, and Secure LTM Devices

2.01

Determine how to secure Self IPs

- Identify which administrative services need to be accessible
- Identify which configurations objects are allowing accessibility
- Identify which services must be enabled for HA availability between devices

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

2.02

Determine how to secure virtual servers

- Determine how to limit access to virtual servers
- Compare and contrast different virtual server types
- Identify LTM profiles setting to limit access to virtual server resources

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

2.03

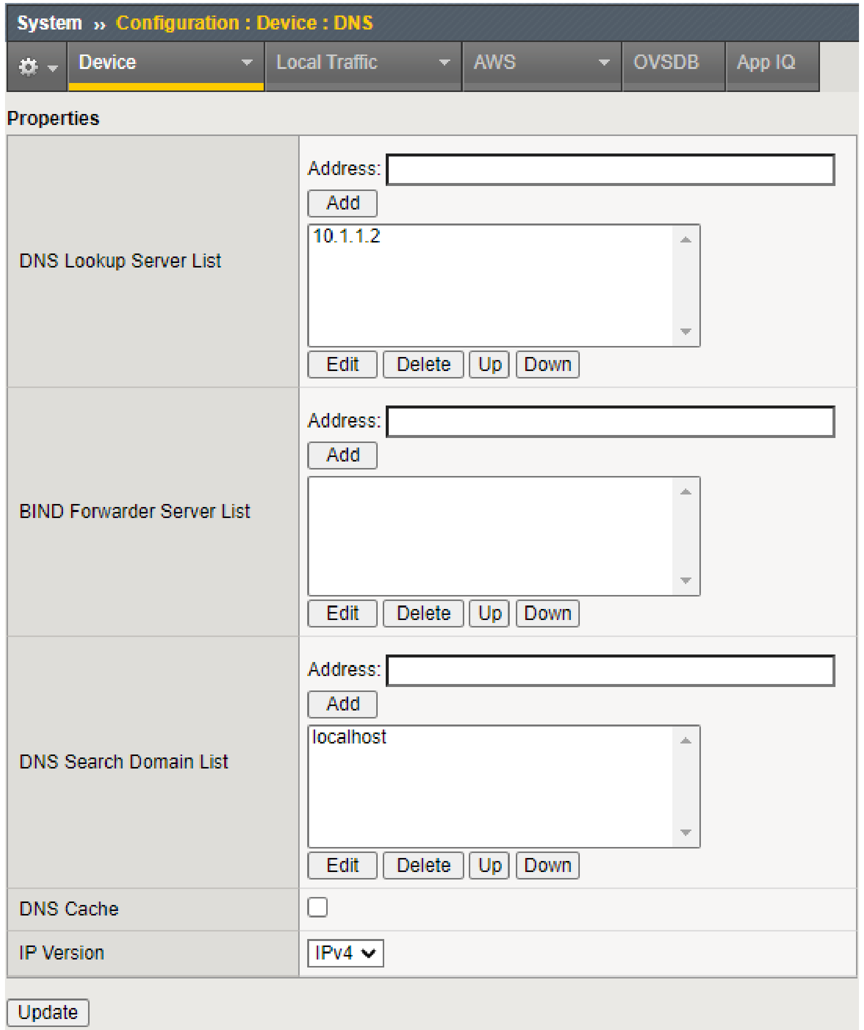
Determine how to perform basic device configuration

- Identify how to synch time/date amongst LTM devices
- Determine how to limit administrative access to LTM device (GUI/CLI)
- Identify how to restrict access to administrative partitions

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

Manual Chapter: General Configuration Properties

- DNS Lookup Server List enables users to use the following for accessing virtual servers, nodes, or other network objects:
    - IP addresses
    - host names
    - fully-qualified domain names (FQDNs)
- The DNS Search Domain List enables BIG-IP to search for local domain lookups to resolve local host names.
- Additionally, you can manually configure the BIND Forwarder Server List that provides DNS resolution for servers and other equipment load-balanced by the BIG-IP system (for the servers that the BIG-IP system uses for DNS proxy services).



Properties

DNS Lookup Server List	Address: 10.1.1.2
BIND Forwarder Server List	Address:
DNS Search Domain List	Address: localhost
DNS Cache	□
IP Version	IPv4

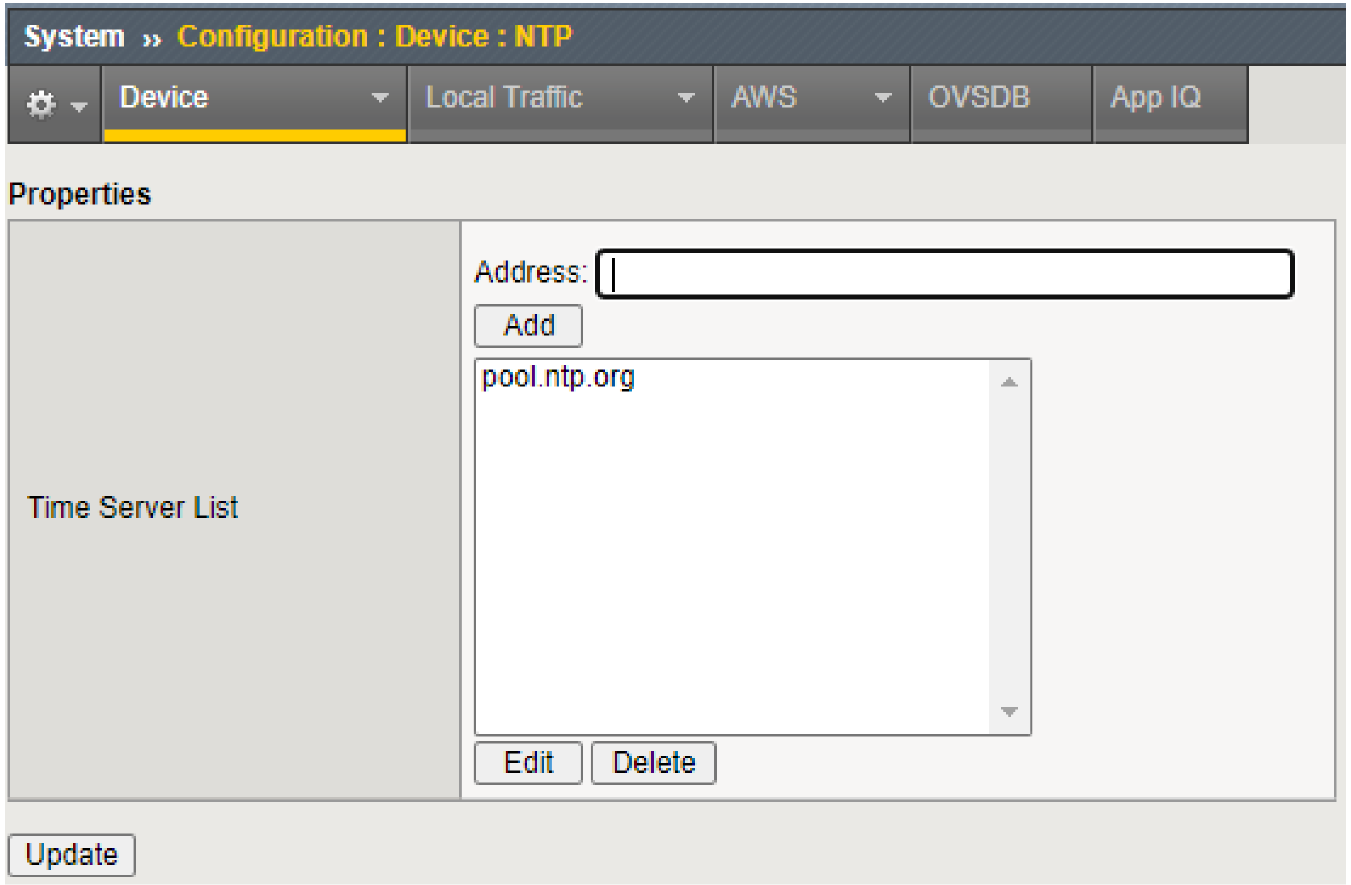
3.09 Show proper configuration for: DNS, NTP, SNMP, syslog

[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



System » Configuration : Device : NTP

Properties

Time Server List

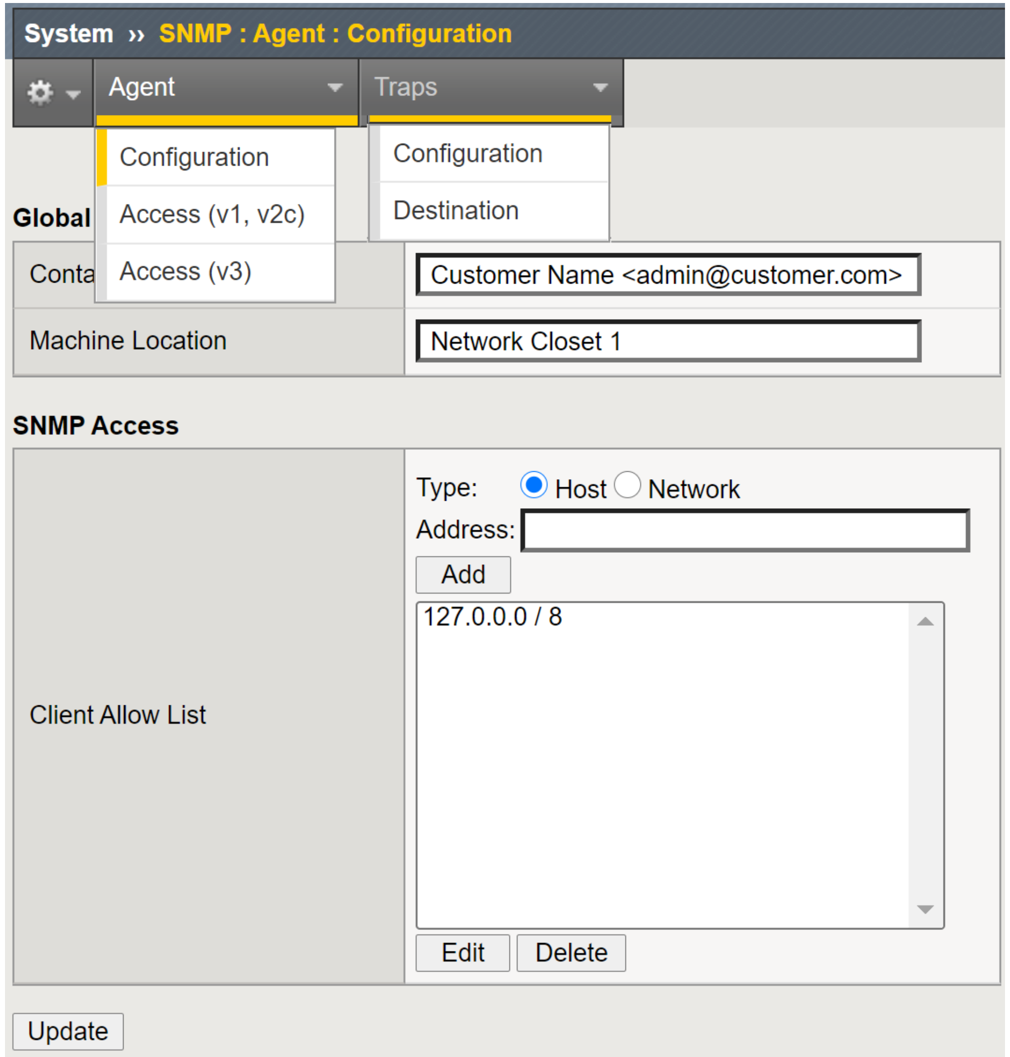
Address:

pool.ntp.org

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

Manual Chapter: Monitoring BIG-IP System Traffic with SNMP

- BIG-IP SNMP agent configuration
  - The primary tasks in configuring the SNMP agent are configuring client access to the SNMP agent and controlling access to SNMP data
- Task Summary
  - Specify SNMP administrator contact information and system location information
  - Configure SNMP manager access to the SNMP agent on the BIG-IP system
  - Grant community access to v1 or v2c SNMP data
  - Grant user access to v3 SNMP data



Conta: Customer Name <admin@customer.com>

Machine Location: Network Closet 1

Client Allow List

Type: ● Host ○ Network

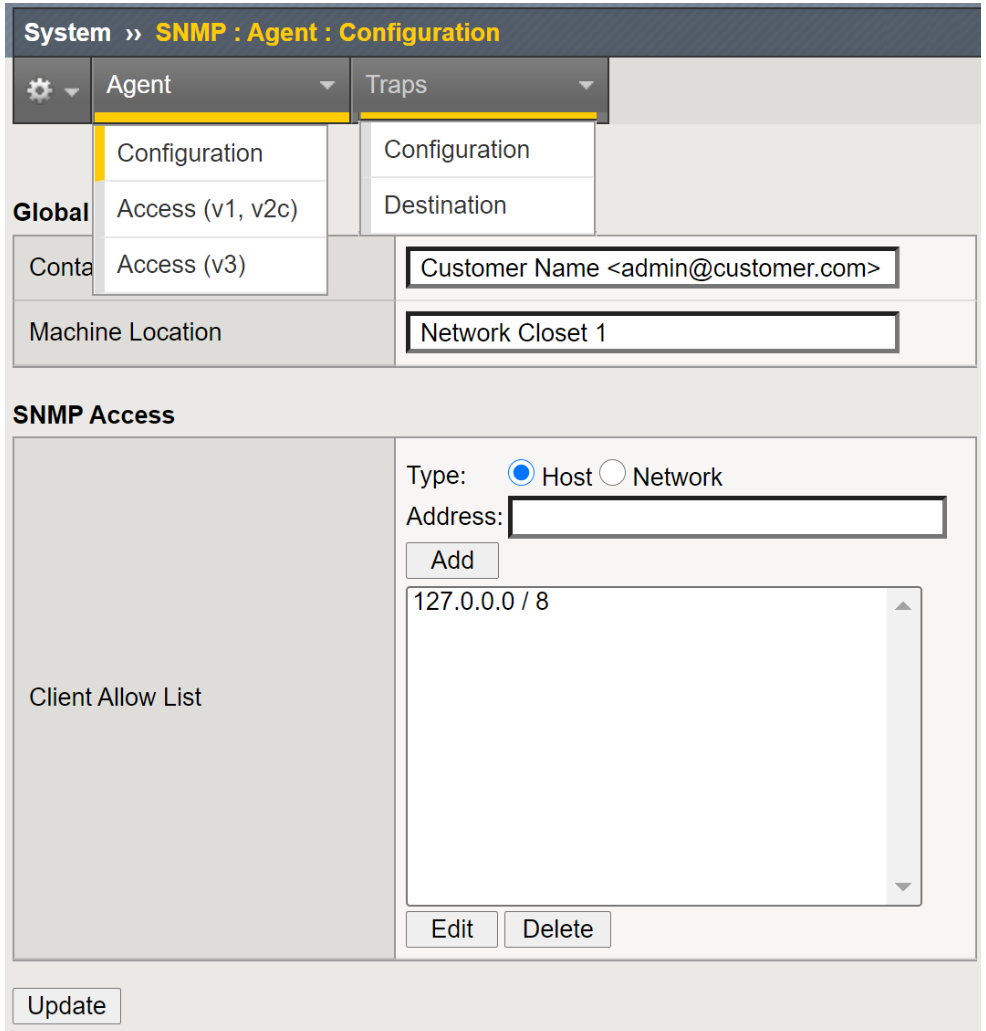
Address:

127.0.0.0 / 8

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

Manual Chapter: Monitoring BIG-IP System Traffic with SNMP

- SNMP trap configuration
  - Configuring SNMP traps on a BIG-IP system means configuring how the BIG-IP system handles traps, as well as setting the destination to which the notifications are sent
- The BIG-IP system stores SNMP traps in two specific files:
  - /etc/alertd/alert.conf - contains default SNMP traps
    - Important: Do not add or remove traps from the /etc/alertd/alert.conf file
  - /config/user_alert.conf - contains user-defined SNMP traps
- Task Summary
  - Enabling traps for specific events
  - Setting v1 and v2c trap destinations
  - Setting v3 trap destinations



System ›› SNMP : Agent : Configuration

Global

Conta

Customer Name <admin@customer.com>

Machine Location: Network Closet 1

SNMP Access

Client Allow List

Type: ● Host ○ Network

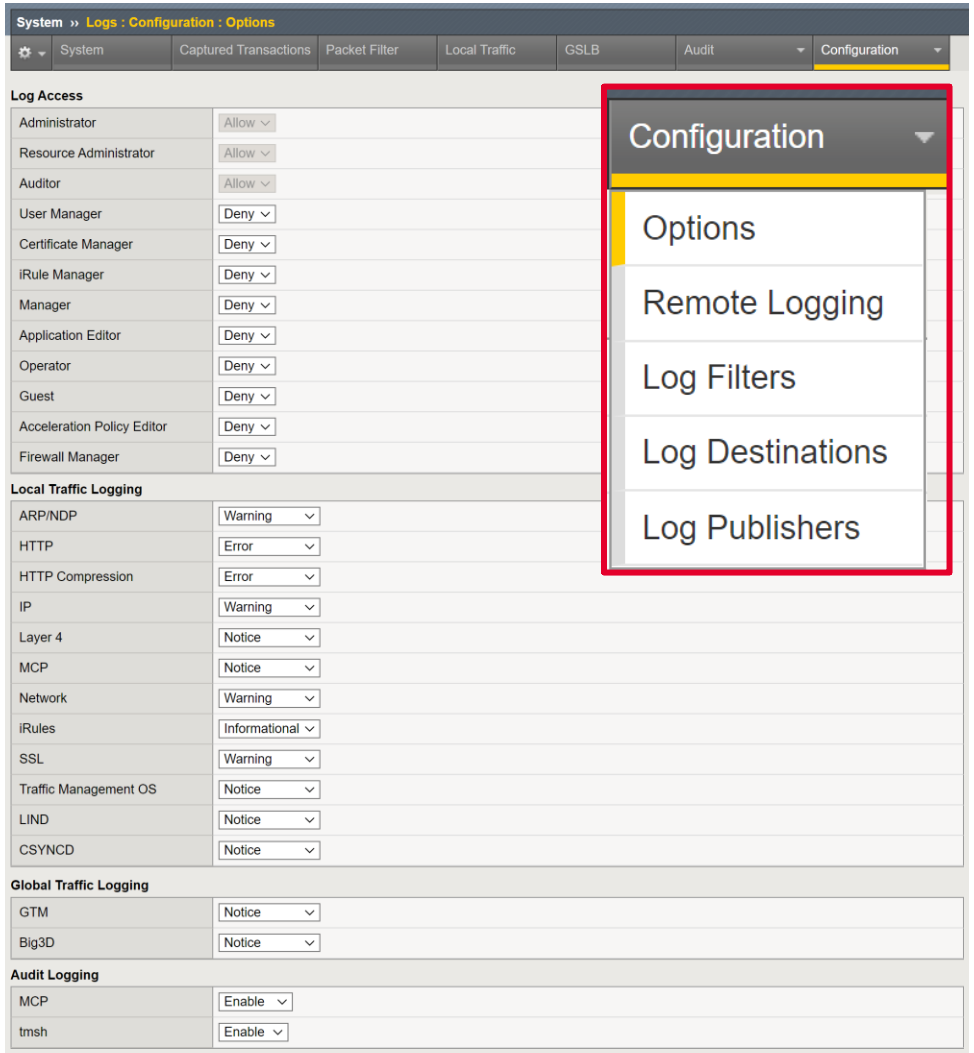
Address:

127.0.0.0 / 8

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 to
- 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

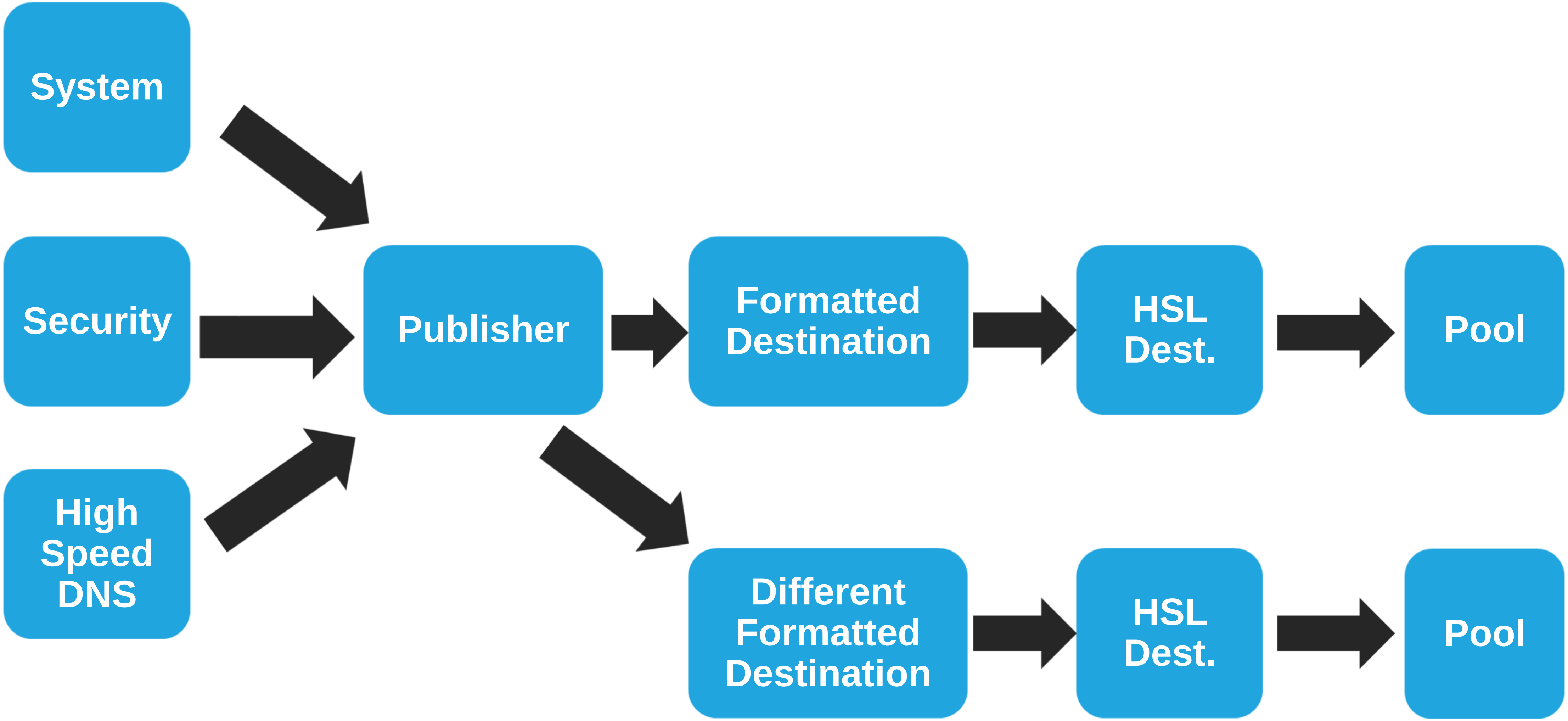
MCP	Enable
tmsh	Enable

Remote Logging Steps

1. Create a Pool of logging server(s)
2. Create an HSL Destination (define the protocol TCP/UDP and Pool)
3. Create a Formatted Destination (define format ie. syslog, arcsight)
4. Create a Publisher
5. Logging Application Steps (varies by application)

- System Logging
  - Linux host daemons, etc.
  - Uses filters
- Security Logging
  - Advanced Firewall Manager, DNS Firewall, Protocol Security Module and the Applications Security Manager
  - Uses Security Logging Profile
- High Speed DNS Query Logging
  - Uses Security Logging Profile

Logging Overview



System

Security

High Speed DNS

Publisher

Formatted Destination

HSL Dest.

Pool

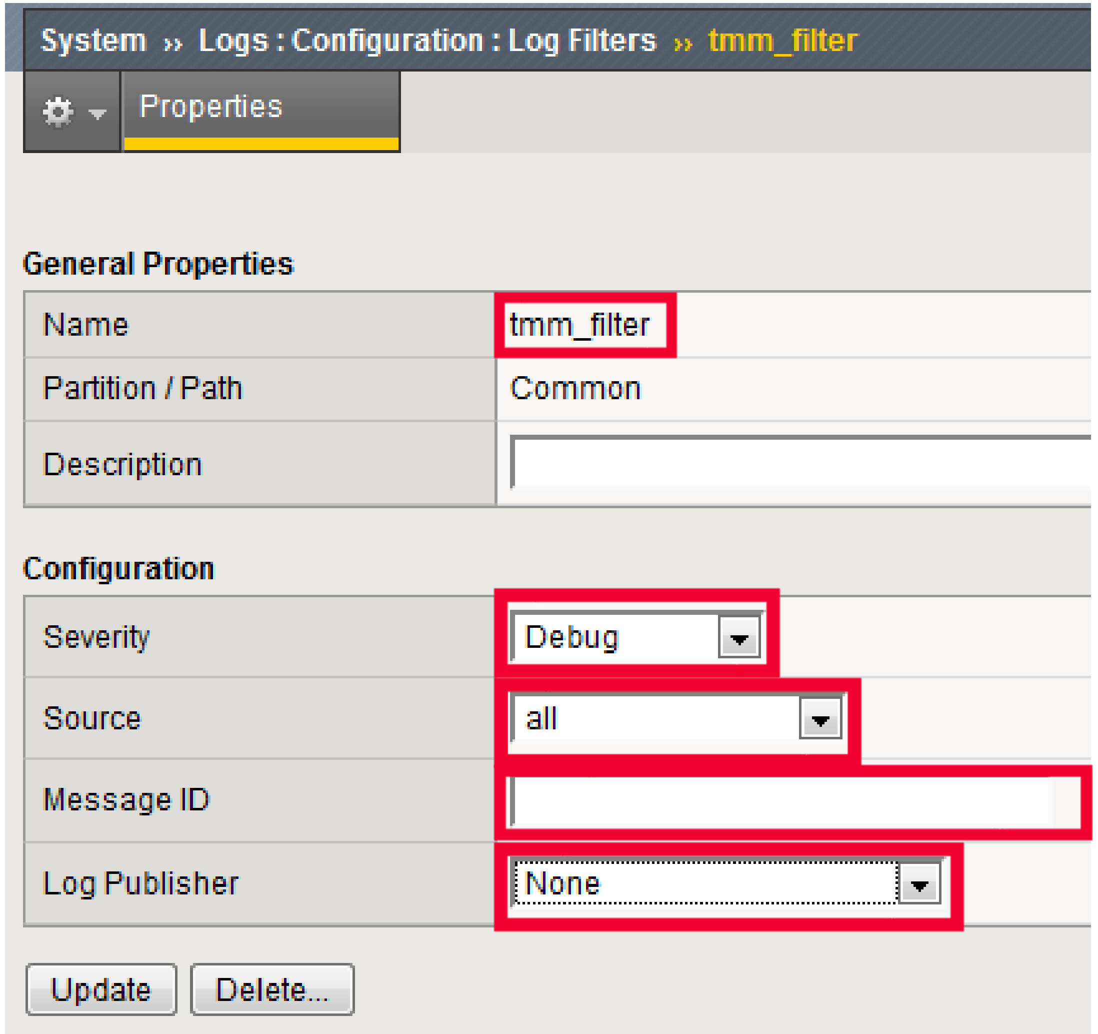
Different Formatted Destination

HSL Dest.

Pool

tmm_filter (aka System Logging filter)

- Under System > Logs > Configuration > Log Filters
- Can create custom filters
  - ○ Name
  - ○ Description (optional)
  - ○ Severity
    - Default is Debug
  - Source
    - ○ List of processes
    - ○ Defaults to all
  - Message ID
  - Log Publisher



General Properties

Name	tmm_filter
Partition / Path	Common
Description	

Configuration

Severity	Debug
Source	all
Message ID	
Log Publisher	None

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

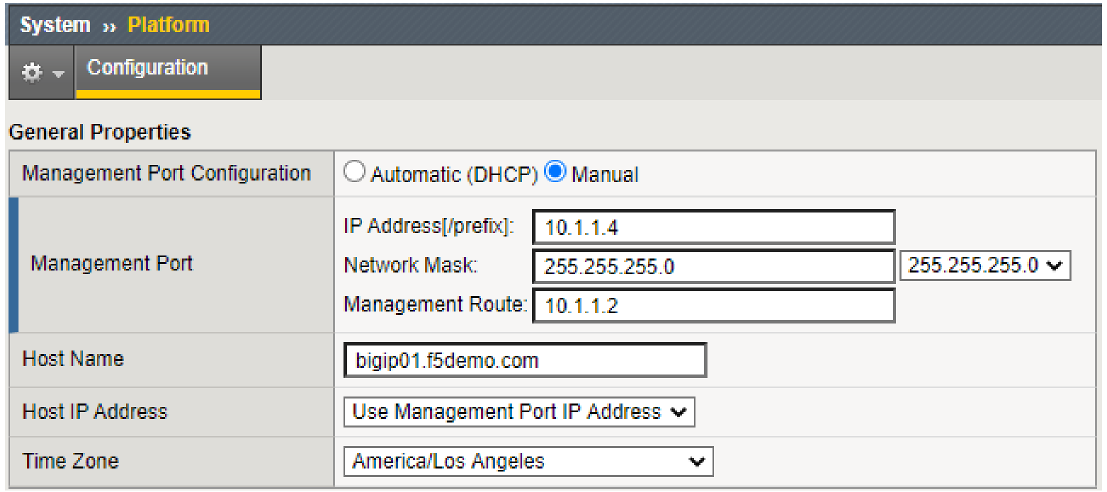
Good old tcpdump

Show services

- tmsh show service <service> or tmsh show service (shows all services)
- From the linux prompt: bigstart status

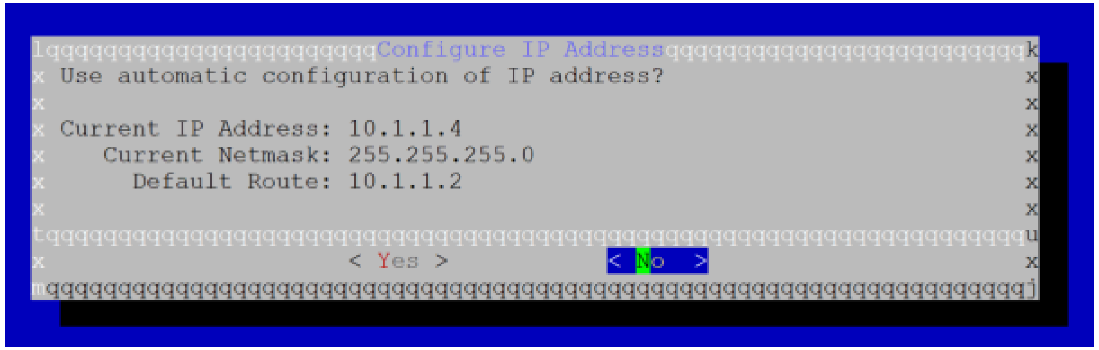
3.03 Identify the configured management—IP address

GUI



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



```
lqqqqqqqqqqqqqqqqqqqqqqqqConfigure 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
```

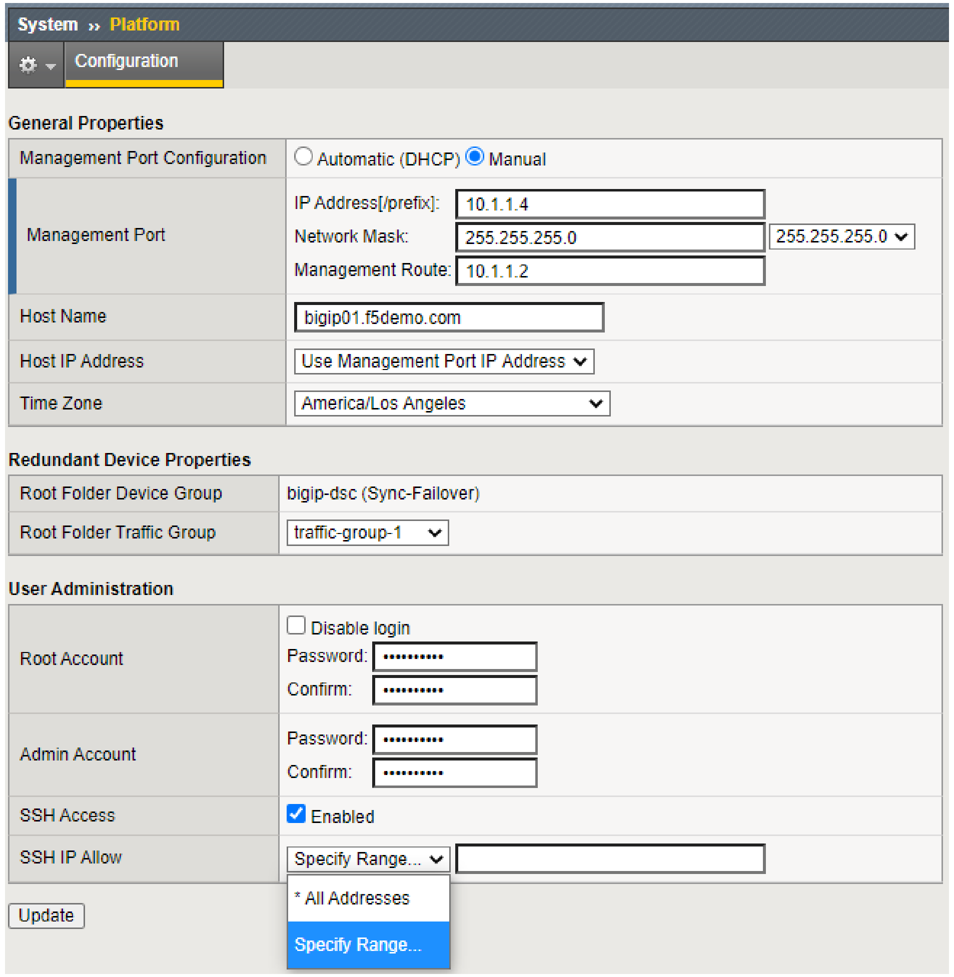
“config” utility at the linux prompt

TMSH

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

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 Show remote connectivity to the BIG-IP Management interface

You connect to the Management interface:

- GUI over HTTPS (port 443)
- Terminal via SSH (port 22)

By default, these ports are open on the OOB Manage IP.

You can also connect to the management interfaces via a self IP address:

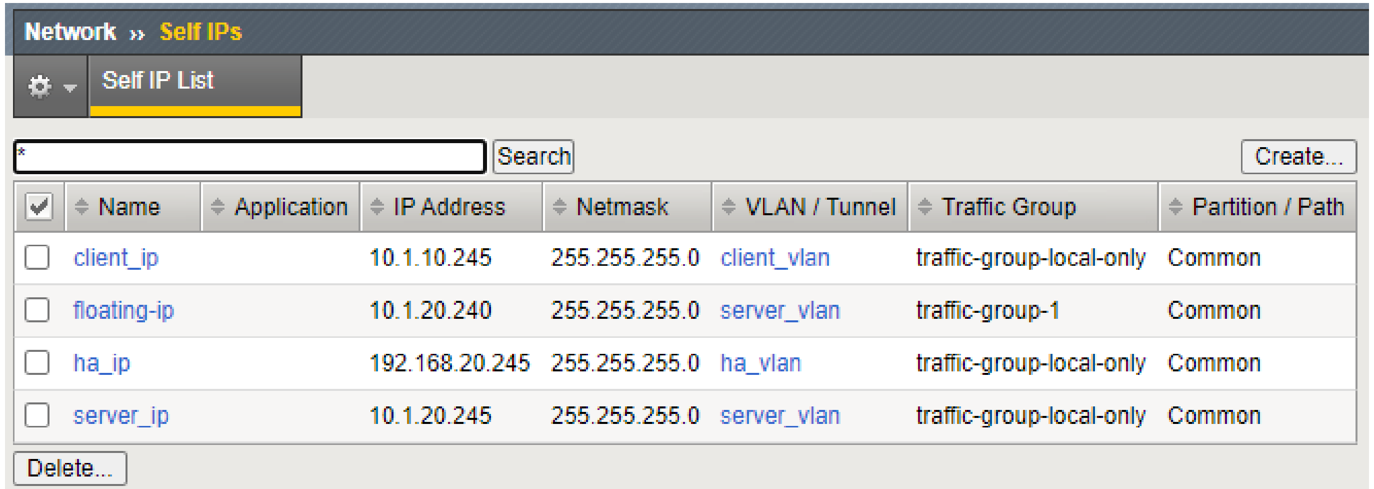
- You must modify the default port lockdown of “None”
- You should never open management interfaces to the internet

3.03 Interpret port lockdown settings to Self-IP

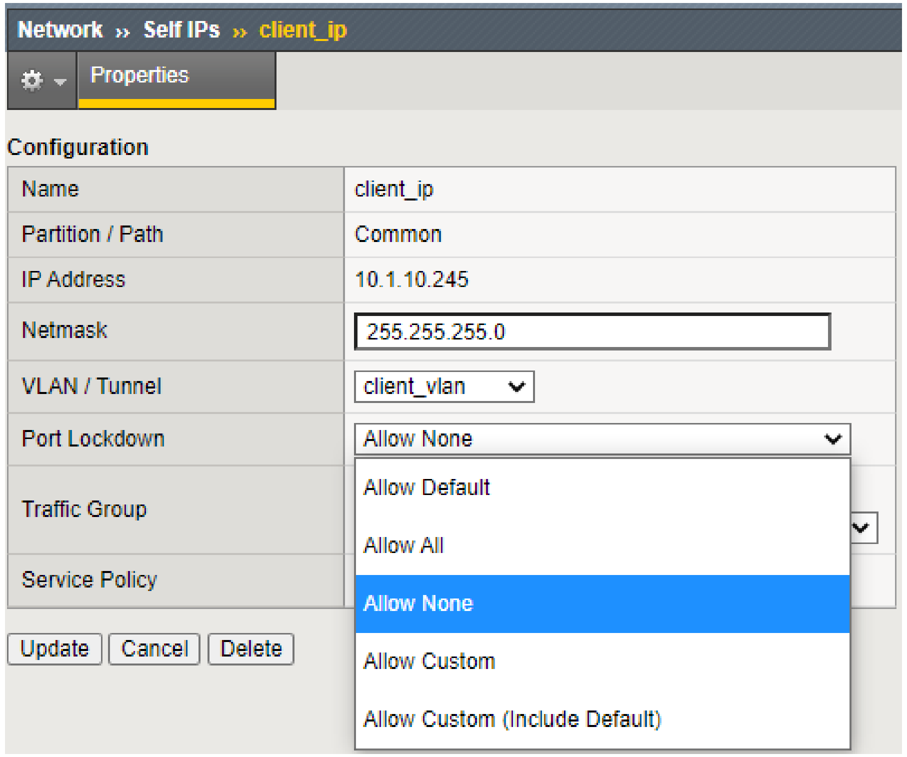
Port Lockdown determines which ports a self IP address will respond to

- By default, Port Lockdown is none, 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	

Port Lockdown options:

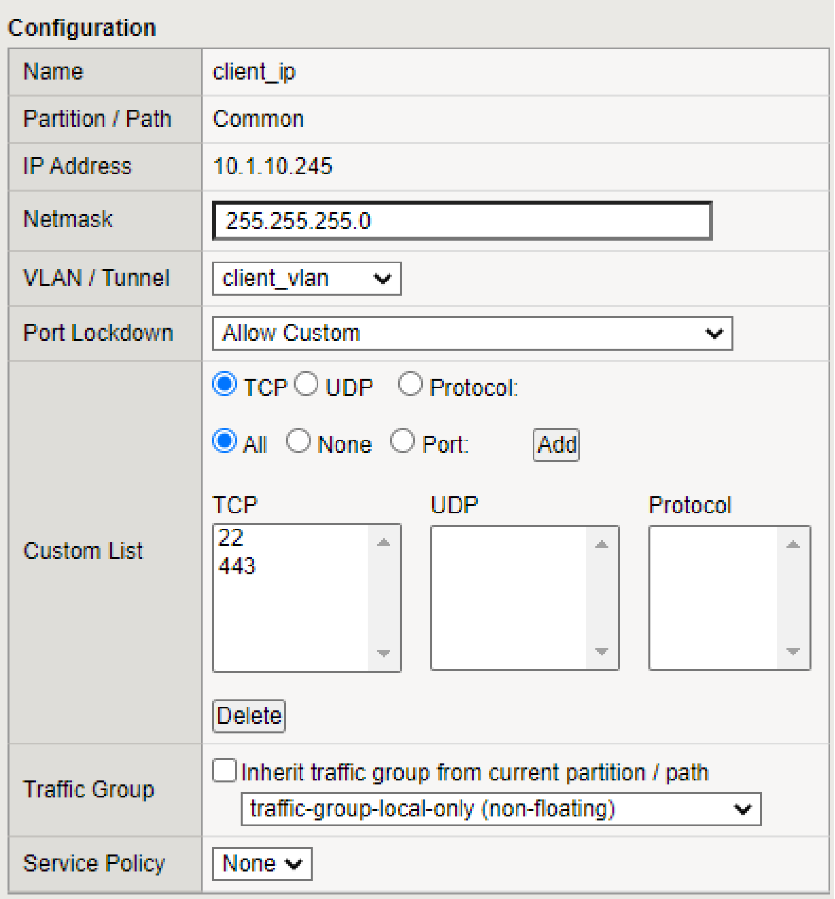
- Allow Default
- Allow All
- Allow None
- Allow Custom
- Allow Custom (Include Default)

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



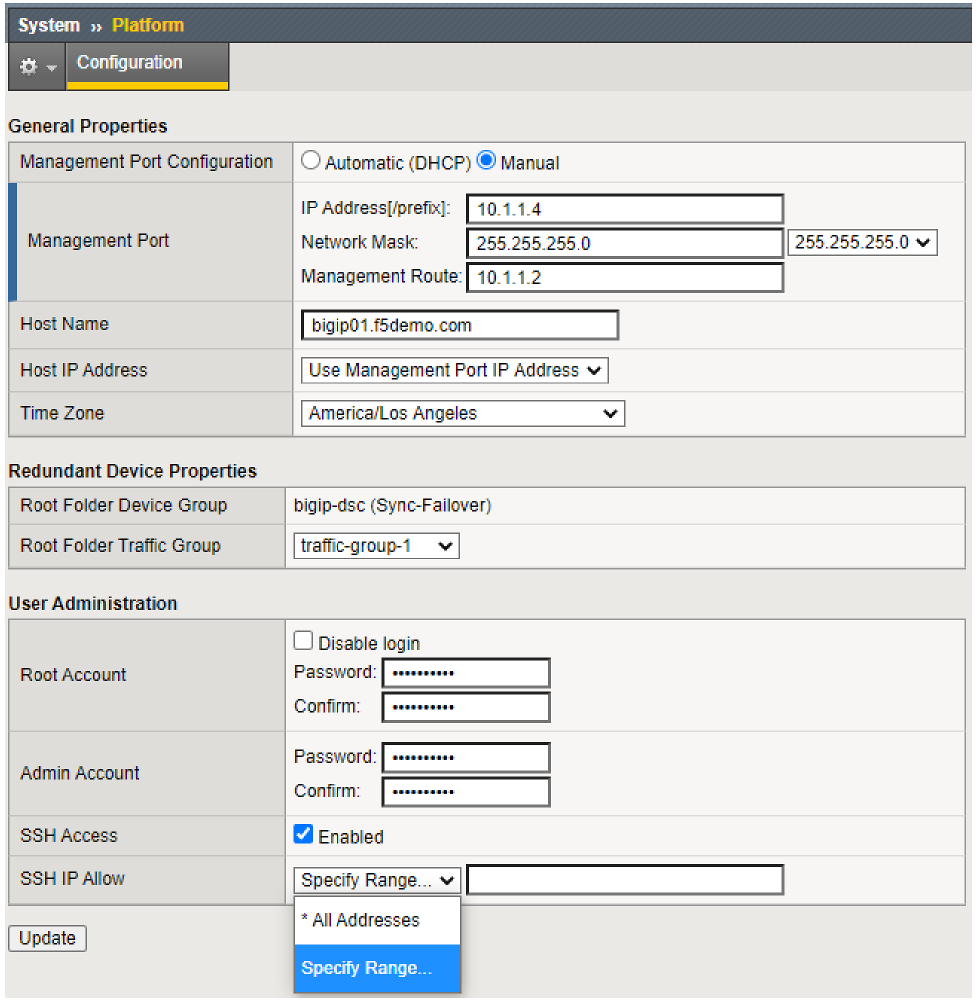
Configuration

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 Identify SSH access list to management—IP address

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



System » Platform

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> }
  - Range uses space ie. {10.1.1.1 10.1.1.10}

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:

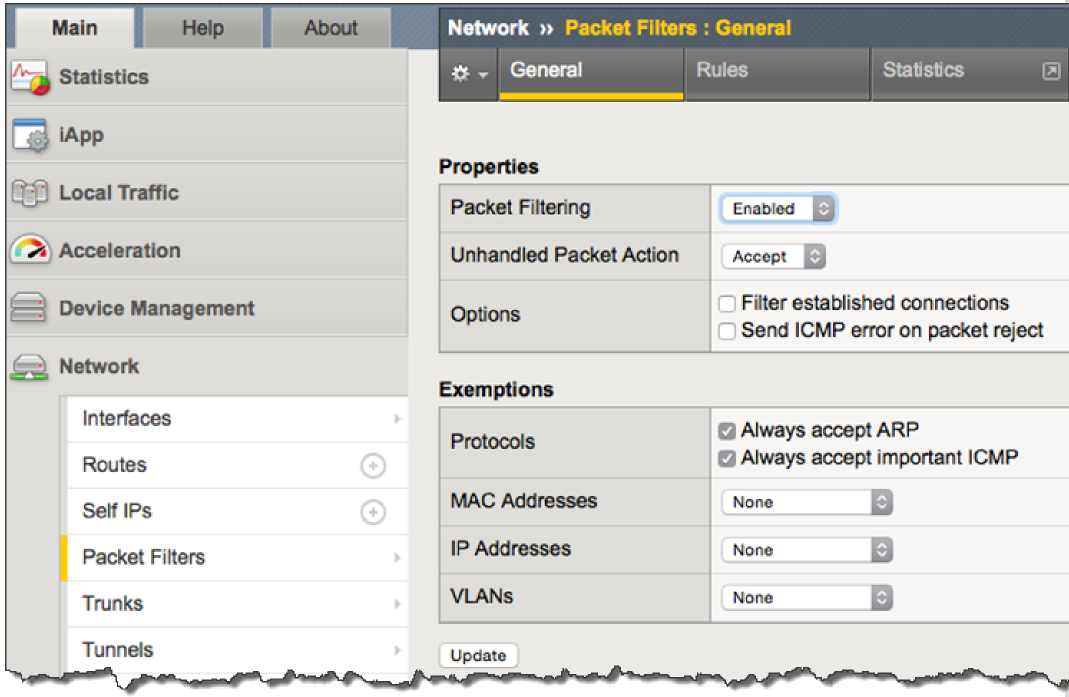
```
(tmos)# list sys httpd
allow
sys httpd {
    allow { All }
}
```

Save the change by entering the following command:

- save /sys config

Restricting access to management ports on Self IPs

(src host 192.168.13.139 or src net 11.1.1.0/24)



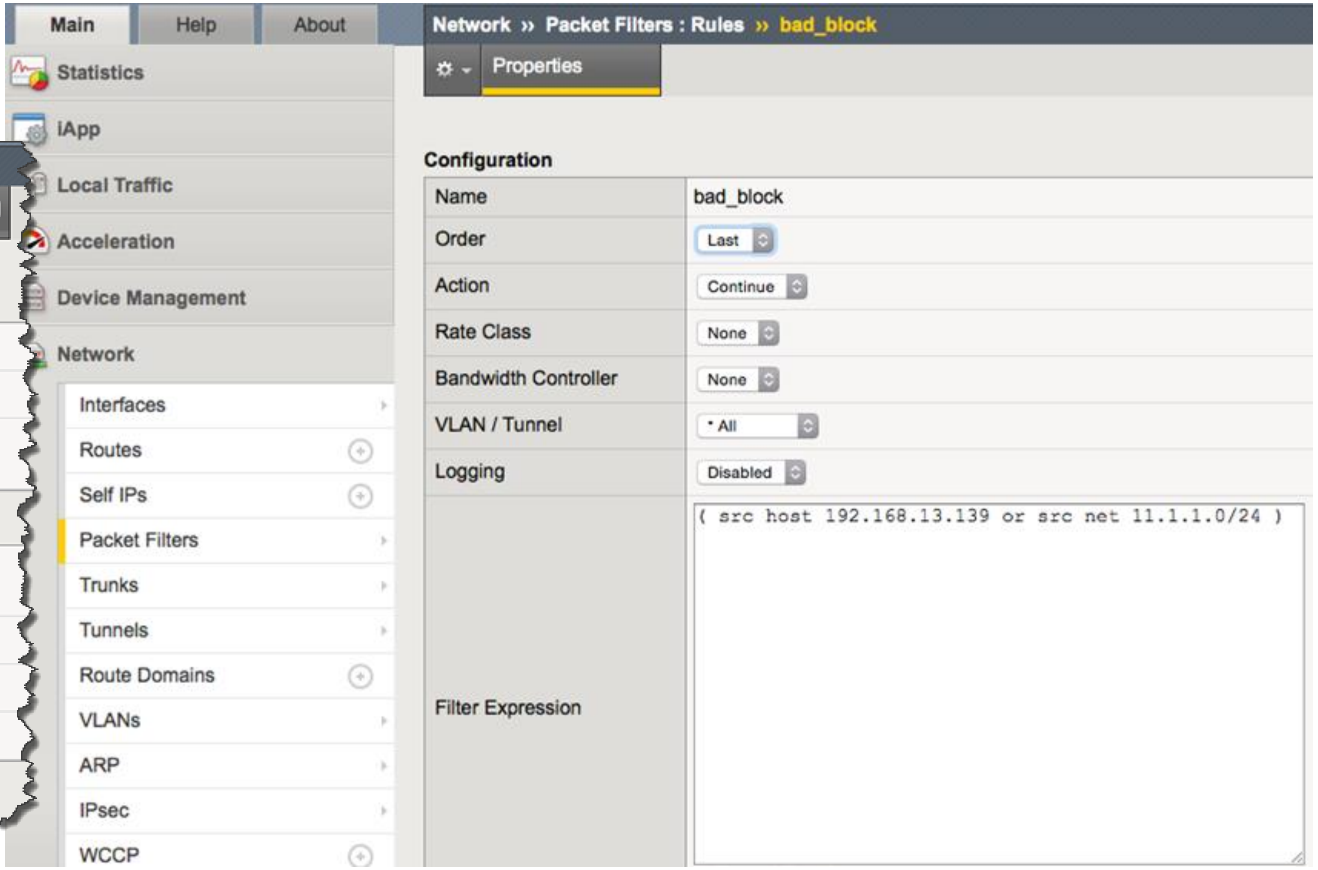
Network » Packet Filters : General

Properties

Packet Filtering	Enabled
Unhandled Packet Action	Accept
Options	□ Filter established connections □ Send ICMP error on packet reject

Exemptions

Protocols	☑ Always accept ARP ☑ Always accept important ICMP
MAC Addresses	None
IP Addresses	None
VLANs	None



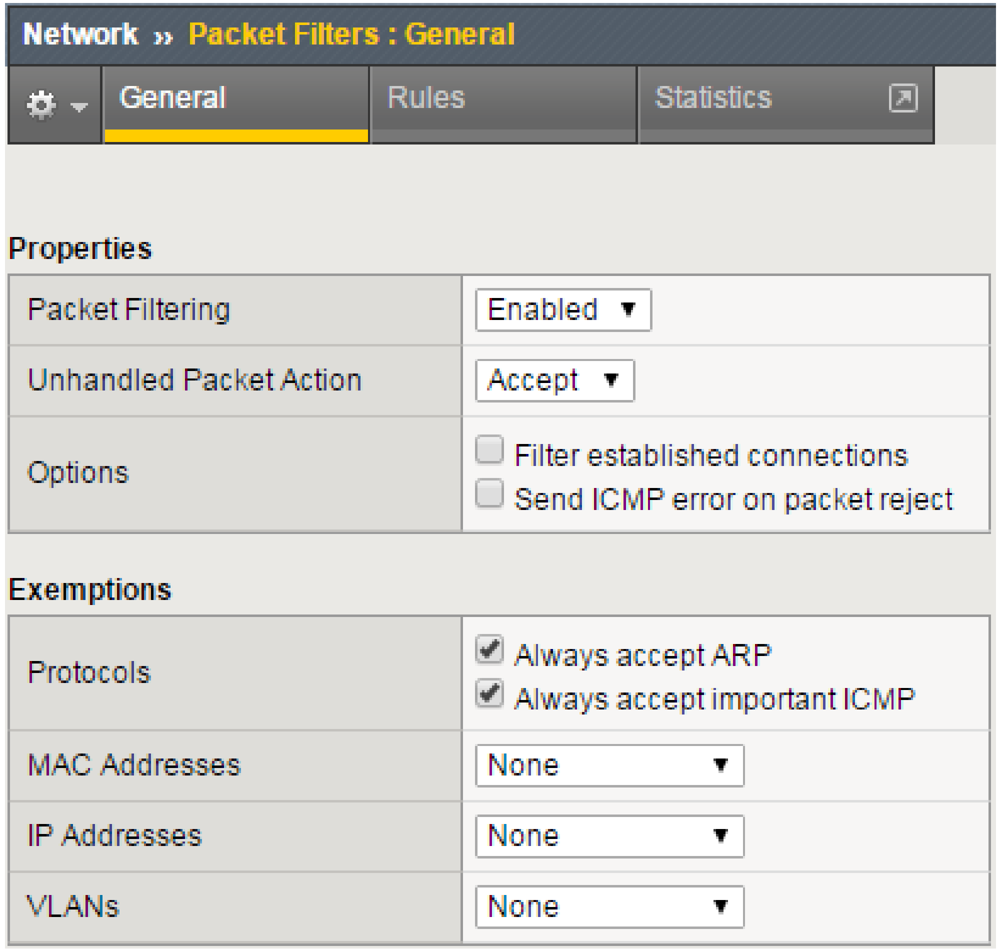
Network » Packet Filters : Rules » bad_block

Configuration

Name	bad_block
Order	Last
Action	Continue
Rate Class	None
Bandwidth Controller	None
VLAN / Tunnel	* All
Logging	Disabled
Filter Expression	(src host 192.168.13.139 or src net 11.1.1.0/24)

Packet Filtering

Disabled by default, but once you enable

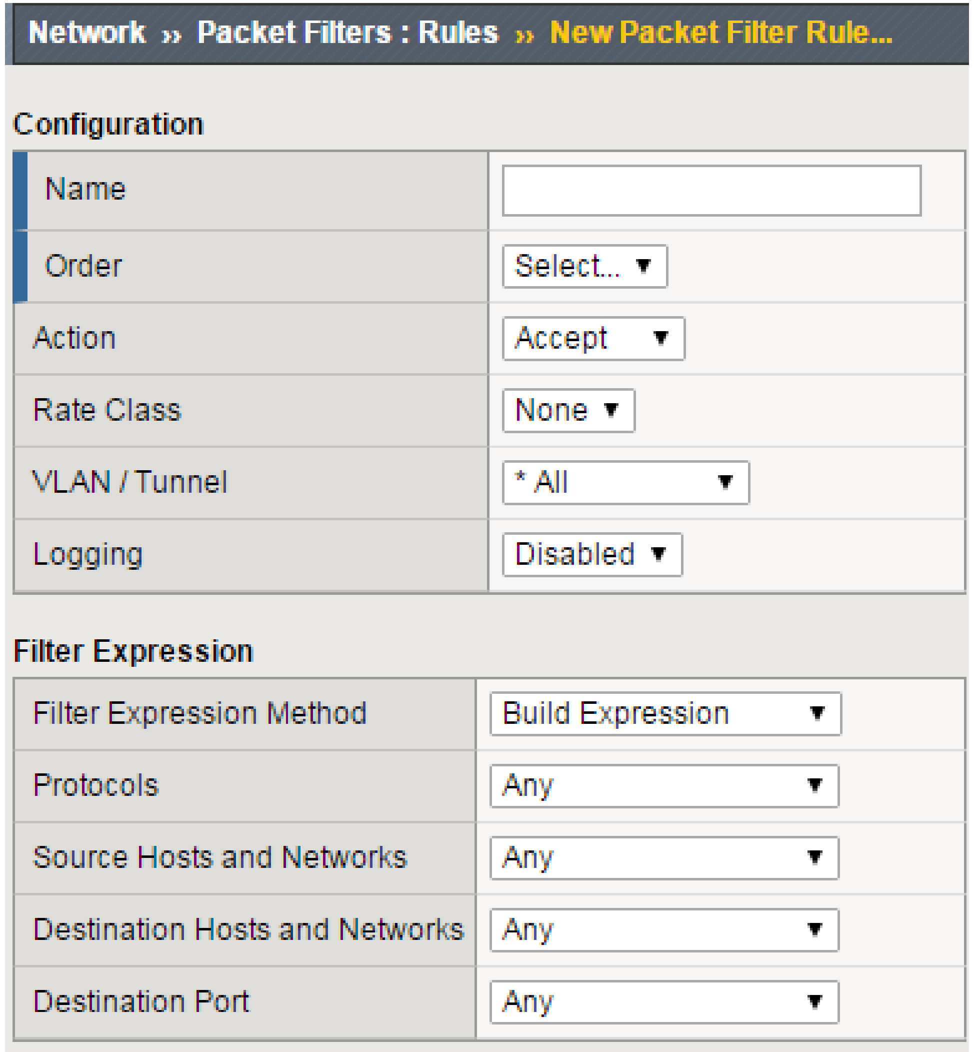


Properties

Packet Filtering	Enabled ▾
Unhandled Packet Action	Accept ▾
Options	□ Filter established connections □ Send ICMP error on packet reject

Exemptions

Protocols	☑ Always accept ARP ☑ Always accept important ICMP
MAC Addresses	None ▾
IP Addresses	None ▾
VLANs	None ▾


Network » Packet Filters : Rules » New Packet Filter Rule...

Configuration

Name	
Order	Select... ▾
Action	Accept ▾
Rate Class	None ▾
VLAN / Tunnel	* All ▾
Logging	Disabled ▾

Filter Expression

Filter Expression Method	Build Expression ▾
Protocols	Any ▾
Source Hosts and Networks	Any ▾
Destination Hosts and Networks	Any ▾
Destination Port	Any ▾

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

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

2.04

Determine how to perform a software upgrade while maintaining application availability

- Identify proper steps to avoid downtime while upgrading LTM software
- Determine necessary steps for migrating LTM configuration to new hardware
- Understand implications of stopping BIG-IP services

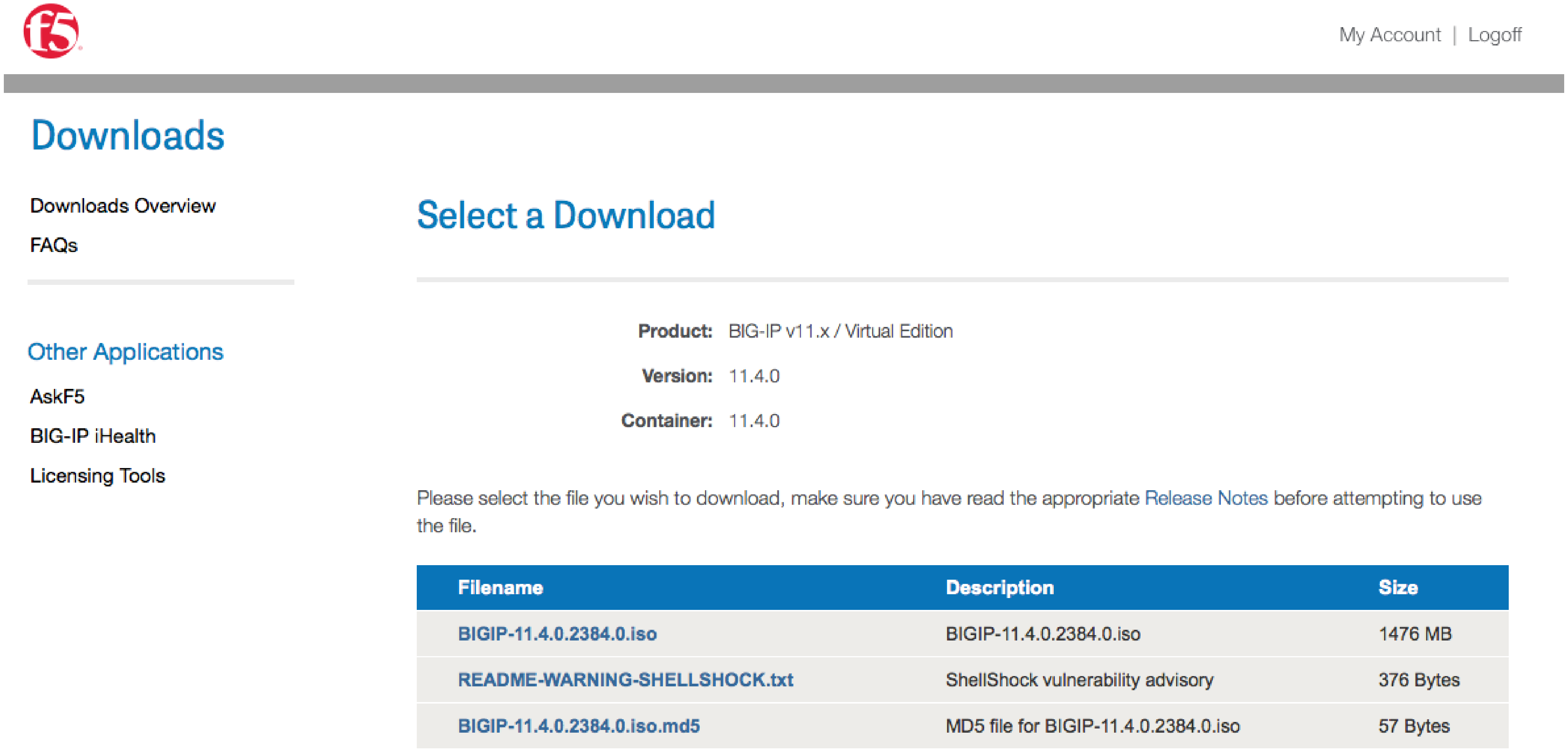
YouTube: Updating BIG-IP HA systems with a point release

This video walks you through the steps to upgrade a BIG-IP HA pair:

- 0:13 Part 1: Installing the point release on the first device
    - 0:40 Validating the configuration
    - 1:53 Verifying the service check date
    - 3:23 Synchronizing the configuration
    - 4:32 Creating and saving a UCS archive
    - 5:52 Importing the ISO file
    - 7:05 Verifying the MD5 checksum
    - 7:45 Disabling the "Automatic with Incremental Sync" option
    - 8:30 Installing and rebooting to the new version
    - 14:16 Verifying the new point release version is active on the newly patched system
    - 15:00 Forcing a failover
- 16:20 Part 2: Installing the point release on the next device
    - 16:25 Repeat these steps
    - 16:49 Verifying the new point release version is active on the newly patched system
    - 17:46 Forcing a failover
- 19:25 Part 3: Performing the final ConfigSync

https://downloads.f5.com

Requires an F5 account



My Account | Logoff

Downloads

Downloads Overview

FAQs

Other Applications

AskF5

BIG-IP iHealth

Licensing Tools

Select a Download

Product:	BIG-IP v11.x / Virtual Edition
Version:	11.4.0
Container:	11.4.0

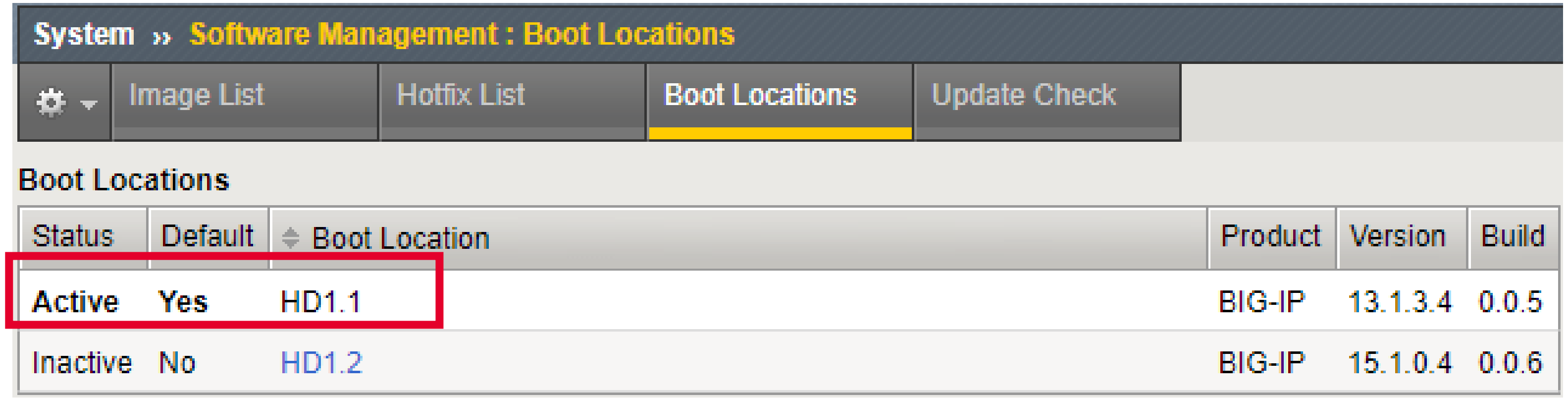
Please select the file you wish to download, make sure you have read the appropriate Release Notes before attempting to use the file.

Filename	Description	Size
BIGIP-11.4.0.2384.0.iso	BIGIP-11.4.0.2384.0.iso	1476 MB
README-WARNING-SHELLSHOCK.txt	ShellShock vulnerability advisory	376 Bytes
BIGIP-11.4.0.2384.0.iso.md5	MD5 file for BIGIP-11.4.0.2384.0.iso	57 Bytes

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
```

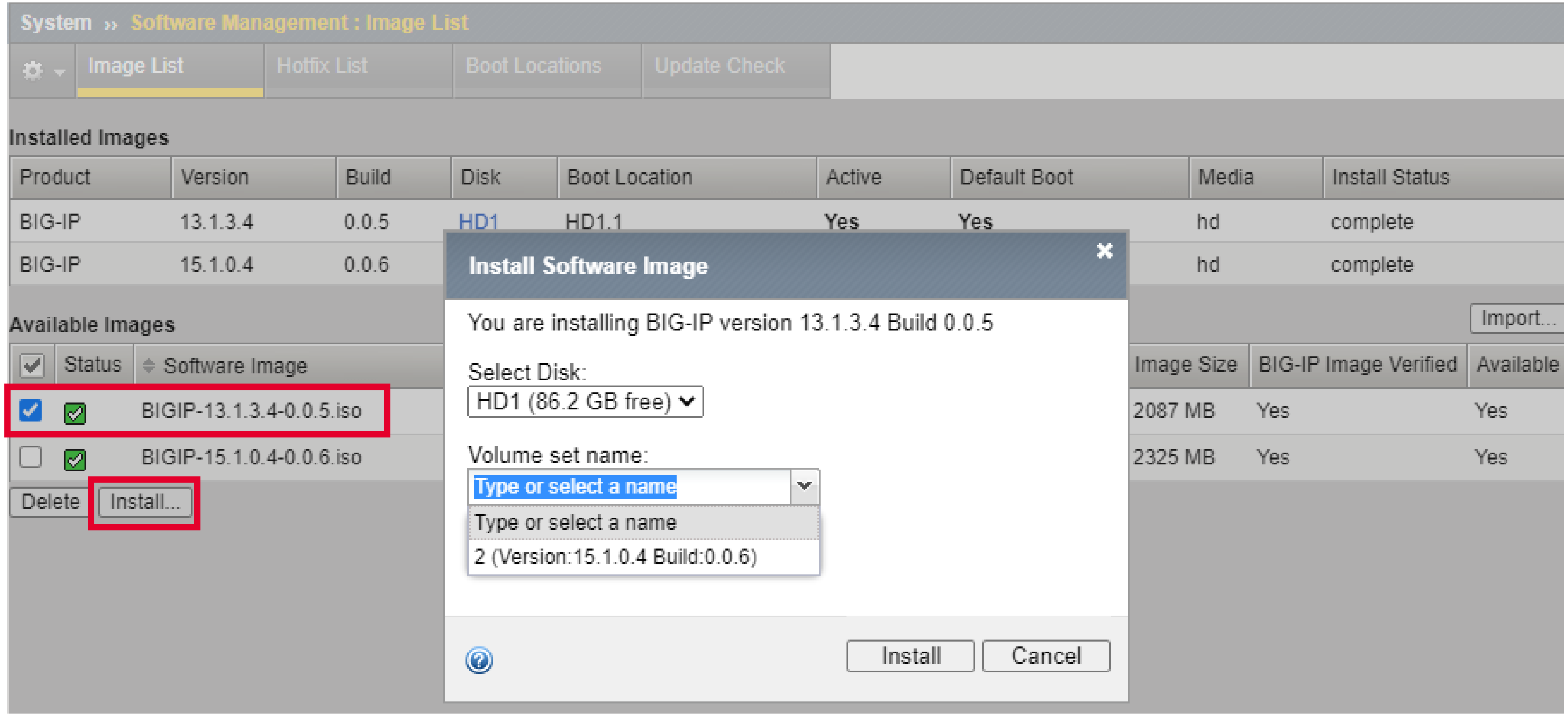


Boot Locations

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)

3.05 Summarize the use case of a UCS backup

K4423: Overview of UCS archives

- A User Configuration Set (UCS) is a backup file that contains BIG-IP configuration data that can be used to fully restore a BIG-IP system in the event of a failure or Return Materials Authorization (RMA) replacement.
- A UCS archive is a compressed file that contains all of the configuration files that are typically required to restore your current configuration to a new system.
- Contents of the UCS archive file:
  - All BIG-IP-specific configuration files
  - BIG-IP product licenses
  - User accounts and password information
  - Domain Name System (DNS) zone files and the ZoneRunner configuration
  - Secure Socket Layer (SSL) certificates and keys
  - Startup ZebOS configuration

3.05 Summarize the use case of a UCS backup

You should create a UCS archive before operations that modify the configuration.

- You can keep archives locally and/or download/upload archives to/from external sources
- By default, UCS archives are stored in /var/local/ucs

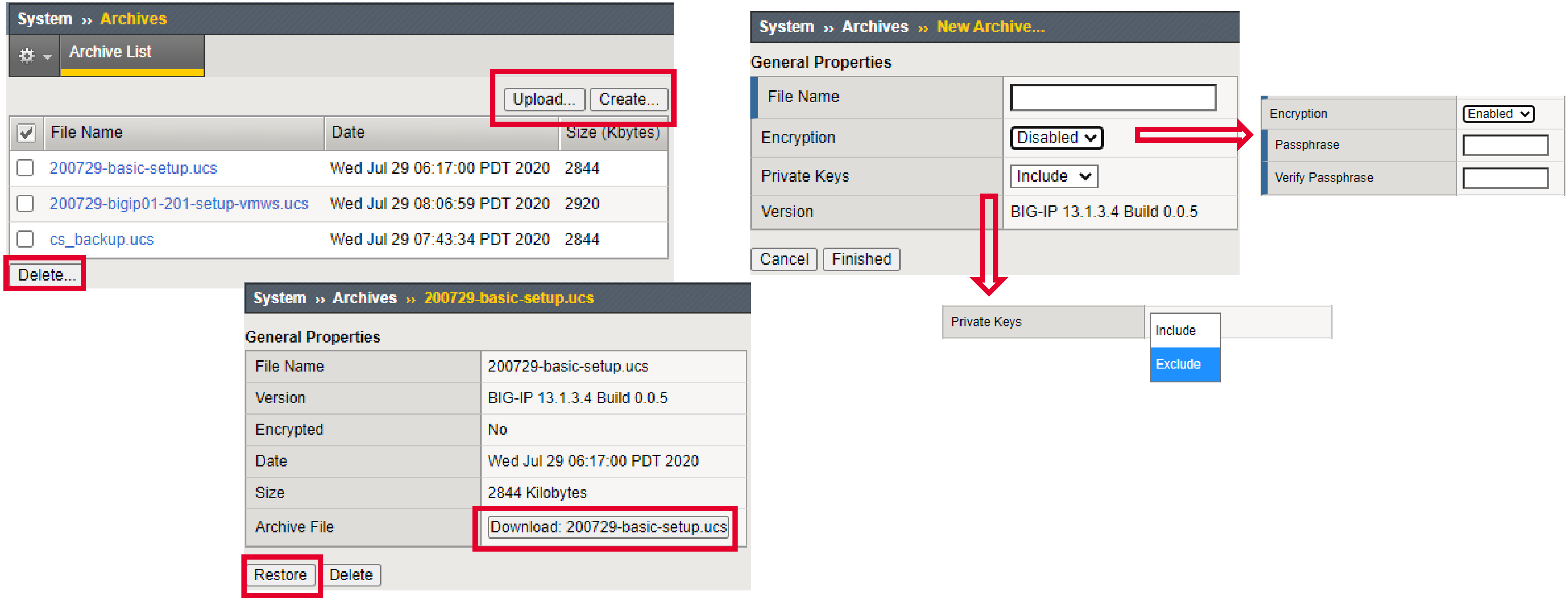
Aside from the obvious, restoring your BIG-IP due to a corrupted/misconfigured configuration, a UCS is used to:

- Restore an RMA
- Manual Chapter: Migration of Configurations Between Different Platforms
- Manual Chapter: Migration of Devices Running the Same Software Version
- Manual Chapter: Migration of Devices Running Different Version Software

3.05 Execute UCS backup and restore procedure

[Manual Chapter: Archives](#)

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



System » Archives

Archive List

☑	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

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

System » Archives » New Archive...

General Properties

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

Encryption	Enabled
Passphrase	
Verify Passphrase	

Private Keys	Include Exclude

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.

3.05 Explain proper long-term storage of UCS backup file

Store passwords and passphrases securely

- After you encrypt configuration object passwords or passphrases on any BIG-IP system, another system can only decrypt them (during a tmsh load config operation) by using the same master key.
- F5 recommends that you retain a record of each configuration object password or passphrase in a secure location on a system other than the BIG-IP system that uses the password or passphrase.
  - Doing so makes it possible for you to restore a UCS configuration archive when the original master key is not available.

Store UCS archives securely

- Make sure that you regularly back up the BIG-IP system configuration and maintain the backup UCS archives in a secure manner.
- The preferred way to store UCS archives securely (encrypts the entire UCS file):
- (tmos) # save sys ucs <ucs name> passphrase <passphrase>

These recommendations can be accomplished via the GUI or TMSH interfaces.

3.05 Explain the contents of the UCS file (private keys)

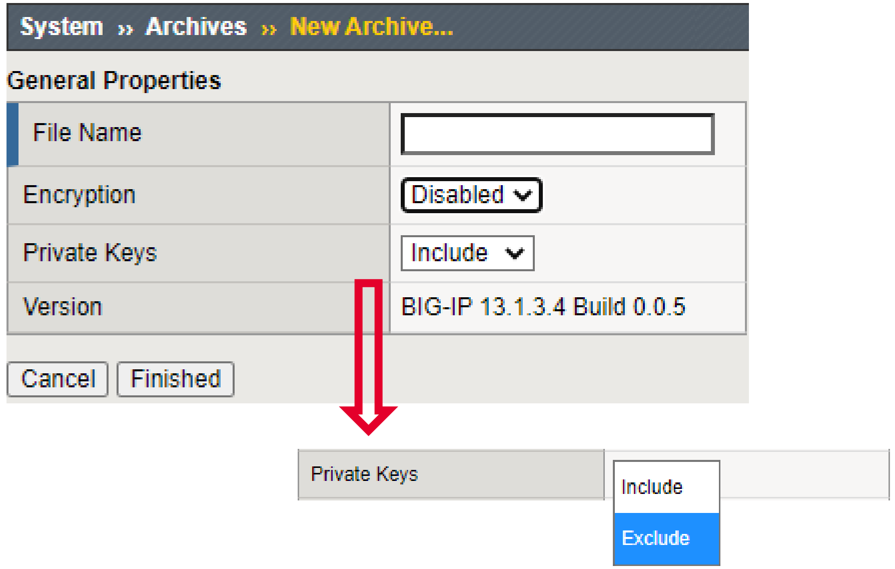
A typical UCS archive contains user accounts, passwords, critical system files, and **SSL private keys**.

- You can explicitly exclude SSL private keys from a UCS archive during the backup process.

From TMSH:

- save sys ucs test-backup no-private-key

From the GUI:



System » Archives » New Archive...

General Properties

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

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

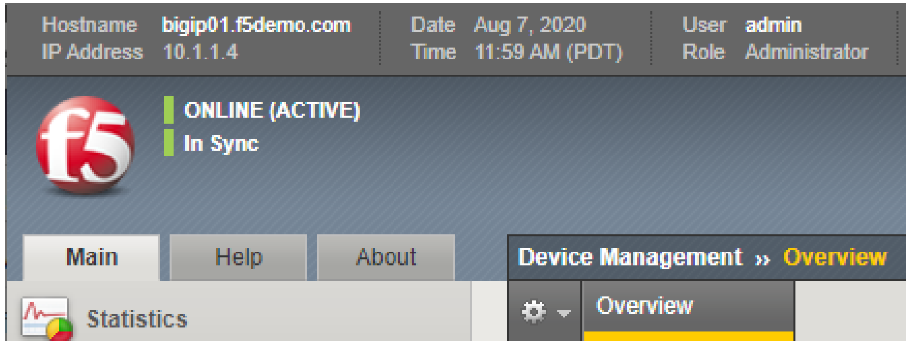
2.05

Determine how to secure Self IPs

- Compare and contrast traffic groups vs. HA groups
- Determine what prevented an expected failover
- Describe the differences between network failover and hardware failover

3.10 Show config sync status

Manual Chapter: Managing Configuration Synchronization



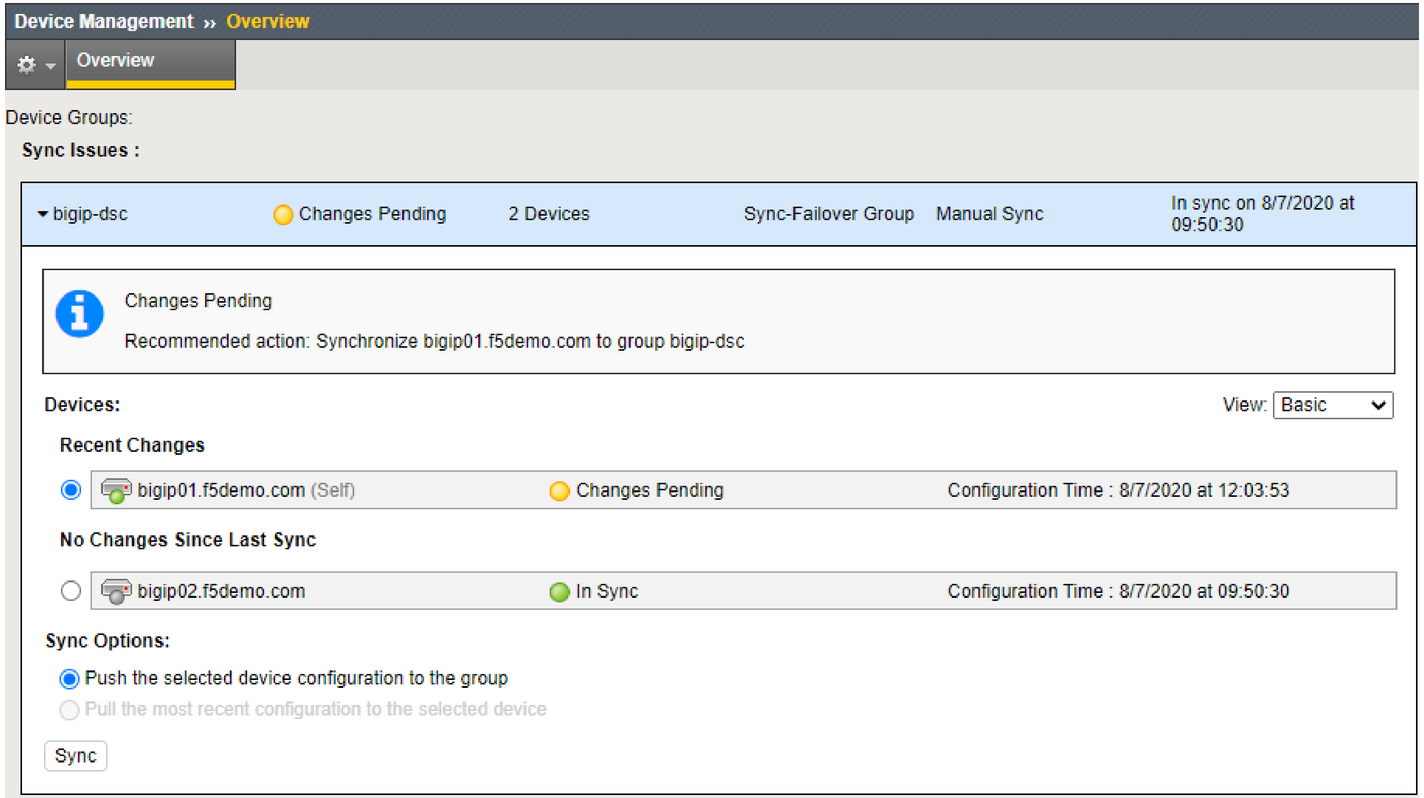
Hostname bigip01.f5demo.com
IP Address 10.1.1.4

Date Aug 7, 2020
Time 11:59 AM (PDT)

User admin
Role Administrator

ONLINE (ACTIVE)
In Sync

By default, synching 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

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

3.10 Explain when a config sync is necessary

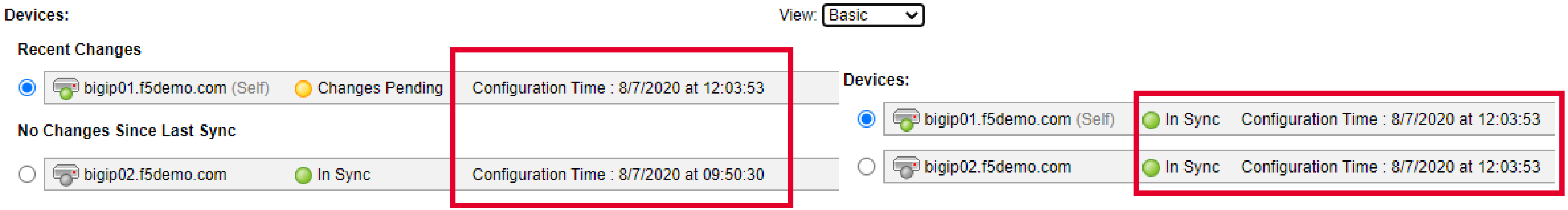
K39735803: When to perform a manual ConfigSync

- When you make a change to a device in the Device Service Cluster (DSC) and automatic sync is not enabled
- Before you begin a software upgrade of a DSC to ensure all configurations are correctly synchronized
- After you complete a software upgrade for a BIG-IP device group. After all of the BIG-IP devices in the device group are upgraded to the new BIG-IP software version.
    - This recommendation applies to device groups configured to use any ConfigSync option, including the Automatic Sync option.
- You want to migrate a device group member to a new BIG-IP hardware platform.
    - Note: For more information, refer to K15496: Migrating a device group member to a new BIG-IP hardware platform..
- You want to migrate a BIG-IP configuration to new VIPRION blades.
    - Note: For more information, refer to K63705154: Migrating a BIG-IP configuration to new VIPRION blades using ConfigSync.
- You are using Automatic Sync, and you want to synchronize changes to device group members and immediately save the running configuration to the configuration files on the peer devices.

3.10 Compare configuration timestamp

K81160517: Modifying the ConfigSync time threshold

Timestamps can be checks on the status page, switching to Advance will give you more information



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

Devices:

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

○ bigip02.f5demo.com In Sync Configuration Time : 8/7/2020 at 12:03:53

Each device checks the remote device's time against its own system time.

- If the time is not within the ConfigSync time threshold default value of three seconds, the command prompt changes to indicate that the time is out of sync (**Peer Time Out of Sync**), and ConfigSync operations may fail.
- You may have to increase the threshold to rectify the issue.
- This a reason configuring NTP on BIG-IP is so important.
- K81160517: Modifying the ConfigSync time threshold shows you how to check and rectify the issue.

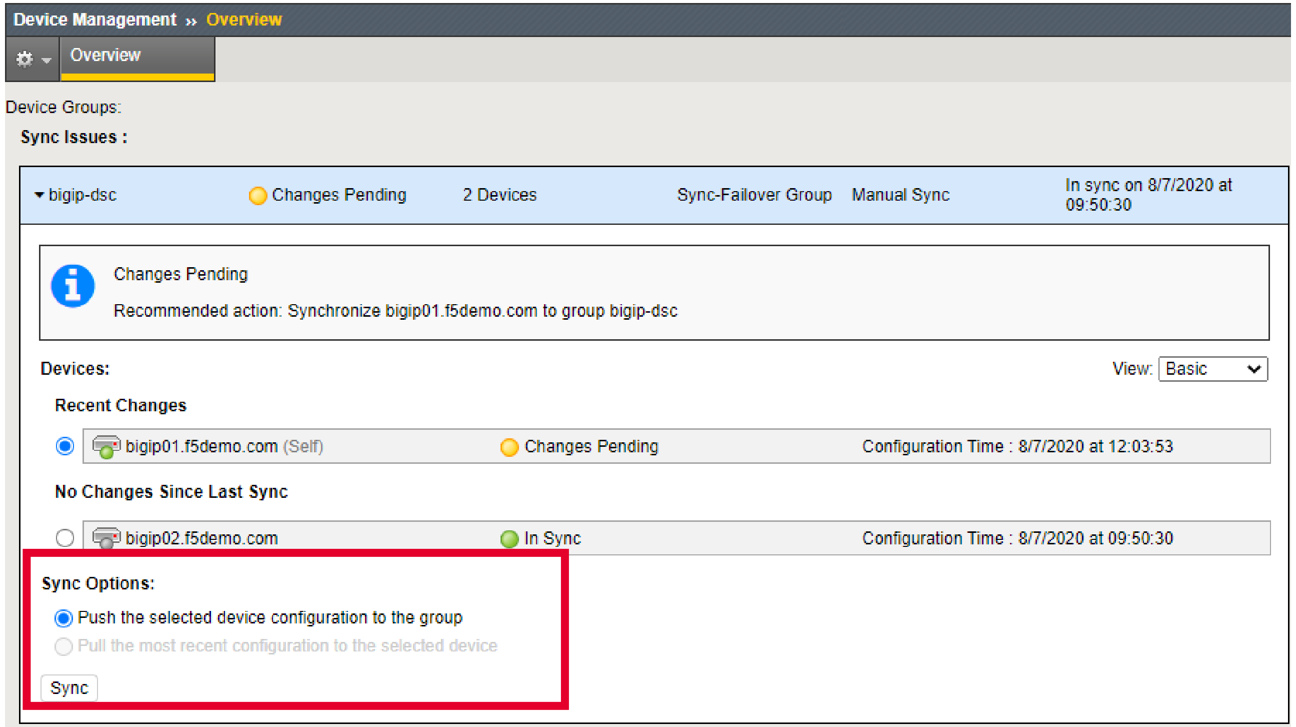
3.10 Demonstrate config sync procedure (GUI)

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 Management » Overview

Overview

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

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.
```

3.10 Report errors which occur during config sync

K13946: Troubleshooting ConfigSync and device service clustering issues

To troubleshoot the ConfigSync operation, perform the following procedures:

- Verifying the required elements for ConfigSync/DSC
- Reviewing common reasons for ConfigSync failures (recommended viewing)
- Viewing the commit ID updates
- Verifying a ConfigSync operation
- Verifying the Sync status
- Understanding Sync status messages (recommended viewing)
- Reviewing the log files for ConfigSync error messages (recommended viewing)

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

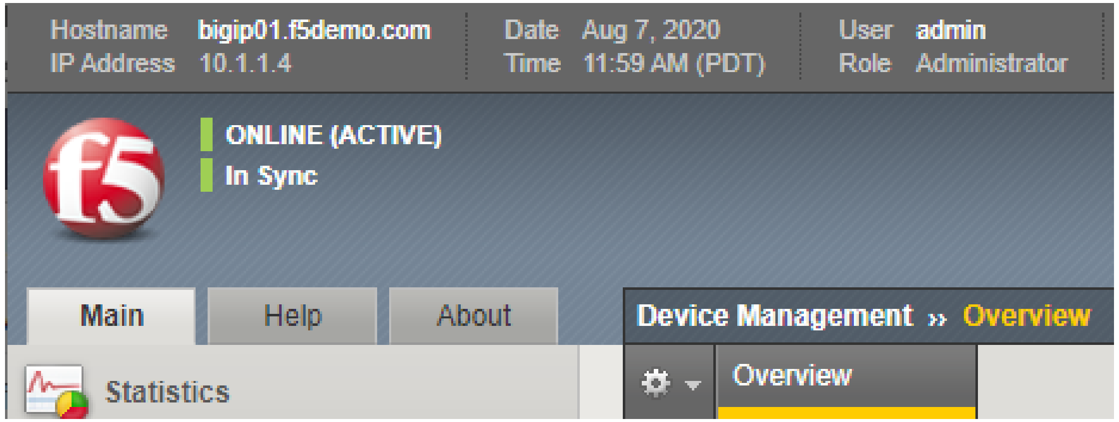
Manual: BIG-IP Device Service Clustering: Administration

For BIG-IPs to be combined into clusters for high availability, certain things must be configured:

- BIG-IPs must have a valid device certificate
- On the device, IP addressing must be defined for failover
- Devices must be placed into a trust group
- Devices in a trust group and then be placed into a failover group

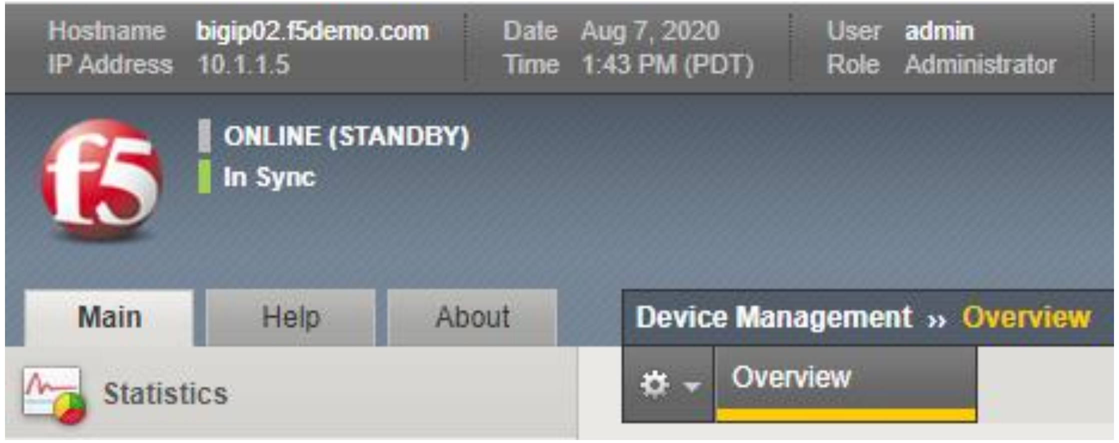
3.02 Report current active/standby failover state

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 #

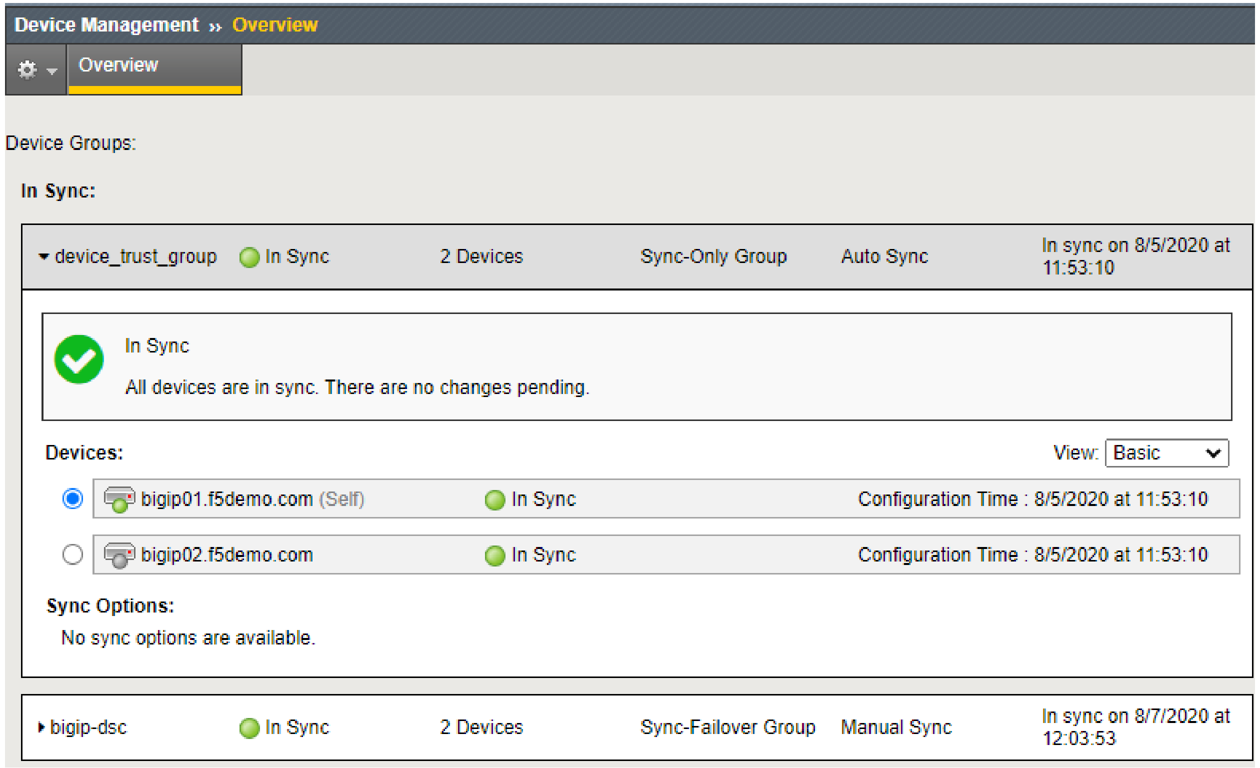
[root@bigip02:**Standby:**In Sync] config #

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

Standby – there are no active traffic groups that can failover

3.02 Show device trust status

Manual Chapter: Managing Device Trust



Device Management » Overview

Overview

Device Groups:

In Sync:

device_trust_group	● In Sync	2 Devices	Sync-Only Group	Auto Sync	In sync on 8/5/2020 at 11:53:10

✓ In Sync

All devices are in sync. There are no changes pending.

Devices: View: Basic

●	bigip01.f5demo.com (Self)	● In Sync	Configuration Time : 8/5/2020 at 11:53:10
○	bigip02.f5demo.com	● In Sync	Configuration Time : 8/5/2020 at 11:53:10

Sync Options:

No sync options are available.

bigip-dsc	● In Sync	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/7/2020 at 12:03:53

```
(tmos)# show cm device-group device_trust_group

-----------------------------------------------------------
CM::Device-Group
-----------------------------------------------------------
Group Name                          device_trust_group
Member Name                         bigip01.f5demo.com
Time Since Last Sync (HH:MM:SS)     50:27:21
Last Sync Type                      full-load-auto-sync
CID Originator                      /Common/bigip02.f5demo.com
CID Time (UTC)                      2020-Aug-05 18:53:10
LSS Originator                      /Common/bigip02.f5demo.com
LSS Time (UTC)                      2020-Aug-05 18:53:10

-----------------------------------------------------------
CM::Device-Group
-----------------------------------------------------------
Group Name                          device_trust_group
Member Name                         bigip02.f5demo.com
Time Since Last Sync (HH:MM:SS)     -
Last Sync Type                      none
CID Originator                      /Common/bigip02.f5demo.com
CID Time (UTC)                      2020-Aug-05 18:53:10
LSS Originator                      /Common/bigip02.f5demo.com
LSS Time (UTC)                      2020-Aug-05 18:53:10
```

3.02 Execute force to standby or offline procedure

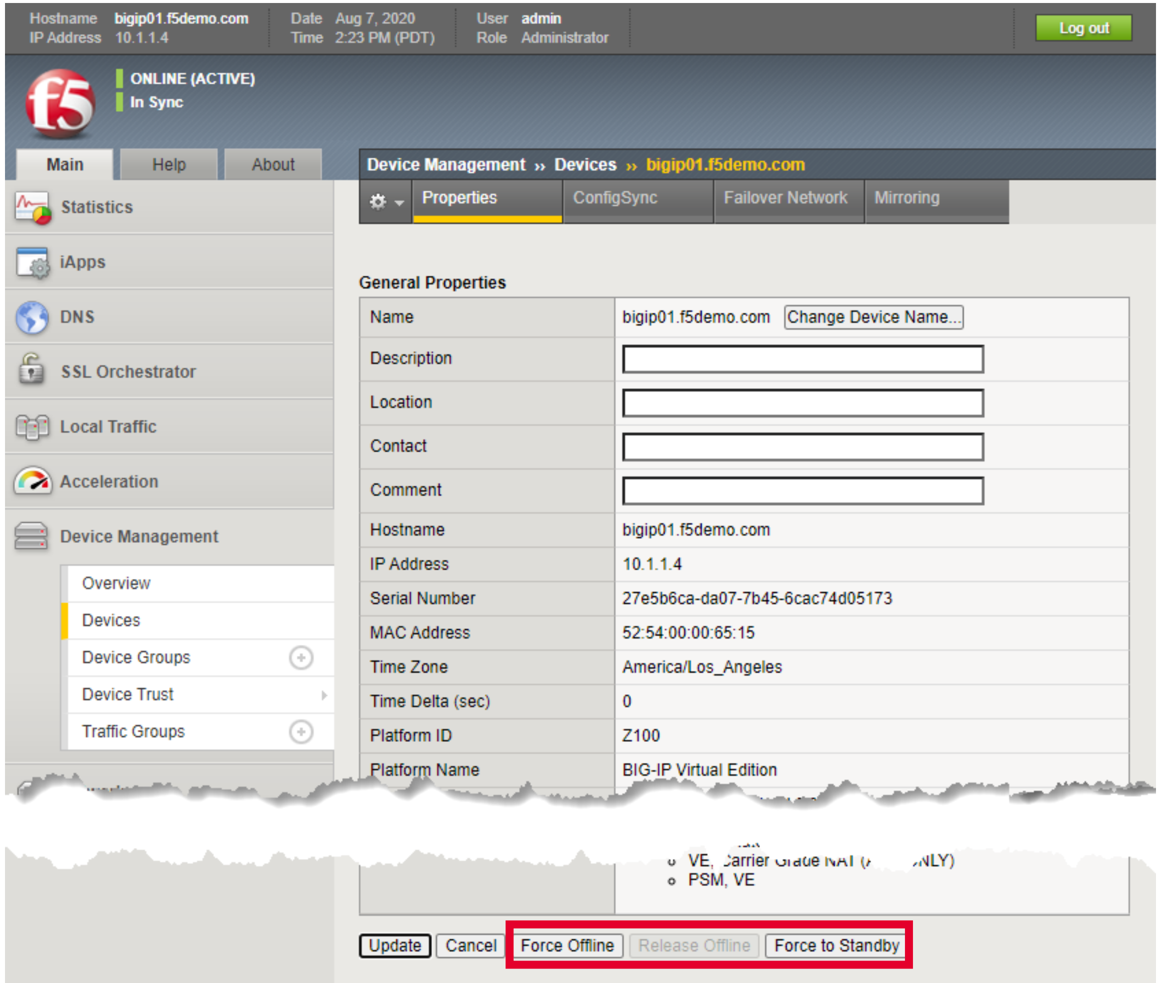
Manual: BIG-IP Device Service Clustering: Administration

(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 Change Device Name...
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 (NLY) ○ PSM, VE

Other HA concepts not explicitly called out in the blueprint

Manual: BIG-IP Device Service Clustering: Administration

Device Service Clusters (DSCs) can consist of more than two BIG-IPs supporting each other:

- Know where to find where failover objects on BIG-IP in the DSC will fail to.
- Understand the difference between Active-Standby and Active-Active.

You probably should have a working knowledge of Device Trust and the Device Trust Group.

Have a working knowledge of mirroring:

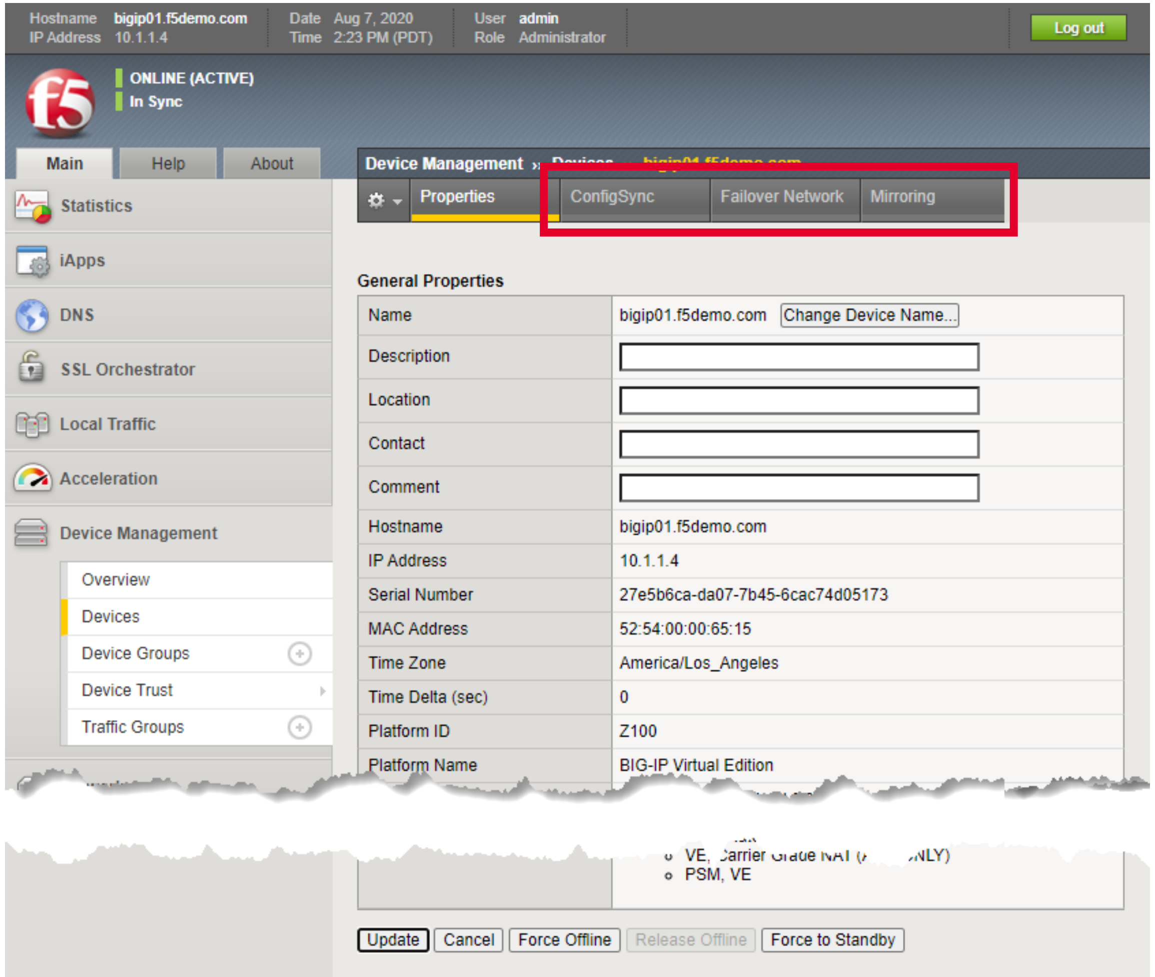
- SNAT
- Persistence
  - Only if persistence records are kept locally on the BIG-IP, not necessary for cookie persistence.
- Connection Table
  - Only for long-term connections, ie. FTP, resource intensive.

Other HA concepts not explicitly called out in the blueprint

Manual: BIG-IP Device Service Clustering: Administration

Devices (Self)

- On the (Self) Device, which is the device you are on, there are several configuration items you show know
  - These must be configured prior to building the device trust group
- ConfigSync - IP address the BIG-IP listens for synchronizing configuration changes (TCP port 4353)
- Failover Network - IP address the BIG-IP uses to send and receive polls to determine the state of other BIG-IPs in the cluster (TCP port 1026)
- Mirroring - IP address where mirrored information is sent and received



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 Change Device Name...
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

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

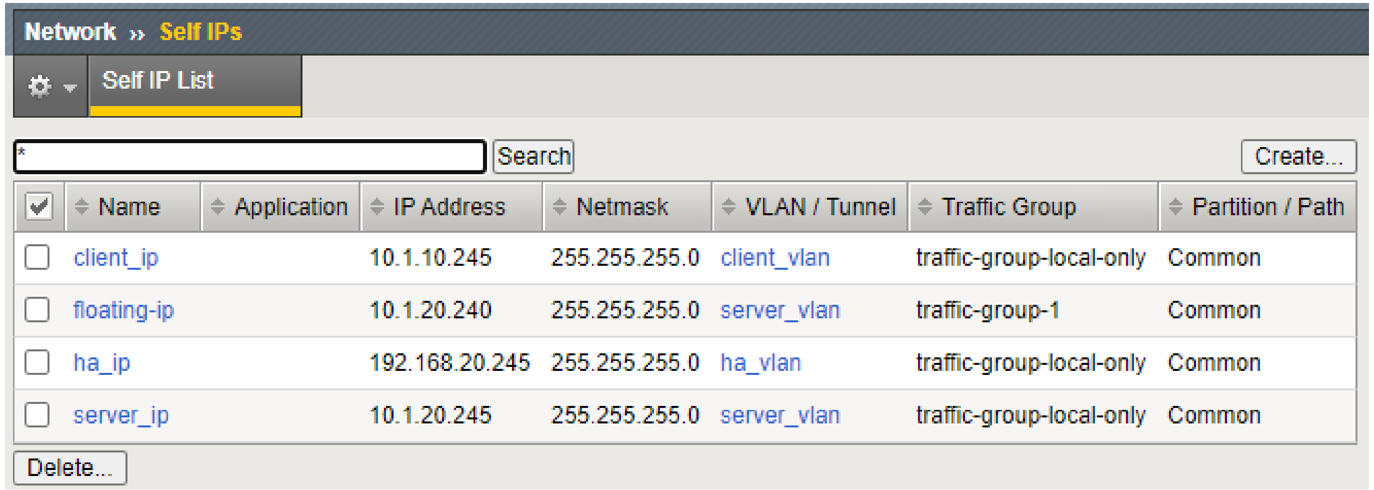
2.06

Apply concepts required to use BIG-IP functionality to fulfill security requirements

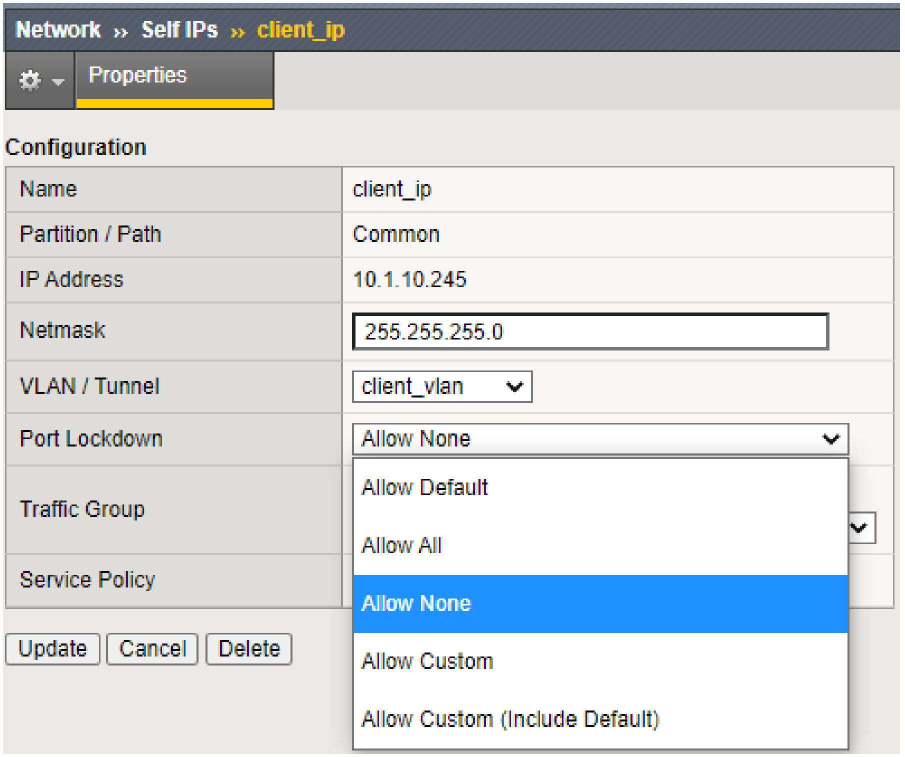
- Make use of port lockdown
- Demonstrate how to restrict access to management interface
- Demonstrate how to restrict access to virtual servers

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, 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

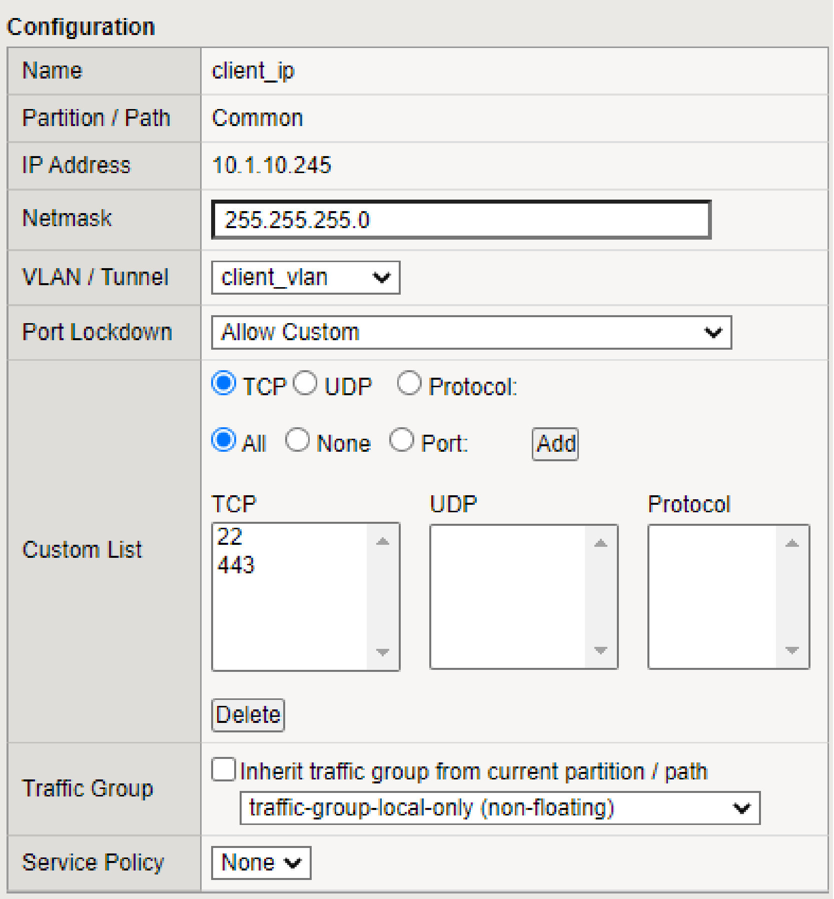
Name	client_ip
Partition / Path	Common
IP Address	10.1.10.245
Netmask	255.255.255.0
VLAN / Tunnel	client_vlan
Port Lockdown	Allow None
Traffic Group	
Service Policy	

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



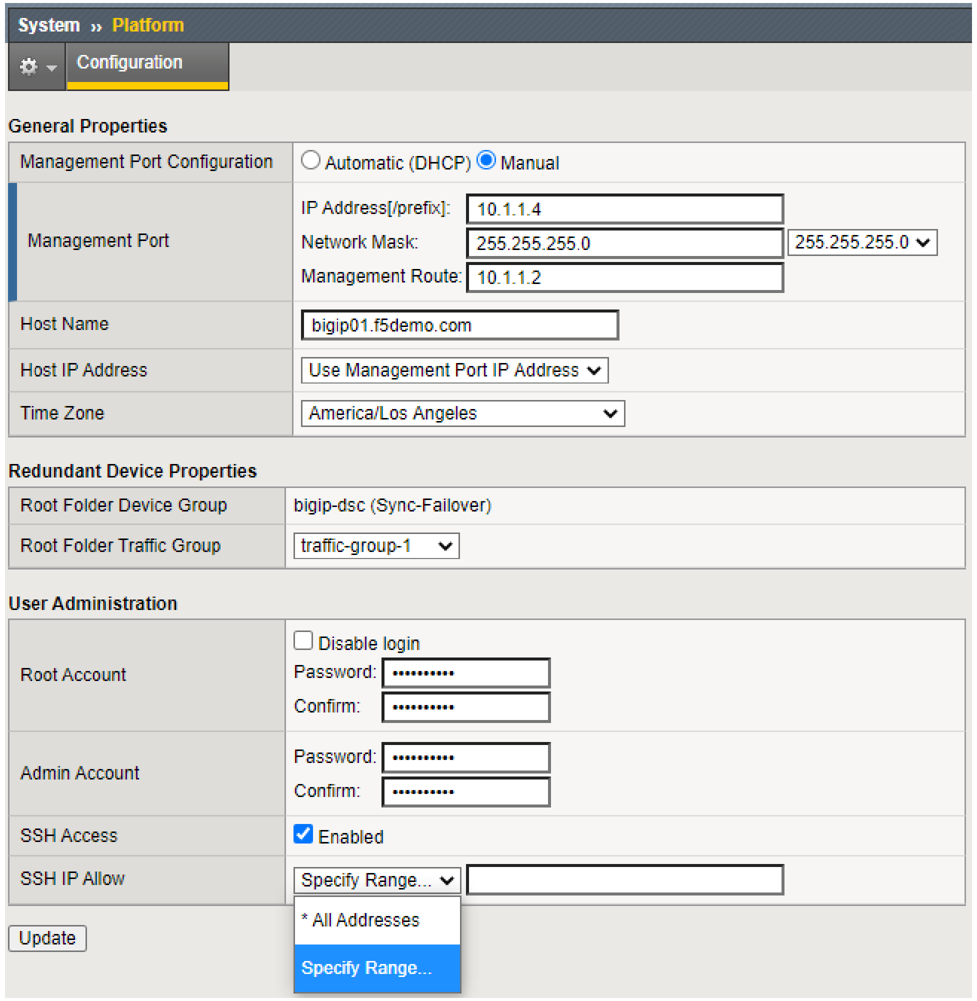
Configuration

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 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> }
  - Range uses space ie. {10.1.1.1 10.1.1.10}

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:

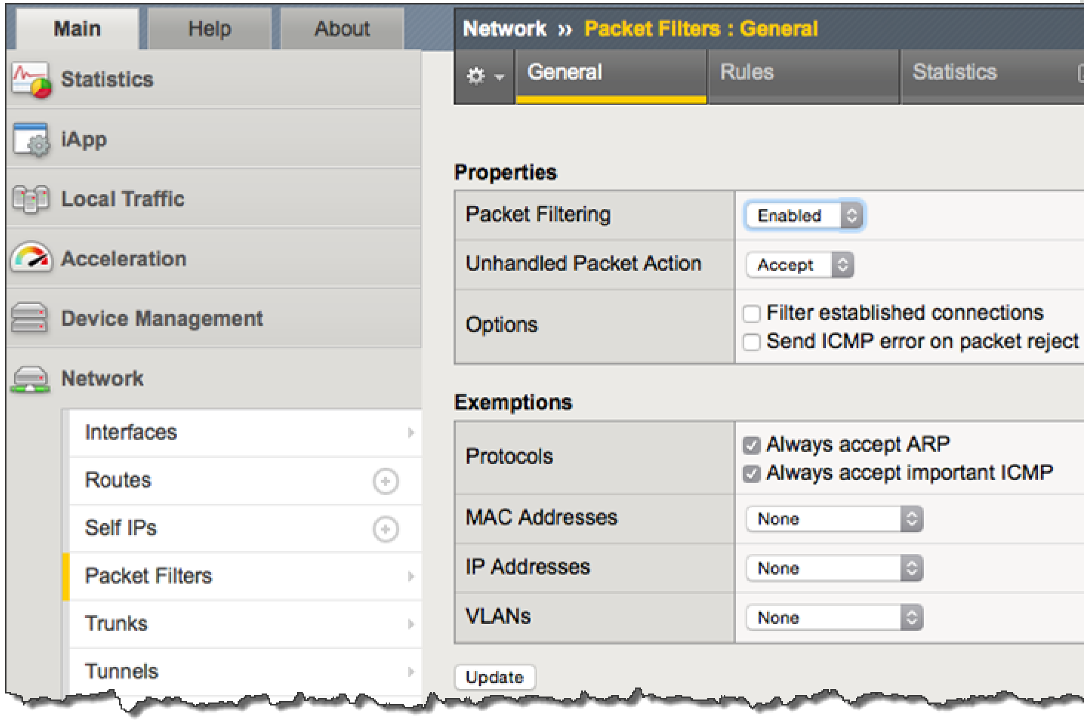
```
(tmos)# list sys httpd
allow
sys httpd {
    allow { All }
}
```

Save the change by entering the following command:

- save /sys config

Restricting access to management ports on Self IPs

(src host 192.168.13.139 or src net 11.1.1.0/24)

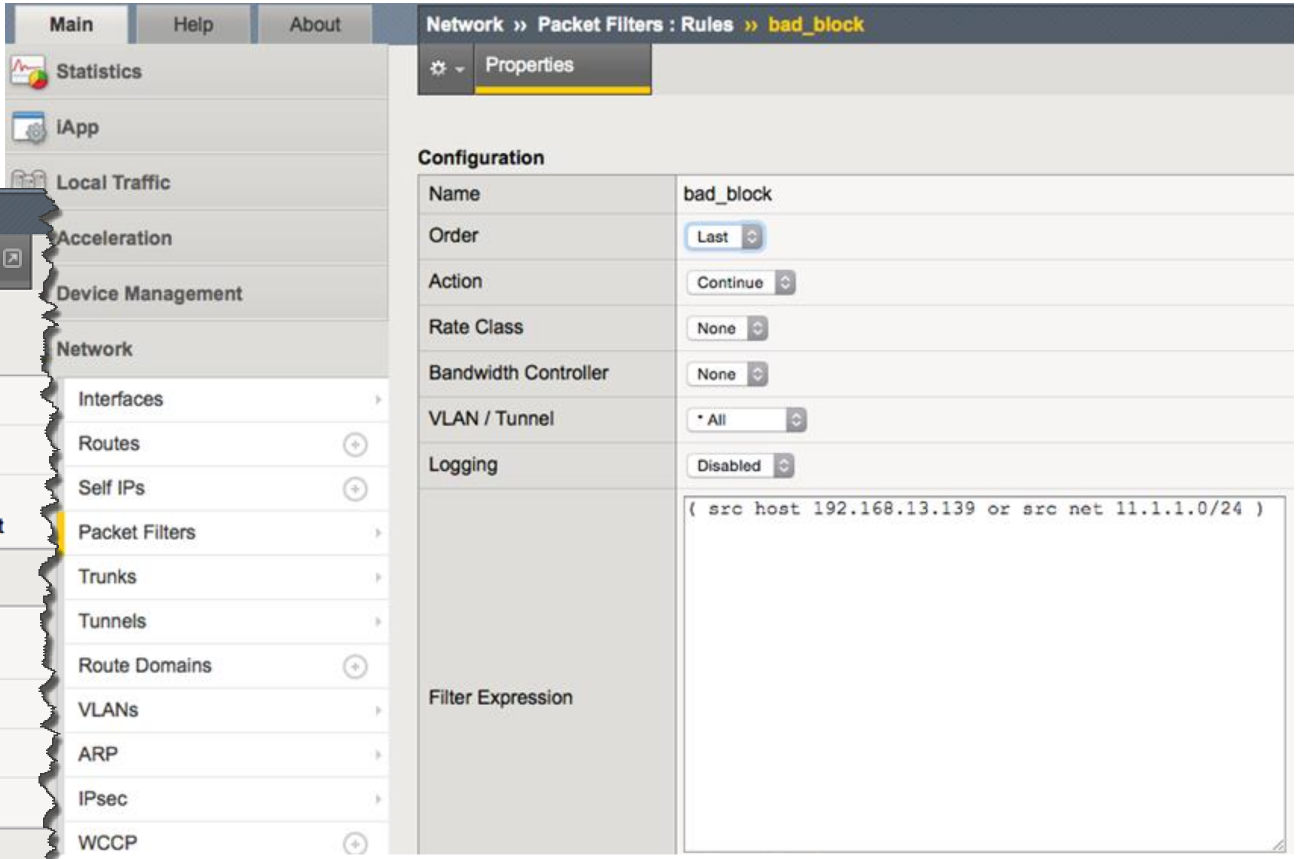


Properties

Packet Filtering	Enabled
Unhandled Packet Action	Accept
Options	□ Filter established connections □ Send ICMP error on packet reject

Exemptions

Protocols	☑ Always accept ARP ☑ Always accept important ICMP
MAC Addresses	None
IP Addresses	None
VLANs	None

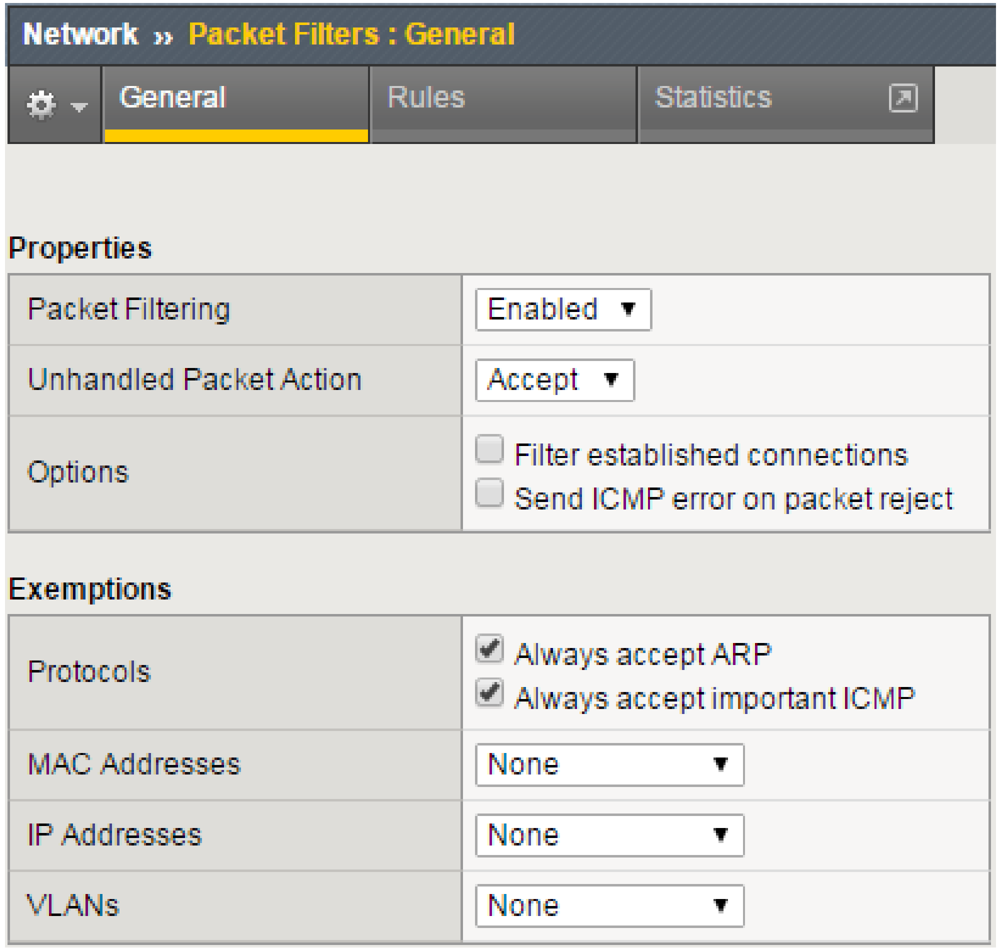


Configuration

Name	bad_block
Order	Last
Action	Continue
Rate Class	None
Bandwidth Controller	None
VLAN / Tunnel	* All
Logging	Disabled
Filter Expression	(src host 192.168.13.139 or src net 11.1.1.0/24)

Packet Filtering

Disabled by default, but once you enable



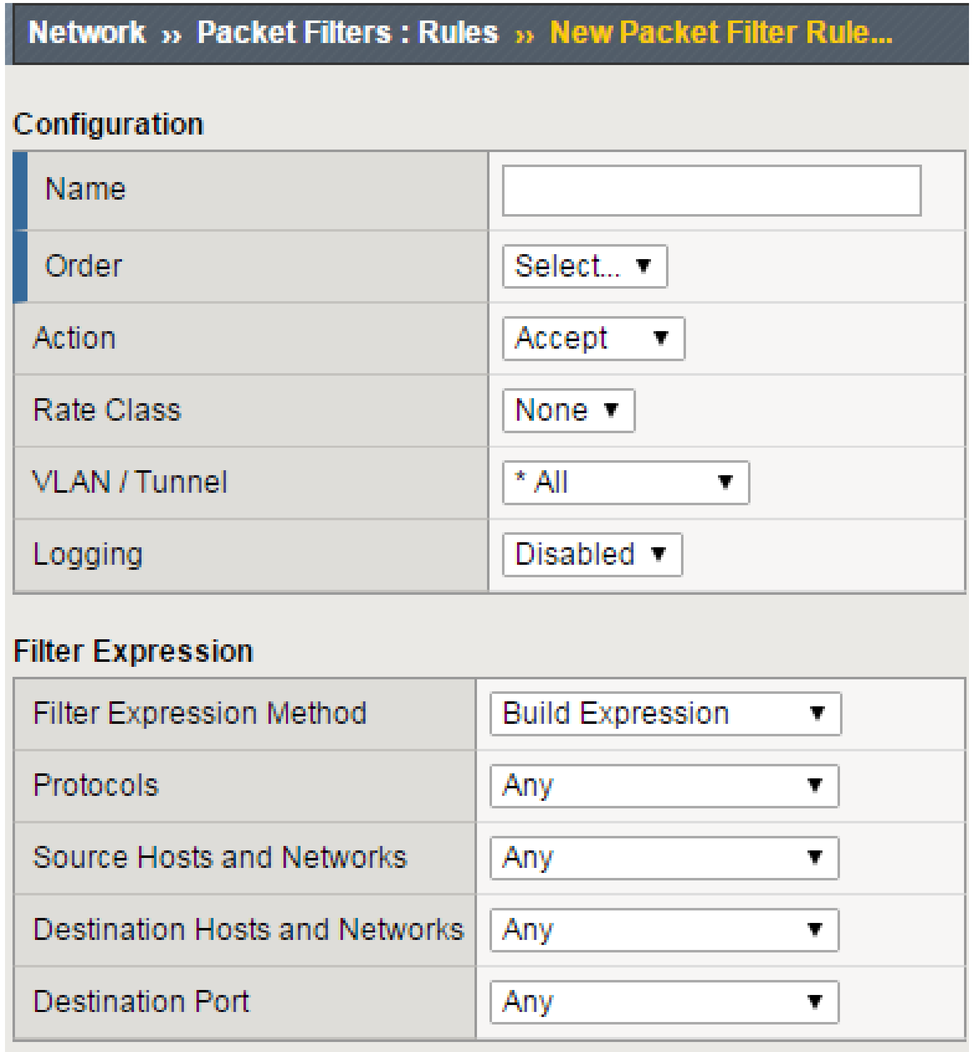
Network » Packet Filters : General

Properties

Packet Filtering	Enabled ▾
Unhandled Packet Action	Accept ▾
Options	☐ Filter established connections ☐ Send ICMP error on packet reject

Exemptions

Protocols	☑ Always accept ARP ☑ Always accept important ICMP
MAC Addresses	None ▾
IP Addresses	None ▾
VLANs	None ▾



Network » Packet Filters : Rules » New Packet Filter Rule...

Configuration

Name	
Order	Select... ▾
Action	Accept ▾
Rate Class	None ▾
VLAN / Tunnel	* All ▾
Logging	Disabled ▾

Filter Expression

Filter Expression Method	Build Expression ▾
Protocols	Any ▾
Source Hosts and Networks	Any ▾
Destination Hosts and Networks	Any ▾
Destination Port	Any ▾

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

2.07

Determine how configuration changes affect existing and new connections

- Predict persistence for existing connections
- Calculate when changes will affect the connections
- Predict load balancing and persistence for new connections
- Determine the impact of virtual server configuration change on traffic

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

2.08

Explain the uses of user roles, administrative partitions, and route domains

- Explain how to restrict access to LTM using user roles
- Discuss the benefits of administrative partitions
- Apply user roles to administrative partitions
- Explain the functionality of route domains
- Summarize how the three technologies can be used together

3.08 Explain how to create a user

Manual: BIG-IP Systems: User Account Administration

User and Password are required

Assign a role

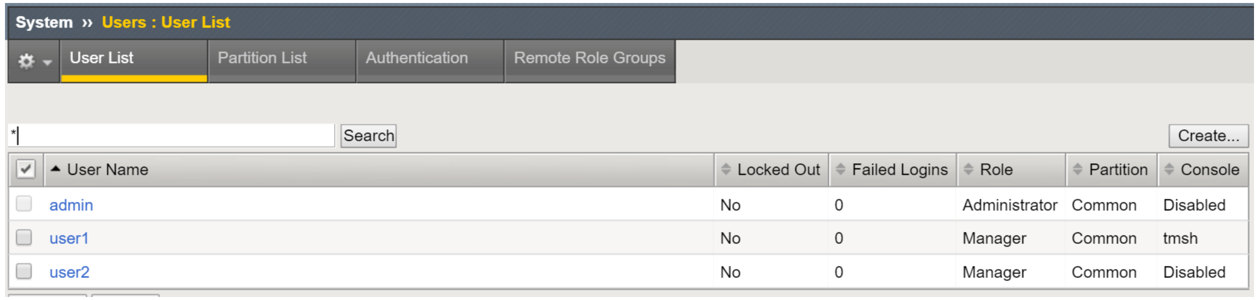
Assign partition access

- A user may be assigned to one partition or All partitions

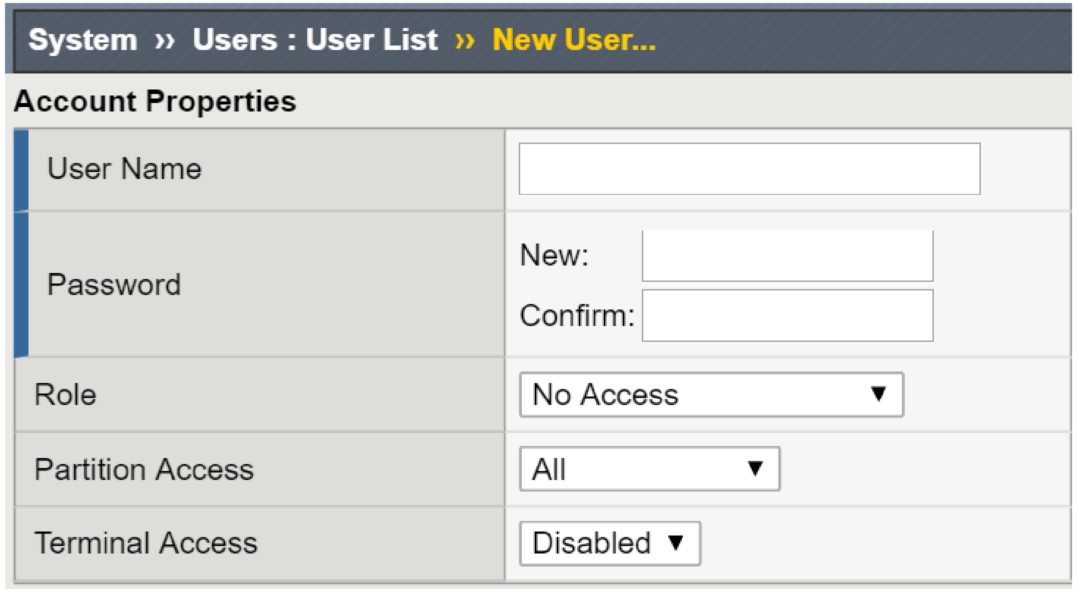
Assign the type of terminal access (Specify the type of CLI access)

- 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



☑	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

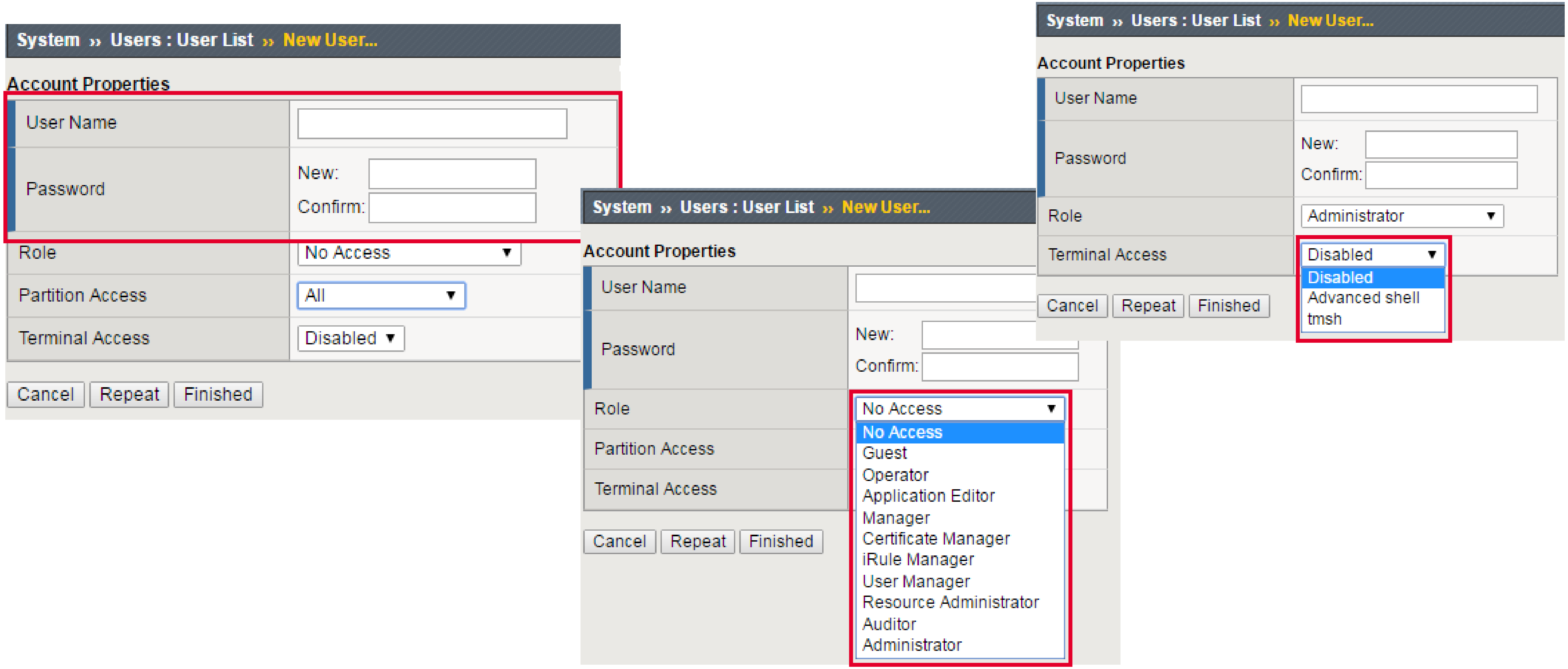


Account Properties

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

3.08 Explain how to create a user

Manual: BIG-IP Systems: User Account Administration



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

Account Properties

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

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

Account Properties

User Name	
Password	New: Confirm:
Role	No Access
Partition Access	
Terminal Access	

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

Account Properties

User Name	
Password	New: Confirm:
Role	Administrator
Terminal Access	Disabled

User Roles (most common)

Manual: BIG-IP Systems: User Account Administration

No Access

- Prevents users from accessing the system.

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.

Application Editor

- Grants users permission to modify existing nodes, pools, pool members, and monitors.

Manager

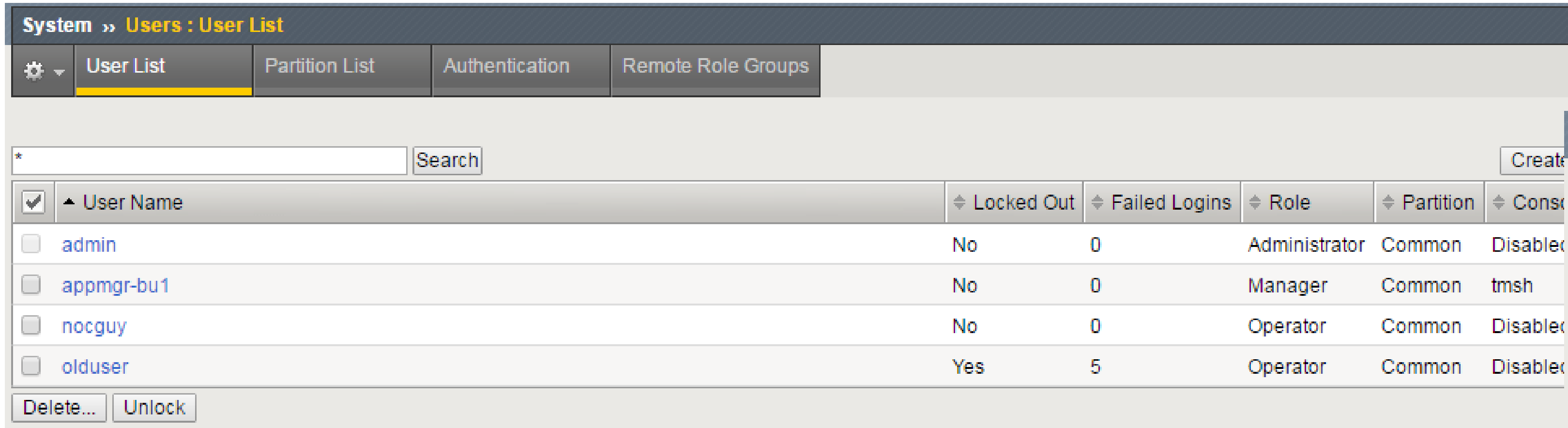
- Permission to create, modify, and delete virtual servers, pools, pool members, nodes, custom profiles, custom monitors, and iRules.

Administrator

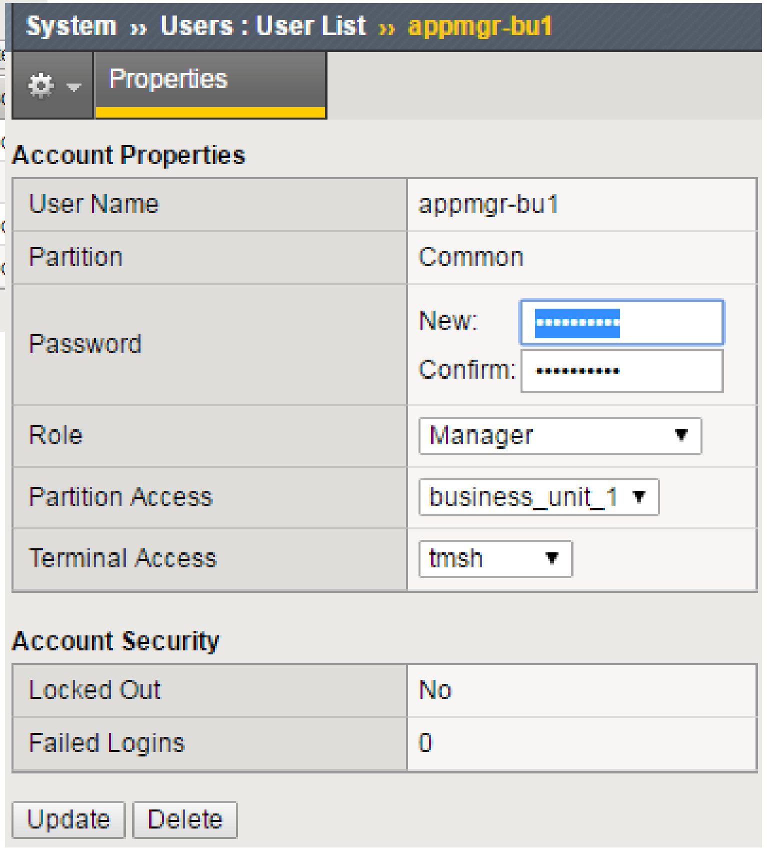
- Grants users complete access to all objects on the system.

3.08 Explain how to modify user properties

Just go back in and change them



	User Name	Locked Out	Failed Logins	Role	Partition	Cons
□	admin	No	0	Administrator	Common	Disablec
□	appmgr-bu1	No	0	Manager	Common	tmsh
□	nocguy	No	0	Operator	Common	Disablec
□	olduser	Yes	5	Operator	Common	Disablec



Account Properties

User Name	appmgr-bu1
Partition	Common
Password	New: •••••••••• Confirm: ••••••••••
Role	Manager
Partition Access	business_unit_1
Terminal Access	tmsh

Account Security

Locked Out	No
Failed Logins	0

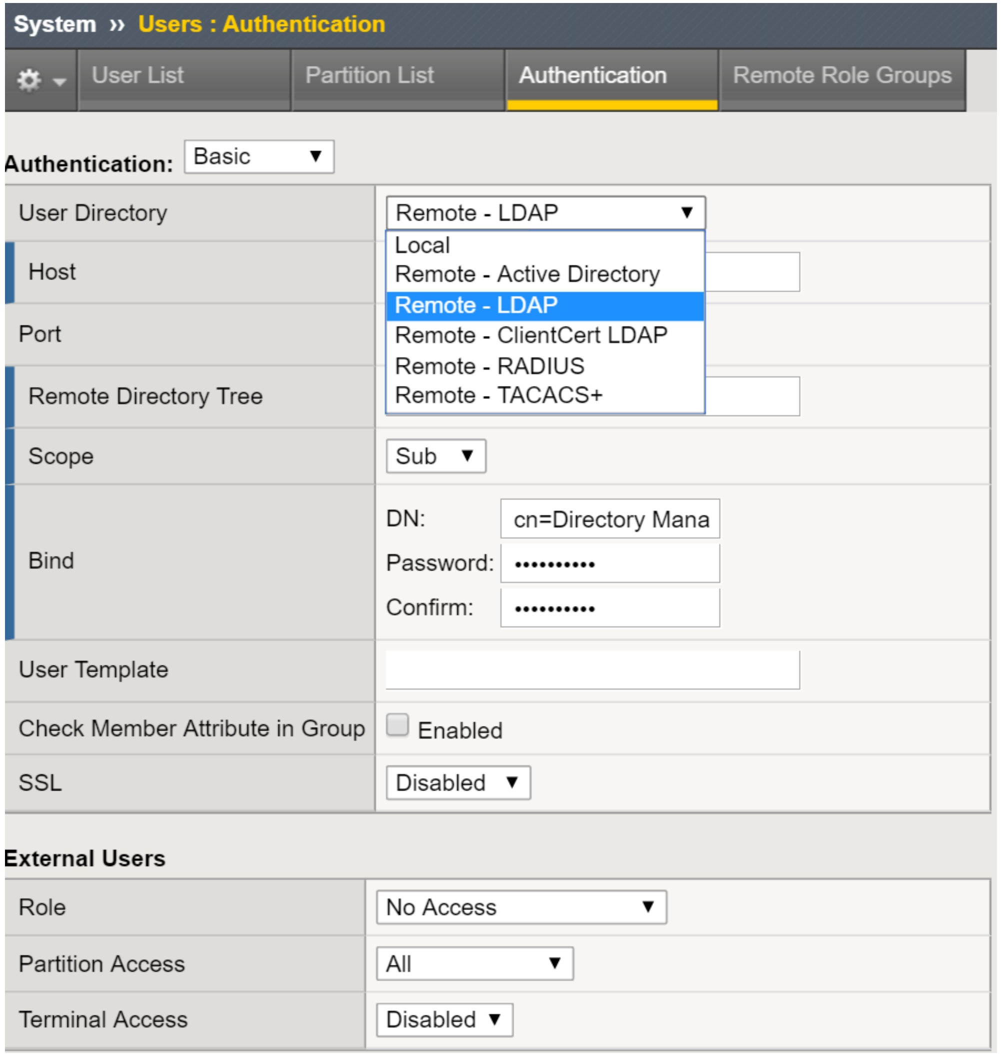
3.08 Explain options for remote authentication provider

Manual: BIG-IP Systems: User Account Administration

Still will always need at 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
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

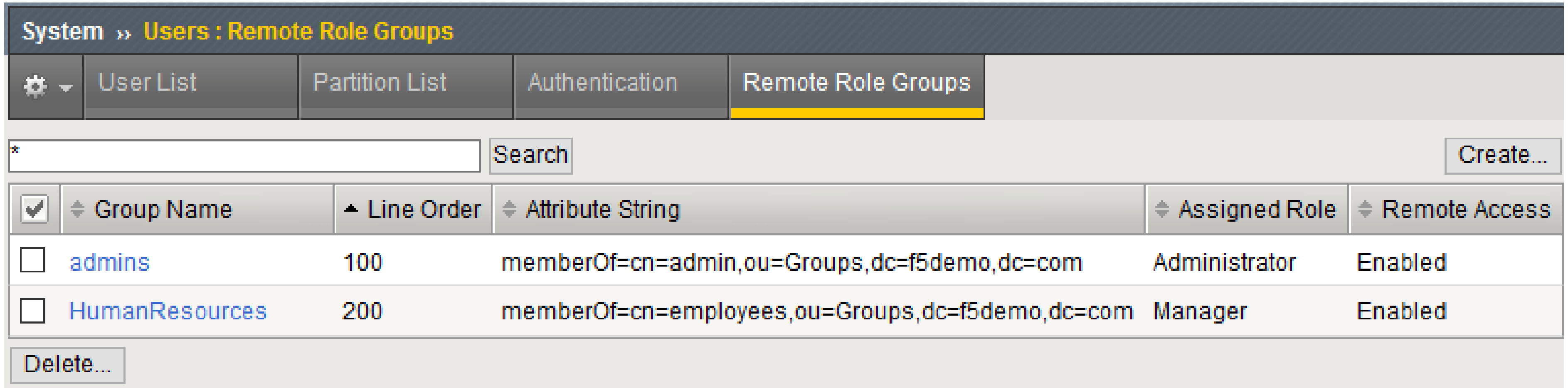
Role	No Access
Partition Access	All
Terminal Access	Disabled

3.08 Explain use of groups using remote authentication provider

Manual: BIG-IP Systems: User Account Administration

For a remote group you can choose to:

- Enable/disable remote access
- Assign a permissions role to members of the group
- Select All/Common/Specific name partition access
- Select the type of terminal access required.



☑	Group Name	Line Order	Attribute String	Assigned Role	Remote Access
□	admins	100	memberOf=cn=admin,ou=Groups,dc=f5demo,dc=com	Administrator	Enabled
□	HumanResources	200	memberOf=cn=employees,ou=Groups,dc=f5demo,dc=com	Manager	Enabled

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

2.09

Determine how to deploy or upgrade vCMP guests and how the resources are distributed

- Explain the different vCMP guest deployment states
- Discuss the relationship between CPU and memory on vCMP
- Select which versions can run on a guest given host version
- Understand the relationship of network configuration objects between vCMP hosts and vCMP guests

Topic Resources

- Manual Chapter: Virtual Servers
- Manual Chapter: Session Persistence Profiles

Breaktime

F5 Learning: Getting Started with BIG-IP

This course is divided into two modules:

The **Administration Module** focuses on basic administrative activities on the BIG-IP system. You'll learn how to activate a new BIG-IP system for operation, including configuring the management port, licensing, provisioning, and basic network configuration. You'll learn how to archive the BIG-IP configuration in support of data center backup and recovery activities. Finally, you'll learn how to verify the proper operation of your BIG-IP system by using the online BIG-IP iHealth® diagnostic tool.

Launch: Getting Started with BIG-IP Part 1: Administration
Demo: Setup Utility

The **Application Delivery Module** focuses on the basic building blocks of BIG-IP configuration in support of application delivery including nodes, pools and pool members, virtual servers, monitors, and profiles. You'll learn how to configure a basic web application that is delivered through the BIG-IP system, and includes round-robin load balancing, HTTP application health monitoring, overcoming routing issues with SNATs, and SSL offload (client SSL termination). You'll also learn how to review the flow of application traffic through the BIG-IP system using local traffic statistics.

Launch: Getting Started with BIG-IP Part 2: Application Delivery
Demo: Application Delivery

To access Getting Started Virtual Labs, please login or create an account in the new LearnF5, then search for "Getting Started with BIG-IP."

F5 Free Training: Getting Started with BIG-IP Local Traffic Manager (LTM)

This course is divided into four modules that are presented in two separate WBTs. The topics presented are organized around a customer scenario that takes an organization's globally expanding e-commerce site from a single server to multiple load balanced back-end servers behind a pair of BIG-IP LTM systems. You'll learn how to implement the high availability feature to establish an active/standby device service cluster. You'll learn how to load balance web application traffic across a pool of non-homogenous servers. You'll learn how to use an iRule to customize traffic flow, selecting the appropriate pool of back-end servers based on the client's preferred content language. And finally, you'll learn how to decrease existing server load reducing concurrent connections and connection rates using OneConnect.

Launch: Getting Started with LTM Part 1: HA and Traffic Processing

Demo: Configure High Availability

Launch: Getting Started with LTM Part 2: iRules and OneConnect

Demo: iRules

F5 Free Training: Getting Started with BIG-IP iHealth

This course is intended to help you get started using BIG-IP iHealth as an online diagnostic tool. You'll learn how to leverage this tool to proactively maintain and more quickly troubleshoot your BIG-IP systems. The course describes how BIG-IP iHealth Diagnostics evolved from an internal tool into a free, online tool available to F5 customers. It explains the four-step process to generate iHealth Diagnostics and introduces iHealth reports. The remainder of the course describes how to use iHealth to identify security vulnerabilities and performance issues, prepare to upgrade your system, and leverage iHealth to troubleshoot system configuration issues and ensure your hardware platform is running at peak performance. The course is based on user-centered simulations and will take 15 minutes to complete.

Launch: Getting Started with BIG-IP iHealth

USE CASE: “Deliver any application on-premises or in the cloud with BIG-IP"

- **Improve website performance and availability:** With BIG-IP Local Traffic Manager, you can ensure your website is always available and performing at its best. By intelligently distributing traffic and managing connections, BIG-IP LTM can optimize website delivery, improve response times, and prevent downtime, even during peak traffic periods.
- **Securely manage and control application traffic:** BIG-IP provides advanced security features that enable you to safely manage and control application traffic. With SSL/TLS offloading, advanced access control, and granular application-level policies, you can protect your applications and sensitive data from malicious attacks and unauthorized access.
- **Simplify application deployment and management**: BIG-IP simplifies application deployment and management with **powerful automation and orchestration capabilities**. With easy-to-use interfaces and tools, you can quickly provision and manage applications, and automate routine tasks to save time and reduce errors. **Comprehensive monitoring and analytics,** gain valuable insights into application performance and make informed decisions to optimize your infrastructure.
- **Secure APIs and microservices:** BIG-IP Local Traffic Manager provides robust API security features that help you protect your APIs and microservices from threats. With support for modern authentication and authorization protocols like OAuth and OpenID Connect, BIG-IP LTM can authenticate and authorize API requests, prevent unauthorized access, and protect sensitive data. Additionally, with advanced traffic management capabilities like rate limiting and content-based routing, you can ensure API availability and performance.