Approfondissement

Formation sur les infrastructures Cloud (VMWare, BIG IP F5, DNS, Openshift, …) et comprendre comment extraire des KPI pour se les approprier sur le domaine Capacitaire.

Agrégation des tutos en heure de vidéo regardée et en totale () :

Administrateur système & Linux : 9h (15h)

Openshift & Docker & Divers: 5h (9h)

Grafana & Prometheus: 6h (9h)

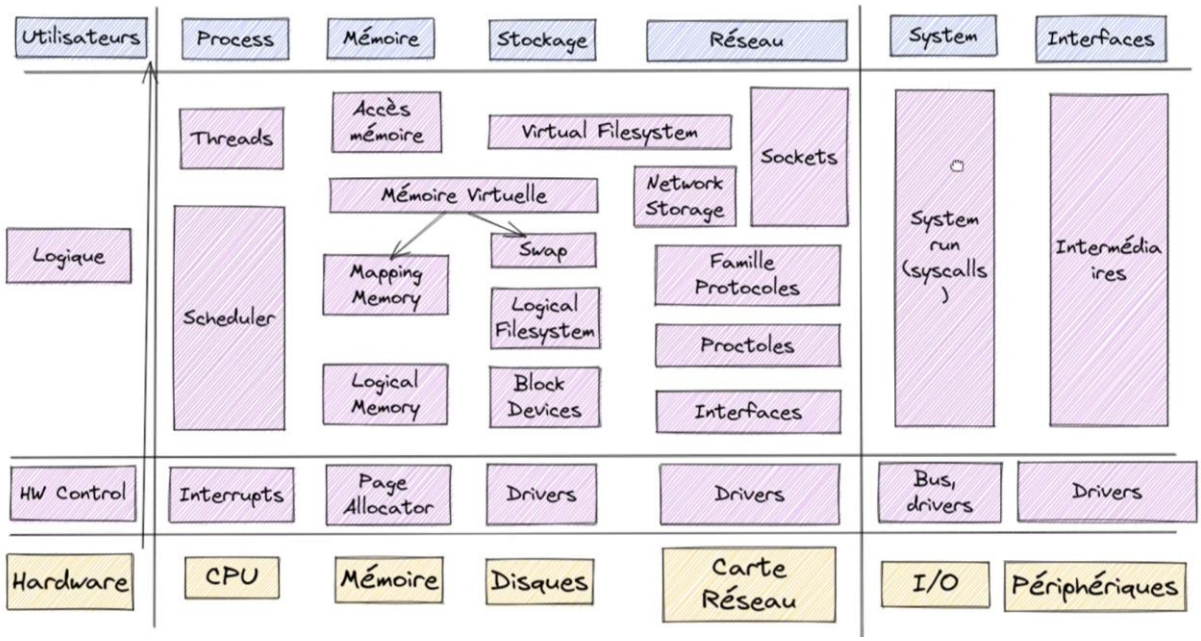
Java & Python: à venir

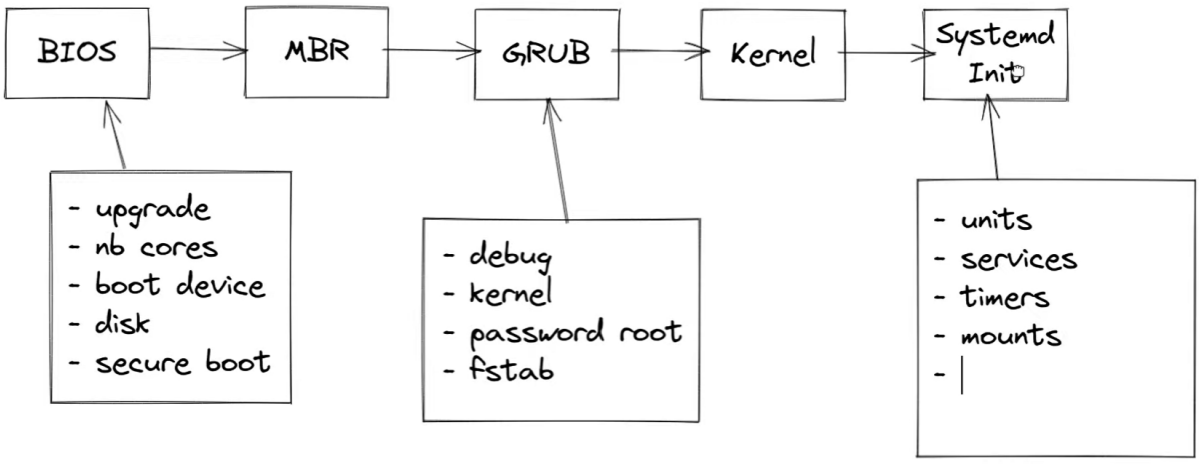
DevOps: 5h _+ (8h)

F5 BIG IP: 5h (11h)

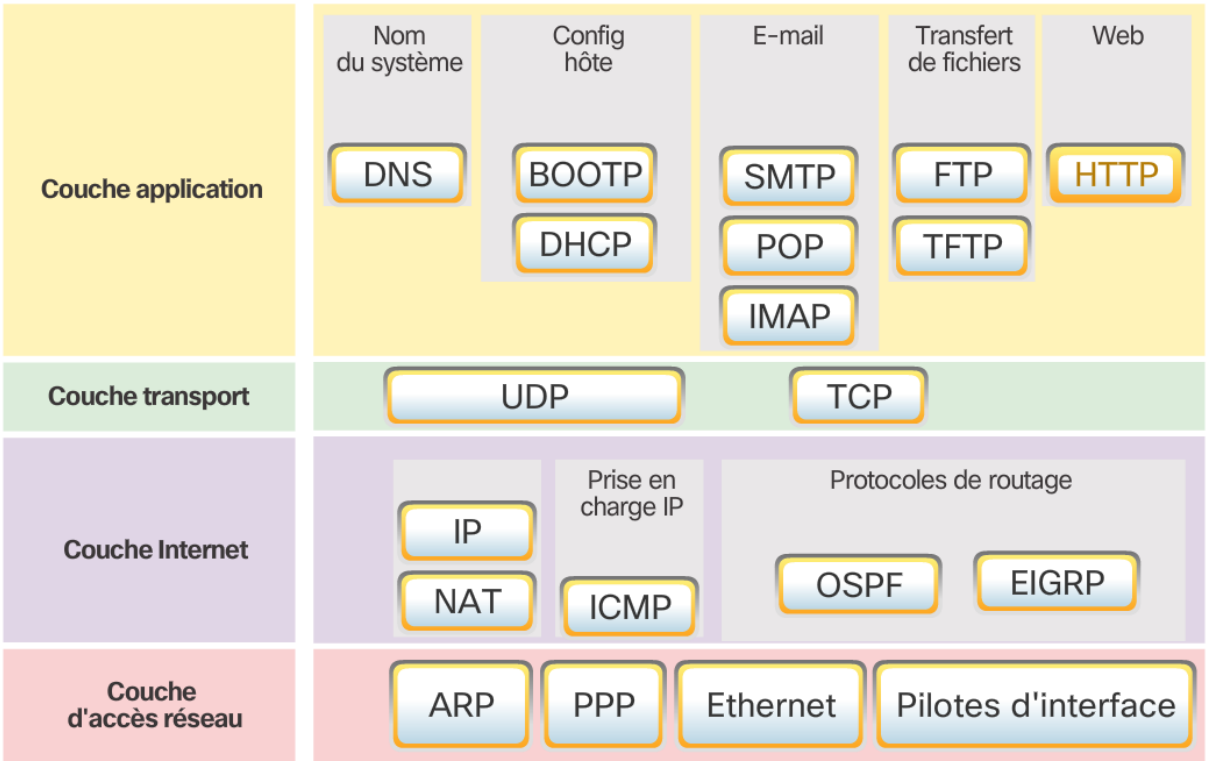
Stat: à venir

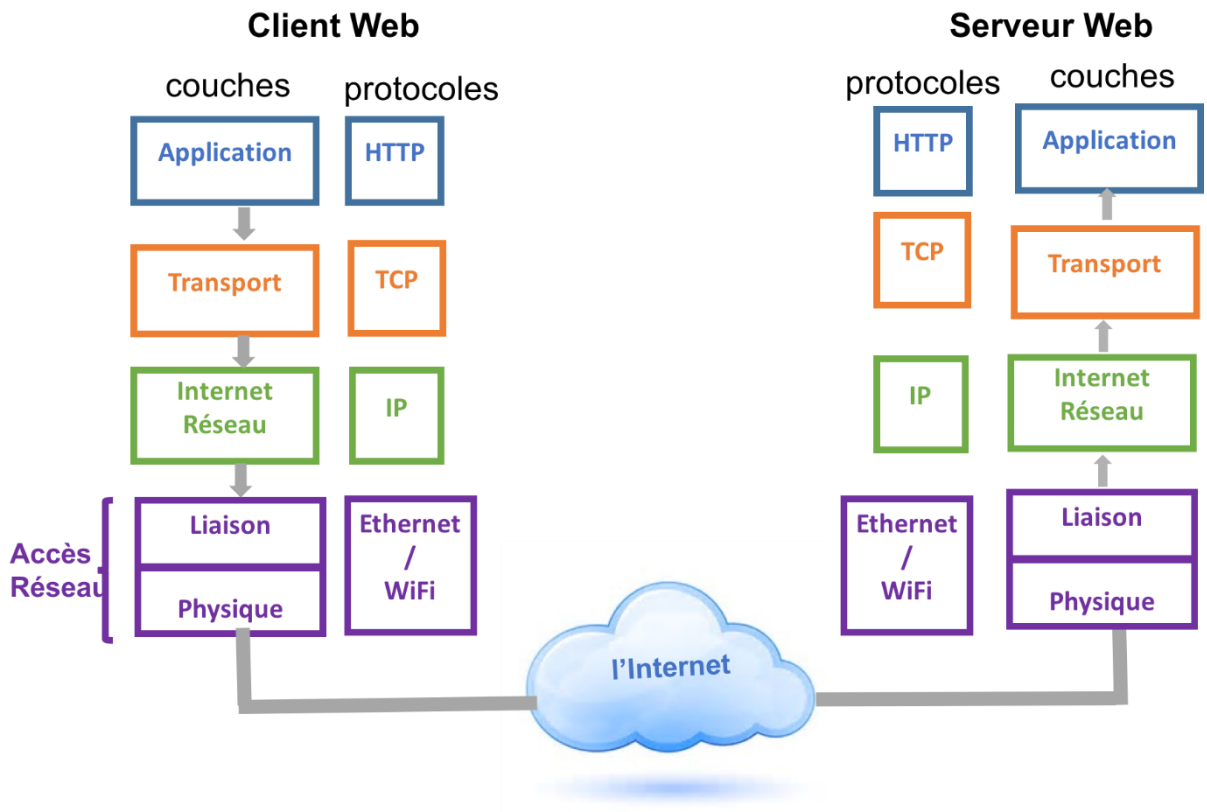
Linux





• ls : ls -l / • cd: cd /home/username/Documents • pwd: pwd • cp: cp source.txt destination.txt • mv: mv oldname.txt newname.txt • rm: rm filename.txt • mkdir: mkdir directory • rmdir: rmdir directory • touch: touch newfile.txt • cat: cat file.txt • less / more: less file.txt • mount/unmount : mount • fsck :fsck /dev/sdX • vim: vim texte.txt • grep: grep “pattern” file.txt • find: find / -name filename.txt	• chmod: chmod 755 script.sh • sudo: sudo apt update • apt / yum / dnf: sudo apt install nginx • tar: tar -xvf archive.tar.gz • ps: ps aux • top / htop: top • vmstat: vmstat • iostat: iostat • free: free -m • df: df -h • du : du -sh /path/to/directory • netstat: netstat -tulnp • sar: sar -u 5 • mpstat: mpstat • pidstat : pidstat


Couche application
Nom du système
DNS
Config hôte
BOOTP
DHCP
E-mail
SMTP
POP
IMAP
Transfert de fichiers
FTP
TFTP
Web
HTTP
Couche transport
UDP
TCP
Couche Internet
IP
NAT
Prise en charge IP
ICMP
Protocoles de routage
OSPF
EIGRP
Couche d'accès réseau
ARP
PPP
Ethernet
Pilotes d'interface


Client Web
couches
protocoles
Application
HTTP
Transport
TCP
Internet Réseau
IP
Liaison
Physique
Ethernet / WiFi
Accès Réseau
Serveur Web
protocoles
couches
HTTP
Application
TCP
Transport
IP
Internet Réseau
Ethernet / WiFi
Liaison
Physique
l'Internet

Métriques

Ressources - Performance – Santé – Openshift – Sécurité

1. Utilisation des Ressources

- **CPU**
    - Utilisation Totale du CPU (75% d'utilisation sur l'ensemble du cluster)
    - Utilisation du CPU par Pod/Nœud (50% d'utilisation CPU sur un pod spécifique)
    - Demandes et Limites de CPU (300m (millicores) demandés, 500m limites)
    - Throttling du CPU (throttling observé lorsque l'utilisation dépasse 90%)
- **Mémoire**
    - Utilisation Totale de la Mémoire (8 GB utilisés sur 16 GB disponibles)
    - Utilisation de la Mémoire par Pod/Nœud (2 GB utilisés sur un pod)
    - Demandes et Limites de Mémoire (256 MB demandés, 512 MB limites)
    - Swapping de Mémoire (100 MB de swap utilisés)
- **Stockage**
    - Utilisation du Disque (500 GB utilisés sur 1 TB disponibles)
    - IOPS (Opérations d'Entrée/Sortie par Seconde) (300 IOPS en lecture, 150 IOPS en écriture)
    - Latence de Stockage (10 ms de latence en moyenne)
    - Taux d'Erreur de Stockage (0.1% d'erreurs sur les opérations de disque)
- **Réseau**
    - Trafic Entrant et Sortant (100 Mbps entrant, 50 Mbps sortant)
    - Taux d'Erreur Réseau (0.05% d'erreurs de paquets)
    - Latence Réseau (20 ms de latence moyenne entre pods)
    - Débit Réseau (1 Gbps de capacité de réseau)

2. Performance des Applications (Grafana & Prometheus)

- **Temps de Réponse**

    - Temps de Réponse des Services (200 ms pour une requête API)
    - Durée des Transactions (500 ms pour une transaction de base de données)
- **Taux d'Erreur**
    - Erreurs d'Application (5 exceptions par minute)
    - Codes d'Erreur HTTP (10 erreurs 404 par jour)
- **Transactions par Seconde (TPS)**
    - TPS des Applications Web (100 requêtes HTTP par seconde)
    - TPS des Bases de Données (50 transactions de base de données par seconde)
- **Saturation des Ressources d'Application**
    - File d'Attente des Requêtes (20 requêtes en attente)
    - Utilisation des Pools de Connexion (70% des connexions de pool utilisées)
- **Performance des Dépendances Externes**
    - Latence des Services Externes/API (150 ms de latence pour un service externe)
    - Taux d'Erreur des Services Externes (2% d'erreurs sur les appels API externes)

3. Santé et Disponibilité

- **Statut des Pods et des Services**
    - État des Pods (95% des pods en état 'Running')
    - Redémarrages de Pods (5 redémarrages inattendus dans les dernières 24 heures)
- **Disponibilité des Services**
    - Uptime/Downtime (99.9% uptime sur les 30 derniers jours)
    - Vérifications de Santé (Health Checks) (100% des pods passent le health check)
- **Performance des Ressources Cluster**
    - Utilisation des Nœuds (70% d'utilisation en moyenne par nœud)
    - Disponibilité des Nœuds (tous les nœuds en statut 'Ready')
- **Événements du Système**
    - Logs d'Événements Kubernetes (10 alertes de niveau critique dans la dernière heure)

- **Taux d'Erreur et Performances des Applications**
    - Taux d'Erreur des Applications (0.5% d'erreurs sur l'ensemble des applications)
    - Performance des Transactions (temps de traitement moyen de 100 ms par transaction)

4. Métriques de Cluster OpenShift

- **État du Cluster**
    - État Global du Cluster (état global 'Healthy')
    - Disponibilité des Nœuds (20 nœuds, tous en statut 'Ready')
- **Planification des Ressources**
    - Utilisation des Ressources par Rapport aux Limites et Demandes (80% des ressources utilisées par rapport aux limites configurées)
    - Saturation des Ressources (saturation détectée sur 2 nœuds)
- **Scaling (Montée et Descente en Charge)**
    - Événements de Scaling Automatique (3 événements de scaling automatique dans la dernière semaine)
    - Performance des Opérations de Scaling (scaling effectué en moins de 2 minutes)
- **Surveillance des Quotas et des Limites**
    - Utilisation des Quotas (90% du quota de CPU utilisé pour un projet)
    - Dépassements de Limites (2 cas de dépassement de limite de mémoire)
- **Surveillance des Services Intégrés**
    - État des Services d'Infrastructure (tous les services d'infrastructure fonctionnent normalement)
    - Performance des Services d'Infrastructure (temps de réponse moyen de 100 ms pour le registre d'images)

5. Sécurité

- **Logs d’Audit**
    - Accès aux Ressources et Modifications de Configuration (50 modifications de configuration enregistrées dans la journée)

    - Activités Administratives (5 actions administratives critiques suivies)
- **Vulnérabilités et Conformité**
    - Rapports de Sécurité (2 vulnérabilités critiques identifiées dans les images de conteneurs)
    - Audits de Conformité (100% de conformité avec PCI-DSS dans le dernier audit)
- **Gestion des Identités et des Accès**
    - Contrôles d'Accès Basés sur les Rôles (RBAC) (200 rôles et politiques RBAC définis)
    - Authentification et Autorisation (99.9% de tentatives d'authentification réussies)
- **Chiffrement et Sécurité des Données**
    - Chiffrement des Données en Transit et au Repos (toutes les données sensibles chiffrées)
    - Gestion des Certificats et des Clés (0 certificat expiré)
- **Sécurité du Réseau**
    - Isolation des Réseaux et des Services (segmentation réseau complète mise en place)
    - Surveillance du Trafic Réseau (détection de 3 tentatives d'intrusion réseau)
- **Gestion des Menaces et des Incidents**
    - Détection des Anomalies (5 anomalies de comportement détectées ce mois)
    - Réponse aux Incidents (temps moyen de réponse aux incidents de 30 minutes)

F5 BIG-IP

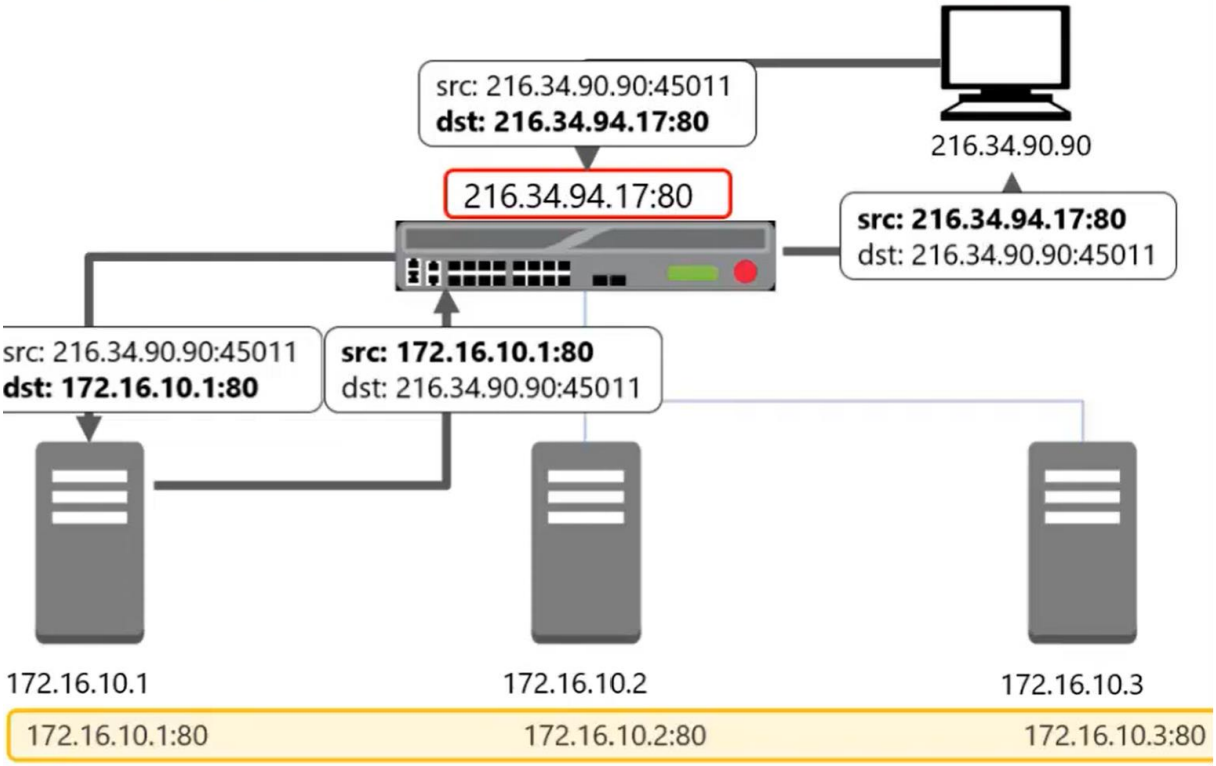
Les nodes : serveur (virtuel ou réel) avec une addresse IP

Pools Members : un nodes avec le service, IP + port

Pools : un groupe pools members

Virtual servers : listeners avec IP+Port, un écouteur associé à un pool (load balancer)

Cheminement des Paquets



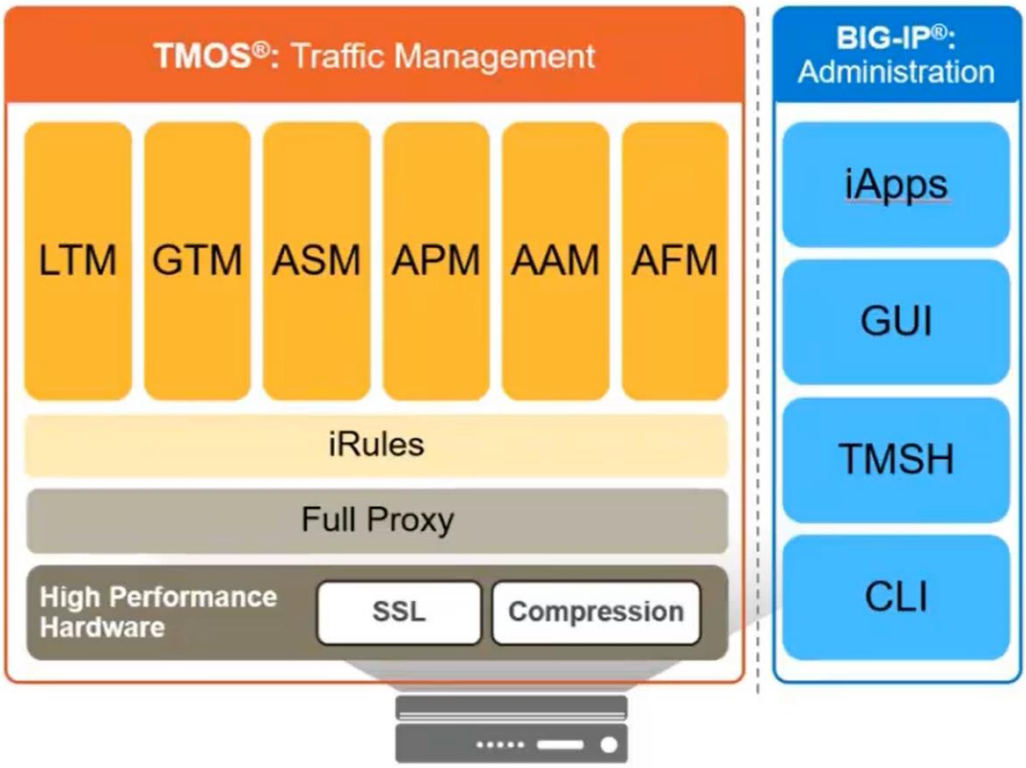
Découvrir l'offre F5

Application Delivery Controller (BIG-IP)

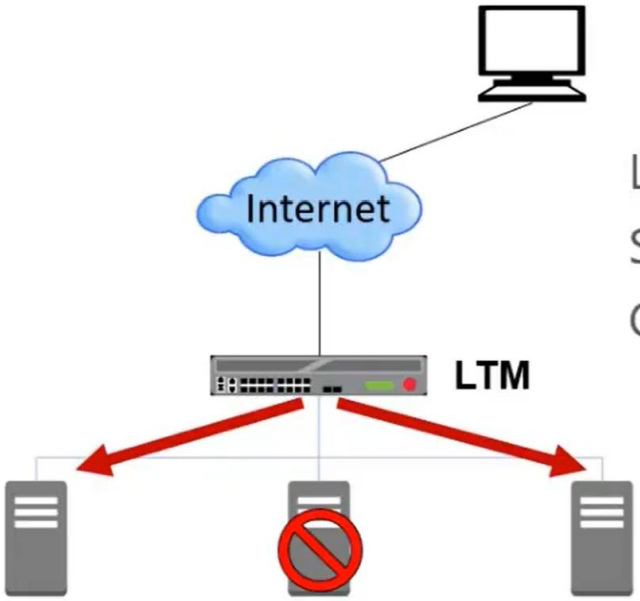
Cloud Security Services (Silverline)

Centralized Management (BIG-IQ)

Le système d'exploitation



BIG-IP Local Traffic Manager (LTM)



Load Balancing

Supervision des serveurs

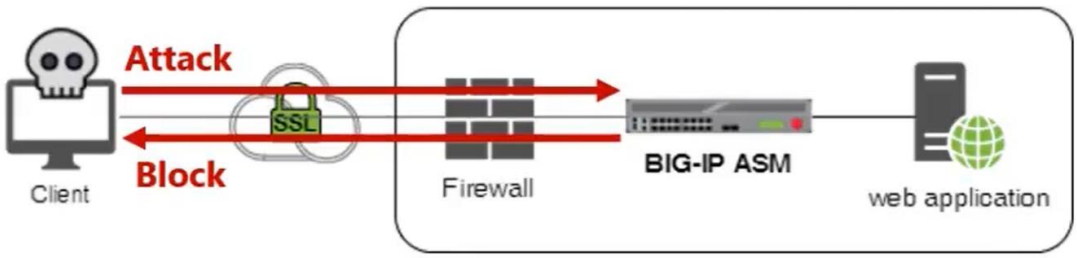
Optimisation du trafic

BIG-IP Domain Name System (DNS)

Anciennement appelé GTM
Serveur DNS intelligent
Load Balancing sur plusieurs Data Center (GSLB)
Résout les requêtes DNS vers l'IP la plus optimale
Supervision des serveurs
Alternative plus sécurisée au serveur BIND

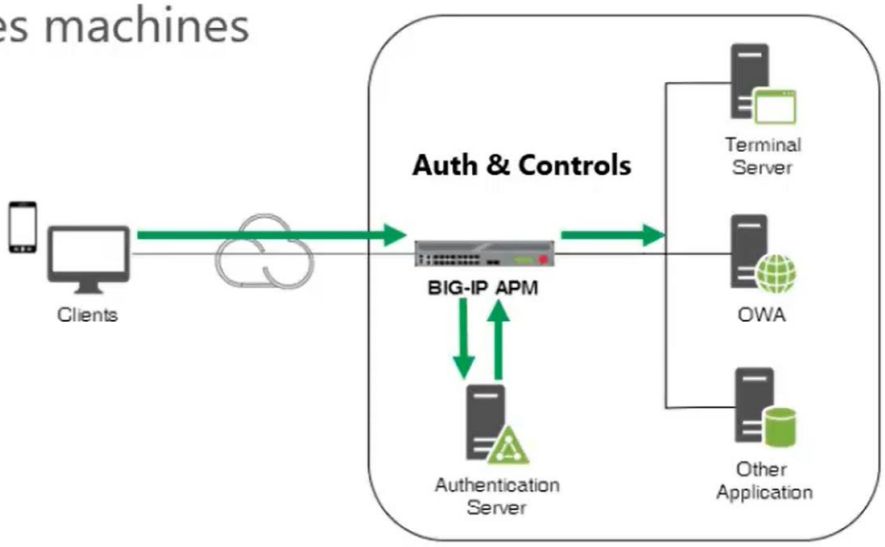
BIG-IP Application Security Manager (ASM)

Bloque les attaques connues et inconnues
Moteur d'apprentissage de l'application
Protection DDoS
Protection des Web Services (XML, JSON)



BIG-IP Access Policy Manager (APM)

Accès distant sécurisé (VPN SSL)
Authentification
Contrôle des machines



BIG-IP Advanced Firewall Manager (AFM)

Stateful Firewall (couches 3-4)
Anti-DoS
IP Intelligence

Les portails Web F5

askF5.com

Portail officiel de support et documentation

devcentral.f5.com

Communauté F5 (forum, codeshare, articles...)

university.f5.com

Formations gratuites sur les produits F5

ihealth.f5.com

Outil de diagnostic de configurations F5

Qu'est ce que le TCPDUMP?

Outil incontournable d'analyse de paquets en ligne de commandes

- Disponible sous UNIX/Linux
- Installé d'office sur F5 BIG-IP
- Supporte plusieurs protocoles (TCP, UDP, ICMP, ARP...)

TCPDUMP « sniffe » le trafic réseau entrant/sortant et le traduit en output

Comment utiliser TCPDUMP?

`tcpdump <options> <filtre>`

Les options modifient le comportement par défaut

Le filtre spécifie les paquets à capturer

```
tcpdump -i eth0 host 10.10.1.1
```

Quelques options TCPDUMP

-i	Spécifie l'interface/vlan d'écoute *-i 0.0* pour toutes les interfaces TMM
-n	Pas de résolution d'IP à nom DNS
-nn	Pas de résolution d'IP ni de port
-s	Longueur de paquet à capturer *-s0* pour ne pas limiter la longueur
-v	Plus de verbosité (ou -vv -vvv)
-w	Output vers fichier au format pcap

BIG-IP Link Controller (LC)

Load Balancing des liaisons internet

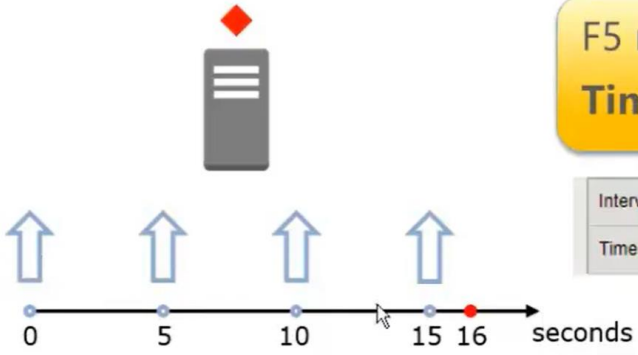
En entrée et en sortie

Selon des critères définies (débit, performance ...)

Configurer un Monitor

Interval et Timeout

- Interval = Fréquence de monitoring
- Timeout = Temps d'attente avant de considérer la ressource Down



F5 recommande:

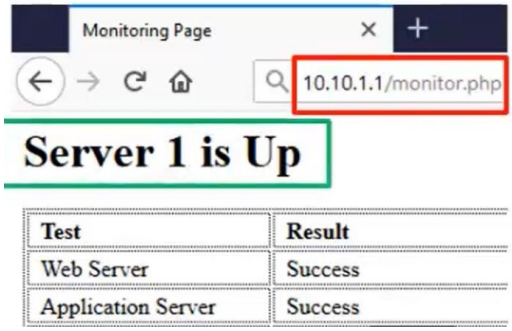
Timeout = (3 x Interval) + 1

Interval	5	seconds
Timeout	16	seconds

Configurer un Monitor

Send String et Receive String

- Send String = Commande à envoyer pour un Content Check
- Receive String = Réponse attendue



Assigner les Monitors

Pour l'utiliser, un Monitor doit être assigné :

- Monitor par défaut pour les Nodes
- A un un Node spécifique
- A un Pool entier
- A un Pool Member spécifique

Configurer un pool

Éléments nécessaires à tenir en compte

Nom (inchangé après création depuis GUI)

Adresse des noeuds et ports

Health Monitor : http, tcp, udp, ...

Load Balancing Method : Round Robin, Least Connections, ...

Types de Monitors

Address Check Monitor
Service Check Monitor
Content Check Monitor

Analyse du contenu du retour de serveur pour une expression
Reverse Setting
Application Monitor (External)

Script externe
Path Check Monitor : ICMP
Performance Monitors : SNMP, BIGIP