F5 301a v14.1 Certification Prep

Presented by:

Daniel Cayer, F5 Solutions Engineer – Sales

&

David Larsen, F5 Solutions Engineer – Sales

Updated: April 2022

The Goal

If you are just starting your study for this exam, this lab will help you determine where your strengths and weaknesses are.

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

 ©2022 F5

Setting Expectations

- This course alone is not enough for you to pass the 301a exam
  - We will provide links to lots of relevant information
- The material is based on the blueprint and also on our personal experiences having written and passed this exam
- We will not have time to cover every topic in depth
  - We will focus on the topics we believe are most important for the exam
- 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 ;)

©2022 F5

F5 Certification Exams

Solutions Expert

Security Solutions 401

Cloud Solutions 402

Future Enterprise

Future Exams

Technology Specialist

LTM Specialist (b) 301b

LTM Specialist (a) 301a

DNS Specialist 302

ASM Specialist 303

APM Specialist 304

Future Exams

Administrator

TMOS Administration 201

Future Exams

Pre-Sales Fundamentals 202

Application Delivery Fundamentals 101

Sales Professional

Exam Structure

- 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 them (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!**

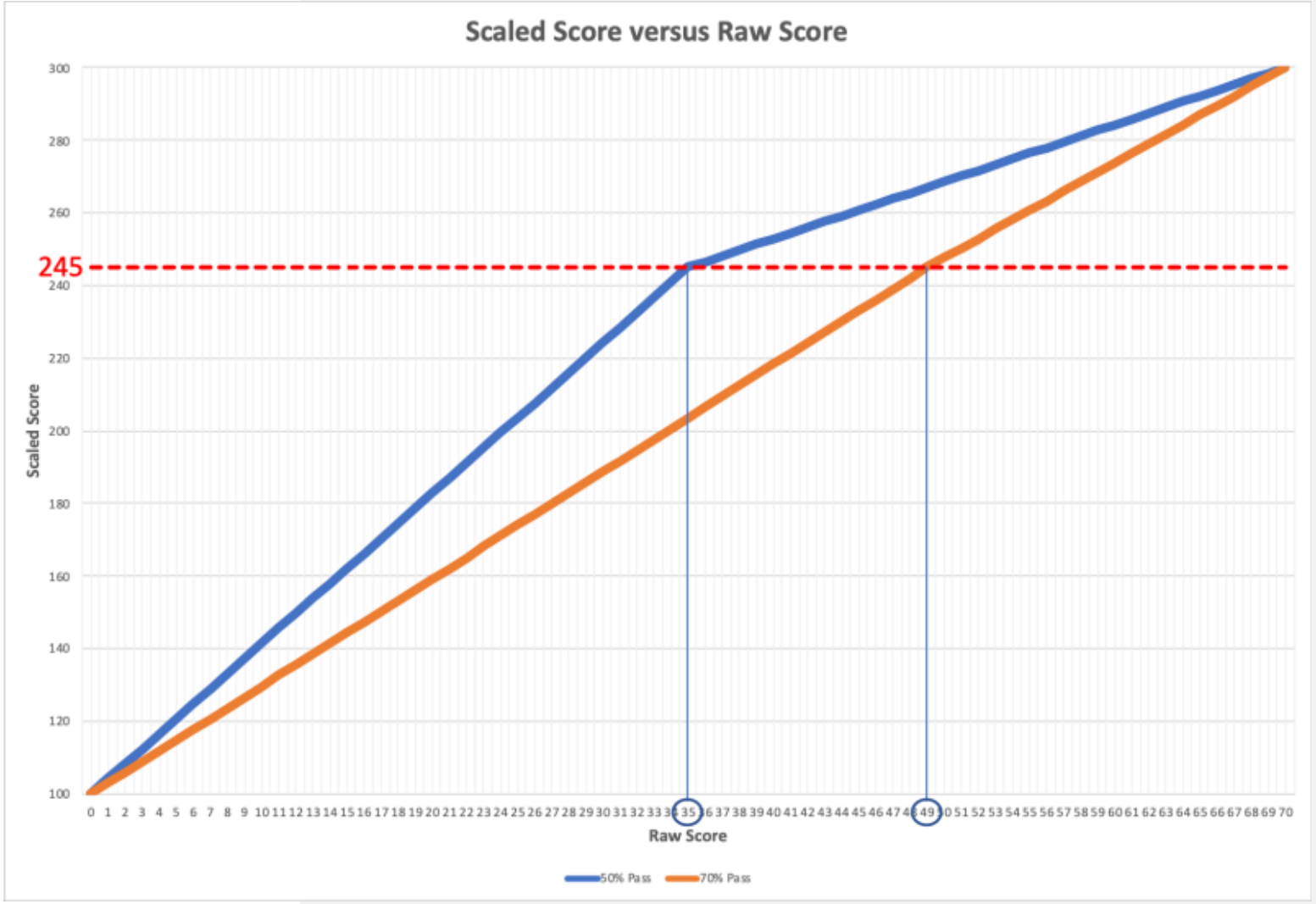
©2022 F5

F5 Exam – Scaled Scoring

- PASS = 245

“Scaled scores ensure that the reported scores across exam forms and versions have the same meaning regardless of difficulty.”

Questions? → **support@cert.f5.com**



 ©2022 F5

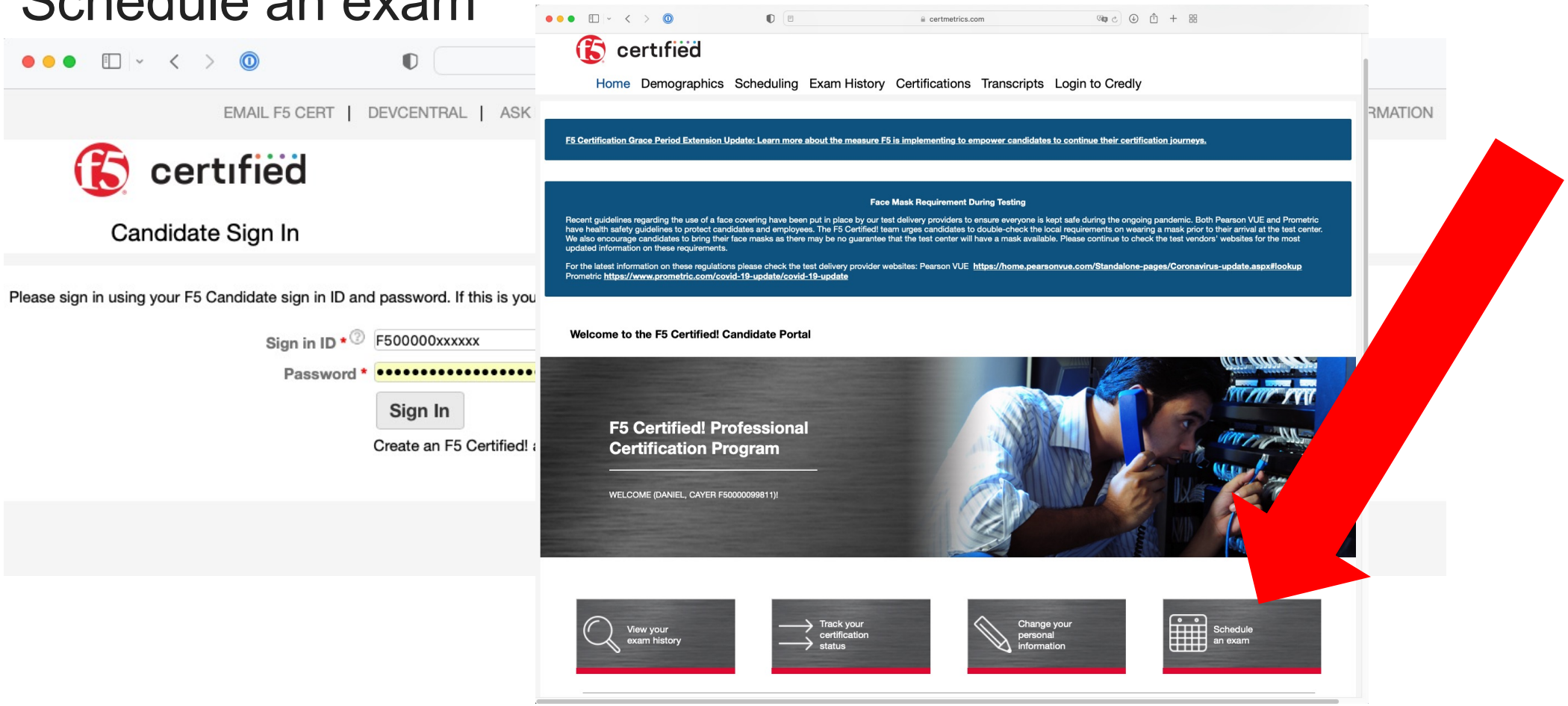
F5 Exams: Multiple Attempt Rules!

- 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

©2022 F5

Scheduling an F5 Certification Exam

- Sign in at https://certification.f5.com (same as for your 201 exam)
- Click “Schedule an exam”



 ©2022 F5

Additional Training Resources

ExamStudio Practice Exams (3rd-party)
Search for ExamStudio link here: https://support.f5.com/csp/article/K90101564

LinkedIn
F5 Certified! 301 Study Group: https://www.linkedin.com/groups/6722166/
F5 Certified Professionals: https://www.linkedin.com/groups/85832

Unofficial Study Guide (*slightly outdated, but very useful*)
https://f5-symposium-2022-301a.readthedocs.io/en/latest/class7/class7.html

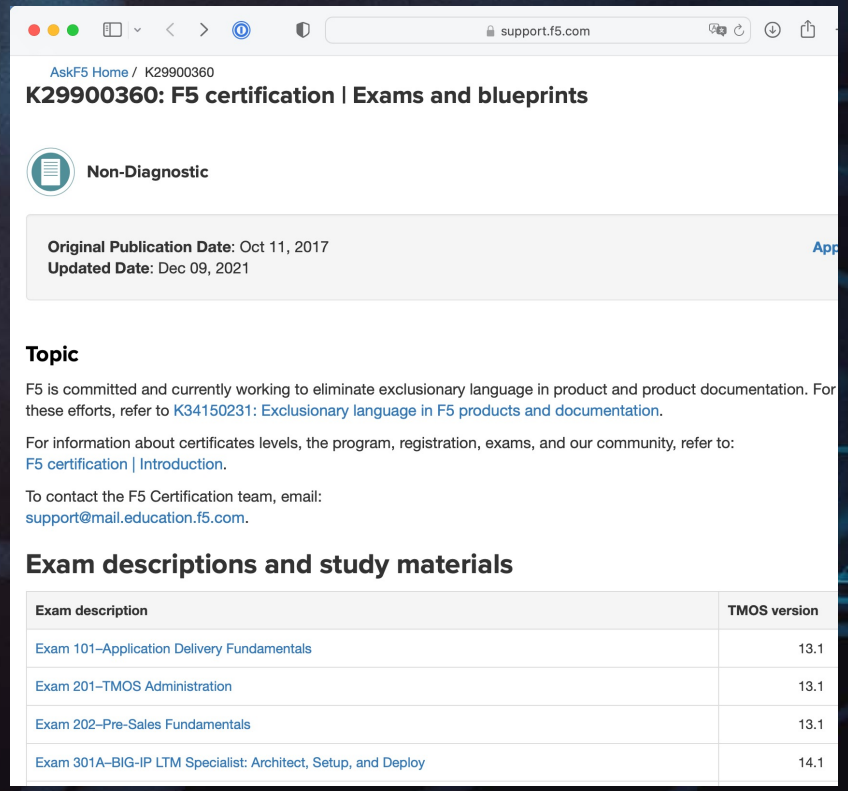
Official BIG-IP LTM 14.1 Knowledge Center
https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20LTM&version=14.1.0

 ©2022 F5

301a - BIG-IP LTM Specialist: Architect, Setup and Deploy

Exam Blueprint

- https://support.f5.com/csp/article/K29900360



support.f5.com

AskF5 Home / K29900360

K29900360: F5 certification | Exams and blueprints

Non-Diagnostic

Original Publication Date: Oct 11, 2017
Updated Date: Dec 09, 2021

Topic

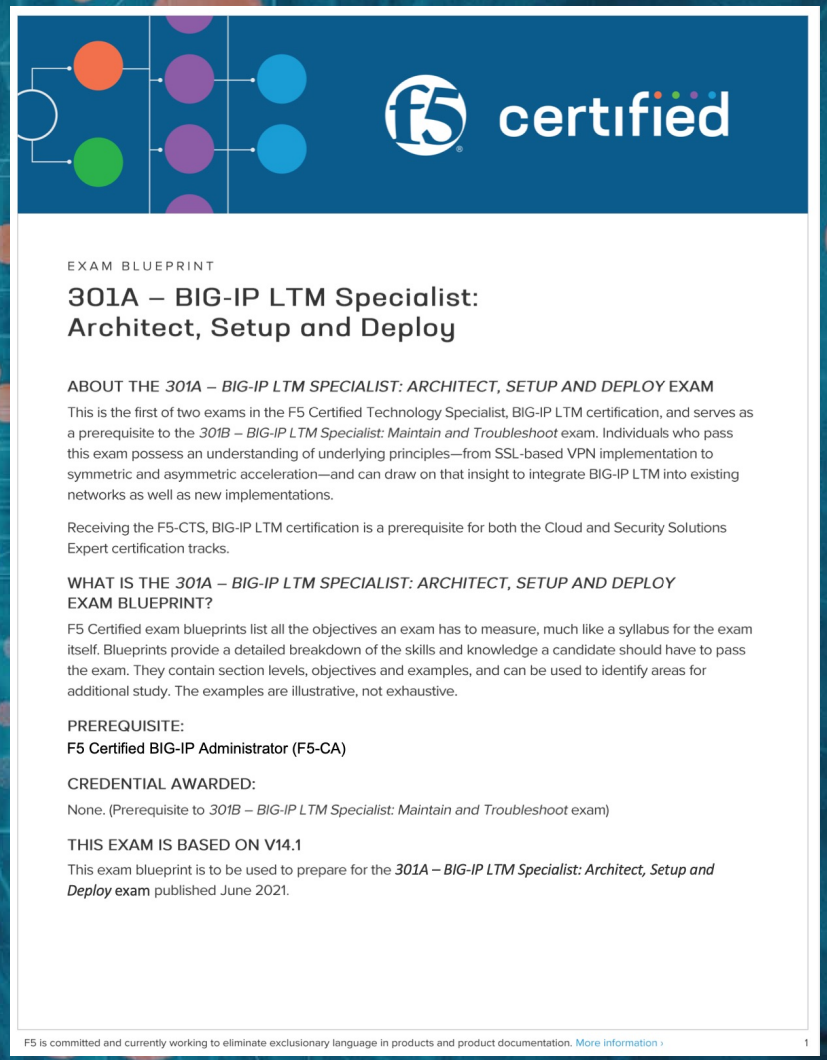
F5 is committed and currently working to eliminate exclusionary language in product and product documentation. For these efforts, refer to K34150231: Exclusionary language in F5 products and documentation.

For information about certificates levels, the program, registration, exams, and our community, refer to: F5 certification | Introduction.

To contact the F5 Certification team, email: support@mail.education.f5.com.

Exam descriptions and study materials

Exam description	TMOS version
Exam 101–Application Delivery Fundamentals	13.1
Exam 201–TMOS Administration	13.1
Exam 202–Pre-Sales Fundamentals	13.1
Exam 301A–BIG-IP LTM Specialist: Architect, Setup, and Deploy	14.1



f5 certified

EXAM BLUEPRINT

301A – BIG-IP LTM Specialist: Architect, Setup and Deploy

ABOUT THE *301A – BIG-IP LTM SPECIALIST: ARCHITECT, SETUP AND DEPLOY* EXAM

This is the first of two exams in the F5 Certified Technology Specialist, BIG-IP LTM certification, and serves as a prerequisite to the *301B – BIG-IP LTM Specialist: Maintain and Troubleshoot* exam. Individuals who pass this exam possess an understanding of underlying principles—from SSL-based VPN implementation to symmetric and asymmetric acceleration—and can draw on that insight to integrate BIG-IP LTM into existing networks as well as new implementations.

Receiving the F5-CTS, BIG-IP LTM certification is a prerequisite for both the Cloud and Security Solutions Expert certification tracks.

WHAT IS THE *301A – BIG-IP LTM SPECIALIST: ARCHITECT, SETUP AND DEPLOY* 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. They contain section levels, objectives and examples, and can be used to identify areas for additional study. The examples are illustrative, not exhaustive.

PREREQUISITE:
F5 Certified BIG-IP Administrator (F5-CA)

CREDENTIAL AWARDED:

None. (Prerequisite to *301B – BIG-IP LTM Specialist: Maintain and Troubleshoot* exam)

THIS EXAM IS BASED ON V14.1

This exam blueprint is to be used to prepare for the ***301A – BIG-IP LTM Specialist: Architect, Setup and Deploy*** exam published June 2021.

F5 is committed and currently working to eliminate exclusionary language in products and product documentation. More information ›

1

Use Case: TLS versions tracking

 ©2022 F5

Connections by TLS version

```
when CLIENTSSL_HANDSHAKE {
        ISTATS::incr "ltm.virtual [virtual name] c [SSL::cipher version]" 1
}
```

[user@murky:Active] ~ # **tmsh show ltm virtual stdsslvip**

```
-------------------------------------------------------------------
Ltm::Virtual Server: stdsslvip
-------------------------------------------------------------------
Status
  Availability     : available
  State            : enabled
  Reason           : The virtual server is available
  CMP              : enabled
  CMP Mode         : all-cpus
  Destination      : 192.168.2.189:443

Traffic                             ClientSide  Ephemeral  General
  Bits In                              872.0K          0        -
  Bits Out                               3.7M          0        -
  Packets In                              943          0        -
  Packets Out                             871          0        -

User-defined  Value
  SSLv3      21
  TLSv1      32
  TLSv1.1    54
  TLSv1.2   282
```

 ©2022 F5

Architect and Deploy Applications

 ©2022 F5

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

©2022 F5

1.02 - Determine whether or not 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

©2022 F5

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

©2022 F5

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 & two arm deployments
- Understand the importance of auto last-hop

©2022 F5

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

©2022 F5

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

©2022 F5

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

©2022 F5

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 fastL4 virtual server types
- Compare and contrast different load balancing methods
- Identify different load balancing method use cases

©2022 F5

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

©2022 F5

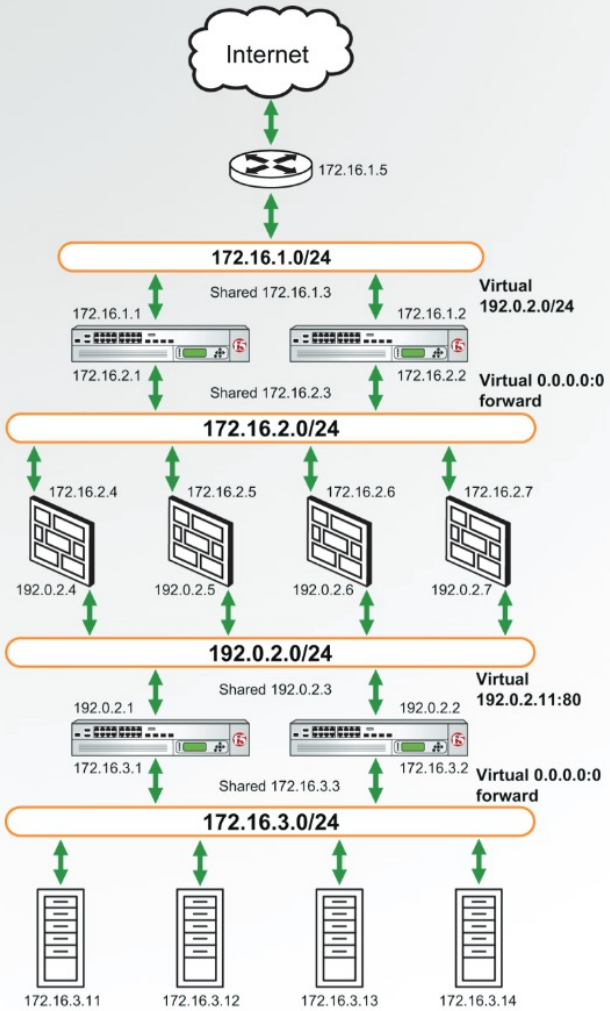
1.06 - Determine how to architect and deploy multi-tier applications using LTM technology

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

©2022 F5

IPv4 Addressing

www.example.com = 192.0.2.0:80



How does it work?

Simplified packet flow

As a request is made for http://www.example.com, the request is routed to 192.0.2.0.

When the request comes from the router to the shared IP address of the first BIG-IP pair, the active BIG-IP LTM reads destination and the virtual servers. If the virtual server covers the request, the BIG-IP LTM allows the traffic in.

The traffic is then sent to one of the firewalls based on the load-balancing algorithm used and the transparent health check status.

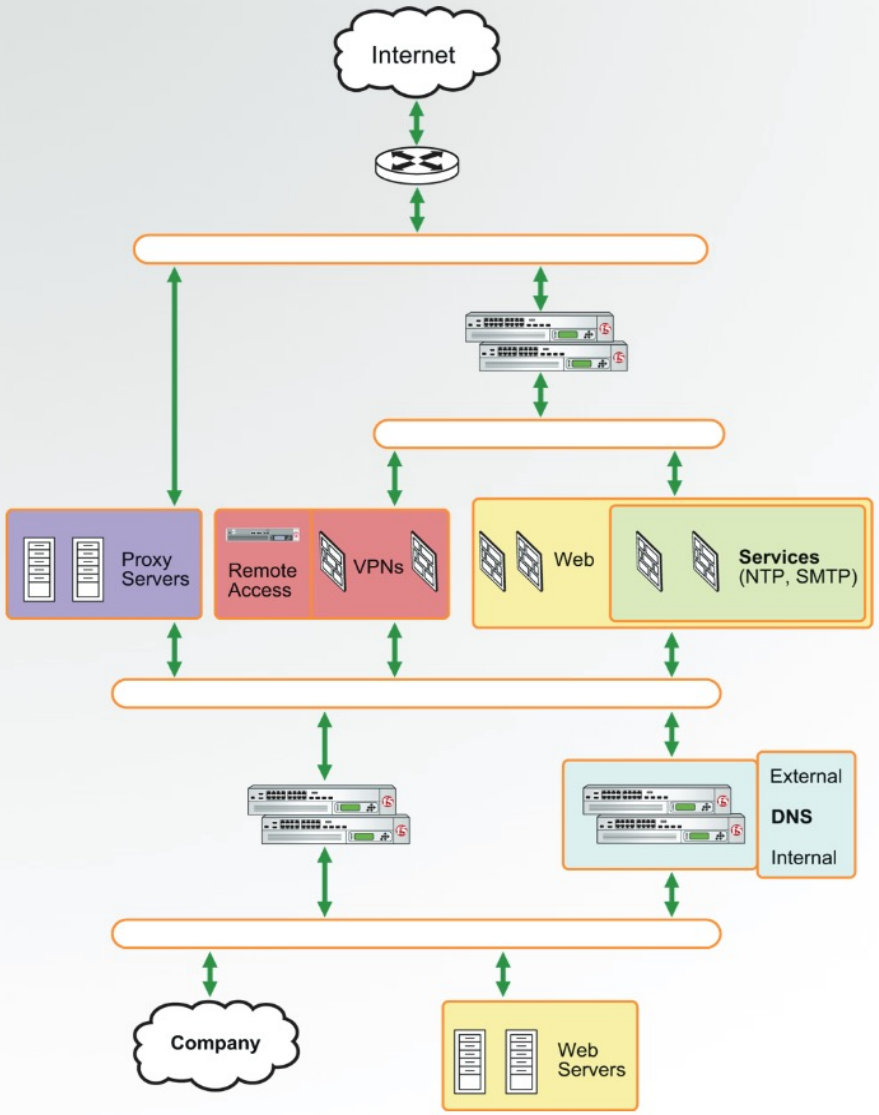
The firewall processes the request and routes the traffic to the shared IP address of the second pair of BIG-IP LTMs.

The BIG-IP LTM recognizes the traffic as bound for the 192.0.2.11:80 virtual server and allows it in. The request is then sent to one of the web servers based on the load-balancing algorithm used and the health checks status.

The return traffic is routed back to the active LTM through the node's default gateway, which is generally the shared alias address of the pair of BIG-IP devices. The "auto last hop" feature, ensures the traffic is sent back to the device that sent the request to the active LTM.

 ©2022 F5

Variations of the sandwich



What makes it work?

Last hop pools–Auto last hop
Using last hop pools when load balancing security devices ensures that the path a response connection takes (from the resource to the client) is the same as the path it took for the original request (from the client to the resource). BIG-IP LTM allows an administrator to specify the last hop pool members manually or to allow the system to determine the last hop automatically using the auto last hop pools feature.

Transparent monitors
Monitors are used to ensure the path through a firewall is functioning. In layer 3 firewall deployments the monitor is defined as "transparent," with a hard coded IP address. When the monitor is assigned to a node, packets will be sent through the node to the IP address assigned. Health checking through a firewall allows the BIG-IP device to ensure that the network, firewall, and end device are all functioning appropriately.

Wild card virtual servers
Virtual servers configured with a 0.0.0.0/0 destination IP address and mask. These types of virtual servers are used to load balance outbound connections as the destination address is usually not known.

Forwarding virtual servers
Forward traffic where no load balancing is required. These are generally used to forward traffic to the Internet on BIG-IP LTM external to the firewall.

Network virtual servers
Allow BIG-IP LTM to load balance traffic for a range of destination IP addresses.

Network Address Translation (NAT)
Network address translation allows the BIG-IP LTM to translate the destination IP address from the virtual server to the load-balanced destination server.

Secure Network Address Translation (SNAT)
Secure network address translation allows the BIG-IP LTM to not only translate the destination IP address from the virtual server to the load-balanced destination server, but also the port. This is often done to protect the servers from unwanted simple attempts to penetrate the network.

Drop–Reject invalid traffic
To help prevent against Denial of Service (DOS) attacks, the BIG-IP LTM can drop or reject invalid traffic that is routed to it. This allows BIG-IP LTM to focus on valid traffic and not disturb the desired traffic's service.

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

©2022 F5

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

©2022 F5

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

©2022 F5

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

©2022 F5

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

©2022 F5

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

 ©2022 F5

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

©2022 F5

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

 ©2022 F5

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

©2022 F5

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

©2022 F5

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

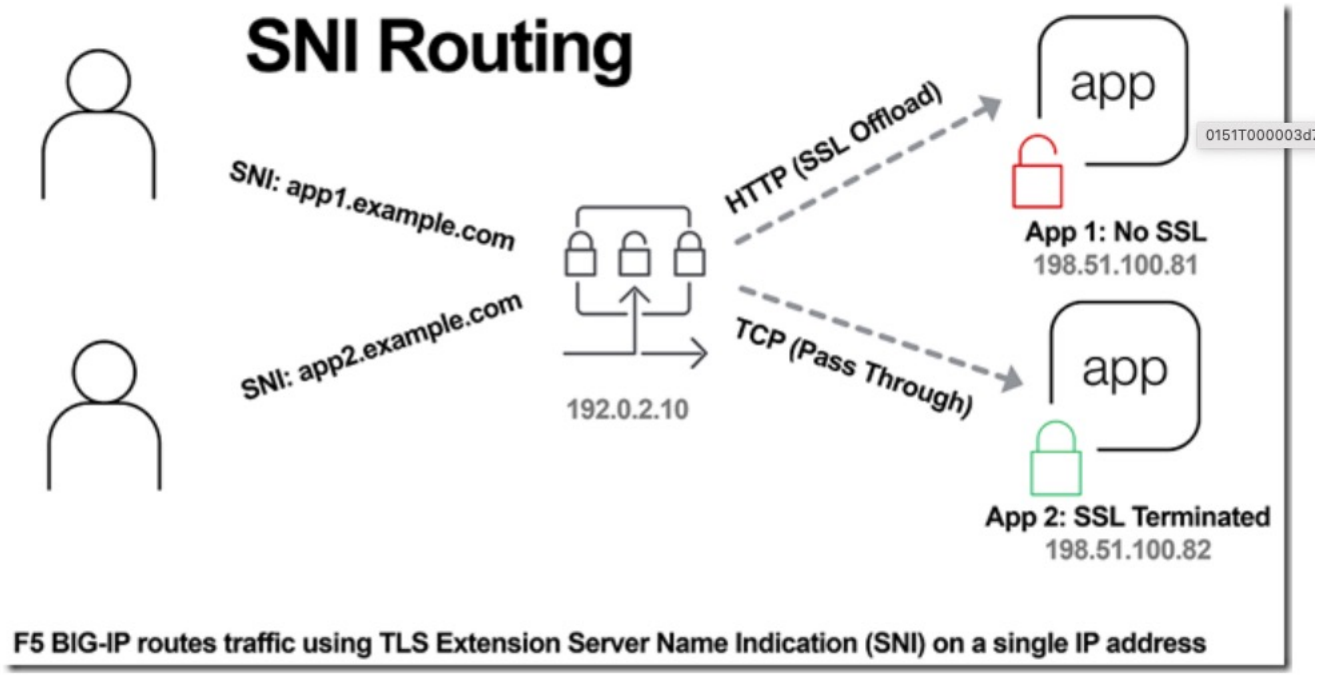
©2022 F5

Use Case: SNI Routing

©2022 F5

Single IP address for multiple TLS based Sites (SNI Routing)

- Cloud Service Providers charge for every single external IP.
- If you have multiple HTTPS sites with different certificates, how do you keep the number of external IP addresses to a minimum?
- TLS SNI value can be grabbed on the TLS Handshake and then based on the Server Name Indicator (SNI) value we can route to different virtual servers with unique certificates and rules.



©2022 F5

Set Up, Administer, and Secure LTM Devices

©2022 F5

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

©2022 F5

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

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

©2022 F5

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

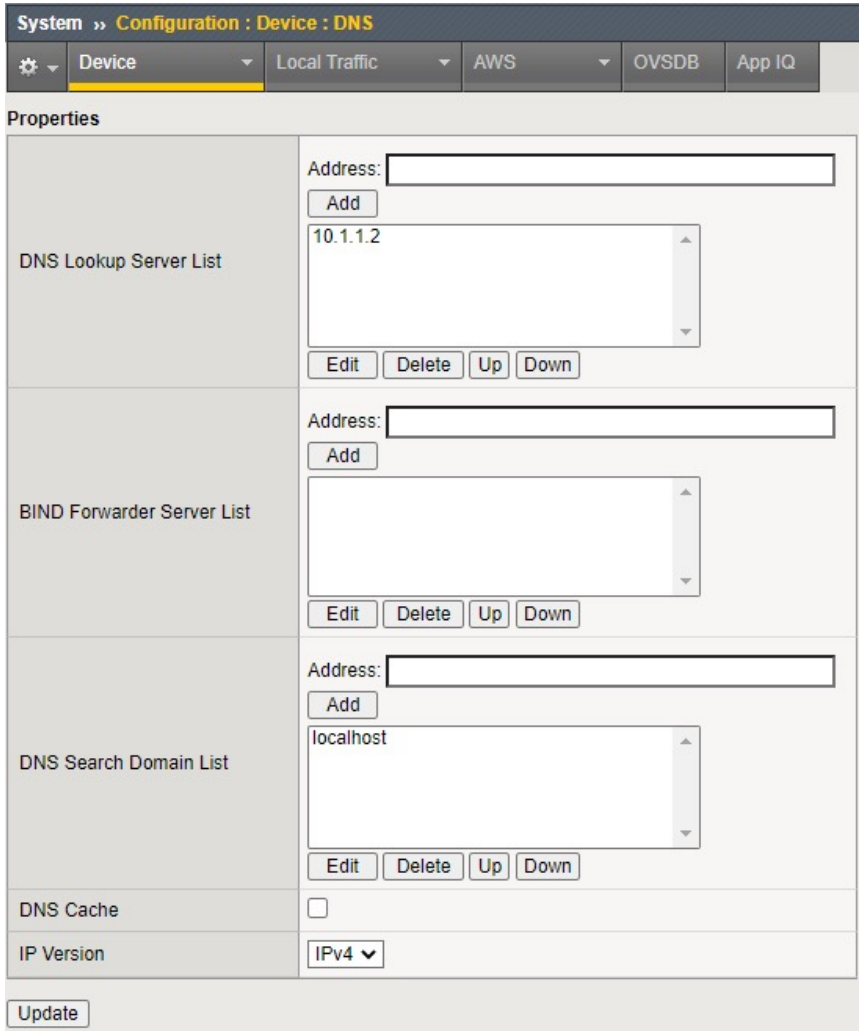
2.03 - Determine how to perform basic device configuration

- 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

©2022 F5

2.03 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).

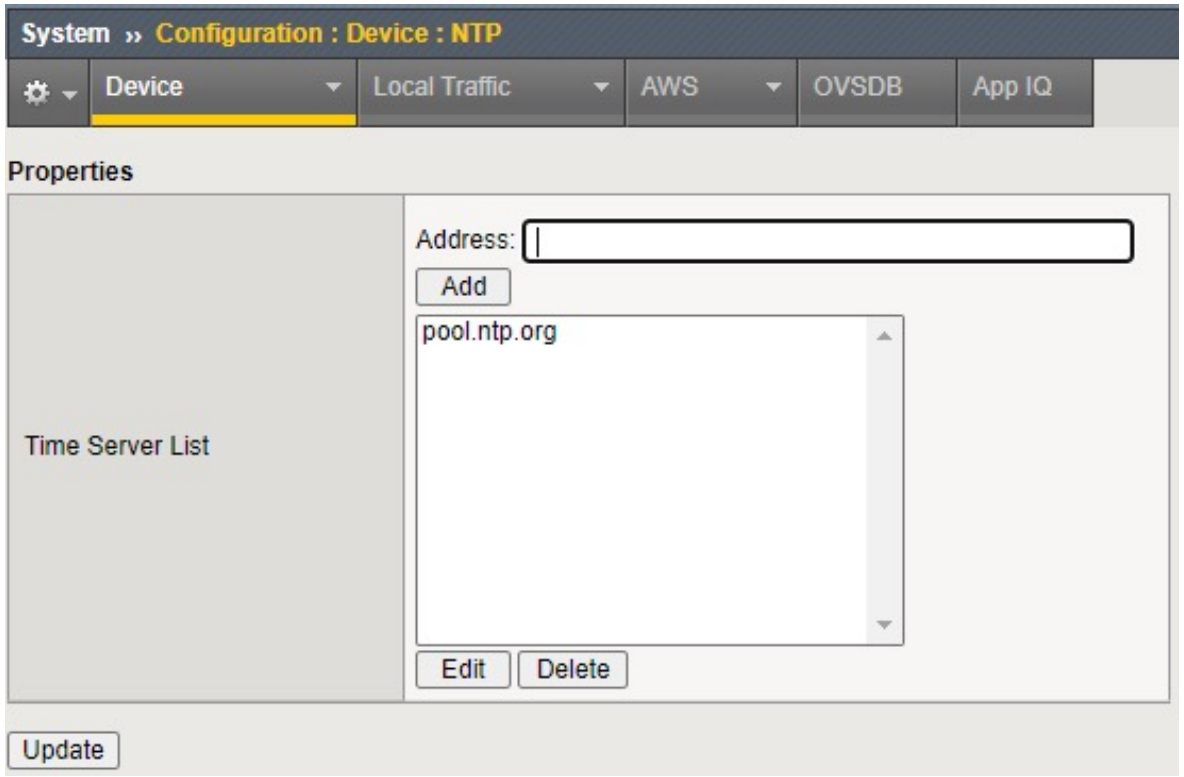


©2022 F5 CONFIDENTIAL

2.03 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



©2022 F5 CONFIDENTIAL

2.03 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

©2022 F5 CONFIDENTIAL

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

©2022 F5

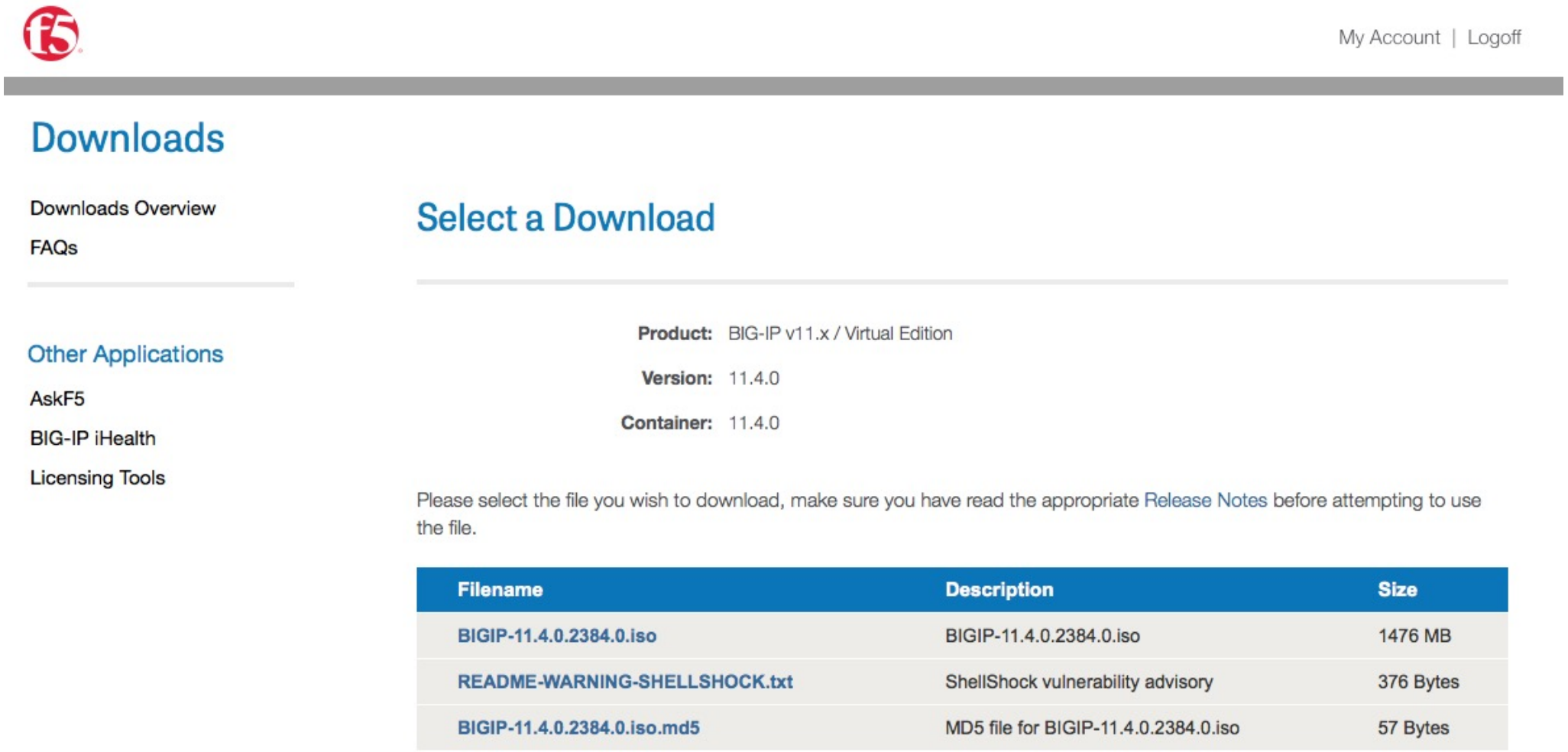
YouTube: Updating BIG-IP HA systems with a point release

- 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**

©2022 F5 CONFIDENTIAL

https://downloads.f5.com

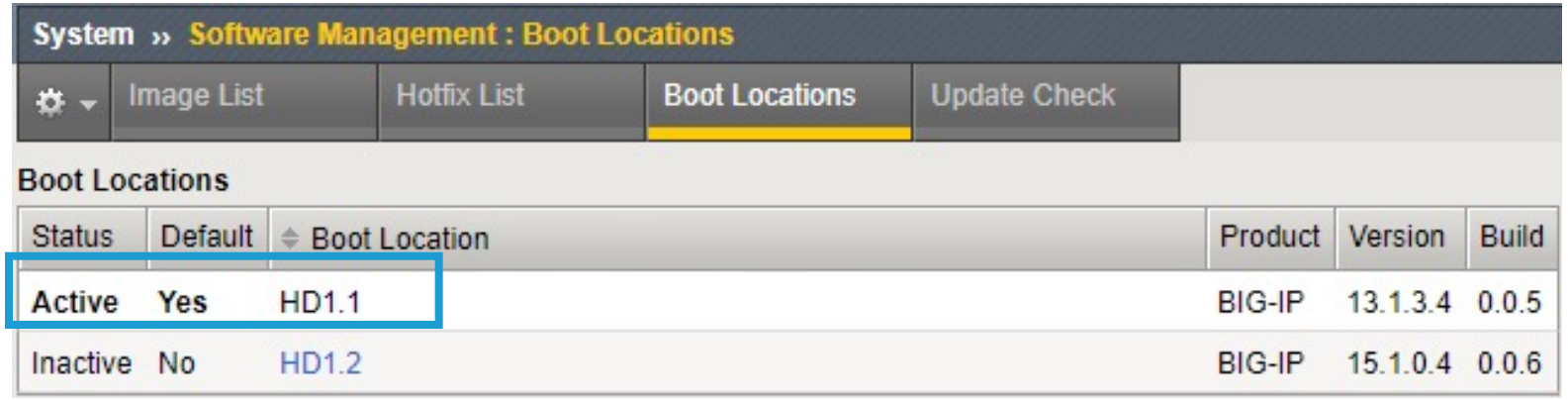
(Requires an f5 account)



 ©2022 F5

2.04 Show currently configured boot location

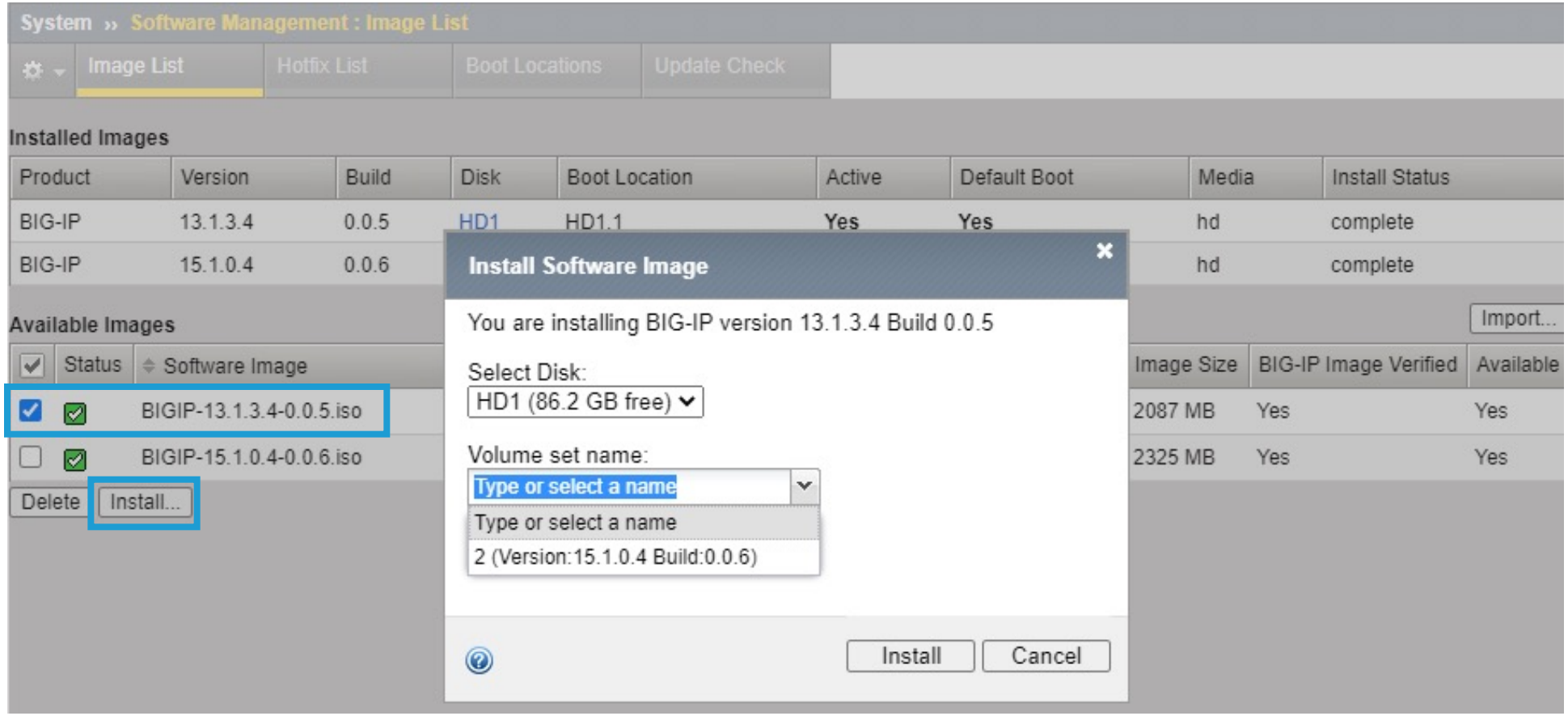
```
(tmos)# show sys software
-----------------------------------------------
Sys::Software Status
Volume  Product   Version  Build  Active    Status
-----------------------------------------------
HD1.1    BIG-IP  13.1.3.4  0.0.5     yes  complete

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



©2022 F5 CONFIDENTIAL

2.04 Demonstrate creating new volume for software images

install sys software image <iso> volume <name>



 ©2022 F5 CONFIDENTIAL

2.04 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

 ©2022 F5 CONFIDENTIAL

2.04 Summarize the use case of a UCS backup

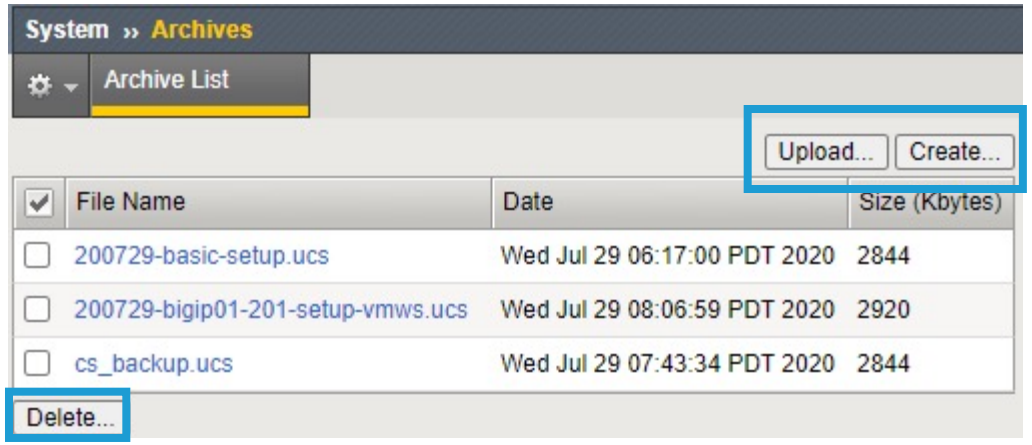
- You should create a UCS archive before operations that modify the configuration.
  - You can keep archives locally and/or download/upload archives to/from external sources
  - By default UCS archives are stored in /var/local/ucs
- Aside from the obvious, restoring your BIG-IP due to a corrupted/misconfigured 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

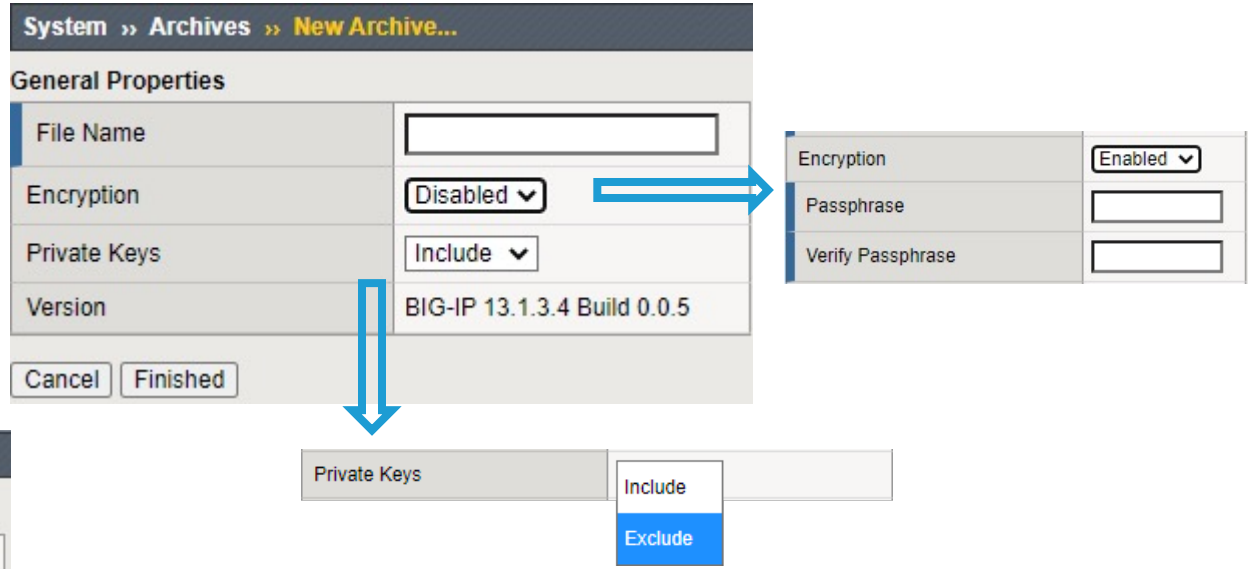
©2022 F5 CONFIDENTIAL

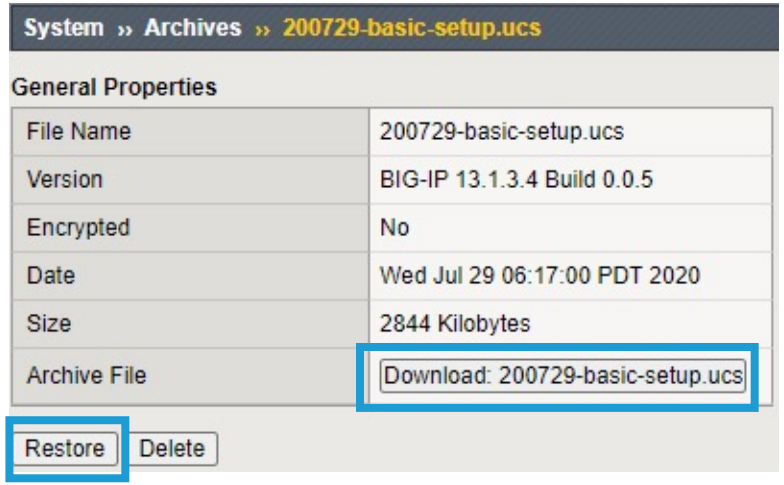
2.04 Execute UCS backup and restore procedure

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

Manual Chapter : Archives







©2022 F5 CONFIDENTIAL

2.04 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 whenloading a UCS.

©2022 F5 CONFIDENTIAL

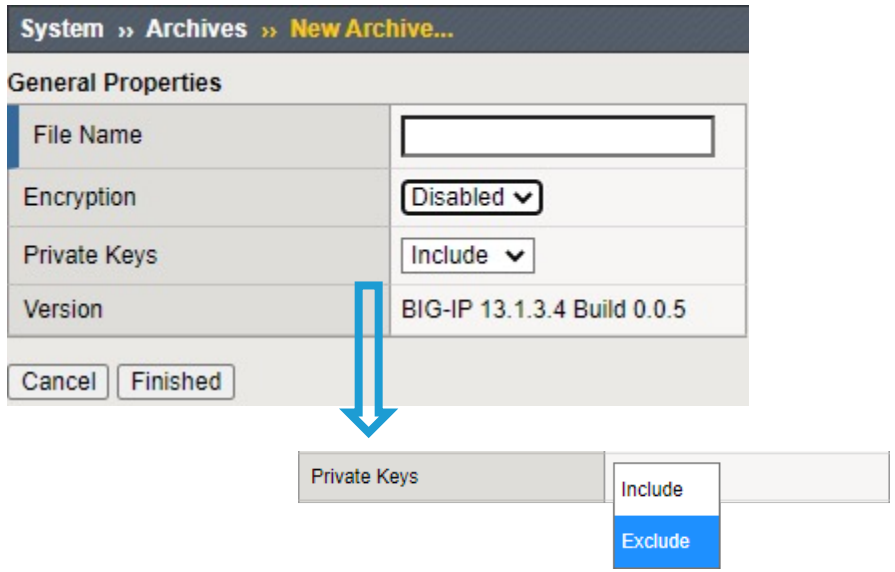
2.04 Explain proper long-term storage of UCS backup file

- 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.

©2022 F5 CONFIDENTIAL

2.04 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:



©2022 F5 CONFIDENTIAL

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

2.05 - Determine how to secure Self IPs

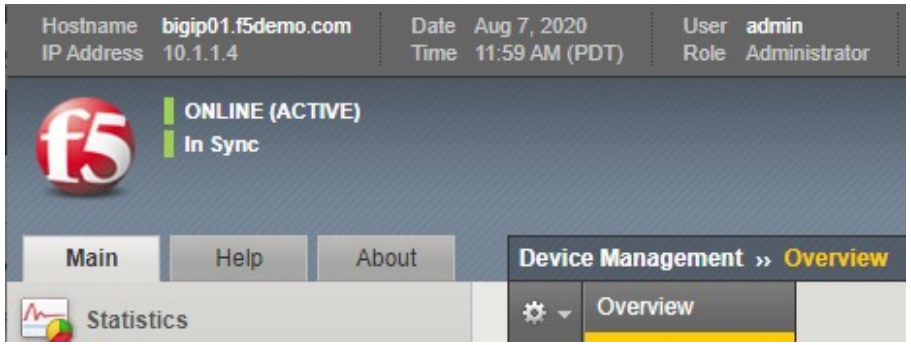
- Compare and contrast traffic groups vs HA groups
- Determine what prevented an expected failover
- Describe the differences between network failover and hardware failover

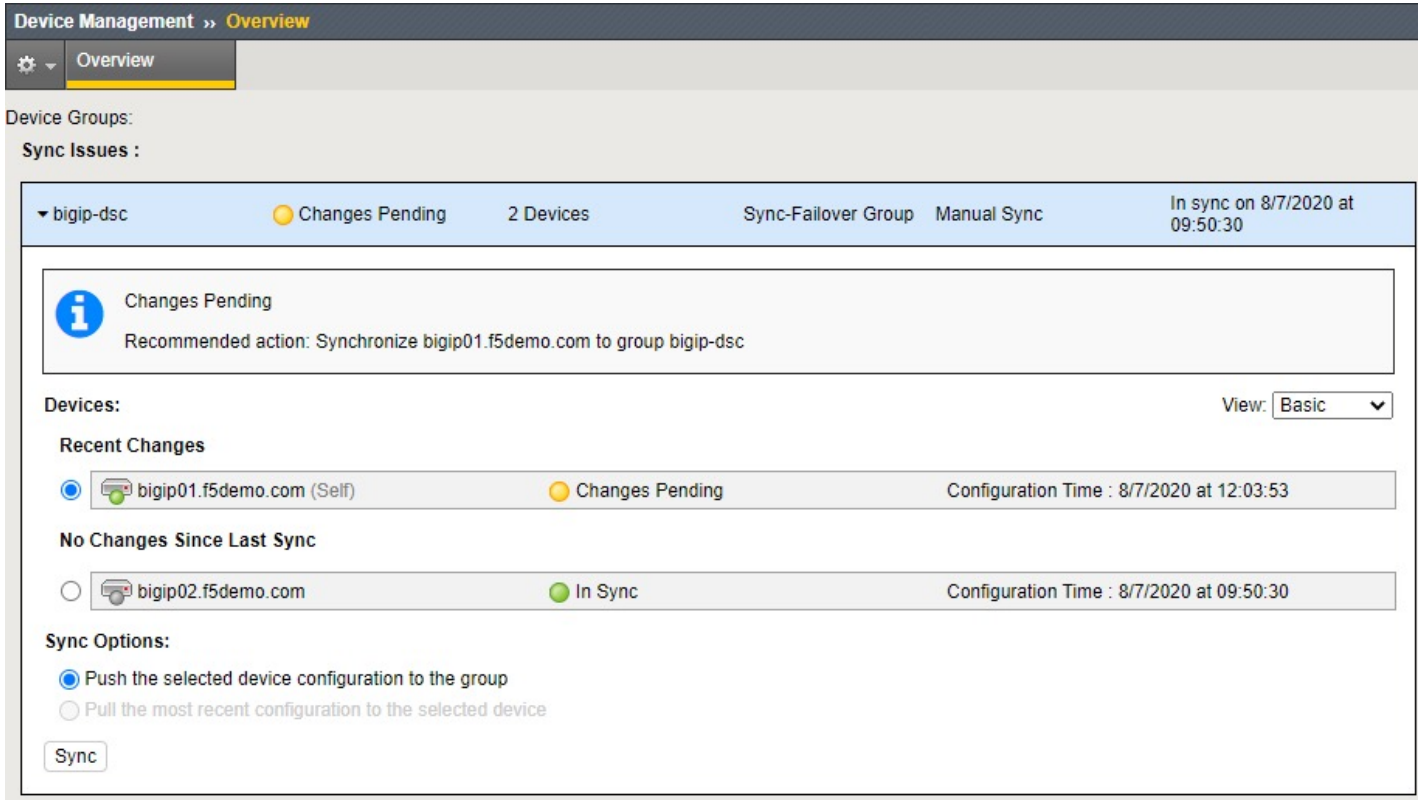
 ©2022 F5

2.05 Show config sync status

By default, synching a configuration is a manual process

Manual Chapter : Managing Configuration Synchronization





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

 ©2022 F5 CONFIDENTIAL

2.05 Explain when a config sync is necessary

K39735803: When to perform a manual ConfigSync

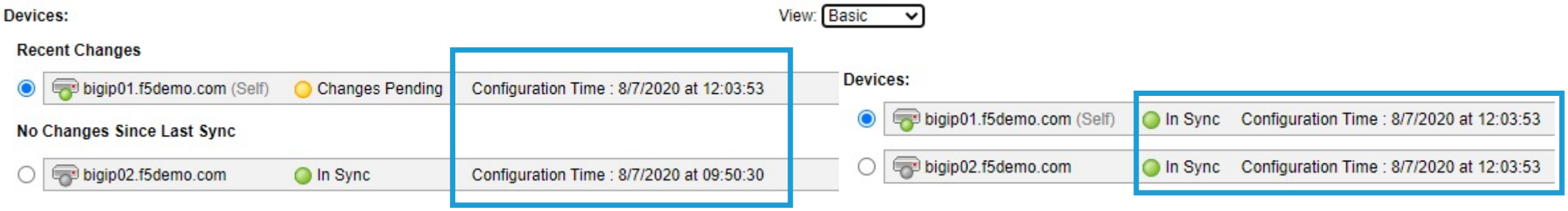
- When you make a change to a device in the Device Service Cluster (DSC) and automatic sync is not enabled
- Before you begin a software upgrade of a DSC to ensure all configurations are correctly synchronized
- After you complete a software upgrade for a BIG-IP device group. after all of the BIG-IP 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.

©2022 F5 CONFIDENTIAL

2.05 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



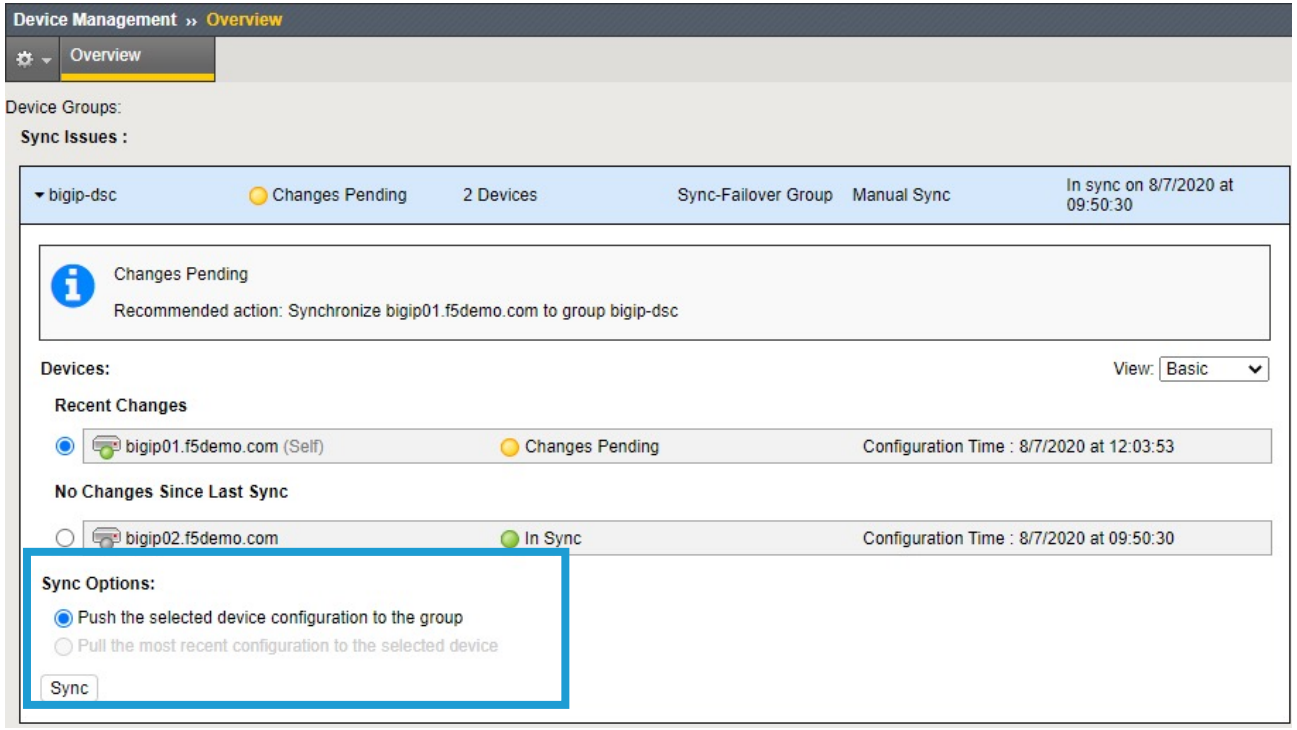
- Each device checks the remote device's time against its own system time.
  - If the time is not within the ConfigSync time threshold default value of three seconds, the command prompt changes to indicate that the time is out of sync (**Peer Time Out of Sync**), and ConfigSync operations may fail.
  - 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.

©2022 F5 CONFIDENTIAL

2.05 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 made changes you regret



 ©2022 F5

2.05 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.
```

 ©2022 F5

2.05 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)

©2022 F5 CONFIDENTIAL

Before we begin: A little more on Device Service Clusters

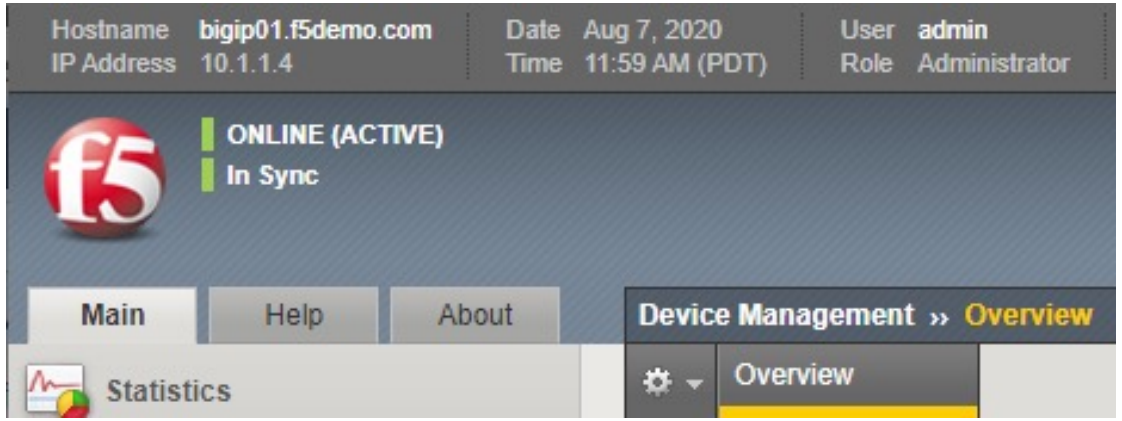
Manual : BIG-IP Device Service Clustering: Administration

- 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

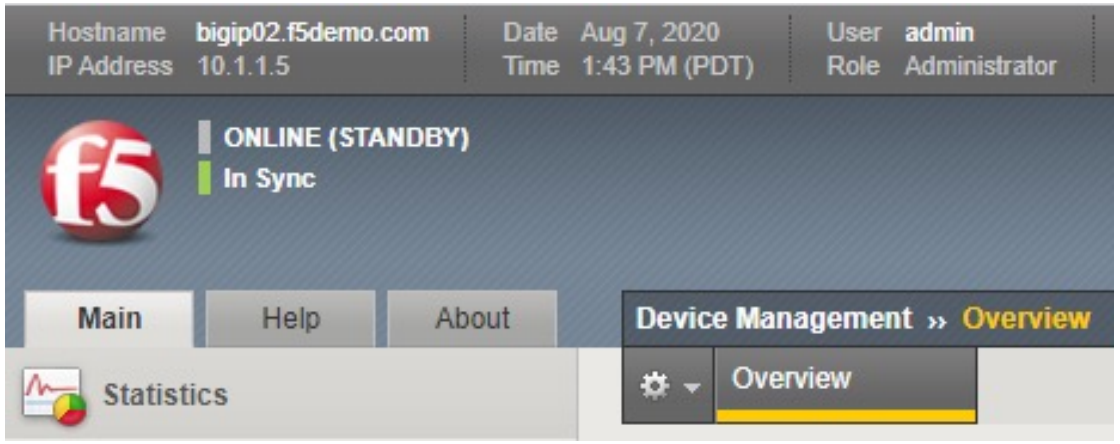
©2022 F5 CONFIDENTIAL

2.05 Report current active/standby failover state

Manual : BIG-IP Device Service Clustering: Administration



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



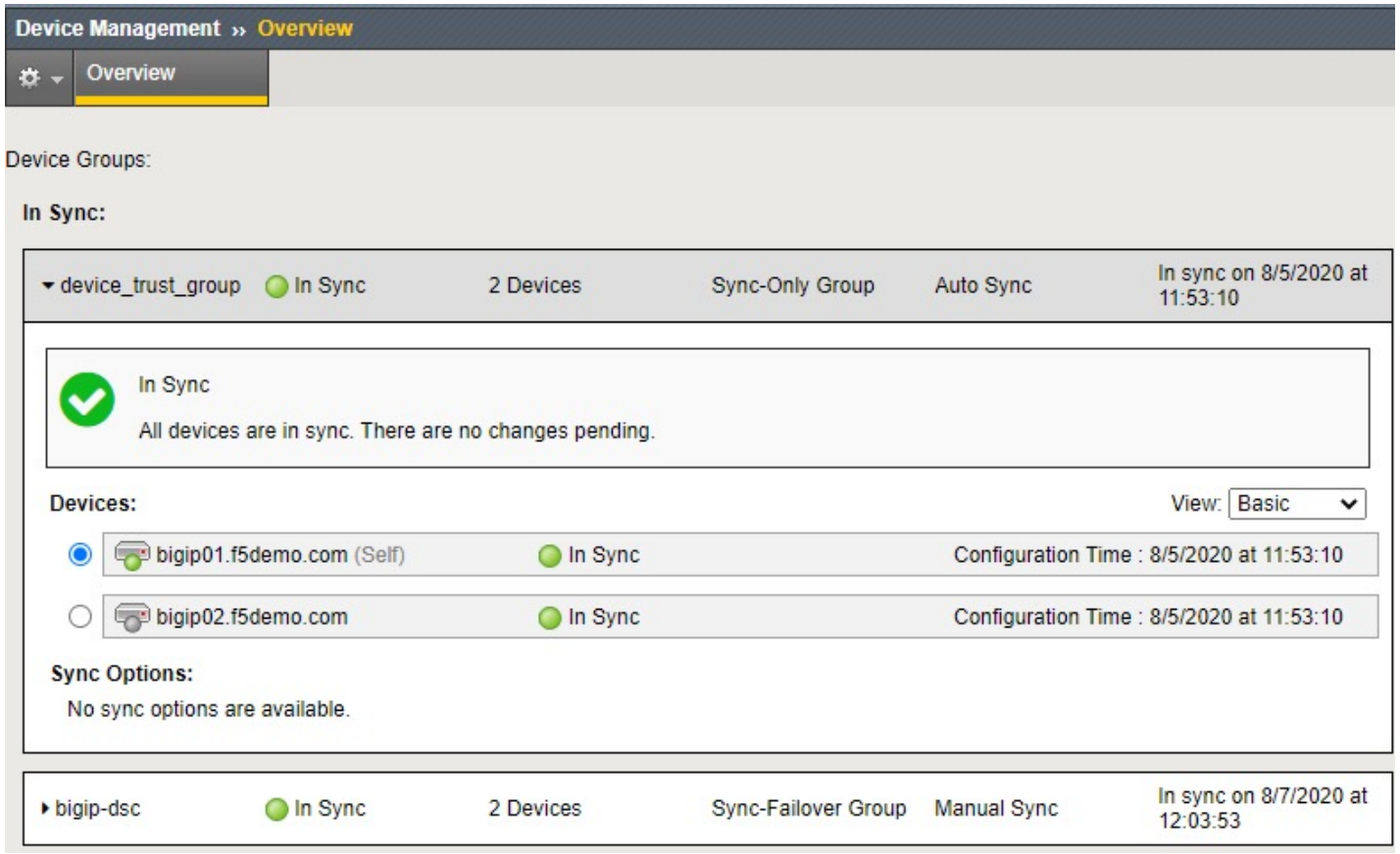
[root@bigip02:**Standby:**In Sync] config #

- Active – there are one of more active traffic groups that can failover
- Standby – there are no active traffic groups that can failover

©2022 F5 CONFIDENTIAL

2.05 Show device trust status

Manual Chapter : Managing Device Trust



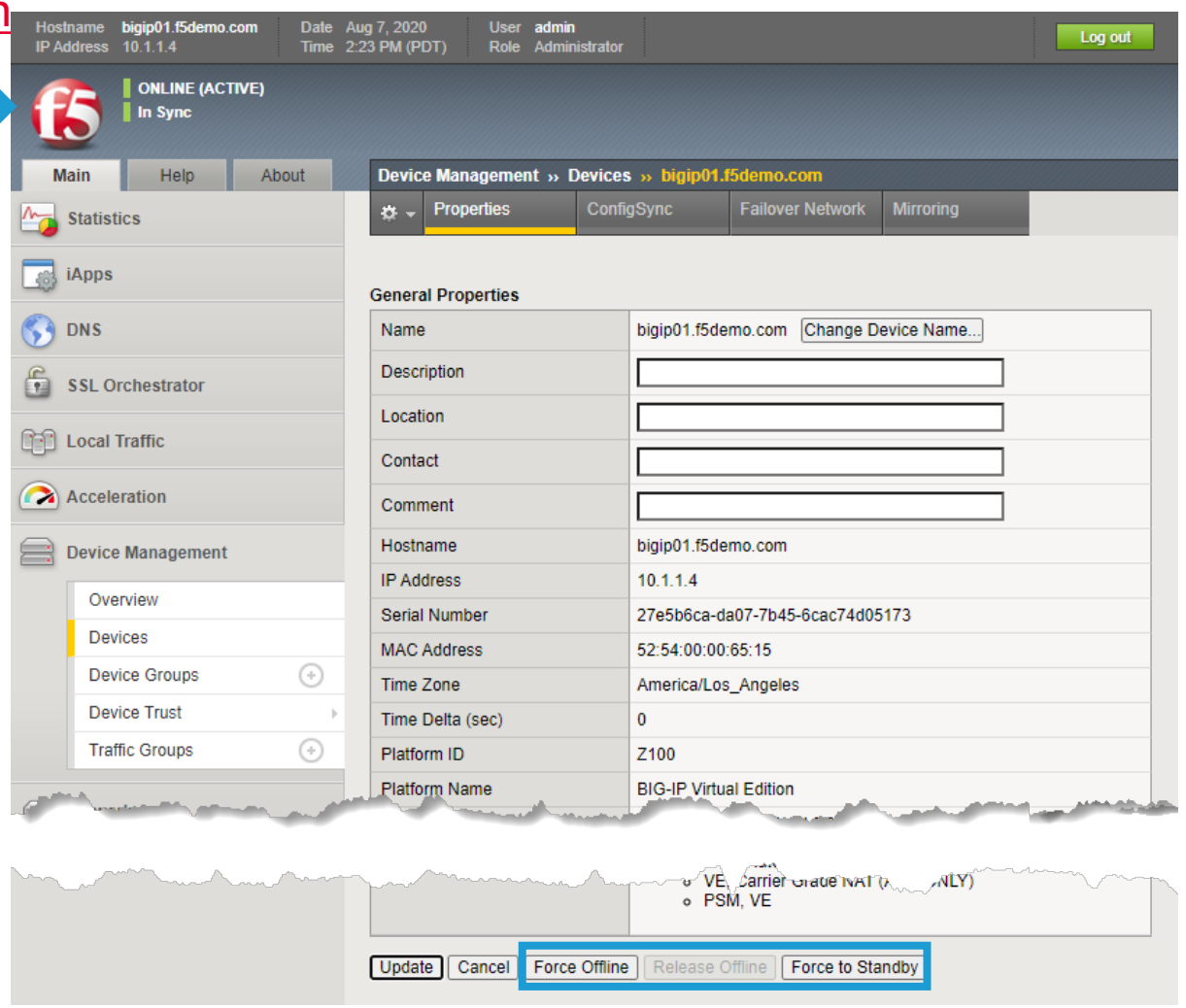

```
(tmos)# show cm device-group device_trust_group

-------------------------------------------------------------
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
```

 ©2022 F5 CONFIDENTIAL

2.05 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.



 ©2022 F5 CONFIDENTIAL

Other HA concepts not explicitly called out in the blueprint

Manual : BIG-IP Device Service Clustering: Administration

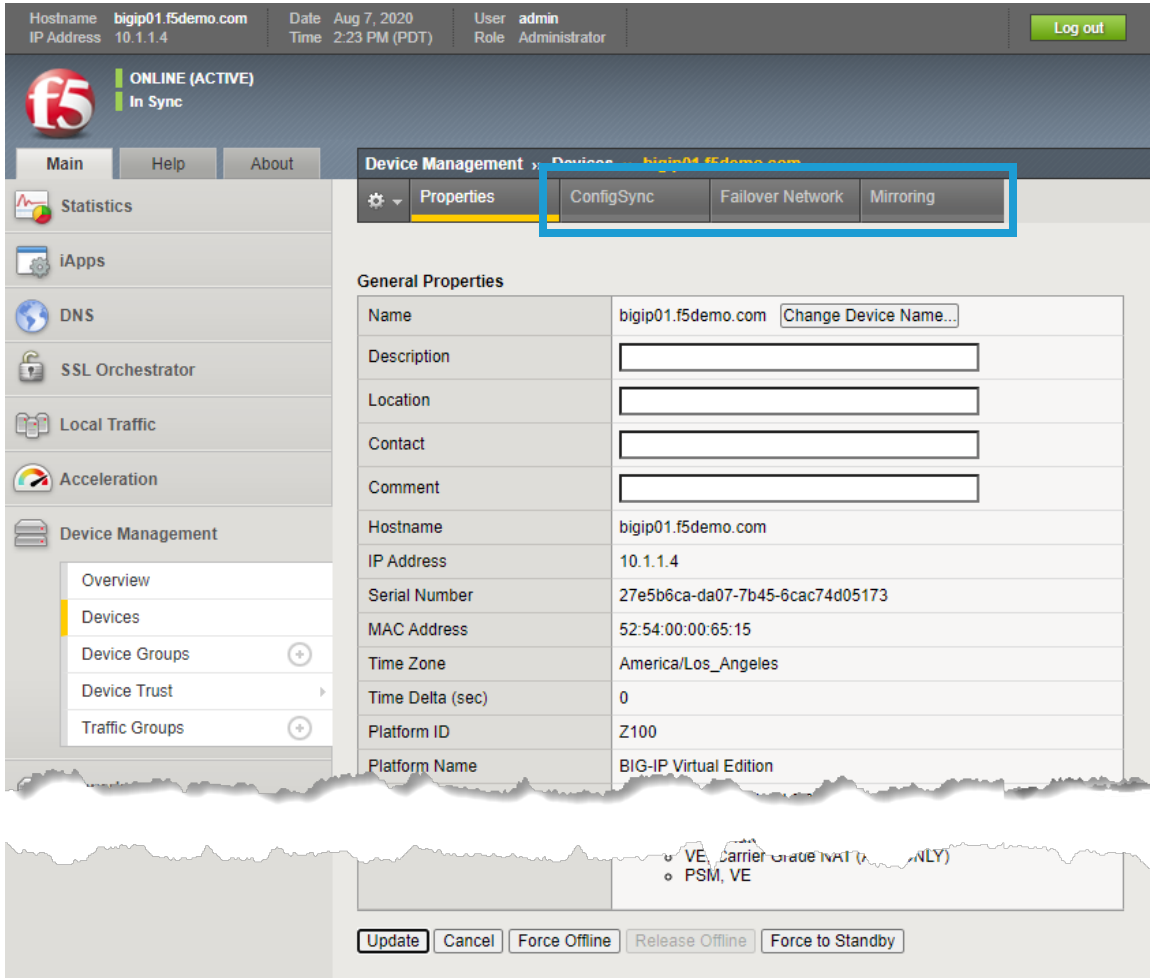
- Device Service Clusters (DSCs) can consist of more than two BIG-IPs supporting each other
  - Know where to find where failover objects on BIG-IP in the DSC will fail to
  - Understand the difference between Active-Standby and Active-Active
- You probably should have a working knowledge of Device Trust 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

©2022 F5 CONFIDENTIAL

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



 ©2022 F5 CONFIDENTIAL

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

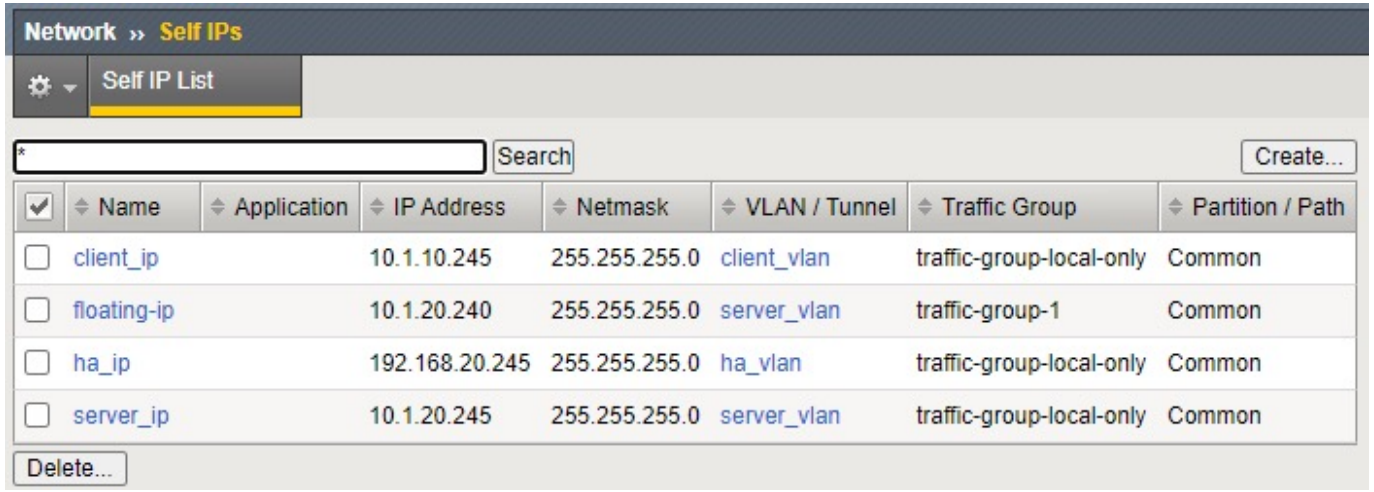
2.06 - Apply concepts required to use BIG-IP functionality to fulfill security requirements

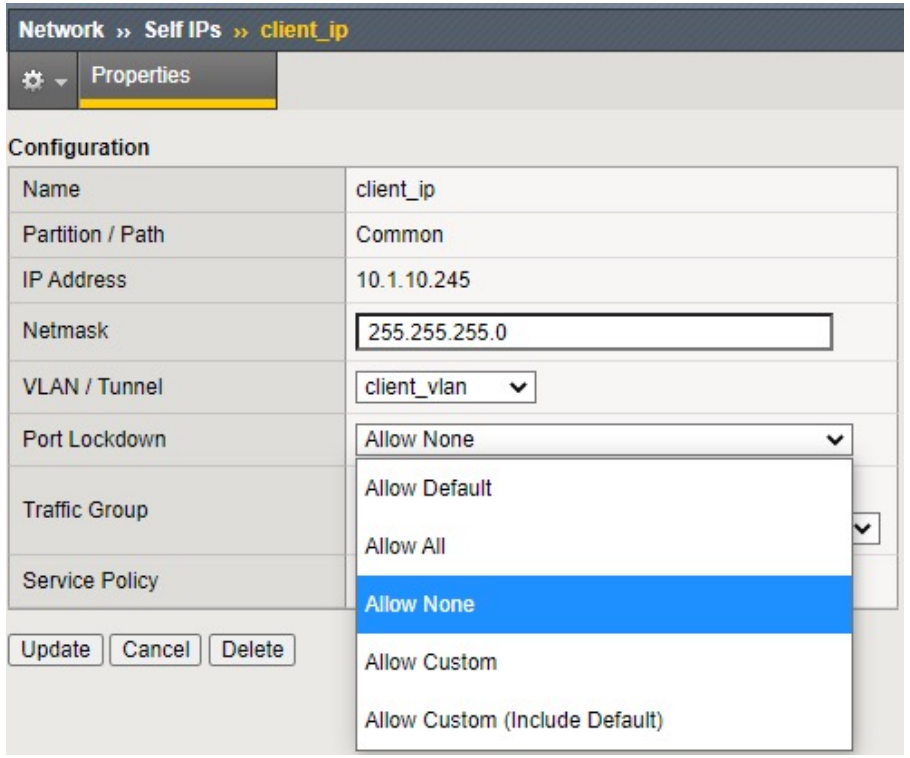
- Make use of port lockdown
- Demonstrate how to restrict access to management interface
- Demonstrate how to restrict access to virtual servers

 ©2022 F5

2.06 Interpret port lockdown settings to Self-IP

- Port Lockdown determines which ports a self IP address will respond too
  - 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





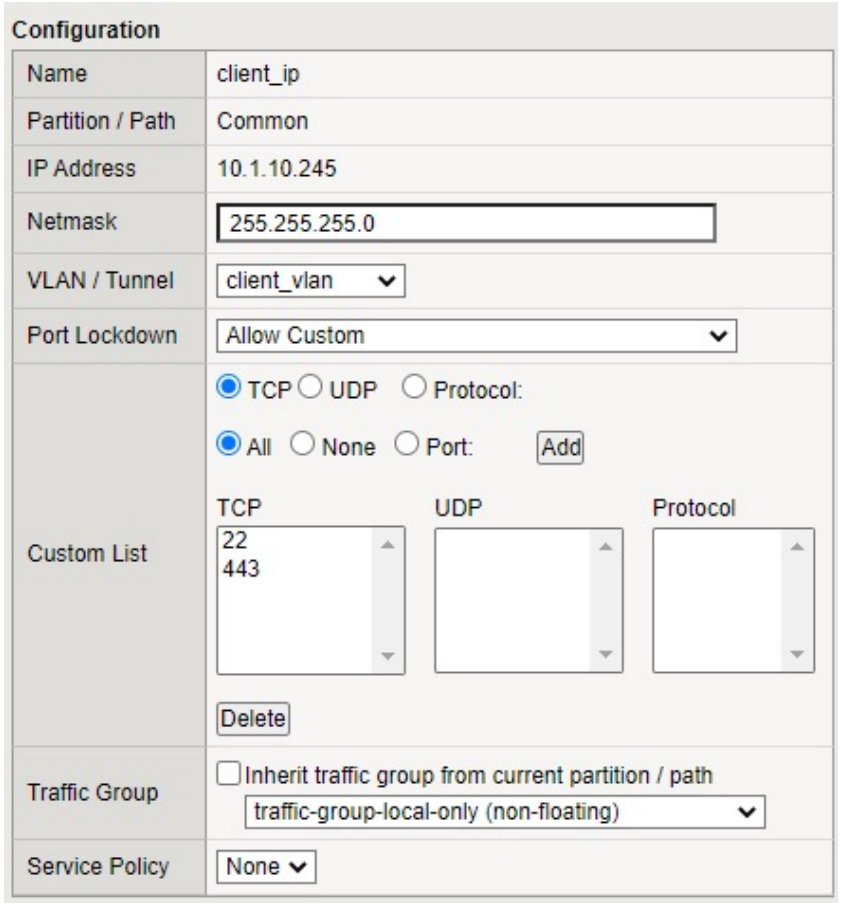
 ©2022 F5 CONFIDENTIAL

2.06 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

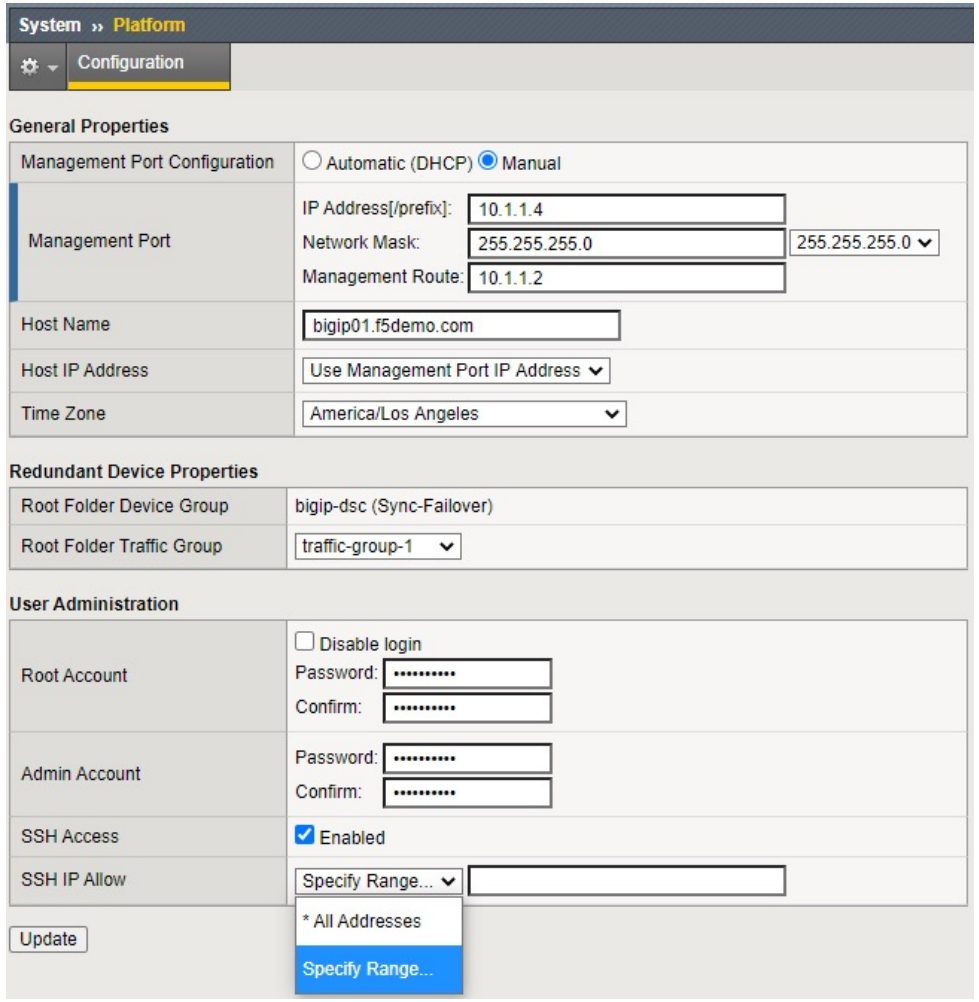



```
list net self
net self client_ip {
    address
10.1.10.245/24
    allow-service {
        tcp:ssh
        tcp:https
    }
```


©2022 F5 CONFIDENTIAL

2.06 Identify SSH 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 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

©2022 F5 CONFIDENTIAL

2.06 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 }
}
```

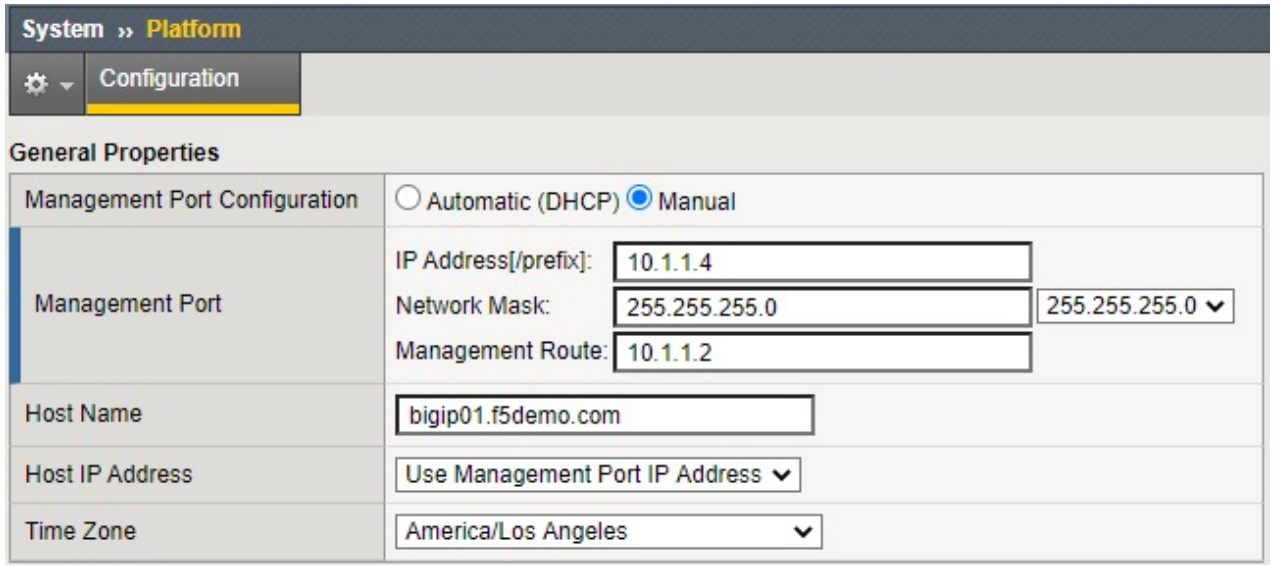
- Save the change by entering the following command:

  save /sys config

©2022 F5 CONFIDENTIAL

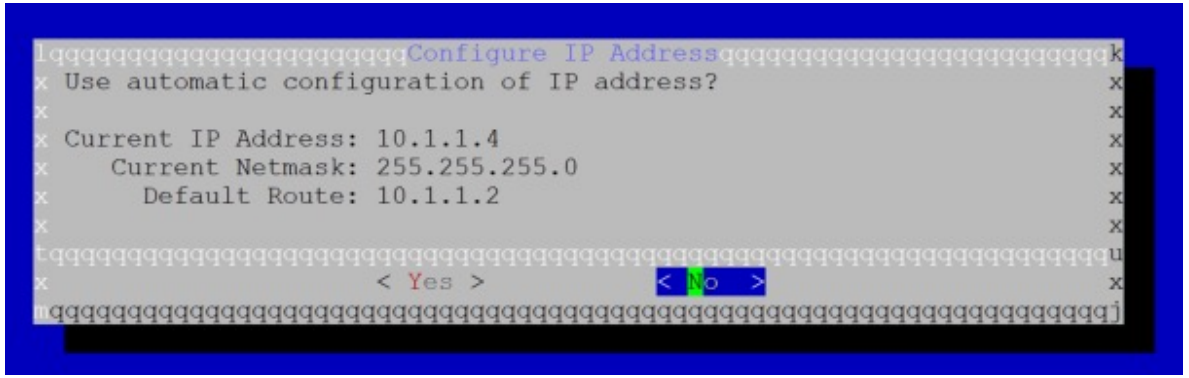
2.03 Identify the configured management-IP address

GUI



TMSH

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



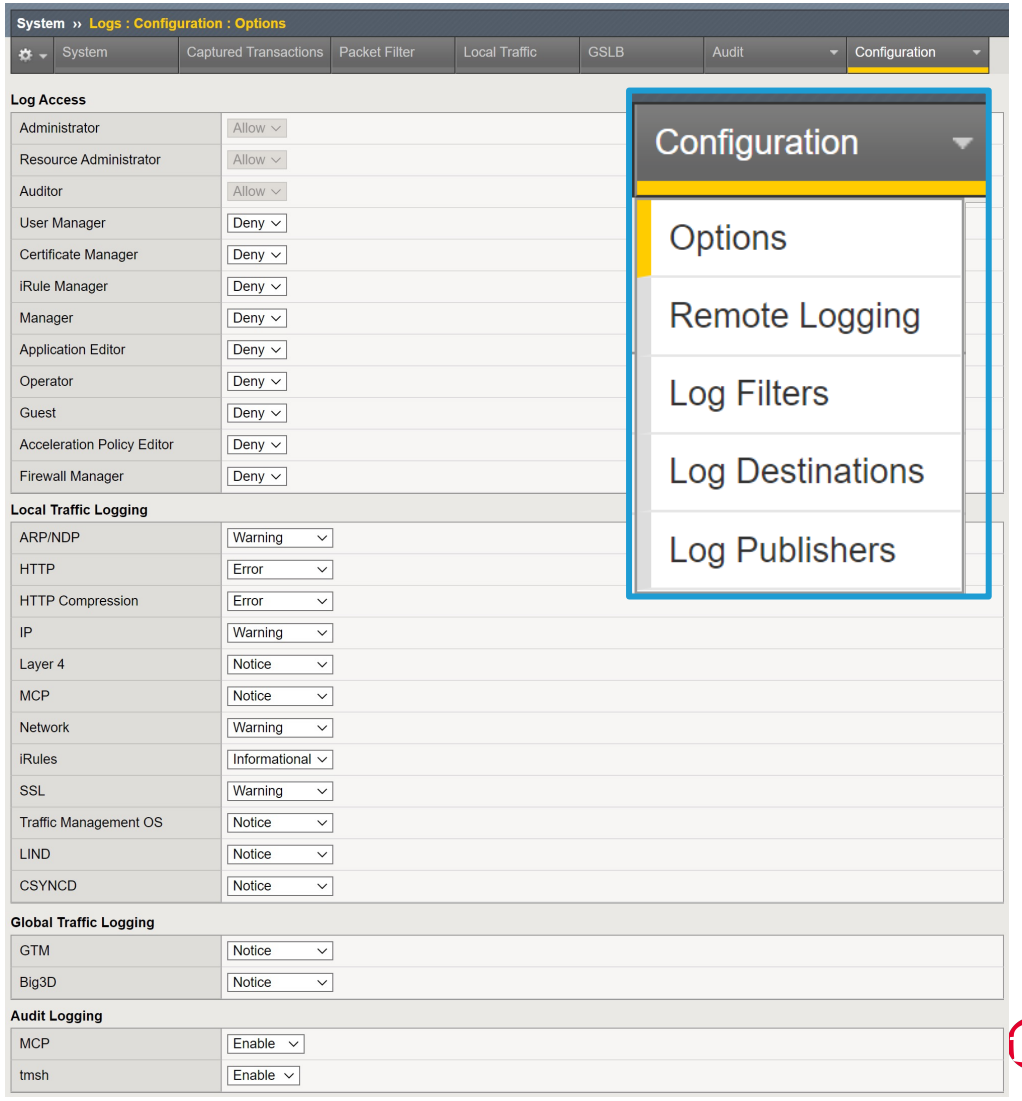
“config” utility at the linux prompt

©2022 F5 CONFIDENTIAL

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



 ©2022 F5 CONFIDENTIAL

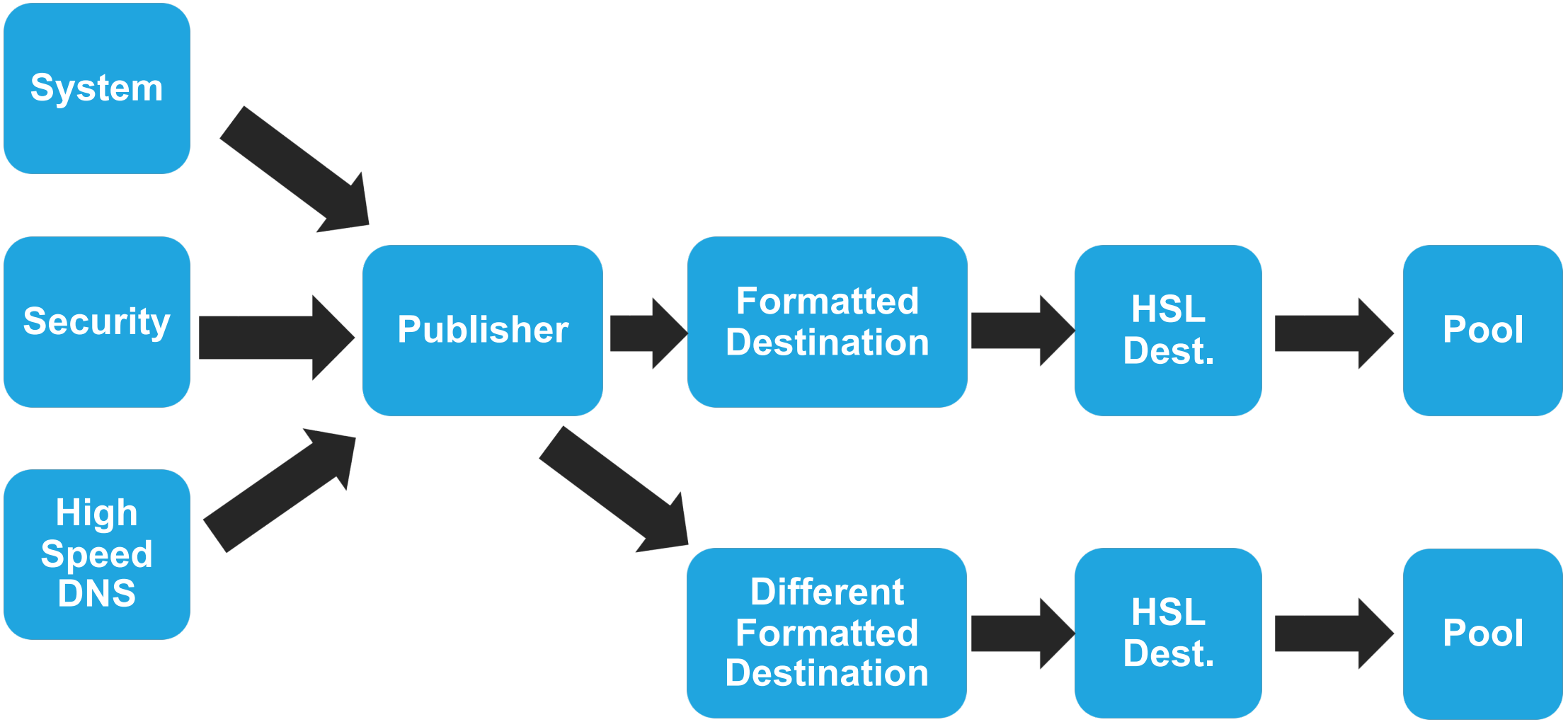
Remote Logging Steps

1. Create a Pool of logging server(s)
2. Create an HSL Destination (define the protocol TCP/UDP and Poo)
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

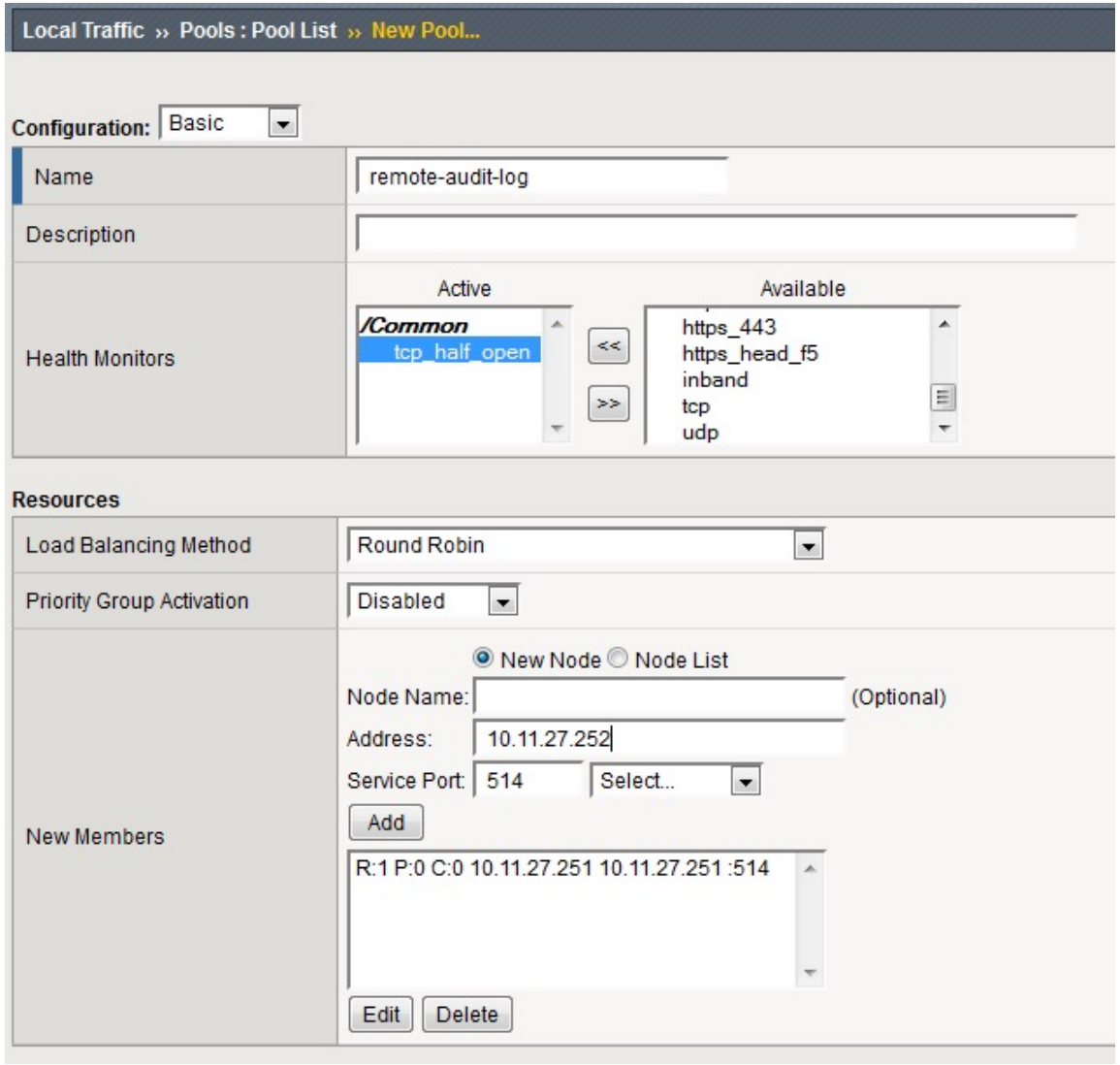
©2022 F5

Logging Overview



©2022 F5

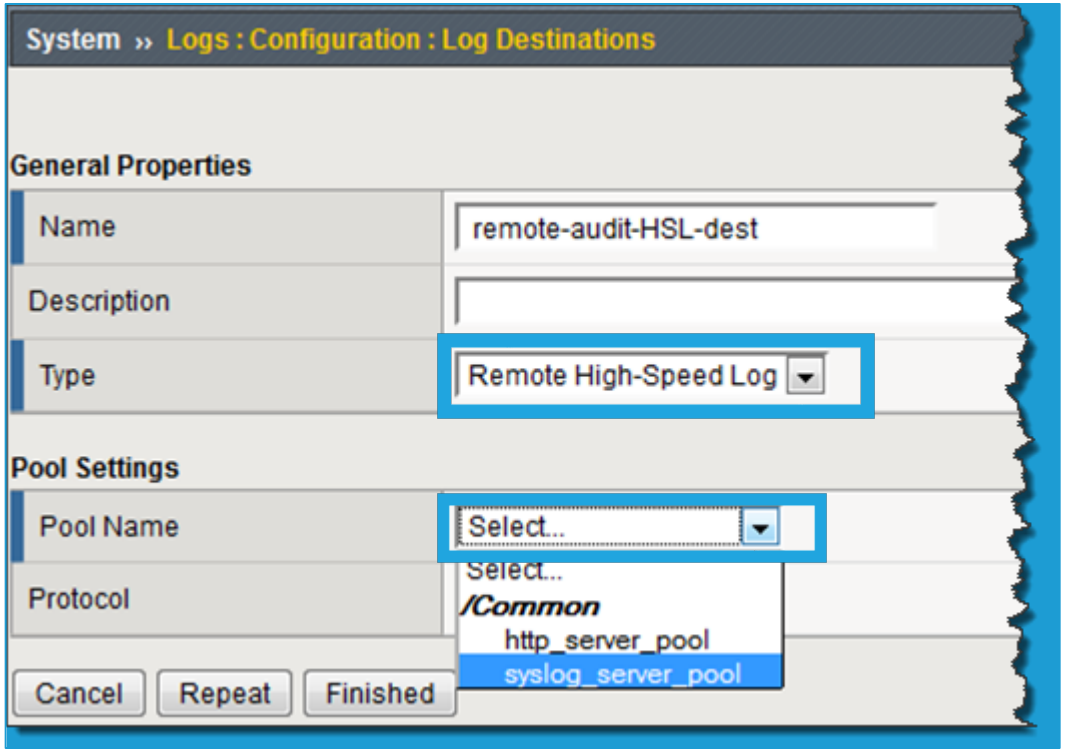
Pool Creation - GUI



 ©2022 F5

High-Speed Log Destination Creation

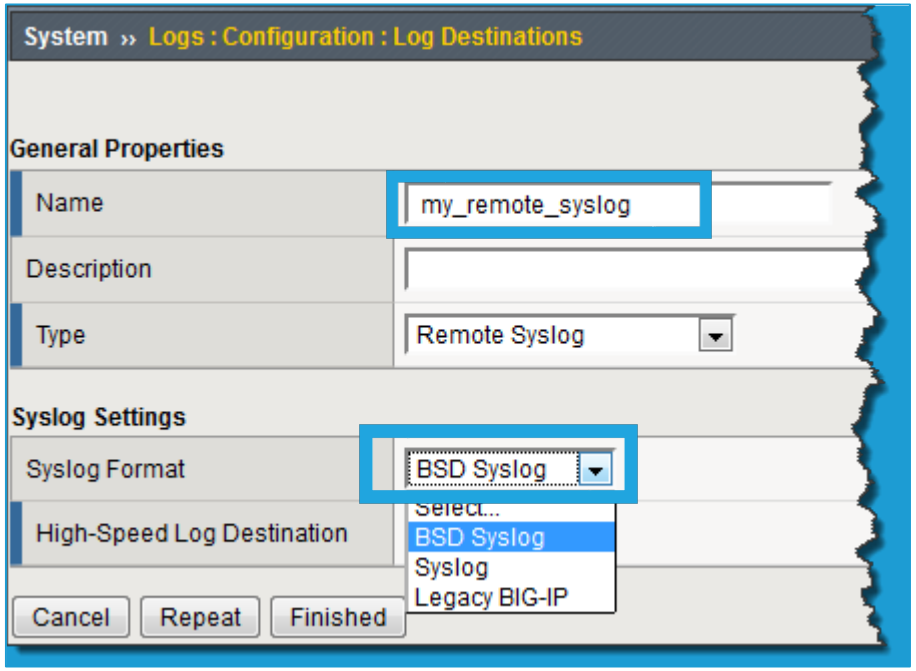
- Unformatted
  - This defines HSL destination the messages go to, not what they look like
  - Must be create before formatted destinations

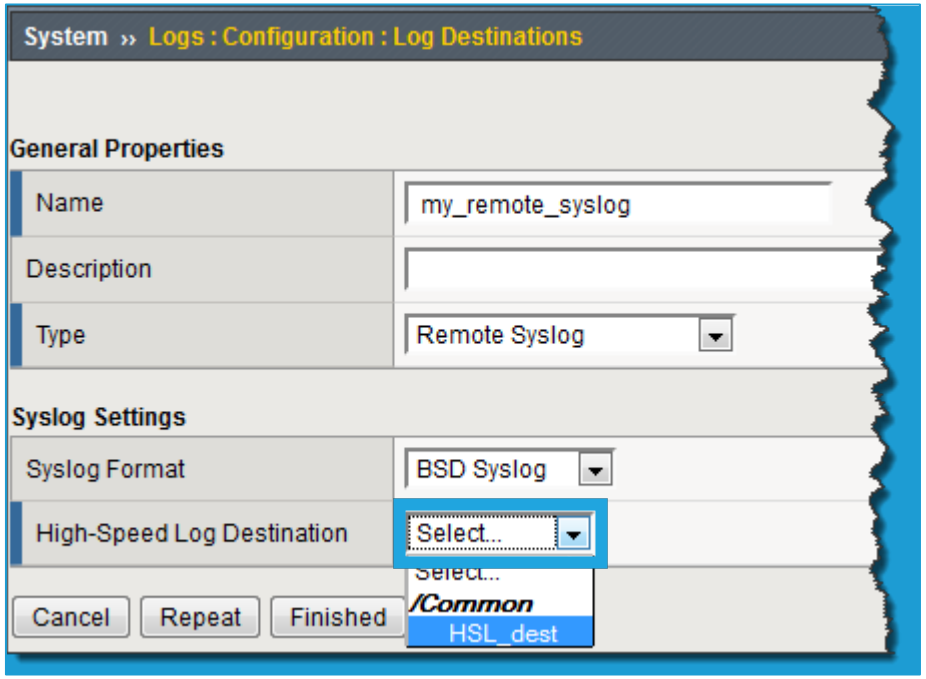


©2022 F5

Remote Syslog Destination Creation

- Name your log destination
  - Select a syslog format
  - Select a High-Speed Log Destination
    - Unformatted Destination you created earlier

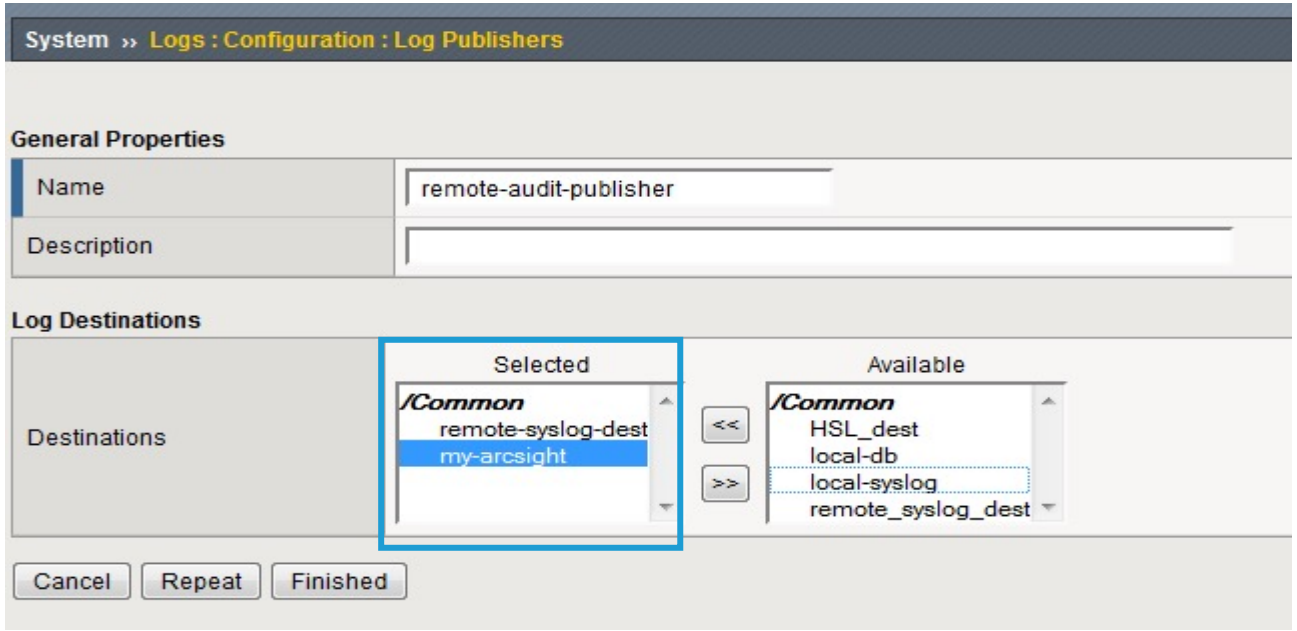




©2022 F5

Log Publisher

- A Publisher is a collection of Destinations
- Configuration Elements:
  - Choose a unique name for this Publisher
  - (Optionally) Enter a Description
  - Select Destination(s) from the available choices



©2022 F5

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

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

©2022 F5

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

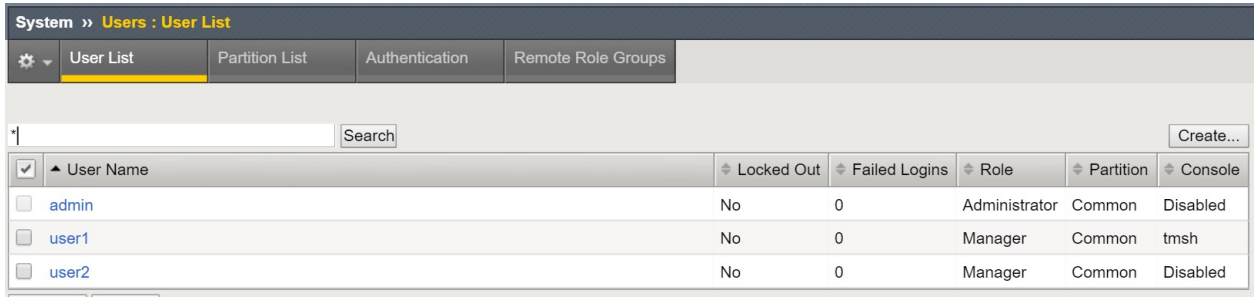
2.08 - Explain the uses of user roles, administrative partitions, and route domains

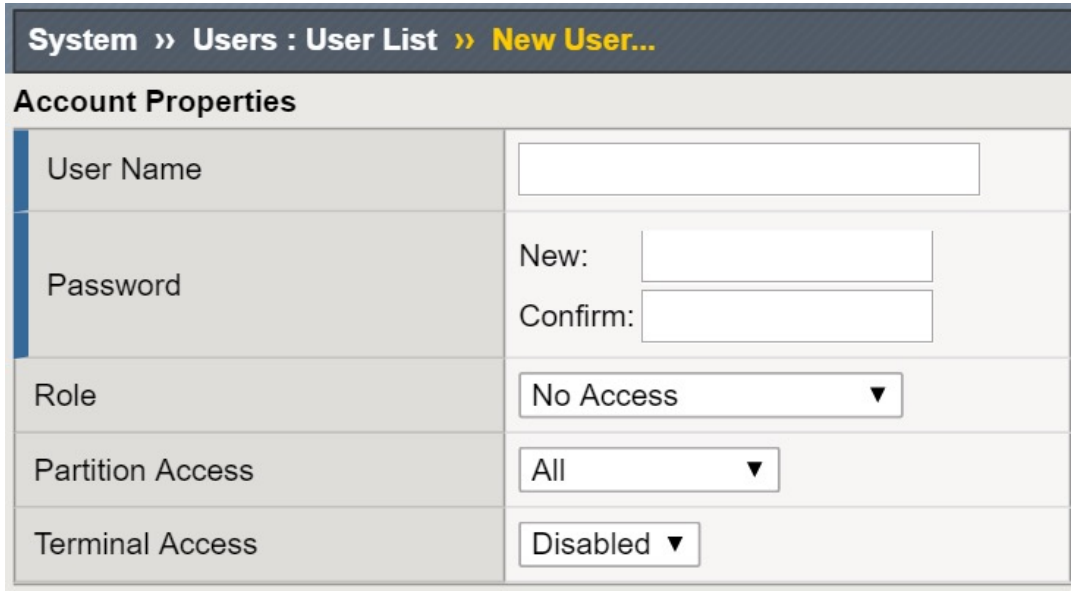
- Explain how to restrict access to LTM using user roles
- Discuss the benefits of administrative partitions
- Apply user roles to administrative partitions
- Explain the functionality of route domains
- Summarize how the 3 technologies can be used together

©2022 F5

2.08 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

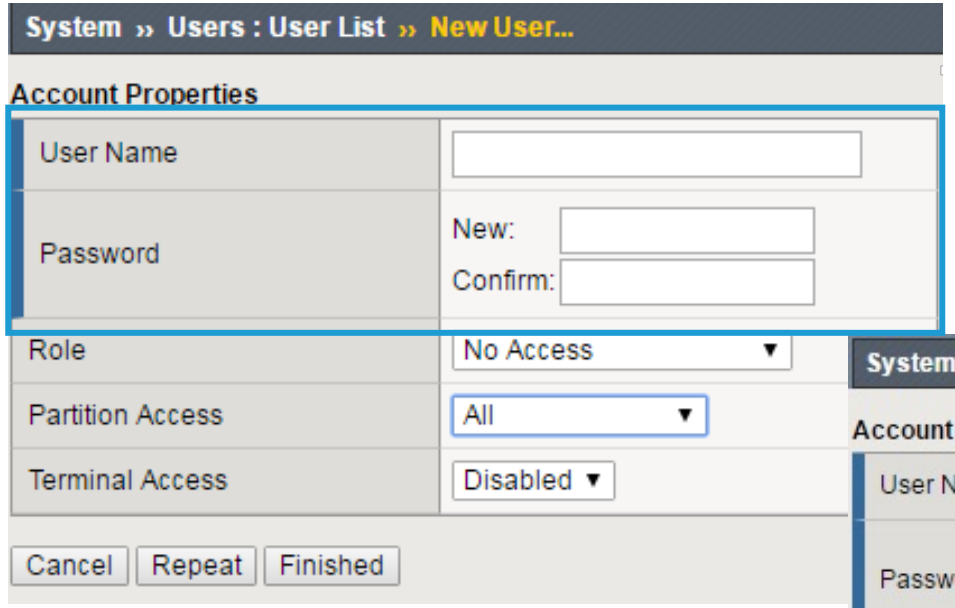
- Advanced Shell

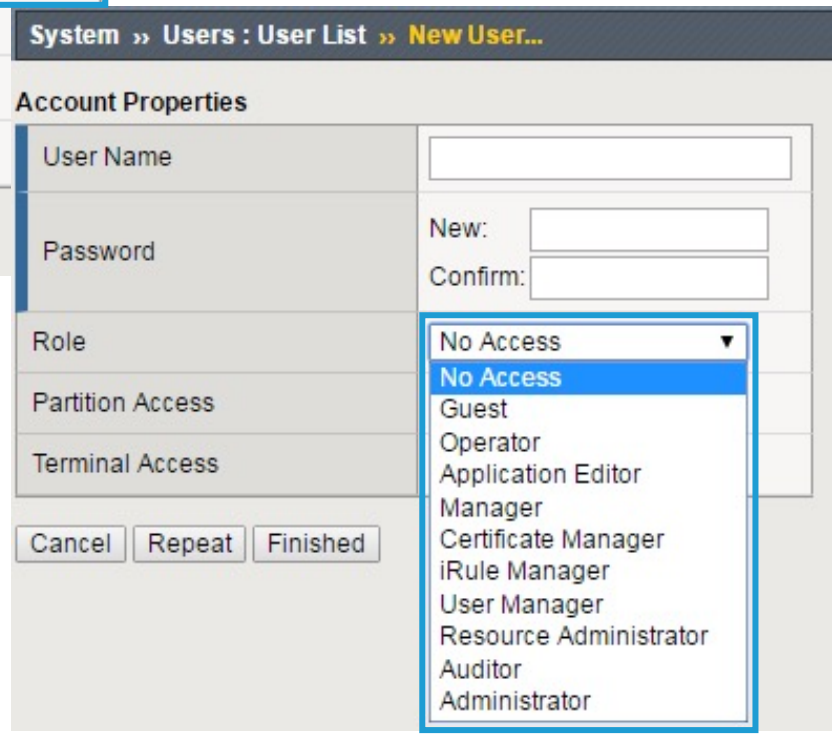
  Permits user access to the Linux prompt

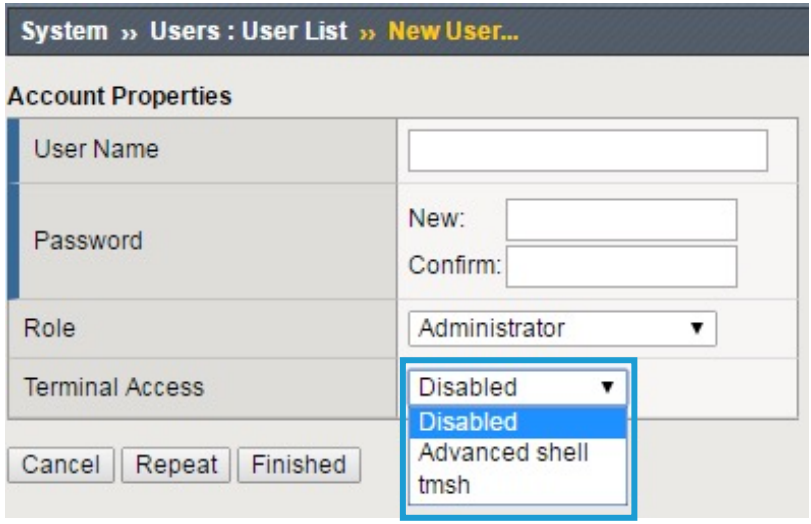
Administrator and Resource Administrator only

2.08 Explain how to create a user

Manual : BIG-IP Systems: User Account Administration







 ©2022 F5

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**

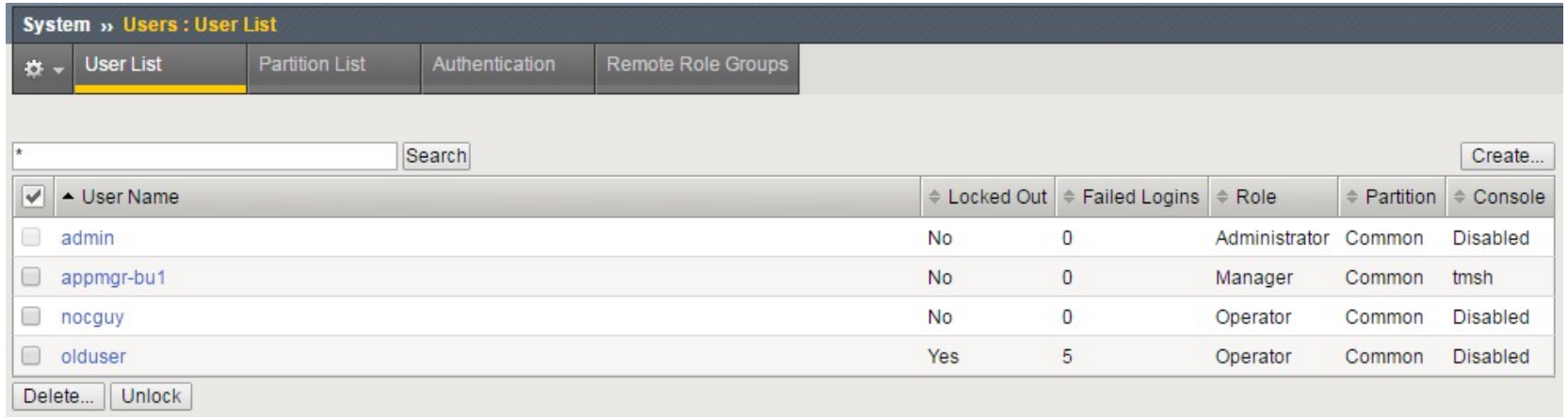
  Grants users permission to modify existing nodes, pools, pool members, and monitors.
- **Manager**

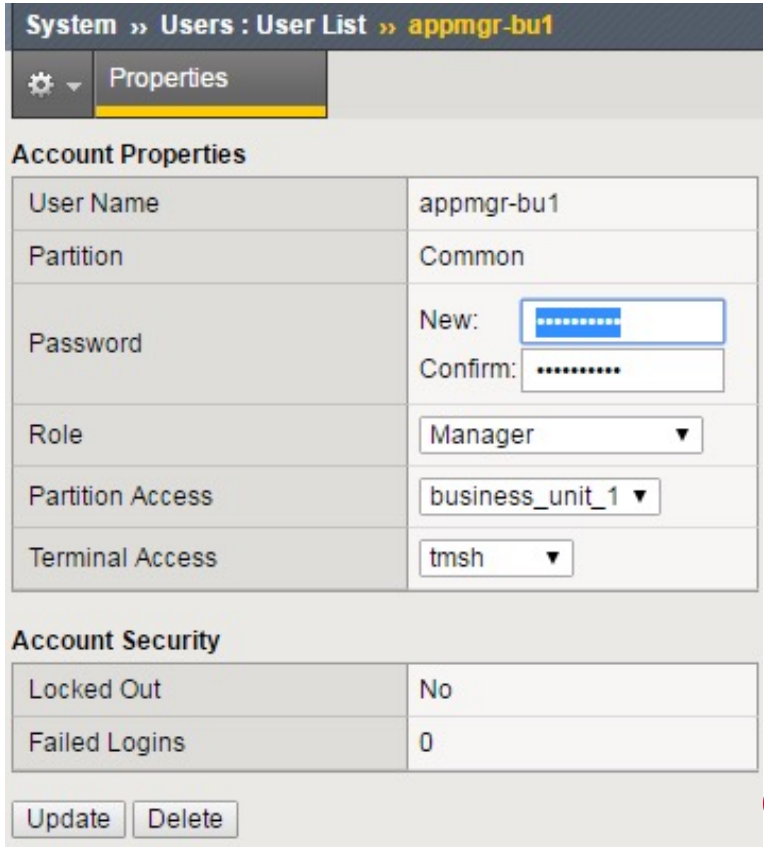
  Permission to create, modify, and delete virtual servers, pools, pool members, nodes, custom profiles, custom monitors, and iRules.
- **Administrator**

  Grants users complete access to all objects on the system.

©2022 F5 CONFIDENTIAL

2.08 Explain how to modify user properties



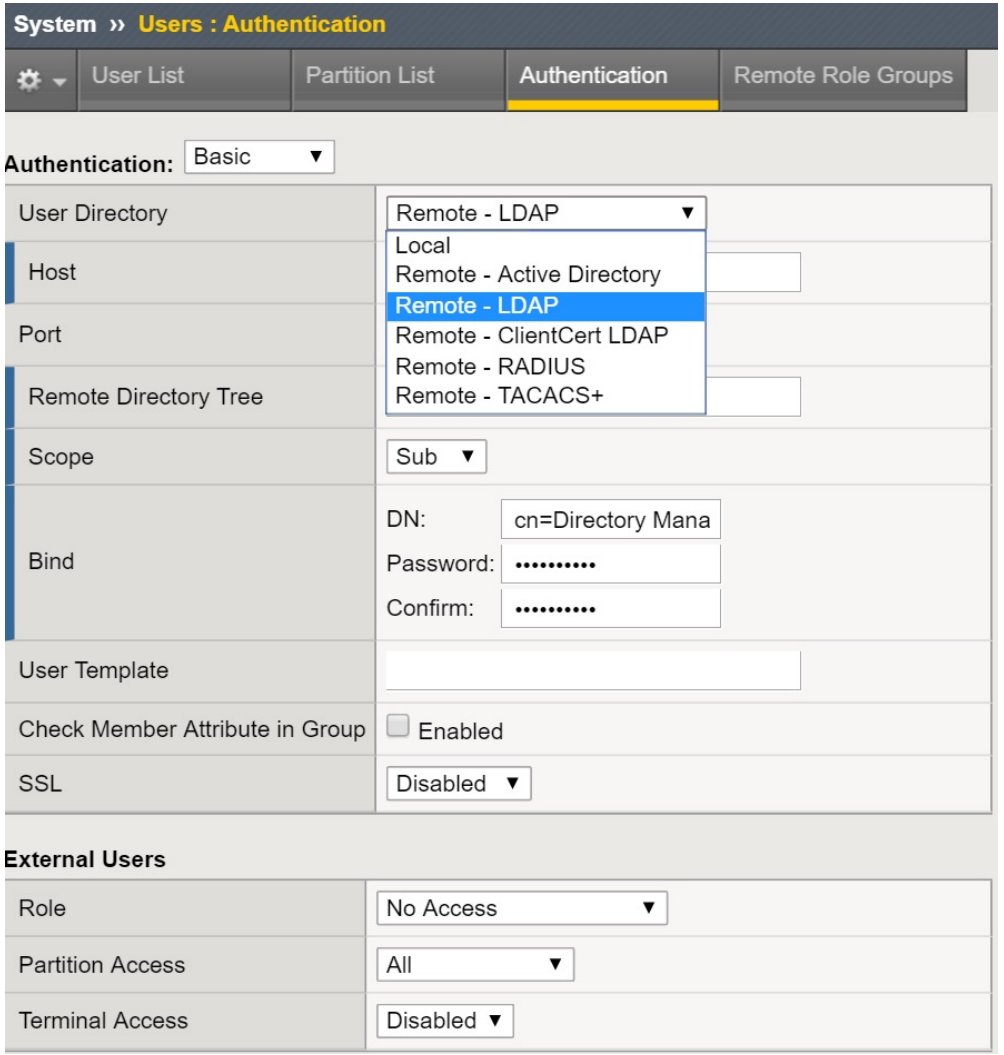


 ©2022 F5 CONFIDENTIAL

2.08 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

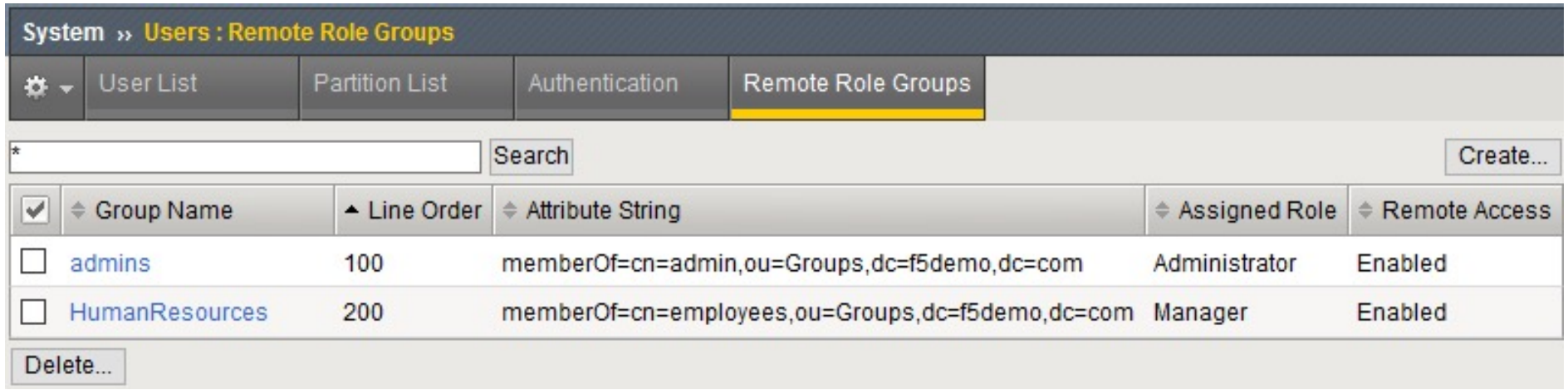


 ©2022 F5 CONFIDENTIAL

2.08 Explain use of groups using remote authentication provider

Manual : BIG-IP Systems: User Account Administration

- For a remote group you can chose 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.



©2022 F5 CONFIDENTIAL

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

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

©2022 F5

Topic Resources

- MANUAL CHAPTER: VIRTUAL SERVERS
- Manual Chapter : Session Persistence Profiles

©2022 F5

 ©2022 F5

 ©2022 F5

F5 Certification Exams

Solutions Expert

Security Solutions 401

Cloud Solutions 402

Future Enterprise

Future Exams

Technology Specialist

LTM Specialist (b) 301b

LTM Specialist (a) 301a

DNS Specialist 302

ASM Specialist 303

APM Specialist 304

Future Exams

Administrator

TMOS Administration 201

Future Exams

Pre-Sales Fundamentals 202

Application Delivery Fundamentals 101

Sales Professional

Secret Sauce!

- Know thyself! Morning person or afternoon person? Schedule exams accordingly
- Prometric has been added as an authorized testing facility (after a several year hiatus)
- 2 forms of photo ID required (license or company badge, and passport for example)
- Dedicate enough time for exam preparation!
- Answer all questions the first time through – no exceptions!
- Mark 10 questions for review at most
- Do NOT change an answer unless you are 100% sure you have initially answered wrong. Your first, best guess is usually correct (you don't want to change a correctly answered question!)
- Use the F5 exam "Blueprint" to understand what topics you will be tested on
- A minute to win it!
- 67.5 seconds per question (80 questions, 90 minutes – do the math..)
- F5 is VERY good at presenting "distractors" to students
- When trying to fill knowledge gaps, map the testing topic section to a Knowledge (K) document
- Aim high, and fight for every question
- Taking a practice exam is absolutely recommended ($25 for each, $40 for two) – no more than 2 attempts

The great Vince Lombardi told his new team in 1959 that they were going to relentlessly chase perfection. He said, we will never achieve this, but in the process, we will catch excellence!

©2022 F5

Reminder: Up Next

You have the option to attend one of the 3 additional sessions below.

Time	Session
12:30pm - 2:00pm	“Upgrade to the Future with Journey”
12:30pm - 2:00pm	“Deliver SaaS with New Distributed Cloud Platform”
12:30pm - 2:00pm	“Automate and Accelerate Your Application Services”

©2022 F5