Getting Started with BIG-IP

Last update: 11 June 2025

Contents

1 – Intro to BIG-IP System

Architecture

- Default deny system
- Full proxy architecture
    - allow client-side connection can have different connection behaviour than server-side connection

Internal Structure

- Two key functions
    - Application delivery services
        - TMOS (Traffic Management OS) → different independent modules run on top of TMOS
        - Examples: LTM, APM
    - Administrative function
        - Linux OS
        - TMOS Shell or GUI

BIG-IP Device

- Pin out references
- LCD
    - Clearing the LCD and Alarm LED remotely

BIG-IP Configuration Tools

- GUI
    - https://<management-ip>
    - https://<self-ip-address>
- CLI
    - Linux; TMOS Shell (TMSH)
    - Console
    - management-ip; self-ip

2 – Setting Up BIG-IP

Configure Management Interface

- Connect via:
  - 192.168.1.245/24 with no default gateway specified
  - Console
- References:
  - Overview of management interface

Changing Default Administrative Passwords

- Password becomes expired on new device installation
- References:
  - First time reset of root and admin passwords
  - Secure password policy configuration

Activating BIG-IP License

- device is preloaded with base registration key
- base key → generated dossier → send dossier to F5 license server → generate license → bring license back to BIG-IP → finish licensing process on BIG-IP
- recommended to perform manually so that backups can be kept at each step

Provisioning BIG-IP System

- Licensing determines software modules
  - Licensed → can be provisioned
  - Unlicensed → can be provisioned but will not work
  - Limited → can be provisioned but have limited functionality
- Provisioning options (Under "Provisioning" column)
  - nominal → minimum resources needed for module functionality (recommended settings)
  - minimum → amount require to enable the module
  - dedicated → module is the only one provisioned on the system. All other modules' provisioning is set to "None".

Installing Device Certificate

- SSL certificates for administrative tasks and inter-system communication
- BIG-IP self-signed (default) / CA-signed certificate (optional)
- Considerations:
  - Correct location: `` `/config/httpd/conf/ssl.crt/server.crt` ``
- References:
  - Overview of BIG-IP device certificates
  - SSL device cert and key pair creation
  - Renewing self-signed SSL device

Platform Configuration

Management

- IPv4 IPv6 dual stack support on management interface

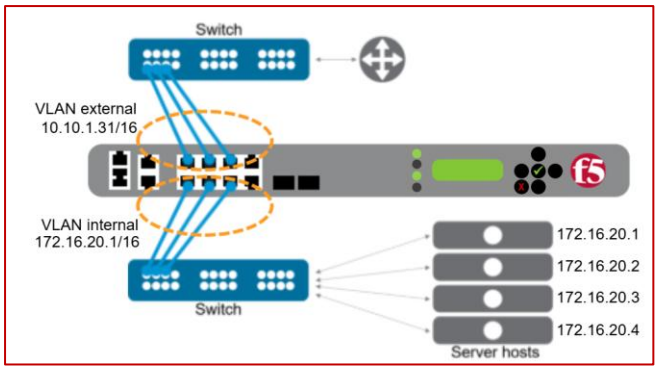
Time

- hardware clock (even when device is unplugged), for initialising the operating system clock during boot
- OS clock, stores time according to time zone configured
  - `` `date MMDDhhmmYYYY.ss` ``
- NTP Configuration

Access

- Recommended use of role based access
- Restricting access to config utility by source IP

Network and High Availability (HA)

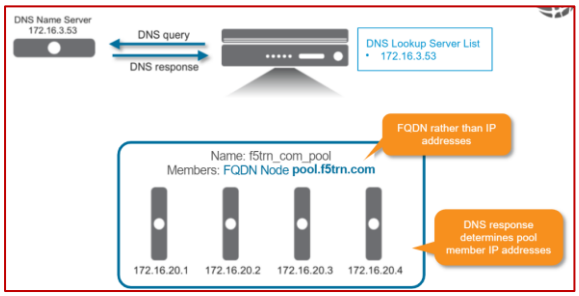


- Self-IP → address space for hosts in the VLAN
  - Static (non-floating) → IP address that the BIG-IP system does not share with another BIG-IP system
  - Floating → BIG-IP systems in a HA device group share
  - Each Self-IP in VLAN are auto assigned a MAC address by BIG-IP system

NTP

- synchronising clocks of computer systems in a network for accurate time
- Add NTP server onto BIG-IP "Time Server List" using IP address of FQDN

Device DNS



3 – Archiving BIG-IP Configuration

- Backup of configuration in the form of user configuration set (UCS) file → compressed file with important configuration information
    - settings for UCS files can be overridden or customised
- Use of TMSH to create a UCS:
  `` `save /sys ucs backup.ucs` ``
  Saved in `` `/var/local/ucs/` ``
- Restoring a configuration from UCS → BIG-IP system auto creates a rotating backup of current configuration and saving is as `` `cs-backup.ucs` ``.
  `` `load /sys ucs restore.ucs` ``
    - number of files in rotation is set in `` `cs_backup_rotate.conf` ``
    - after backup rotation, loaded UCS is placed in stored configuration (disk) and then load the new configuration into memory (running configuration)
    - reboot may be required