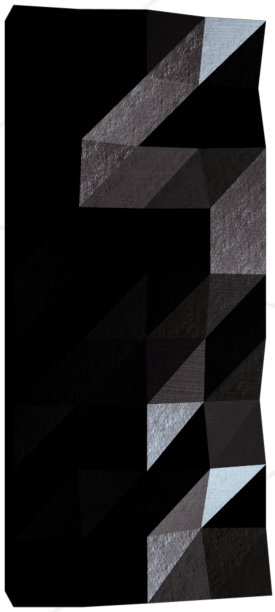

Roger-Skyline-2

Le Retour De La Vengeance De l'Adminsys

Skyline formation@slash16.org
42 Staff pedago@staff.42.fr

Résumé: Ce document est un sujet de création d'infrastructure similaire à celle de l'école par exemple. Vous y apprendrez notamment qu'un grand pouvoir implique de grandes reponsabilités.

Table des matières

Chapitre I

Préambule

Ce document est un dossier Top Secret concernant la mission `Roger-Skyline-2 Le Retour De La Vengeance De l'Adminsys`, plus communément appelée `Opération Mojitos Sous Les Tropiques`. Ce dossier contient les informations nécessaires à la production de mojitos tactiques de précision :

1. Du Rhum genre celui-ci.
2. Du sucre de Cannes.
3. De la menthe bien fraîche.
4. Du Perrier.
5. Des glacons.
6. Des citrons verts.
7. Et encore du Rhum (on sait jamais, cela peut servir).

On dit merci qui ?

Merci l'Équipe `Slash16` !

Chapitre II

Introduction

`Slash16` est un réseau de personnes passionnées par l'administration système et réseau et/ou le développement opérationnel (DevOps).

Nous avons pour but aussi de permettre une unification des connaissances entre ses membres via la mise en place de projet communs, de conférences, ou de tout autre activité rentrant dans le cadre du partage de connaissances et d'expérience professionnelle.

C'est pourquoi nous avons décidé de vous offrir deux sujets :

- Un sujet d'initiation ;
- Un sujet de création d'une infrastructure complète.

Avec ceci, vous aurez le droit à des vidéos dans votre e-learning pour comprendre les notions essentielles dont vous aurez besoin.

Chapitre III

Objectifs

Ce sujet a pour but de vous faire créer une infrastructure type entreprise. Cela signifie que vous apprendrez à mettre en place les éléments suivants :

- Coeur de Réseau
  - Gateway
  - DHCP
  - DNS
  - LDAP
  - SSL
- Services Utilitaires
  - Mail
  - Versioning
  - Backup
- Services de Production
  - Load Balancers
  - Databases
  - Workers
- Services de Pré-Production
  - Preprod DB
  - Preprod Worker
- Services de Controle
  - Automatisation
  - Monitoring

Chapitre IV

Consignes générales

Peu de règles sur ce projet, mais des règles importantes :

- L'intégralité des services demandés sur ce sujet **DOIVENT** rentrer dans les 10 VM fournies. Soyez donc attentifs si une partie du sujet demande un serveur ou un service. Si aucun indices ne vous permet de déterminer sur quel serveur doit exister un service, cela signifie que c'est votre responsabilité de déterminer comment regrouper des services différents sur un même serveur hote.
- Vos serveurs **DOIVENT** avoir des noms qui permettent d'identifier clairement et imédiatement leurs roles dans l'architecture.
- Vous **DEVEZ** rediriger les interfaces web des services sur des ports de votre choix de la Gateway . Par exemple : L'IP de la Gateway est `10.42.42.42`, l'interface web du service de Versioning est accessible sur le port `4242`, donc accessible dans votre navigateur sur `https://10.42.42.42:4242`,
- Vous **DEVEZ** faire en sorte que l'ensemble de vos serveurs soit au moins sécurisés de la manière suivante :
  - L'accès `SSH` **DOIT** se faire avec des publickeys.
  - L'accès `SSH` en root aux machines **NE DOIT PAS** être disponible directement, mais plutôt avec un user ayant les droits de devenir root.
  - Il **NE DOIT** y avoir aucun port ouvert autres que ceux des services disponible sur le serveur.
- La durée de ce projet est de 90 jours à partir de l'attribution de vos 10 VMs. Ces 90 jours incluent le temps des soutenances. Vous devez donc organiser votre temps en fonction de cette contrainte. Il n'est pas possible de mettre ce timer en pause.
- Une fois le timer de 90 jours écoulé, vos 10 VMs seront définitivement détruites automatiquement. Pensez donc à sauvegarder ce que vous souhaitez conserver au dela des 90 jours par vos prepres moyens. Il n'y aura ni backup ni archivage de vos VMs de notre coté.
- Le nombre de VMs disponibles en même temps pour tous les participants à ce projet est limité. Si aucun groupe de 10 VMs n'est disponible lorsque vous créez votre team, votre team sera placée dans une file d'attente. Vous serez notifié par

mail lorsque qu'un groupe de 10 VMs aura pu vous être attribué. Bien entendu le timer de 90 jours se déclanchera à ce moment là.

- Pour que ce soit vraiment bien clair pour tout le monde, le temps des soutenances fait **parti** des 90 jours avant la destruction de vos VMs. C'est votre responsabilité de gérer votre temps.

`Avant de commencer, nous vous conseillons de lire le sujet complètement.`

Chapitre V

Partie obligatoire

Dans cette architecture, nous allons utiliser le vocabulaire suivant :

Serveur : Un serveur est un dispositif informatique matériel (serveur physique) ou logiciel (serveur virtualisé ou VM) qui offre des services, à différents clients.

Service : Un service est une fonctionnalité ou partie de fonctionnalité mise à disposition par un composant logiciel pour assurer une tâche particulière.

`Donc service ≠ serveur, ok ?`

V.1 On est toujours copain ?

Suivre (encore) Slash16 sur Facebook, Twitter et Linkedin au cas ou vous auriez échoué la première fois.

V.2 Coeur de Réseau

Un Coeur de Réseau est l'ensemble des services nécéssaires au bon fonctionnement du réseau de l'infrastructure. Cet élément est donc particulièrement vital et doit être réalisé avec le plus grand soin.

V.2.1 Gateway

Votre premier serveur sera la gateway. Une gateway est une machine qui sépare votre réseau interne du réseau externe. Cela vous permettera d'utiliser une seule IP externe donnant accès à l'ensemble de vos serveurs internes qui auront donc des IP internes.

Connectez-vous sur `ibm-cloud.42.fr` pour y découvrir vos 10 VMs. Vous trouverez en particulier leurs noms, leurs IPs internes (`192.168.X.X`) et dans le cas particulier de la premiere VM, l'IP externe de votre groupe (`10.17.X.X`). Cette premiere VM doit être utilisée comme gateway. Vous devez la configurer afin de permettre les elements suivants :

- Le NAT des machines internes. Cela permettera aux machines internes d'acceder à l'exterieur via la gateway.
- Au fur et a mesure de la creation des services sur vos machines internes, vous devrez rediriger le port correspondant à ce service vers la machine hôte depuis la gateway.
- La redirections des ports SSH de chaque machine interne tel qu'expliqué dans la vidéo.

V.2.2 DHCP

Un DHCP est un service qui distribue des IP à toutes les machines du réseau local. Vous devez donc mettre en place un DHCP qui va associer l'adresse MAC de chacune de vos VMs à l'IP de votre choix correspondant au range indiqué dans le BackOffice `ibm-cloud.42.fr` de la forme `192.168.X.0/24`.

Cela signifie que à partir du moment où votre DHCP est fonctionnel, vous **NE DEVEZ PLUS JAMAIS** utiliser les IPs internes données dans le BackOffice `ibm-cloud.42.fr`, mais uniquement celles attribuées par le DHCP, y compris la gateway.

V.2.3 DNS

Un DNS est un service qui associe un nom de domaine à une adresse IP.

Vous devez donc mettre en place un DNS qui va associer l'ensemble de vos IPs internes au nom de domaine `slash16.local`. Chaque sous-domaine de `slash16.local` correspondra aux IPs internes de vos services. Par exemple, le serveur DHCP aura pour DNS `dhcp.slash16.local`. Vous devrez étendre la configuration du DNS au fur et à mesure de la mise en place des services de votre architecture.

V.2.4 LDAP

Un LDAP est un service d'annuaire permettant de recenser les utilisateurs de votre architecture. Vous devez mettre en place un LDAP qui contiendra les membres de votre groupe de projet ainsi que le compte admin.

La racine de votre LDAP **DOIT** être de cette forme : `DC=slash16,DC=local`.

V.2.5 SSL

Un certificat SSL atteste de l'identité d'une entreprise et permet de chiffrer les données échangées sur un réseau. Dans le cadre de cet exercice, vous utiliserez un certificat SSL auto-signé,

Vous devez mettre en place un certificat SSL auto-signé sur l'ensemble de vos services qui l'acceptent, en particulier et au minimum :

- Les Mails : `SMTPS`, `IMAPS`, `POP3S`
- le LDAP : `LDAPS`
- Tout ce qui utilise du `HTTP` (LB, Versioning, Monitoring, Worker de PreProd) : `HTTPS`

V.3 Services Utilitaires

Les services dits "utilitaires" regroupent les services utiles et transversaux d'une infrastructure.

V.3.1 Mail

Vous devez mettre en place un service mail utilisant `Postfix` et `Dovecot`. Celui-ci sera utilisé par l'ensemble de vos services en tant que `relayhost`. Votre service mail doit :

- Filtrer le SPAM autant que possible.
- Fournir une boite mail pour chaque utilisateur du LDAP présent et à venir. Vous devez donc faire en sorte qu'un utilisateur ajouté dans le LDAP ait un compte mail de manière automatique.
- Supporter `SMTPS`, `IMAPS`, et `POP3S`.

V.3.2 Versioning

Vous devez mettre en place un service de Versioning comme GitLab, Subversion ou Bitbucket qui vous servira à versionner le code de production de vos utilisateurs d'une part, et les configurations de vos services que vous jugerez nécessaires d'autre part. Vous **DEVEZ** utiliser le LDAP comme méthode d'authentification pour votre service.

V.3.3 Backup

Vous devez réaliser un service de backup de tous les services de votre infrastructure. Toutefois, c'est à vous de determiner les fichiers et dossiers qu'il est pertinent de sauvegarder pour chacun de vos services. Vous êtes libres d'utiliser un script maison ou un logiciel adapté.

`Attention à l'espace disque !`

V.4 Services de Productions

Les services de productions sont les services utilisés par les clients finaux de votre infrastructure. Par exemple, servir une application web, un service de jeu vidéo multi-joueur, un service de streaming multimédia, etc. Dans le cadre de ce projet, nous vous demandons de mettre en place les services de production d'une application web simple.

V.4.1 LoadBalancers

Un LoadBalancer (LB) est un service permettant de répartir la charge de vos services sur plusieurs serveurs de production (quelque soient ces services). Nous appelerons Workers ces serveurs de production.

Vous devez faire en sorte que la répartition de charge sur les workers soit faite en round-robin. Vous devez faire en sorte que la perte d'un des Workers soit totalement transparente pour les utilisateurs. Vous devez mettre en place un mécanisme permettant de limiter l'impact de la perte d'un LB (idéalement le rendre totalement transparent).

V.4.2 DataBases

Vous devez mettre en place deux serveurs de base de données (DB). Un des deux serveurs **DOIT** fonctionner en lecture et en écriture, ce sera le serveur `Master`, et l'autre **DOIT** fonctionner en lecture uniquement, ce sera le serveur `Slave`. Ces serveurs **DOIVENT** être répliqués, ce qui signifie que les DB doivent avoir le même contenu.

V.4.3 Workers

Les Workers sont donc les serveurs chargés de traiter les requêtes et de renvoyer les réponses à l'utilisateur final.

Vous devez mettre en place deux Workers servant l'application web suivante qui **DOIT** être disponible à l'adresse `www.slash16.local` :

- L'application web **PEUT** être codée avec le langage et les technos que vous voulez tant qu'elle reste compatible avec les éxigences de ce sujet.
- L'utilisateur arrive sur une page de connexion dont le formulaire sera lié aux DBs.
- Apres avoir entré son login et son mot de passe, l'utilisateur est redirigé vers l'une ou l'autre des deux pages suivantes en fonction de son status :
- Si l'utilisateur est "administrateur", il aura alors accès à un formulaire d'ajout d'utilisateur et de modification de n'importe quel mot de passe des utilisateurs presents dans la DB.
- Si l'utilisateur n'est pas "administrateur", il aura alors accès à un formulaire de modification de son mot de passe.
- Dans tous les cas, à chaque connexion, à chaque création d'utilisateur, et à chaque modification de mot de passe, l'application envoie un mail à l'utilisateur concerné en utilisant le service mail de votre infrastructure.

- Le code source de cette application web **DOIT** être versionné sur le service de Versioning choisi.

`Les utilisateurs présents dans la DB de cette application web n'ont aucun rapport avec les utilisateurs présents dans le LDAP. Les utilisateurs administrateurs de cette application web ne sont donc absolument pas administrateurs sur l'infrastructure.`

V.5 Services de PréProduction

La PréProduction est un ensemble de services ISO à ceux de la Production. Ces services permettent aux developpeurs des applications clientes de tester leur travail dans des conditions identiques à celles de la Production.

V.5.1 Préprod DB

Vous devez mettre en place un service de DB permettant une utilisation identique de l'application web de Production. Bien entendu, ce service de DB sera completement independant du service de DB de Production. Vous **DEVEZ** écrire un script qui met la DB de préproduction ISO à la production. Evidemment, vous **DEVEZ** le faire de manière intelligente pour ne pas impacter les services de production, locker les tables du master n'est pas envisageable.

V.5.2 Preprod Worker

Vous devez mettre en place un service de Worker permettant une utilisation identique de l'application web de Production. Bien entendu, ce service de Worker sera complètement independant du service de Worker de Production. Vous devez écrire un script qui met le Worker de préproduction ISO à la production. La préprod aura aussi accès au depot de production sur le service de Versioning pour réaliser vos mises en préproduction. Cela implique donc **OBLIGATOIREMENT** la présence d'une branche Git de production et d'une branche Git de preproduction.

V.6 Services de Contrôle

Les services de Contrôle sont les services qui permettent d'améliorer et de simplifier la maintenance et le deployement de l'infrastructure.

V.6.1 Automatisation

Un service d'automatisation a pour but de permettre à l'adminsys de ne plus intervenir directement sur ses serveurs mais uniquement à partir de ce service.

Vous devez donc mettre en place un service d'automatisation avec le logiciel de votre choix, comme par exemple, Ansible, Salt, Puppet ou Chef. Votre service d'automatisation devra contenir l'ensemble de vos scripts de mise en production, mise en pré-production, de déploiement de nouvelles configurations sur vos serveurs, de backup, etc...

V.6.2 Monitoring

Vous devez mettre en place un service de monitoring qui monitore l'ensemble de vos services et de vos serveurs avec le logiciel de votre choix, comme par exemple, Shinken, Centreon, ou Zabbix. Celui-ci devra disposer d'une interface web. Vous **DEVEZ** utiliser le LDAP comme méthode d'authentification pour votre outil de monitoring.

Dans le cas ou vous choisissez de réaliser le service de Syslog présent dans la section bonus de ce sujet, vous **DEVEZ** faire en sorte que les logs de ce service soit sur une interface web pour la consultation des logs de votre Syslog.

Chapitre VI

Partie bonus

Une fois la partie obligatoire de votre architecture fonctionnelle et testée de manière exhaustive, vous pouvez ajouter les services listés dans ce chapitre. Pendant la soutenance, l'évaluation de la partie bonus ne sera prise en compte que si et seulement si tous les points de la partie obligatoire ont été obtenus.

VI.1 Syslog

Vous pouvez mettre en place un service Syslog qui regroupe l'ensemble des logs de vos machines.

Vous **DEVEZ** faire en sorte que les erreurs de type `Emergency`, `Alert` et `Critical` vous soient envoyées par mail.

Attention, tous les services ne savent pas syslogger nativement, à vous de trouver des solutions pour que leurs logs soient quand même exportés.

VI.2 VPN

Vous pouvez mettre en place un service VPN pour accéder à l'ensemble de vos machines sur un réseau extérieur. Celui-ci **DOIT** être lié à votre LDAP.

VI.3 XMPP/Jabber

Vous pouvez mettre en place un service de type `XMPP` comme Jabber.

Celui-ci **DOIT** être lié à votre LDAP et contiendra les canaux nécessaires à vos utilisateurs.

VI.4 FTP

Vous pouvez mettre en place un service FTP. Celui-ci **DOIT** être lié à votre LDAP et être en FTPS.

Chapitre VII

Rendu et peer-évaluation

Rendez votre travail sur les serveurs qui vous sont attribués. Seul le travail présent sur vos serveurs sera évalué en soutenance.