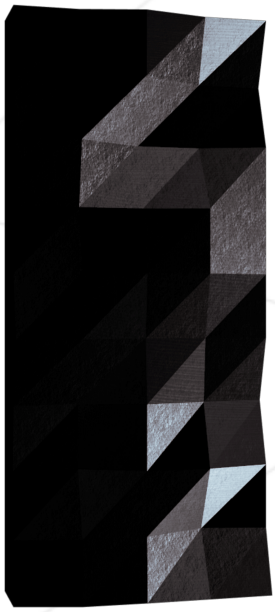

Roger-Skyline-2

Return of the Sysadmin

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

Summary: This document is about creating an infrastructure similar to that of the school. In particular, you will learn that great power implies great responsibility.

Contents

Chapter I

Foreword

This document is a Top Secret file concerning the mission `Roger-Skyline-2: Return of the Sysadmin`, also known as `Operation Mojitos Under The Tropics`. This file contains the information needed to produce high precision tactical mojitos:

1. Rum like this one.
2. Sugar.
3. Fresh mint.
4. Mineral water.
5. Ice cubes.
6. Limes.
7. More rum (we never know, it might come in handy).

Whom do we thank?

We thank team `Slash16`!

Chapter II

Introduction

`Slash16` is a network of people passionate about system and network administration and/or development operations(DevOps).

We also aim to share knowledge among our members through joint projects, conferences, or any other activities with the goal of sharing knowledge and professional experience.

That's why we've decided to offer you two subjects:

- A subject on initiation.
- A subject on creating a complete infrastructure.

In addition to this document, you have the access to e-learning videos to help you understand the essential concepts you will need.

Chapter III

Goals

This subject is intended to make you create a company-type infrastructure. This means that you will learn how to set up the following:

- Core Network
  - Gateway
  - DHCP
  - DNS
  - LDAP
  - SSL
- Utility Services
  - Mail
  - Versioning
  - Backup
- Production Services
  - Load Balancers
  - Databases
  - Workers
- Pre-Production Services
  - Pre-Production DB
  - Pre-Production Worker
- Control Services
  - Automation
  - Monitoring

Chapter IV

General instructions

This project has few rules, but they are important:

- All services requested in this subject **MUST** fit into the 10 VMs provided. So be careful if part of the subject requires a server or a service. If there are no clues to determine which server a service should exist on, it means that it is your responsibility to determine how to group different services on a single host server.
- Your servers **MUST** have names that clearly identify their roles in the architecture.
- You **MUST** redirect the services' web interfaces to ports of your choice from the Gateway. For example: The IP of the Gateway is 10.42.42.42, the web interface of the Versioning service is accessible on port 4242, therefore accessible in your browser on `https://10.42.42.42:4242`.
- You **MUST** make sure that all of your servers are at least as secure as follows:
  - SSH access **MUST** be done with public keys.
  - SSH root access to machines **MUST NOT** be available directly, but rather with a user being able to get root access rights.
  - There **MUST NOT** be any open ports other than those that belong to the services available on the server.
- The duration of this project is 90 days from the attribution of your 10 VMs. These 90 days include the time of the defenses. You must therefore organize your time according to this constraint. It is not possible to pause this timer.
- Once the 90-day timer has elapsed, your 10 VMs will be destroyed automatically. So remember to save what you want to keep beyond 90 days by your own means. There will be no backup or archiving of your VMs on our side.
- The number of VMs available at the same time for all participants in this project is limited. If no group of 10 VMs is available when you create your team, your team will be placed in a queue.

You will be notified by email when a group of 10 VMs will have been assigned to you. Of course, the 90-day timer will be triggered at that moment.

- To make it really clear for everyone, the time of the defenses is part of 90 days before the destruction of your VMs. It's your responsibility to manage your time.

```
Before you begin, we advise you to read the subject completely.
```

Chapter V

Mandatory part

In this document, we will use the following vocabulary:

Server: A server is a hardware (physical server) or software (virtualized server or VM) computing device that provides services to different clients.

Service: A service is a feature or functionality made available by a software component to perform a particular task.

So, service ≠ server, ok?

V.1 Are we always friends?

Follow (again) Slash16 on Facebook, Twitter and Linkedin in case you have failed the first time.

V.2 Core Network

Core Network is a set of services required for proper functioning of network infrastructure. This element is therefore particularly vital and must be done with great care.

V.2.1 Gateway

Your first server will be the gateway. A gateway is a server that separates your internal network from the external network. This will allow you to use a single external IP to access all of your internal servers which will have internal IPs.

Log in to `ibm-cloud.42.fr` to discover your 10 VMs. You will find, in particular, their names, their internal IPs (192.168.X.X) and, in the particular case of the first VM, the external IP of your group (10.17.X.X). This first VM must be used as a gateway. You must configure it to allow the following:

- NAT of internal machines. This will allow the internal machines to access the outside world via the gateway.
- As you create the services on your internal machines, you will need to redirect the port corresponding to this service to the host machine from the gateway.
- SSH port redirection of each internal machine as explained in the video.

V.2.2 DHCP

A DHCP is a service that distributes IPs to all machines in the local network. You must therefore set up a DHCP which will associate the MAC address of each of your VMs with the IP of your choice corresponding to the range indicated in the BackOffice of `ibm-cloud.42.fr` in the form `192.168.X.0/24`.

This means that from the moment your DHCP is functional, you **NEVER** have to use the internal IPs given in the BackOffice of `ibm-cloud.42.fr`, but only those assigned by DHCP, including the gateway.

V.2.3 DNS

A DNS is a service that associates a domain name with an IP address.

You must set up a DNS that will associate all of your internal IPs with the `slash16.local` domain name. Each subdomain of `slash16.local` will correspond to the internal IPs of your services. For example, the DHCP server will have `dhcp.slash16.local` for DNS. You will have to extend the configuration of the DNS as the services of your architecture are put in place.

V.2.4 LDAP

LDAP is a service used to register the users of your network architecture. You need to set up an LDAP that will contain the members of your project group as well as the admin account.

The root of your LDAP **MUST** be of this form: `DC=slash16,DC=local`.

V.2.5 SSL

An SSL certificate certifies the identity of a company and allows to verify the data exchanged on a network. As part of this exercise, you will use a self-signed SSL certificate.

You must set up a self-signed SSL certificate on all of your services that accept it, in particular and at least:

- Mail : `SMTPS`, `IMAPS`, `POP3S`
- LDAP : `LDAPS`
- Everything that uses `HTTP` (LB, Versioning, Monitoring, PreProd Worker) : `HTTPS`

V.3 Utility services

The so-called "utility" services include the useful and versatile services of an infrastructure.

V.3.1 Mail

You must set up a mail service using `Postfix` or `Dovecot`. This one will be used by all of your services as `relayhost`. Your mail service must:

- Filter SPAM as much as possible.
- Provide a mailbox for each user in LDAP - present and future.
  You must therefore ensure that a user added to the LDAP receives an email account automatically.
- Support `SMTPS`, `IMAPS`, and `POP3S`.

V.3.2 Versioning

You must set up a versioning service such as GitLab, Subversion or Bitbucket which will allow you to version the production code of your users on one hand, and the configurations of your services which you will consider necessary on the other hand. You **MUST** use LDAP as the authentication method for your service.

V.3.3 Backup

You must set up a backup service for all services of your infrastructure. However, it is up to you to determine the files and folders that are necessary to save for each of your services. You are free to use a homemade script or adapted software.

`Watch out for disk space!`

V.4 Production Services

Production services are the services used by end users of your infrastructure. For example, serving a web application, a multiplayer video game, a multimedia streaming service, etc. As part of this project, we ask you to set up the production services of a simple web application.

V.4.1 LoadBalancers

A LoadBalancer (LB) is a service that allows you to load your services on multiple production servers (regardless of these services). We will call these servers Workers.

You have to make sure that the load distribution on the workers is done in round-robin. You have to make sure that the loss of one of the Workers is totally invisible to the users. You need to put in place a mechanism to limit the impact of the loss of a LB (ideally, make it completely irrelevant).

V.4.2 DataBases

You must set up two database (DB) servers. One of the two servers **MUST** work in read and write - it will be the `Master` server, and the other **MUST** work in read only - this will be the `Slave` server. These servers **MUST** be replicated, which means that the DBs must have the same content.

V.4.3 Workers

So, workers are the servers responsible for processing requests and sending back the answers to the end user.

You must set up two workers serving the following web application that **MUST** be available at `www.slash16.local` :

- The web application MAY be coded with the language and technologies you want as long as it remains compatible with the requirements of this topic.
- The user arrives on a login page whose form will be linked to the DBs.
- After entering the login and the password, the user is redirected to one of the two following pages according to their status:
- If the user is "administrator", they will have access to a form for adding users and changing any password of the users present in the DB.
- If the user is not "administrator", they will have access to a form to change their password.
- In any case, any time you log in, create a user, or change your password, the application sends an email to the user via the mail service of your infrastructure.

- The source code of this web application **MUST** be versioned on the chosen Versioning service.

The users present in the DB of this web application have nothing to do with the users present in the LDAP. Administrator users of this web application are absolutely not administrators on the infrastructure.

V.5 Pre-Production Services

Pre-Production is a set of ISO services to those of Production. These services allow developers of client applications to test their work in conditions identical to those of Production.

V.5.1 Pre-Production DB

You must set up a DB service allowing the identical use of the Production web application. Of course, this DB service will be completely independent of the Production DB service. You **MUST** write a script that puts the ISO preproduction DB into production. Obviously, you **MUST** do it in an intelligent way so as not to impact the production services; locking the tables of the master is not possible.

V.5.2 Pre-Production Worker

You must set up a Worker service allowing the identical use of the Production web application. Of course, this Worker service will be completely independent of the Production Worker service. You must write a script that puts the ISO Preproduction Worker into production. Pre-production will also have access to the production part of the Versioning service to make your preproduction releases. This implies **MANDATORY** presence of a production Git branch and a preproduction Git branch.

V.6 Control Services

Control services are services that improve and simplify the maintenance and deployment of the infrastructure.

V.6.1 Automation

An automation service aims to allow the sysadmin to not intervene directly on their servers but only from this service.

You must set up an automation service with the software of your choice, such as Ansible, Salt, Puppet or Chef. Your automation service must contain all of your production scripts, pre-production, deployment of new configurations on your servers, backup, etc...

V.6.2 Monitoring

You need to set up a monitoring service that monitors all of your services and servers with the software of your choice, such as Shinken, Centreon or Zabbix. These will have a web interface. You **MUST** use LDAP as the authentication method for your monitoring tool.

In case you choose to implement the syslog service from the bonus section of this subject, you **MUST** make sure that the logs of this service are on a web interface for viewing the logs of your Syslog.

Chapter VI

Bonus part

Once the mandatory part of your architecture has been exhaustively tested, you can add the services listed in this chapter. During the defense, the evaluation of the bonus part will be taken into account if and only if all points of the mandatory part have been obtained.

VI.1 Syslog

You can set up a syslog service that groups all the logs of your machines.

You **MUST** make sure that Emergency, Alert and Critical errors are sent to you by email.

Attention: not all services know syslogger natively, so you must find solutions so that their logs are still exported.

VI.2 VPN

You can set up a VPN service to access all your machines on an external network. This **MUST** be linked to your LDAP.

VI.3 XMPP/Jabber

You can set up an XMPP type service like Jabber.
It **MUST** be linked to your LDAP and contain the necessary channels for your users.

VI.4 FTP

You can set up an FTP service. It **MUST** be linked to your LDAP and use FTPS.

Chapter VII

Submission and peer-correction

Do your work on the servers assigned to you. Only the work present on your servers will be evaluated during the defense.