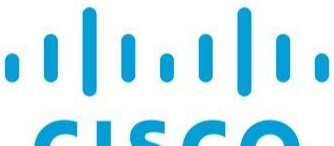
AP 1.2

Evolution d’un système d’informations

Mise en place d’une plateforme collaborative CLOUD

Mise en place d’un réseau



Sommaire

Rédacteurs : M. Tamisier / B. Jousseaume

Introduction

Cet AP s'articule autour de 2 activités principales :

- la mise en place d'une solution qui permet de mettre en place un service de stockage et de partage de copies de fichiers locaux en ligne utilisable en entreprise mais aussi pour une utilisation domestique
- la mise en place d'une infrastructure Réseaux à l'aide de l'outil Cisco Packet Tracer qui peut être vu comme un outil d'apprentissage mais aussi, comme outil permettant de tester des architectures Réseaux avant un déploiement en grandeur nature.

Vous devez établir un planning prévisionnel de cet ensemble de travaux qui devront être effectués en 3 semaines et demi .

Il peut être intéressant pour vous de tenir un planning en temps réel qui vous permettra de porter un jugement critique juste des missions réalisées et d'en tirer des enseignements pouvant vous aider lors de prochaines missions.

Ces deux missions sont à réaliser de manière individuelle.

En cas de problèmes, vous pouvez vous aider de ressources trouvées sur l'Internet. Seules des sources très récentes peuvent, le cas échéant, vous être utiles.

Les documentations fournies ont été réalisées en tenant compte des dernières versions des différents services à mettre en place.

Le serveur devra être mis en place sur la ferme de virtualisation dans votre espace dédié.

Soyez rigoureux et bon travail !!!

« Face à la roche, le ruisseau l'emporte toujours, non pas sa force, mais par sa persévérance. »
Confucius.

Conditions de réalisation

L'ensemble des activités seront à réaliser SEUL

Durée totale des activités: 3 semaines

Structure du document :

Ce document décrit vous accompagne dans la réalisation des différentes missions. Des compléments d'informations vous accompagneront dans votre lecture :
- des encarts **verts** compléteront vos connaissances générales
- des encarts rouge nommés **« Infos Cyber »** compléteront vos connaissances liées aux domaines de la **cybersécurité**

Les activités à réaliser

Mise en place d'une plateforme collaborative CLOUD

Travail à rendre n°1

→ **Cahier de recettes** de la mise en place de la solution Nextcloud et de la mise en place de la solution de sécurisation fail2ban.
→ **Cahier de recettes** de la mise en place de la sauvegarde
+ contenu script
+ paramètres CRON
→ **Fiches Serveurs et clients** **(voir modèle en Annexe en fin de documents)**

→ **Facultatif** : Cahier de recettes de la connexion avec le Smartphone

Mise en place d'un réseau

Travail à rendre n°2

→ **Cahier de recettes** de la mise en place de votre maquette
→ **Fichier Packet Tracer (format .pkt)**

Vous venez de passer des jours, des mois voire des années à travailler sur la mise en production d'une mise à jour, d'une nouvelle fonctionnalité ou pour corriger une régression ? Vous ne pouvez pas vous permettre, lors de la mise en ligne, de générer, potentiellement à nouveau, des régressions ?

*Il n'y a qu'une **solution** : **mettre en place un cahier de tests / cahier de recette.***

Un cahier de tests, qu'est-ce que c'est ? Comment le définir ? Comment l'appliquer ? C'est par ici.

1 Qu'est ce qu'un cahier de test ?

Le cahier de tests

Un cahier de tests – en général – est un document qui regroupe de nombreux points permettant de mener à bien votre mise en production. On retrouve, pêle-mêle : les limites du projet, les responsabilités, les documents applicables et de référence, un glossaire si besoin, les éléments à tester, les environnements… Il peut servir de support de communication entre le donneur d'ordre et les équipes en charge du projet (qu'ils soient internes ou externes à l'entreprise), pour optimiser au mieux la collaboration des deux parties. Il doit être mis en place en amont de la phase de test et l'accompagnera tout du long, et même après.

Un cahier de recette est propre à chaque projet, nous ne pouvons pas vous proposer une version standard prête à l'emploi. Toutefois, vous pouvez vous inspirer de cette trame généraliste :

- **Présentation du projet :**
  - Historique des révisions (le cas échéant)
  - Contexte
  - Objectif
  - Responsabilités
  - Documents applicables
- **Prérequis :**

- Périmètre du test, ce qu'il faut tester
- Environnement du test
- Les équipes concernées

- **Liste des tests :**
  - Description du processus de test étape par étape. (on parle ici de fiche de tests)

Ainsi, l'idée du cahier de recette est de fournir un plan d'action détaillé destiné au réalisateur des tests, regroupant l'ensemble des tests qui devront être effectués. Il est articulé autour de fiches de tests. Mais de quoi parle-t-on ?

2 Les fiches de tests

Les fiches de tests sont de véritables cartes routières ! Elles décrivent précisément les actions à conduire pour réaliser les tests.

Dans chaque fiche de test, il est nécessaire de définir les critères suivants :

- Le mode opératoire précis de la séquence de test qui va être réalisée, sous forme de points d'actions à effectuer
- Les résultats attendus pour chaque point d'action
- Les références du dossier de tests définissant les données métier exploitées au cours de chaque processus

Les fiches de test permettent de faciliter la qualification des problèmes rencontrés au cours de la recette et donc de mieux les gérer. C'est un gain de temps considérable qui peut bien souvent vous éviter ce ressenti : « j'ai repéré l'erreur, j'oublie de la corriger et je la retrouve à nouveau plus tard. »

Exemple d'une fiche de test :

Nom de la fiche : Module de connexion
Objectif : Vérifier le bon fonctionnement du module de connexion à l'espace client
Pré-requis : L'utilisateur doit avoir un compte actif
Cas de test : FT-001

N°	ACTION	ATTENDU
1	Aller sur le site cloudflare.fr et cliquer sur le bouton « se connecter »	Ouverture de la page cloudnetcare.fr/connexion
2	Rentrer une adresse email invalide sans @	Message d'erreur : Veuillez rentrer une adresse email contenant un @
3	Rentrer une adresse email valide sans comte actif	Message d'erreur : « Désolé, adresse email inconnue »
4	Rentrer une adresse email valide avec compte actif sans mot de passe	Message d'erreur : « Merci de saisir votre mot de passe »
5	Rentrer une adresse email valide avec compte actif et bon mot de passe	Connexion au tableau de bord du client

3 Utilité du cahier de test

Un cahier de tests va fiabiliser, normer, encadrer votre projet, et permet de mettre en place un process pour éviter les erreurs.

Le cahier de recette va lever toute ambiguïté sur votre phase de tests, de sa réalisation, à ses résultats attendus.

Il va également servir d'outil de dialogue entre prestataire(s) et client(s), pour clarifier au mieux le projet. Dans les grandes lignes, lorsque vous allez définir votre cahier, vous vous poserez les questions nécessaires pour identifier les points clés de votre phase de tests.

Il peut également servir de base de négociation pour une demande d'offre auprès d'une société de test, car il va permettre d'estimer avec précision les délais et coûts du projet en question. Le prestataire pourra également avoir un œil critique sur le cahier et suggérer des améliorations.

Le cahier de tests a également d'autres fonctions plus précises, telles que :

- La constitution de l'équipe en charge du projet
- La gestion de la recette
- L'identification des besoins et des exigences à satisfaire
- L'organisation de l'exécution du projet

Sa réalisation n'est pas à prendre à la légère. Il est nécessaire d'y consacrer de nombreuses heures pour pouvoir façonner un document réellement efficace et qui vous permettra de faire un premier pas vers la professionnalisation de vos tests de non régression. On ne peut affirmer que plus aucune de vos mises en production ne sera à l'origine de régression, mais vous éliminerez, à coup sûr, la très grande majorité des erreurs. Il faut également prendre en compte que sur les environnements aux multiples parcours il est difficile de tout tester (application web ou mobile).

Dans quels cas/quand l'utiliser ?

Le cahier de test est un document fondateur de la relation contractuelle entre les équipes et le chef de projet ou prestataires et clients. Il doit donc être réalisé en amont de l'action souhaitée (phase de tests, lancement de projet, etc....), tout au long de celle-ci, et même en post-projet.

Pour réaliser un projet ou une phase de tests efficace, il faut correctement formuler et identifier les contraintes et besoins de ces derniers, pour ne pas passer à côté d'informations essentielles. Son utilisation est très souvent utile. Il est toujours bon d'en formaliser un, quel qu'en soit le sujet.

4 Pour conclure.

Pour résumer, la rédaction d'un cahier de test est d'une importance capitale pour la bonne conduite de vos tests de non régression. Prenez le temps de le définir, de déterminer les points sensibles de votre développement et la typologie des tests à mettre en place.

Le temps passé à sa réalisation sera largement compensé par le temps économisé à intervenir sur les régressions ! Et comme toujours, le temps, c'est ...

AP 1.2 Evolution du système d'information Phase 1	Mise en place d'une plateforme collaborative CLOUD

Le contexte est celui de la société « SIO Communication » qui désire mettre à disposition de l'ensemble de ses salariés un service sécurisé de stockage de fichiers en ligne accessible depuis un navigateur de type Nextcloud.

Cette application nécessite :

- un **serveur Web** (Apache/Nginx, ...) ;
- l'accès à une **base de données relationnelle** (MySQL, PostgreSQL, SQLite) avec la possibilité pour les deux services d'être sur la même machine physique.

L'accès à l'application Nextcloud nécessite une machine cliente disposant d'un navigateur et/ou d'un smartphone.

Nextcloud est un logiciel libre qui permet de créer et gérer un serveur de stockage et de partage de fichiers en ligne. Le projet est dérivé (fork) du logiciel ownCloud qui a été lancé en 2010 par Frank Karlistschek afin de permettre aux utilisateurs d'avoir le contrôle de leurs données sur le *cloud* en hébergeant leur propre serveur.

Dans son utilisation basique, l'application permet d'*uploader* des fichiers via une interface Web ou WebDAV[1], puis de visualiser ces fichiers sous la forme d'un bureau en ligne.

De nombreuses applications Nextcloud viennent se greffer et ajouter des fonctionnalités comme la détection de virus, la journalisation des accès et des changements de fichiers, le versionnage, le chiffrement des fichiers, l'édition collaborative de fichiers.
Il est également possible d'installer un logiciel client (disponible pour GNU/Linux, Mac OS et Windows) permettant de synchroniser les fichiers présents sur le disque dur du client avec les fichiers stockés sur le serveur Nextcloud. Cette synchronisation peut s'effectuer entre plusieurs postes et plusieurs utilisateurs.

L'architecture se base sur des briques éprouvées de l'open source, notamment pour la partie serveur : PHP, Javascript, Ajax et SQLite, MySQL ou PostgreSQL comme base de données.

En ce qui concerne la gestion des utilisateurs, l'application s'interface avec LDAP/Active Directory.

Infos Cyber :

Nextcloud se repose sur des technologies WEB :

- Service APACHE (serveur HTTP)
- Langage PHP
- Base de données Mariadb (fork de MySQL)

Cette activité ne prend pas en compte les impératifs liés à la Cybersécurité comme, par exemple, la mise en place des échanges en HTTP**S,** ou bien encore, la sécurisation de la base de données.

1

Aussi, si vous souhaitez mettre en production cette solution, il faudra impérativement prendre en compte ces impératifs.

Missions à réaliser

À l'aide du dossier documentaire et de l'annexe 1, réalisez les travaux suivants :

Préparation de votre environnement de travail

Dans un premier temps, vérifiez votre maquette de travail en testant la connectivité de l'ensemble :

- le client **Windows** à installer si nécessaire (tester l'accès à Moodle, l'accès à l'internet)
- le smartphone connecté au wifi (tester la connexion à Moodle)
- routeur pour la connexion internet (tester le fonctionnement des passerelles utilisées);
- serveur **Debian** qui hébergera Nextcloud.

Les accès Wifi sont disponibles via une borne wifi dont le SSID est « **SIOAP** » (SSID : nom de la borne visible lors de la recherche de bornes WIFI sur votre smartphone ou votre ordinateur).
Pour des raisons de sécurité le **SSID** est **caché**. Il faut donc créer une connexion Wifi en tenant compte de cela.
Les accès sont sécurisés à l'aide du protocole WPA2 ; la clé a utiliser est « **WiFiBtsSio49** »

Installation de Nextcloud

- Installez Nextcloud sur une nouvelle machine de type Debian **sans interface graphique**.

  Vous devez notamment donner les informations de connexion au serveur de base de données. Vous choisirez 'password' comme mot de passe pour le compte administrateur de Nextcloud.

- Créez 2 utilisateurs standards locaux sur Nextcloud, en plus du compte administrateur et testez les fonctionnalités de base du nouveau service en ligne à partir de ces utilisateurs (création et upload de fichiers, etc.).

Contre-mesure avec Fail2ban

fail2ban est une application qui analyse les événements (fichiers journaux / logs) de divers services (SSH, Apache, ...) en cherchant des correspondances entre des motifs définis dans ses filtres et les entrées des logs.
Lorsqu'une correspondance est trouvée une ou plusieurs actions sont exécutées.
Typiquement, fail2ban cherche des tentatives répétées de connexions infructueuses dans les fichiers journaux et procède à un bannissement en ajoutant une règle au pare-feu pour bannir l'adresse IP de la source.

Infos Cyber :

Fail2ban ne doit pas être considéré comme un outil de sécurisation absolu d'un service. Ses objectifs sont d'éviter de surcharger les logs du système avec des milliers de tentatives de connexion et de limiter la portée des attaques répétées provenant d'une même machine.

Un serveur avec un accès SSH sur le port standard, par exemple, recevra très rapidement des centaines, voire des milliers de tentatives de connexions provenant de différentes machines. Ce sont généralement des attaques par force brute lancées par des robots.
Fail2ban en analysant les logs permet de bannir les IP au bout d'un certain nombre de tentatives ce qui limitera le remplissage des logs et l'utilisation de la bande passante.
Ceci va également rendre les attaques par force brute ou par dictionnaire beaucoup plus difficiles mais ce n'est pas une sécurité absolue contre ce type d'attaque.

Mais cela n'améliore en rien la sécurité du service concerné. Si l'accès SSH n'est pas suffisamment sécurisé (mot de passe faible par exemple) fail2ban n'empêchera pas un attaquant d'arriver à ses fins.
Autrement dit, utilisez votre temps de travail pour analyser vos configurations et sécuriser vos services plutôt que d'installer et paramétrer des outils d'analyse de logs plus ou moins gourmands en ressources système.

Afin **d'administrer** à distance le **serveur** à **distance** et de manière **sécurisée**, nous allons activer le protocole/application SSH.

Le protocole SSH est intégré dans toutes les versions de systèmes d'exploitation et nous pouvons donc l'utiliser en tapant des commandes en utilisant l'utilitaire intégré « **Termina** » sous linux appelé aussi « **Invite de commandes** » sous Windows. Cela nous permet entre autre de prendre le contrôle à distance ou de lancer le transfert de fichiers. On peut aussi utiliser des utilitaires graphiques comme « **putty** » pour se connecter .

Exemples d'utilisation du protocole/application ssh :

Connexion à distance avec ssh :
`ssh administrateur@192.168.1.7` permet d'accéder à distance au serveur se trouvant à l'adresse 192.168.1.7 en utilisant un utilisateur s'appelant « administrateur »

Copie de fichiers en utilisant un tunnel chiffré à l'aide de SSH :
`scp toto.txt cedric@192.168.10.15:/home/cedric/doc` permet de copier le fichier toto.txt sur l'ordinateur se trouvant à l'adresse 192.168.10.15 en se connectant en tant que « cedric ». Le fichier sera copié dans le répertoire `/home/cedric/doc`

A noter : les connexions avec l'utilisateur « root » ne sont plus possibles par défaut pour des raisons liées à la cybersécurité.

- Démarrez Fail2ban. Authentifiez-vous en SSH 3 fois avec un mot de passe erroné, soit en utilisant une connexion à distance sur le serveur , soit en réalisant une copie de fichier vers le serveur avec SCP. Putty et SCP utilisent le protocole SSH pour sécuriser la connexion.
  Consultez les logs afin de repérer l'adresse IP bannie

- Décrivez ce que vous observez et testez à nouveau en désactivant Fail2ban.

Anticiper une panne / une attaque Cyber

Il est coutume en informatique de mettre en place des PCA/PRA afin de prévenir de toute panne ou attaque qui pourrait entraîner un arrêt de services empêchant tout accès aux serveurs ou une perte de données sensibles.

Ces données peuvent être des informations de configuration ou le contenu d'une base de données.

PCA : Plan de Continuité d'Activité

Le PCA s'emploie à garantir une haute disponibilité au niveau de la production. Il comprend un ensemble de procédures, moyens, équipements et architectures requis afin de permettre la continuité de l'activité de la société quels que soient les sinistres qui pourraient survenir.

PRA : Plan de Reprise d'Activité

Le PRA est considéré comme un complément du PCA ou comme un palliatif en cas d'absence du PCA. Il se compose de processus à mettre en œuvre après la survenue d'un incident pour permettre à l'entreprise de reprendre son activité normale directement ou progressivement.

Dans ce cadre, il est important de mettre en place des dispositifs permettant d'anticiper tout problème.

De ce fait, il vous est demandé de mettre en place une solution permettant de **sauvegarder** :
- les fichiers de configuration de Nextcloud (fichier config.php – une simple copie peut suffire)
- la base de données utilisée par cette solution

Les fichiers à sauvegarder devront être compressés.
Cette sauvegarde devra être effectuée tous les jours à 20 heures.
Les sauvegardes seront réalisées dans le répertoire /sauvegarde

Fichiers à sauvegarder et leurs chemins d'accès :

. Dossier documentaire sur Nextcloud

Installation de Nextcloud à partir des sources

→ Installation d'un serveur LAMP (Linux, Apache, MySQL, PHP) :

Un **serveur LAMP** est nécessaire ainsi que d'autres paquets en dépendances afin de permettre le bon fonctionnement de l'installation.

```
apt install curl apache2 php php-mysql php-mbstring php-gd php-json php-curl php-intl mcrypt php-imagick php-xml php-zip php-ldap mariadb-server
```

Toujours sur votre serveur, installez aussi les paquets suivants :

```
apt install fail2ban ssh
```

En effet, vous aurez besoin d'un serveur SSH afin de transférer des fichiers vers votre serveur de manière sécurisée.

→ Téléchargement et décompression :

Nous partons d'une distribution **Debian** fraîchement ins tallée sans environnement graphique de bureau. La version de Nextcloud utilisée est la 27.

Pour des raisons évidentes liées à la stabilité et à la cybersécurité, vous devez installer la version la plus récente de Nextcloud.
Il est donc nécessaire de **vérifier sur le site la version actuellement disponible** et d'adapter les instructions suivantes en conséquence.

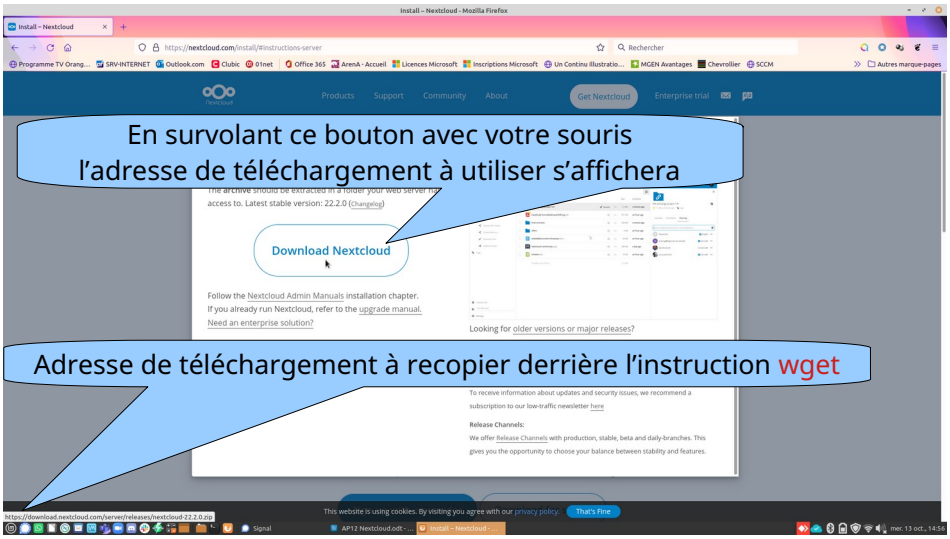
La version actuelle de Nextcloud est :

Pour récupérer cette version sur votre serveur, vous avez, entre autres, les deux solutions suivantes :

Directement depuis votre serveur :

- `wget https://download.nextcloud.com/server/releases/latest.zip`
  `unzip latest.zip` (après avoir éventuellement installé unzip `apt install unzip`)
  `mv nextcloud /var/www/html`
  `chown -R www-data /var/www/html/nextcloud/`

Important : Afin de télécharger la dernière version dans les meilleures conditions, suivre les indications suivantes



Dans cette activité, nous n'aborderons pas la configuration d'Apache. Nextcloud sera accessible en utilisant l'url **<ip-nom-serveur>/nextcloud** via le virtualhost présent par défaut sur Apache.

Nous faisons le choix aussi de laisser le serveur web et la base de données sur le même serveur afin de simplifier certaines procédures d'installation.

Remarque concernant l'adressage IP :

Pour le serveur Nextcloud, vous devez choisir un adressage IP cohérent avec votre environnement. Si ce dernier est opérationnel, vous devez pouvoir accéder au serveur Nextcloud à l'aide de son adresse IP. Les accès DNS seront envisagés un peu plus tard dans l'année.

Attention, en cas de changement ultérieur d'adresse IP ou de nom pour le serveur Nextcloud, vous devez changer le contenu du fichier **config.php** situé dans le répertoire **config** de Nextcloud.

L'étape suivante consiste à se connecter au serveur de **base de données** afin de **créer la base de données** ainsi qu'un utilisateur qui aura les privilèges sur cette base. Pour cela, il faut auparavant exécuter les commandes suivantes :

1- Lancer la commande suivante permettant d'initialiser la **sécurisation** de notre serveur MariaDB

```
mysql_secure_installation
```

Cette commande permet notamment d'initialiser un **mot de passe** pour le compte **root**. Ensuite, répondre ***Oui*** à toutes les questions posées.

Il est recommandé de choisir un mot de passe associé à l'utilisateur "root" assez difficile lors de l'installation du serveur de base de données car MySQL peut aussi être "brute forcé" (technique utilisée par les « pirates » pour retrouver des mots de passe).

Le mot de passe utilisé pour la base de données est :

2- Se connecter au serveur de base de données avec la commande mysql

```
mysql
```

3- Créer l'utilisateur propriétaire sur la base de données via les commandes mysql suivantes :

Création de la base de données « nextcloud »
```
create database nextcloud;
```

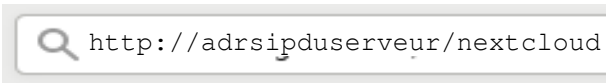
Création de l'utilisateur propriétaire et activation de ses droits
```
grant all privileges on nextcloud.* to 'nextcloud'@'localhost' identified by 'password';
```

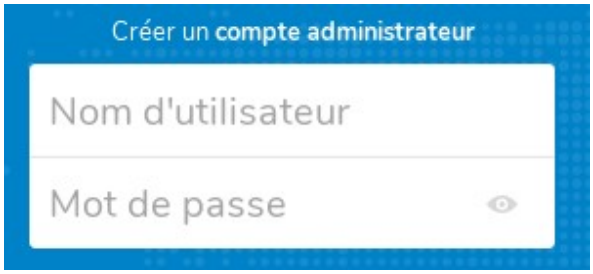
Validation des changements
```
flush privileges;
```

Sortie du mode de gestion de la base de données
```
quit
```

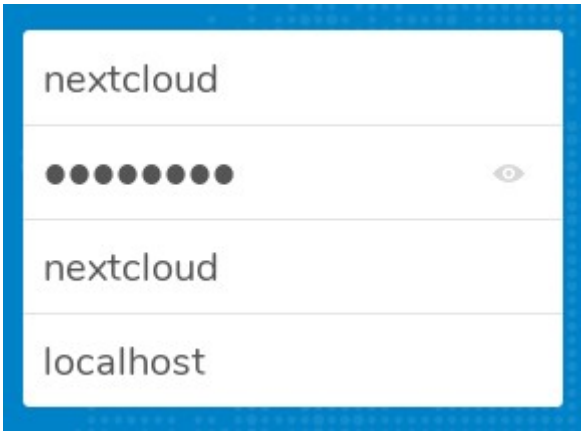
Dans cet exemple, l'utilisateur propriétaire de la base de données est **`nextcloud`** et son mot de passe est **`password`**.

Il faut ensuite revenir sur le **navigateur** (firefox, chrome, etc) de la machine cliente afin d'administrer le serveur Nextcloud avec son adresse IP ou son nom.





Un accès au site via un navigateur permet la finalisation de l'installation. Choisissez '**admin**' comme login. Pour les besoins de l'activité, le mot de passe **'password'** sera affecté à ce compte.



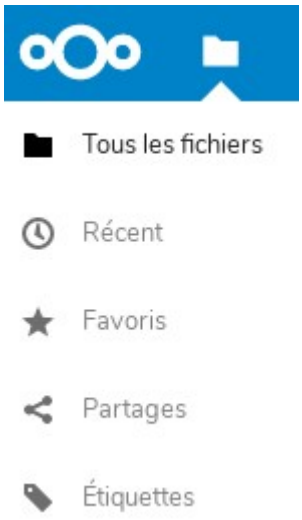
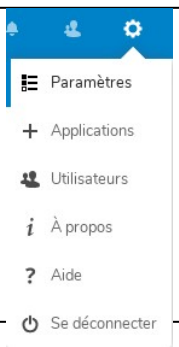
Dans la partie basse de l'écran, un autre formulaire demande de saisir les informations de connexion à la base de données.

Compte tenu des travaux précédents sur le serveur MariaDB, il faut indiquer **`nextcloud`** comme nom d'utilisateur et **`password`** comme mot de passe. Le nom de la base de données étant **`nextcloud`**.

Il faut enfin cliquer sur `Terminer l'installation`. Une fois l'installation terminée, la page d'accueil de Nextcloud est visible avec une connexion en tant qu'administrateur.

NB : l'espace de stockage des fichiers partagés par Nextcloud a été configuré automatiquement dans `/var/www/html/nextcloud/data`.

La configuration du serveur Nextcloud se réalisera ensuite via l'interface d'administration :

	Le menu de gauche permet : • d'accéder à la liste des fichiers ; • de voir les favoris ainsi que les partages ; Ce menu est enrichi lorsque l'on clique sur Paramètres dans le menu de droite.
	Le menu déroulant de droite permet : • de configurer l'espace propre à chaque utilisateur (langue, notifications, mot de passe…) ; • d'administrer Nextcloud et de gérer les utilisateurs si on est connecté en tant qu'administrateur .

Ces menus s’adaptent selon que l’individu connecté soit administrateur ou simple utilisateur.

Lors de vos phases de tests et de découverte de Nextcloud, vous pouvez aller « faire un tour dans la rubrique « Applications » dans laquelle vous pourrez découvrir des extensions « prêtes à l’emploi » afin d’enrichir votre solution Nextcloud !!!

Vous pourrez mesurer ainsi l’intérêt de ce type de solution dans le domaine de l’entreprise et peut-être… chez vous !!!

Contre-mesure avec fail2ban

Nextcloud possède par défaut un ensemble de dispositifs permettant **d'éviter** les **attaques** par dictionnaire appelées aussi « attaques **brute force** ». Aucun réglage particulier est à effectuer.

Ce n'est pas le cas des autres services mis en place sur les serveurs ; services demandant de l'authentification.

Dans notre cas de figure, nous allons **mettre en place le protocole SSH** afin de permettre et de sécuriser les **accès à distance**. Ce dernier est très robuste mais peut être encore plus sécurisé en mettant en place l'outil **fail2ban**.

Présentation de fail2ban

Pour d'éviter les attaques par dictionnaire sur les mots de passe, il est possible d'utiliser l'outil **fail2ban** afin de détecter des adresses IP associées à des tentatives répétées d'authentification. L'administrateur peut alors mettre en place une politique de bannissement d'une durée qui dépend de la configuration mise en place.

Infos Cyber : ***D'après doc.ubuntu-fr.org :***

Fail2ban lit les fichiers journaux (logs) de divers services (SSH, Apache, ...) à la recherche d'erreurs d'authentification répétées et ajoute une règle dans le parefeu (iptables) pour bannir l'adresse IP de la source.

Le but de Fail2ban est d'empêcher une attaque qui, par force brute, trouve un identifiant/mot de passe permettant l'accès à un service.

Les postes serveurs ne dormant jamais, ils sont la cible d'attaques automatiques en provenance de partout. Et sans un tel outil, qui sanctionne les tentatives, plus un serveur est rapide à répondre, plus il est menacé.

Le paramétrage par défaut de la sanction est de 10mn, alors faisons un petit calcul : si un attaquant du service SSH fait 5 tentatives toutes les 10mn (il ne se fait sanctionner qu'à 6 erreurs), alors sans jamais se faire bloquer, il pourra effectuer 5×(60/10)×24×365=262800 tentatives par an, soit plus d'un quart de million. Alors supposons qu'un individu dispose de 10 postes (10 IP) d'où lancer une attaque, il aura effectué au bout d'un an 2.6 millions d'essais, et avec 100 ou 1000 postes, 26 millions ou 260 millions. On voit donc bien que 10 minutes n'est pas une sanction suffisante.

Par rapport au blocage par défaut (600s), un blocage de 1h est bien plus réaliste (**3600**s), ou même 1 journée (**86400**s), ou pourquoi pas 1 semaine (**604800**s).. Un blocage définitif est possible en affectant -1 à la directive bantime.

Il faut bien veiller à ajouter en liste blanche vos adresses IP les plus communes, car l'erreur est humaine, donc il ne faudrait pas vous bloquer l'accès à votre serveur. La liste 'ignoreip' est séparée d'espaces, donc si votre IP est 8.8.8.8, éditez le fichier `/etc/fail2ban/jail.conf` :

```
[DEFAULT]
ignoreip = 127.0.0.1 8.8.8.8
findtime = 3600
bantime = 86400
```

Pour spécifier à Fail2ban quels services il doit surveiller, éditez le fichier `/etc/fail2ban/jail.conf`

Dans la partie jail vous trouverez des blocs du type :

```
[SSH]
enabled=true
port=ssh,ftp
filter=sshd
logpath=/var/log/auth.log
maxretry=6
```

Ce sont des réglages par défaut, que nous allons ensuite personnaliser.

Installation et configuration de Fail2ban pour SSH

Après avoir installé Fail2ban, il faut créer un paragraphe qui va décrire la surveillance de SSH. Cette configuration spécifique s'ajoute dans le fichier /etc/fail2ban/.

`apt install fail2ban` (normalement déjà effectué)
`apt install iptables` (module parefeu : afin de compléter les actions de fail2ban)

Supprimer tous fichiers se trouvant dans le répertoire `/etc/fail2ban/jail.d` .Par défaut, vous devriez trouver que le fichier `defaults-debian.conf`.

Créer un fichier dans le répertoire `/etc/fail2ban/jail.d` nommé `monsshd.conf` avec le contenu suivant :

```
[sshd]
backend = auto
enabled = true
maxretry = 3
```

`enabled` : active la surveillance de ssh par Fail2ban.

`maxretry` : le nombre d'échecs tolérés. **Ici, nous le passons à 3. Par défaut, pour tous les services à contrôler, il est positionné à 5 (cf contenu du fichier `/etc/fail2ban/jail.conf`– Soyez curieux aller voir son contenu ☺)**

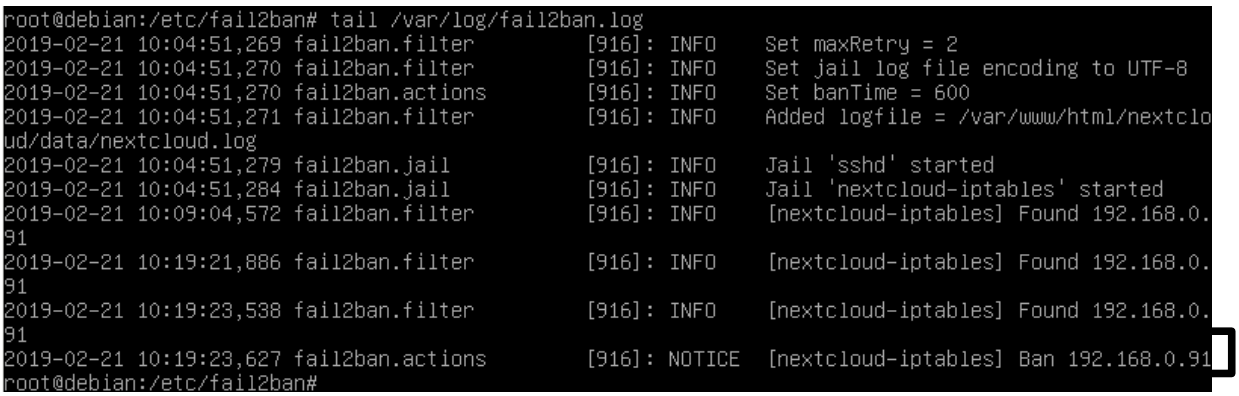
Rappel : ces règles viendront compléter, adapter des régles déjà présentes par défaut dans le fichier de configuration de fail2ban. Cette démarche permet de personnaliser les réglages à nos besoins.

Test de la configuration

Après avoir redémarré Fail2ban, vous pouvez vérifier que la configuration dédiée à ssh est bien prise en compte avec le commande `fail2ban-client status`

La consultation des logs permet de tracer les bannissements effectués par fail2ban.

```
tail /var/log/fail2ban.log
```



Fail2ban : Commandes importantes

Pour savoir si votre jail est actif, vous devriez le voir affiché, après avoir taper cette commande :

```
fail2ban-client status
```

Cette commande affiche tous les jails que fail2ban traite.

Pour savoir si une de vos jails de votre fail2ban a bannis une ou plusieurs IP, taper cette commande :

```
fail2ban-client status [Nom du jail]
```
exemple : `fail2ban-client status nextcloud`

Cette commande va afficher le nombre de tentative lu dans vos logs, le nombre de bannis et, le plus intéressant, les IPs qui sont bannis temporairement.

Dé-bannir une IP de l'un de vos jails

Une de vos adresse IP se retrouve blacklisté suite à une mauvaise manips répété ou un test de sécurité. Vous pouvez le retirer de la liste des IP blacklisté de fail2ban avec cette commande :

```
fail2ban-client set [nom du jail] unbanip [IP concerné]
```
exemple : `fail2ban-client set nextcloud unbanip 192.168.1.5`

Bannir manuellement une IP sur l'un de vos jails

Vous voulez tester plus rapidement l'interdiction d'un accès d'un PC, ou bloquer une personne malveillante. Renseignez son IP dans cette commande :

```
fail2ban-client set [nom du jail] banip [IP à bannir]
```
exemple : `fail2ban-client set nextcloud banip 80.41.36.70`

Installation et configuration de l'application Nextcloud sur un client Windows & smartphone

Installation sur un client Windows ou Linux

1- Sur votre client, télécharger puis installer le client Nextcloud à l'adresse suivante : https://nextcloud.com/install/#install-clients
2-La paramétrer en suivant les paramètres précédemment indiqués
3- Tester !

Installation sur un smartphone

1- Vérifier que votre smartphone soit bien connecté au wifi de la section
2- Se rendre sur votre gestion d'applications
3- Rechercher l'application NEXTCLOUD
4- La paramétrer en suivant les paramètres précédemment indiqués
5- Tester !

SAUVEGARDE de la SOLUTION
Automatisation / Sauvegarde & Restauration

Compresser/Décompresser des fichiers

Pour compresser un ensemble de fichiers, l'usage est le suivant :

```
zip -r nom_du_fichier.zip repertoire_ou_fichier
```

Le commutateur -r indique que le contenu du répertoire doit être compressé ainsi que ses sous-répertoires.

Pour décompresser un fichier, l'usage est le suivant :

```
unzip nom_
```

Automatiser des tâches

1 Programmer des actions avec crontab

Pour planifier des actions avec crontab, vous pouvez lancer la commande `crontab -e`

Voici de manière schématique la syntaxe à respecter d'un **crontab**:

*Copier vers le presse-papier*Code :

```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,
thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  user command to be executed
```

Le fichier de configuration de est constitué des différentes lignes. Chaque ligne correspond à une action.

Prenons l'exemple suivant :

Copier vers le presse-papier

```
mm hh jj MMM JJJ [user] tâche > log
```

- **mm** : minutes (00-59).
- **hh** : heures (00-23) .
- **jj** : jour du mois (01-31).
- **MMM** : mois (01-12 ou abréviation anglaise sur trois lettres : jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec).
- **JJJ** : jour de la semaine (1-7 ou abréviation anglaise sur trois lettres : mon, tue, wed, thu, fri, sat, sun).
- **user (facultatif)** : nom d'utilisateur avec lequel exécuter la tâche.
- **tâche** : commande à exécuter.
- **> log** (facultatif) : redirection de la sortie vers un fichier de log. Si un fichier de log n'est pas spécifié, un mail sera envoyé à l'utilisateur local.

Pour chaque unité, on peut utiliser les notations suivantes :

- **1-5** : les unités de temps de 1 à 5.
- ***/6** : toutes les 6 unités de temps (toutes les 6 heures par exemple).
- **2,7** : les unités de temps 2 et 7.

Exemples

Exécution tous les jours à 22h00 d'une commande et rediriger les infos dans sauvegarde.log :

```
00 22 * * * /root/scripts/sauvegarde.sh >> sauvegarde.log
```

Exécution d'une commande toutes les 6 heures :

```
00 */6 * * * /root/scripts/synchronisation-ftp.sh
```

Exécution d'une commande toute les heures :

```
00 */1 * * * /usr/sbin/ntpdate fr.pool.ntp.org
```

Exécution d'une commande toutes les minutes uniquement les lundis :

```
* * * * 1 /root/script/commandes-du-lundi.sh
```

Exécution d'une commande une fois par an à une heure précise (ici le 25 décembre à 00h15) :

```
15 00 25 12 * echo "Le père Noël est passé !"
```

Exécuter chaque jour, de chaque mois à 2:15 la commande eix-sync

```
15 02  * *  * /usr/bin/eix-sync
```

Vous pouvez vous référer au complément page 37
afin de simplifier vos réglages

Bases de données : Sauvegarde/Restauration

MySQLdump est un outil permettant la sauvegarde et la restauration de données dans une base MySQL.
Il est possible d'agir sur toutes les bases de donnée du système, une seule base, une seule table ou de faire une sélection de table d'une ou plusieurs bases comme le montre les exemples suivants :

Sauvegarde de toutes les bases de données
```
mysqldump --user=login_mysql --password=password_mysql --all-databases > dump_bdd.sql
```
Sauvegarde d'une seule base de donnée
```
mysqldump -u login_mysql -p password_mysql --databases nom_bdd > dump_bdd.sql
```
Sauvegarde de plusieurs bases de données
```
mysqldump -u login_mysql -p password_mysql --databases nom_bdd1 nom_bdd2 > dump_bdd.sql
```
Sauvegarde d'une seule table
```
mysqldump -u login_mysql -p password_mysql -B nom_bdd --tables nom_table > dump_bdd.sql
```

Sauvegarde de plusieurs tables
```
mysqldump -u login_mysql -p password_mysql -B nom_bdd --tables nom_table1 nom_table2 > dump_bdd.sql
```

Infos Cyber :

Les sauvegardes sont rarement laissées sur le serveur contenant les données. Elles sont la plupart du temps, transférées sur un serveur dédié au stockage des sauvegardes.

Les sauvegardes n'étant pas chiffrées, une attaque de type « **man of the middle** » pourrait permettre l'interception de ces derniers et donc des données sauvegardées.

Dans de tels cas de figure, il faudra prévoir impérativement un transfert chiffré de type « `scp` » ou via un VPN.

L'**attaque de l'homme du milieu** (**HDM**) ou *man-in-the-middle attack* (**MITM**), parfois appelée **attaque du monstre du milieu** ou *monster-in-the-middle attack*1,2 ou **attaque de l'intercepteur**, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre.

CONCLUSION

La gestion des mots de passe reste un élément essentiel de la sécurité des systèmes d'informations. Très souvent, il s'agit de la seule protection sur laquelle s'appuient les utilisateurs pour protéger leurs données personnelles. Utilisés dans presque tous les services de la vie quotidienne (messagerie, réseaux sociaux, cloud…), ils peuvent être compromis s'ils ne sont pas sécurisés.
De plus en plus d'articles de presse mettent en avant leur fragilité. La CNIL donne ainsi des conseils pour les sécuriser[1] et reste habilitée à sanctionner les entreprises qui ont des politiques de mots de passe trop laxistes au titre de la protection des données[2].

https://www.cnil.fr/fr/mots-de-passe-des-recommandations-de-securite-minimales-pour-les-entreprises-et-les-particuliers

Visualiser la vidéo « [Vidéo] Comment créer un bon mot de passe » que vous retrouverez dans la partie « Veille technologique » de votre plateforme

NEXTCLOUD & MOI

Il est tout à fait possible de reproduire cette activité chez vous, afin de remplacer des solutions comme Google Drive, Dropbox et autres qui sont reconnues pour ne pas suivre la RGPD du fait qu'elles soient hébergées sur le territoire américain.

RGPD : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Cela nécessiterait l'activation de la DMZ sur votre BOX ainsi que l'utilisation de DNS Dynamique.

Pour cela, vous pouvez installer NEXTCLOUD une une machine de type Raspberry PI pour un budget avoisinant les 40/50 euro au total. Des boitiers en kit sont disponibles, mais on peut en fabriquer en

https://www.blog-nouvelles-technologies.fr/19068/construisez-votre-boitier-pour-le-raspberry-pi-en-lego/

1
2

Le **Raspberry Pi** est un nano-ordinateur monocarte à processeur ARM de la taille d'une carte de crédit conçu par des professeurs du département informatique de l'université de Cambridge dans le cadre de la fondation Raspberry Pi3.

Le Raspberry Pi fut créé afin de démocratiser l'accès aux ordinateurs et au *digital making*4 (terme anglophone désignant à la fois la capacité de résolution de problèmes et les compétences techniques et informatiques)5. Cette démocratisation est possible en raison du coût réduit du Raspberry Pi, mais aussi grâce aux logiciels libres4. Le Raspberry Pi permet l'exécution de plusieurs variantes du système d'exploitation libre GNU/Linux, notamment Debian, et des logiciels compatibles. Il fonctionne également avec le système d'exploitation Microsoft Windows : Windows 10 IoT Core6, Windows 10 on ARM (pour l'instant[Quand ?] relativement instable), celui de Google Android Pi7 et même une version de l'OS/MVT d'IBM accompagnée du système APL\3602.

Il est fourni nu, c'est-à-dire la carte mère seule, sans boîtier, câble d'alimentation, clavier, souris ni écran, dans l'objectif de diminuer les coûts et de permettre l'utilisation de matériel de récupération. Néanmoins des « kits » regroupant le « tout en un » sont disponibles sur le web à partir de quelques dizaines d'euros seulement.

Son prix de vente était estimé à 25 américains, soit 19,09 , début . Les premiers exemplaires ont été mis en vente le pour environ 25 8[réf. non conforme]. En , plus de dix millions de Raspberry Pi ont été vendus. De multiples versions ont été développées, les dernières sont vendues un peu plus de 25 pour le B+, à un peu plus de 30 pour le Pi 2 (2015), un peu plus de 35 pour le Pi 3 (2016), 5 pour le Raspberry Pi Zero (2016), 10 pour le Raspberry Pi Zero W (2017), 15 pour le Raspberry Pi Zero WH (2018) et 40 pour le Raspberry Pi 4 (varie selon la quantité de mémoire).

Le Raspberry Pi est utilisé par des créateurs du monde entier car son prix le rend très attirant.

https://www.kubii.fr/215-raspberry-pi

→ Modèle de démonstration disponible ←

AP 1.2 Evolution du système d'information Phase 2	Mise en place d'un réseau

L'activité sera réalisé sur la plateforme d'apprentissage CISCO Packet Tracer.

Dans le cadre de la société « SIO Communication », nous allons **modéliser leur réseau** / **réaliser une maquette réseau,** dans le but de faire un certain nombre de tests et de s'assurer du bon fonctionnement de l'infrastructure mise en œuvre.

Pour cela nous allons utiliser l'outil **Cisco Packet Tracer**.

Packet Tracer est un logiciel développé par Cisco. C'est un simulateur de matériel réseau Cisco (routeurs, commutateurs). Cet outil est créé par Cisco Systems qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, ou ayant participé, aux programmes de formation Cisco (Cisco Networking Academy). Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau.

Packet Tracer (PT) permet de simuler le fonctionnement d'une architecture réseau. Il permet ainsi de tester une configuration virtuellement et est très utile aux administrateurs réseaux notamment pour déterminer si l'architecture « pensée » est viable et efficace.

Très Important : Pour des questions de compatibilité, nous utiliserons pour cette année scolaire **exclusivement la version 8.0.0.0212 de Packet Tracer.**

Il est disponible via la plateforme Moodle

Au lancement Packet Tracer demande un identifiant/mot de passe

mettre : Chevro49@laposte.net/Chevro49

Missions à réaliser

À l'aide du logiciel **Packet Tracer** et en vous aidant des **annexes 2 & 3**, il vous est demandé de **modéliser** les infrastructure suivantes et de réaliser un **cahier de recettes** pour chacune :

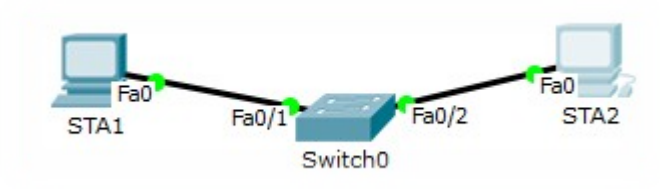
Annexe 2, un document de prise en main de Packet Tracer

Annexe 3 : Configurations à donner aux machines

Pour chaque infrastructure, tous les hôtes doivent communiquer entre eux.

Infrastructure n° 1	

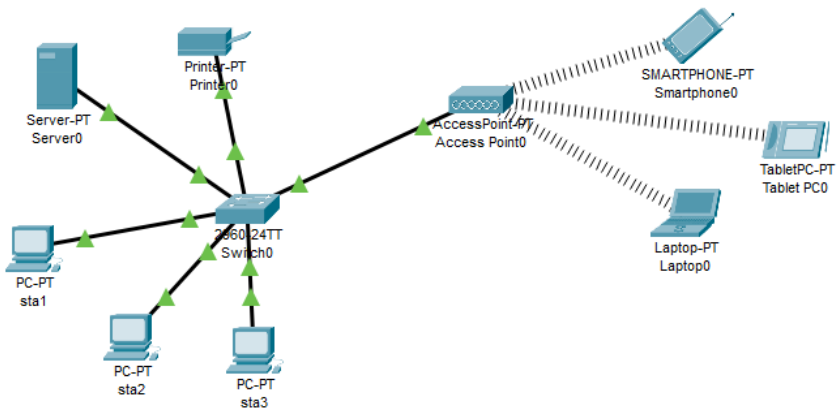
Créer dans un 1ier temps, l'infrastructure suivante :



Un **switch**, commutateur ou commutateur réseau en français, **est** un équipement qui fonctionne comme un pont multiports et qui permet de relier plusieurs segments d'un réseau informatique entre eux. Le **switch est** chargé d'analyser les trames qui arrivent sur les ports d'entrée.

Infrastructure n° 2	

Compléter votre infrastructure avec d'autres hôtes de réseau (PC, serveur, imprimante, borne Wi-Fi, smartphone, tablette, pc portable), pour obtenir ceci :

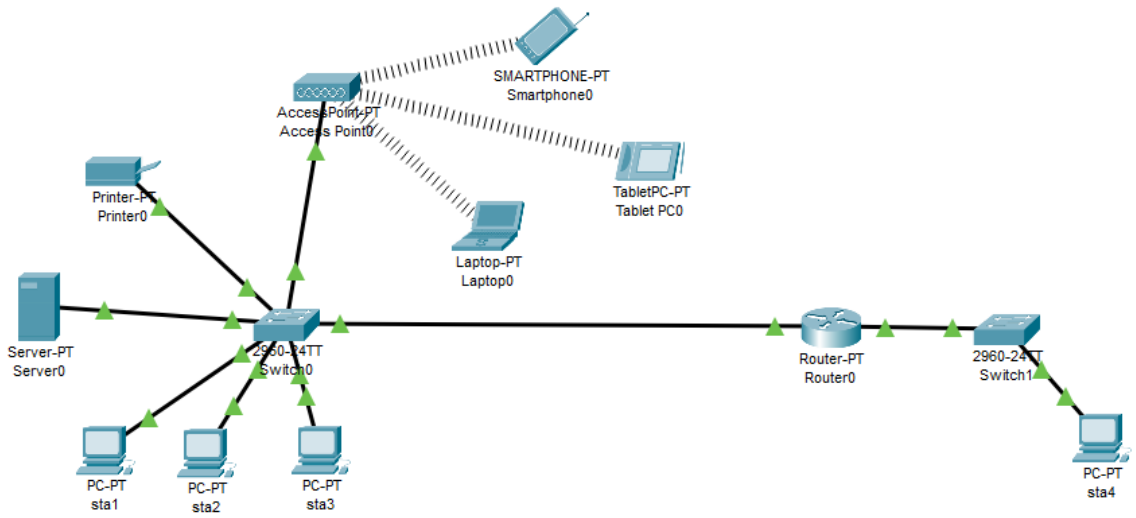


• **Infrastructure n° 3**	•

Nous allons maintenant rattacher un nouveau réseau à notre infrastructure.

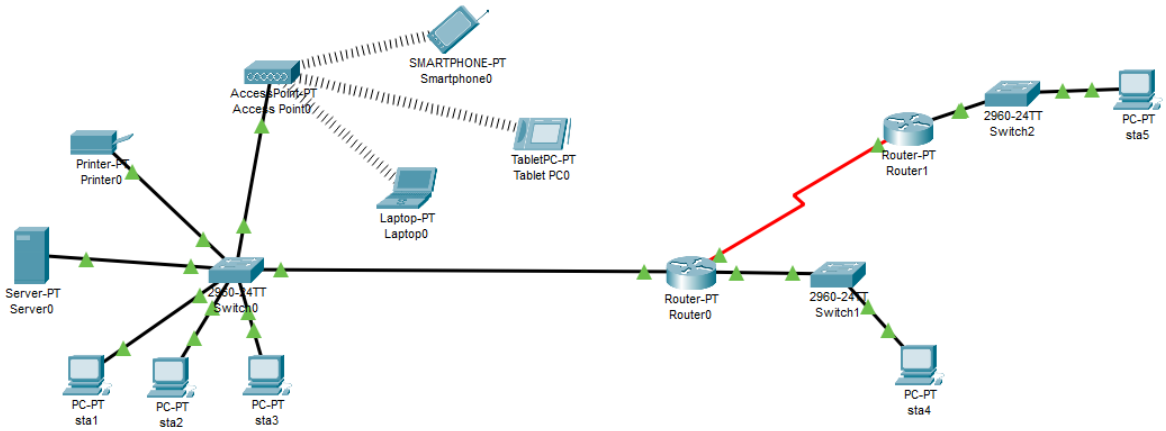
Pour cela un routeur, un switch et une sta4 seront ajouté. Le nouveau réseau IP sera 192.168.1.128 /25

Un **routeur** est un équipement matériel informatique dont la fonction principale consiste à orienter les données à travers un réseau. Il permet, entre autres, de faire circuler des données entre deux interfaces réseau. Il peut également être présenté comme une **passerelle** entre plusieurs serveurs et facilite alors l'accès aux ressources disponibles sur le réseau pour les utilisateurs.



Infrastructure n° 4	

Poursuivons l'évolution de l'infrastructure, avec l'ajout d'un site distant :



ANNEXES

ANNEXE 1

Exemple de « fiche type » Serveur voire Clients

A adapter en fonction des besoins

SRV-Type	

Numéro de version	Auteur

L'objectif de ce serveur est de

Configuration de la machine virtuelle	(supprimer services non utilisés)

Rôles	Actif	Non actif	Observations
Annuaire (AD)			
DHCP			
DNS			
WINS			
WEB			
FTP			
SGBD			
Firewall			
PROXY			
Portail captif			

Paramètres	Valeurs
Système d’exploitation	
Adresse IP	
Masque de sous-réseaux	
Passerelle	
VLAN	
DNS	
NTP	
PROXY	

Sécurité	

Service	Nom utilisateur	Mot de passe
Ex : Active Directory	Administrateur	M0t2p@sse

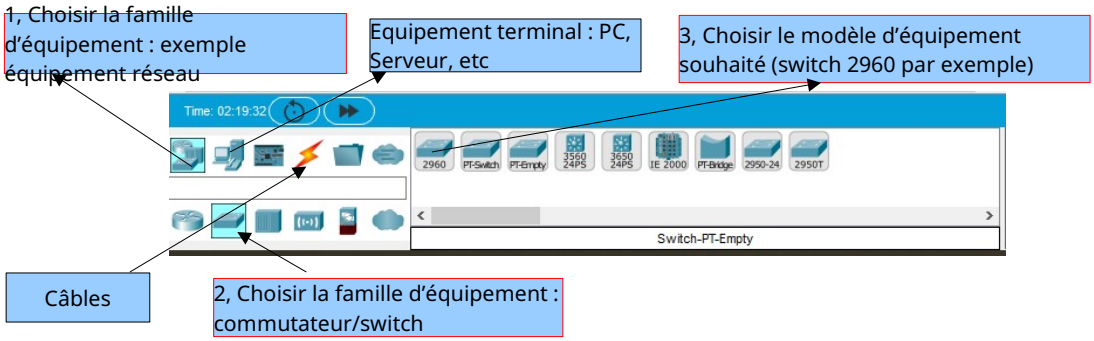
Mode opératoire	

ANNEXE 2

1. Ajout des postes et du commutateur

Le coin inférieur gauche de l'écran de Packet Tracer affiche une dizaine d'icônes (8 à 12 selon les versions) qui représentent les catégories ou les groupes de périphériques, tels les routeurs, les commutateurs ou les périphériques terminaux.

Pour ajouter les équipements, placez le curseur sur les catégories pour afficher leur nom dans la case. Pour sélectionner un périphérique, commencez par choisir le type d'équipement pour que les options correspondantes s'affichent dans la zone en regard des listes de catégories. Choisir alors le modèle d'équipement souhaité.

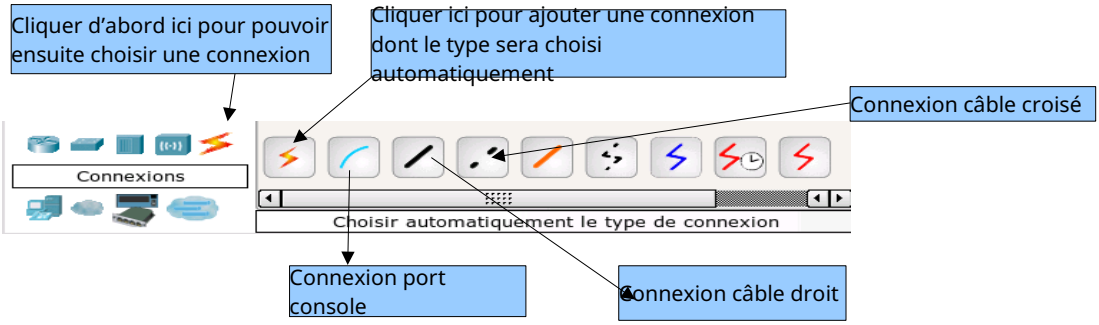


2. Ajout des connexions

Pour mettre en place les connexions, utilisez la catégorie « câbles » (« Connections » en anglais),

La mise en place des connexions peut se faire :

- soit en choisissant le type de connexion ;
- soit en laissant le simulateur choisir les interfaces et le type de connexion adapté (en fonction des équipements).



Remarque : Si vous avez un doute sur le choix du câblage à mettre en œuvre, vous pouvez utiliser les connexions automatiques.

Remarque : après un court moment (une vingtaine de secondes, le temps que les interfaces du commutateur s'activent lorsque le commutateur a vérifié que tout est conforme), il devrait y avoir des points verts aux deux extrémités de chaque câble de connexion (comme dans la réalité). Si ce n'est pas le cas, vérifiez le type de câble sélectionné.

Pour supprimer une liaison non conforme, cliquer sur la croix dans la barre d'outils, puis cliquer sur la liaison (ou n'importe quel élément d'ailleurs) à supprimer.

3. Configuration des noms d'hôtes et des adresses IP sur les PC

Cliquer sur PC0 : une fenêtre PC0 s'affiche.

Sélectionner l'onglet Config, puis FastEthernet0. Dans le champ Display Name, nommez le PC. Par exemple « STA1 ».

Sélectionner l'onglet (bouton sur la gauche) FastEthernet0, puis ajouter l'adresse. Par exemple : IP 192.168.1.1 et le masque de sous-réseau 255.255.255.0.

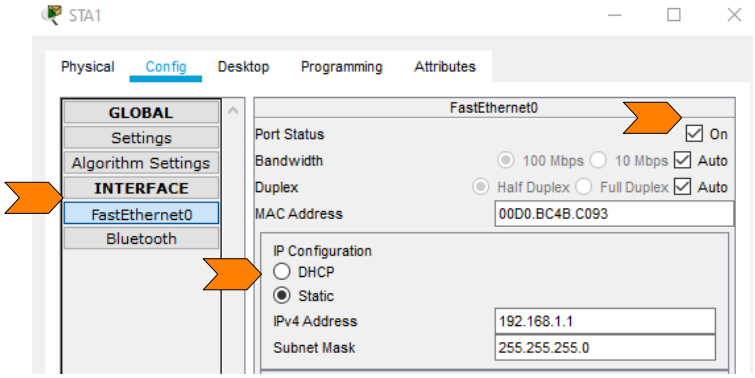
Fermer la fenêtre de configuration en cliquant sur la croix « x » dans le coin en haut à droite.

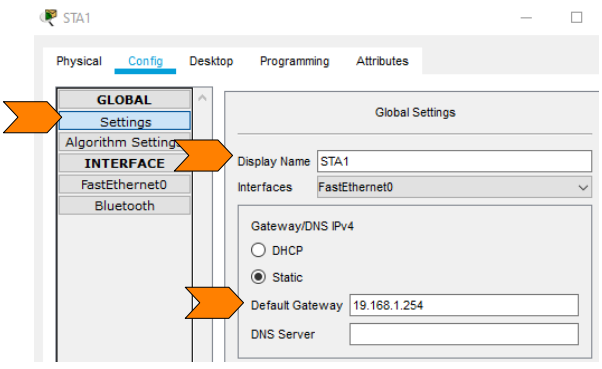
Les postes (sta, serveur, imprimante) ont tous une passerelle. Onglet Config puis Settings : champ Default Gateway..

Le port correspondant à la carte réseau doit être actif (allumé) sinon la carte est désactivée.

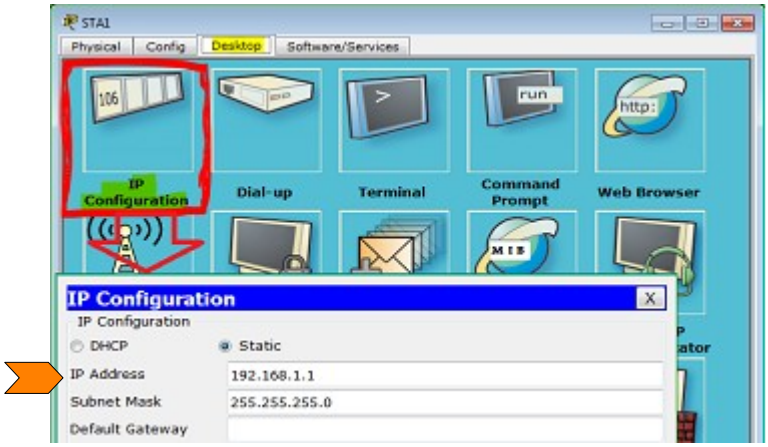
Port Status coché ON

!! Attention aux routeurs, où les ports sont, par défaut, **désactivés** !!





Remarque : il est possible de configurer différemment les adresses IP d'un poste notamment via

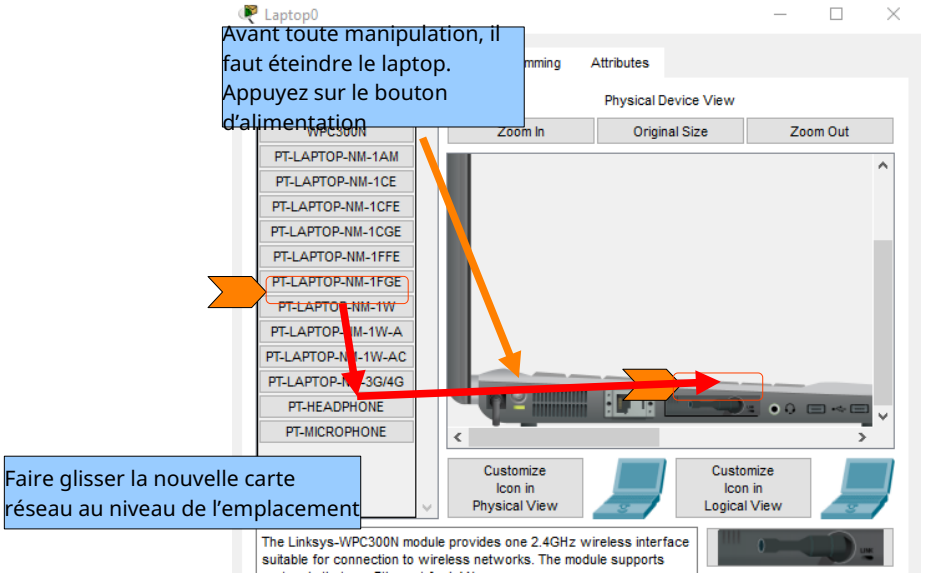


4. Modifier la carte réseau du laptop

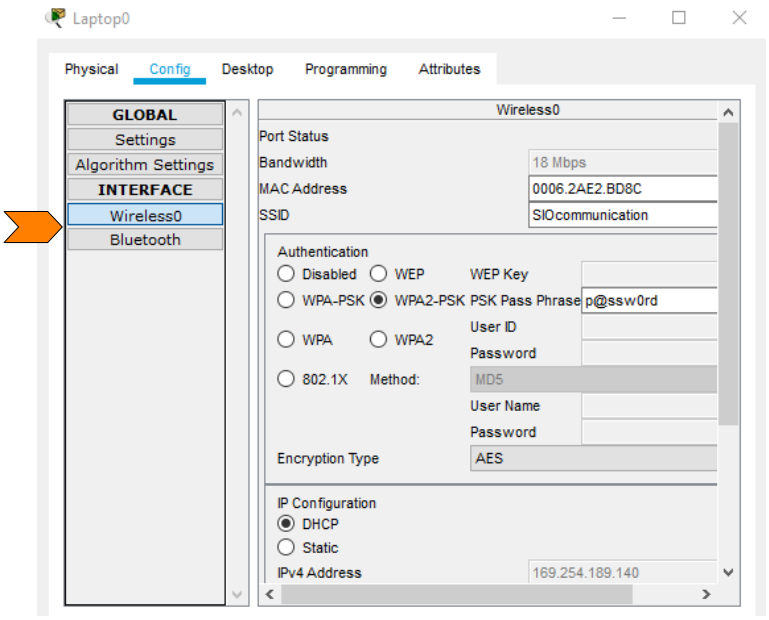
Le laptop (ou ordinateur portable) sera connecté en sans-fil dans notre infrastructure.

A l'ajout du laptop il est défini avec une carte réseau standard en Ethernet (avec câble Ethernet et port RJ45). Il faut donc modifier la carte réseau.

Pour cela il faut supprimer la carte réseau Ethernet et ajouter la carte réseau sans-fil.

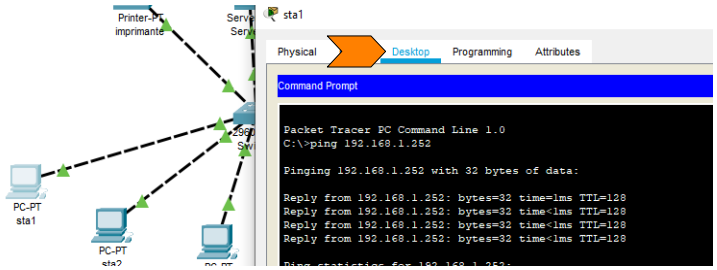


Ne pas oublier de rallumer le laptop après manipulation.



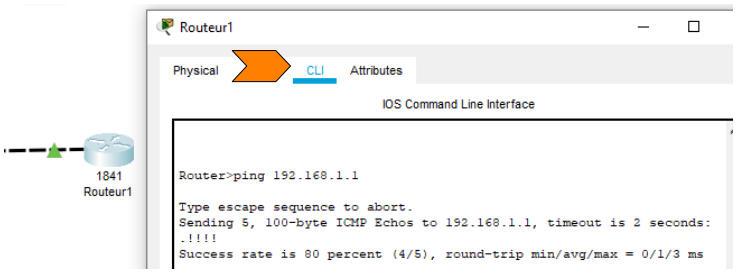
5. Réaliser les tests nécessaires

- Sur la station (onglet desktop/command prompt), réaliser un **ping**….



La commande **ipconfig /all** permet de voir toute la configuration IP ainsi que l'adresse physique et MAC du PC

- Sur le routeur (CLI/ ping….)

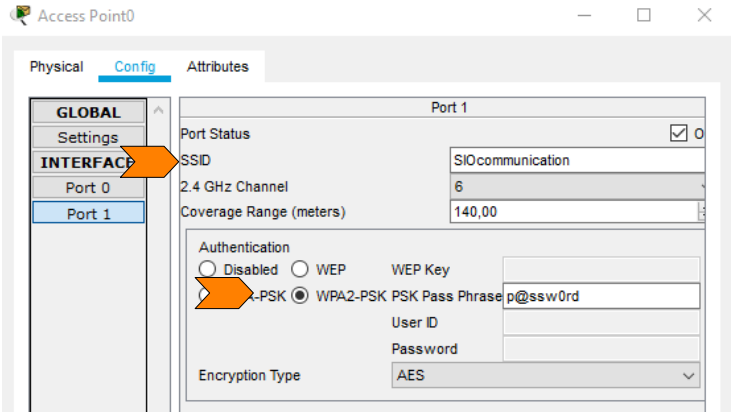


ANNEXE 3

Configuration IP des différents hôtes

Infra N°	Hôte	Adresse IP	Masque de sous-réseau	Passerelle	Modèle sous Packet Tracer
1	sta1	192.168.1.1	255.255.255.128	192.168.1.126	PC
1	sta2	192.168.1.2	255.255.255.128	192.168.1.126	PC
2	sta3	192.168.1.3	255.255.255.128	192.168.1.126	PC
2	Server0	192.168.1.100	255.255.255.128	192.168.1.126	Server
2	Printer0	192.168.1.120	255.255.255.128	192.168.1.126	Printer
2	Smartphone0	192.168.1.10	255.255.255.128	192.168.1.126	Smart Device
2	TabletPC0	192.168.1.11	255.255.255.128	192.168.1.126	Wireless Tablet
2	Laptop0	192.168.1.12	255.255.255.128	192.168.1.126	Laptop
3	sta4	192.168.1.129	255.255.255.128	192.168.1.254	PC
3	Router0 (2 interfaces) + 3ième interface (réseau inter-routeur)	192.168.1.126	255.255.255.128		PT Router
3		192.168.1.254	255.255.255.128		
4		192.168.3.2	255.255.255.252		
4	sta5	192.168.2.1	255.255.255.0	192.168.2.254	PC
4	Router1 (2interfaces)	192.168.2.254	255.255.255.0		PT Router
4		192.168.3.1	255.255.255.252		

Les switchs utilisés sous Packet Tracer sont les modèles 2960.

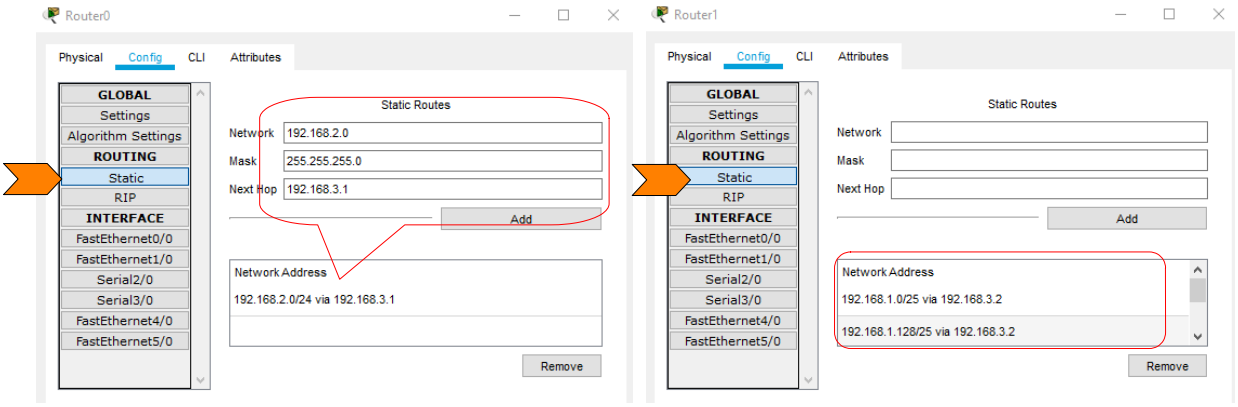


Paramétrage du réseau sans-fil ou Wi-Fi :

Sur un réseau Wi-Fi (« *Wireless Fidelity* »), les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau (SSID = *Service Set IDentifier*) afin de pouvoir communiquer.

Elles doivent aussi utiliser la même méthode d'authentification.

Paramétrage du routage sur les 2 routeurs (pour dernière infrastructure – étape 4) :



Commandes Linux particulières utilisées dans ces différentes activités

Comme vu en TC1, les composants de Linux fonctionnent un peu à la manière d'un « Play Store » sous Androïd.
On les retrouve sur des serveurs « miroirs » définis lors de l'installation.
On peut interagir avec à l'aide de la commande apt-get ou apt, l'évolution de cette dernière.

A chaque fin d'installation, il faut réaliser une première vérification des mises à jour :
```
apt update
apt upgrade
```

Si vous désirez installer une application, il faut utiliser la commande apt install suivi du nom du « paquet » correspondant à l'application souhaitée :
Exemple : pour l'installation des Tools de Vmware.
```
apt install open-vm-tools
```

Téléchargement de fichiers

Les serveurs sous Linux sont majoritairement installés sans interface graphique.
Afin de pouvoir télécharger un fichier qui se trouve sur l'internet, nous pouvons utiliser la commande wget.

Exemple : `wget https://www.monordinateur.fr/pilotes/epson.zip`

Planification sauvegarde

La planification de tâches permet l'exécution de tâches à un moment donné.

Afin de tester la bonne exécution des tâches, il est conseillé de faire des planifications très courtes ; planifications qui seront à rétablir un fois le recettage effectué.

Afin de vous aider dans l'écriture de la commande de planification CRON, vous pouvez vous aider du site suivant : https://crontab.guru/