



Objectif de la séquence

L'objectif de la séquence est de créer et maintenir un réseau d'entreprise dans le cloud.

Vous êtes administrateur réseau.

Votre entreprise souhaite avoir un premier retour d'expérience sur l'installation et la maintenance d'un de ces services dans le cloud.

Elle décide d'externaliser dans le cloud AWS son site web institutionnel. Celui-ci est basé sur la solution WordPress. Il vous est demandé de vous former, d'installer le CMS WordPress et d'organiser la sauvegarde de ce CMS (web et bdd)

Vous devez mettre en place le réseau de l'entreprise composé d'un serveur web et d'un serveur de base de données.

Vous devrez également mettre en place la politique de sauvegarde de l'entreprise en cas de défaillance matérielle et/ou d'attaque sur ce réseau.

Cela comprend :

- La sauvegarde régulière des informations de la base de données
- La sauvegarde des données du CMS

La séquence est découpée en plusieurs modules :

- Activité 1 – Se former au cloud, cas AWS
- Activité 2 - Créer l'infrastructure du SI dans le cloud AWS
- Activité 3 - Mise en place de la politique de sauvegarde et de restauration du réseau

Durée

- 1 séance de 5 h

Livrable

- Votre compte rendu avec les résultats attendus et les réponses aux questions



I. Objectif de l'activité 3

L'activité 3 consiste à sauvegarder et restaurer le serveur WordPress de l'entreprise.

Pour cela, il faut avant tout définir la politique de sauvegarde et de restauration de l'entreprise.

Document Cours

- ✓ Politique de sauvegarde et restauration d'un SI

II. Plan de sauvegarde et restauration du SI

Le plan de sauvegarde et restauration est défini ainsi :

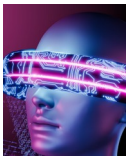
II.1 Éléments à sauvegarder

- Serveur Web WordPress
- Serveur base de données

II.1.1 Serveur Web

Concernant le serveur web, les éléments à sauvegarder sont les suivants

Répertoire	Contenu
/var/www/wordpress	Site web "WordPress"



II.1.2 Serveur Base de données

Concernant le serveur base de données, les éléments à sauvegarder sont les suivants

- Serveur RDS via snapshot et sauvegarde programmée

II.2 Objectif de récupération RPO et RTO

Les indicateurs RPO et RTO du SI sont définis ainsi

Indicateurs	Temps maximum
RPO	2 heures
RTO	4 heures



II.3 Choix des types de sauvegardes

Les sauvegardes à mettre en place seront de type **différentiel**.

II.4 Stratégie de sauvegarde

Le tableau ci-dessous synthétise les fréquences des sauvegardes selon les éléments à sauvegarder.

II.4.1 Fréquence

Serveur	Répertoire ou service	Fréquence
EC2	/var/www/wordpress	Toutes les 12 heures
Base de données	RDS	Toutes les 24 heures

II.4.2 Planification

Compte tenu du fait que les utilisateurs du SI (Web et BDD) sont essentiellement sur le fuseau horaire de paris, les sauvegardes seront effectuées à 2 h (GMT+2)

II.4.3 Emplacement des sauvegardes

Les sauvegardes seront stockées à deux endroits différents pour limiter la corruption des données

- En local sur les serveurs
- À distance sur l'infrastructure de l'entreprise (option dans l'activité)

II.4.4 Sécurité des sauvegardes

Les données sauvegardées doivent être protégées contre les accès non autorisés.

Pour cela :

- Les données seront sauvegardées au repos via un chiffrement GPG symétrique
- Lors du transfert des sauvegardes, SCP sera utilisée

II.4.5 Politique de rétention

La politique de rétention définies est la suivante.

Elle équilibre le besoin de stocker des sauvegardes anciennes avec les coûts de stockage.



Sauvegardes	Durée de rétention
Sauvegardes journalières	Conserver les sauvegardes quotidiennes pendant 7 jours
Sauvegardes hebdomadaires	Conserver les sauvegardes hebdomadaires pendant un mois
Sauvegardes mensuelles	Conserver les sauvegardes mensuelles pendant un an

II.5 Automatisation des sauvegardes

- Les sauvegardes de l'EC2 seront automatisées en utilisant les logiciels `tar` (pour créer les sauvegardes complètes et différentielles) et `cron` (pour automatiser la sauvegarde)
- Les sauvegardes du RDS sont programmées via le service de sauvegarde spécifique.

II.6 Surveillance des sauvegardes

Un mail sera envoyé à l'administrateur en cas d'échec de la sauvegarde. (option dans l'activité)

II.7 Test de restauration

Une fois la stratégie de sauvegarde mise en place, la procédure de restauration sera testée pour s'assurer que les données sauvegardées peuvent être récupérées.

De plus un scénario de sinistre sera simulé pour vérifier si les délais de récupération RTO sont respectés. *

* Cette tâche sera réalisé optionnellement



III. Réalisation du plan de sauvegarde et restauration

Vous allez réaliser le plan de sauvegarde et restauration du SI tel que défini dans le chapitre précédent.

III.1 Le serveur Web-dossier `/var/www/wordpress`

Outils

tar : [https://fr.wikipedia.org/wiki/Tar_\(informatique\)](https://fr.wikipedia.org/wiki/Tar_(informatique))

cron : <https://fr.wikipedia.org/wiki/Cron>

Vous allez configurer les sauvegardes chiffrées (complètes et différentielles) du répertoire `/var/www/wordpress` du serveur web

Vous allez créer avant tout des sauvegardes manuelles, puis les chiffrer, puis automatiser le processus.

III.1.1 Création d'une sauvegarde complète

Soit les commandes suivantes

- Créer l'arborescence de répertoire pour les archives

```
mkdir -p /home/admin/backup/web-site
```

- Créer la sauvegarde complète

```
tar --create -gzip \  
--listed-incremental=/home/admin/backup/web-site/backup.snar \  
--file=/home/admin/backup/web-site/WordPress_full_$(date +%F).tar.gz \  
/var/www/wordpress
```

Q1 Expliquer les options de la ligne de commande précédente

Tâche1. Configurer la sauvegarde complète du répertoire `/var/www/wordpress` dans le répertoire `/home/admin/backup/web-site`



Résultats attendus

- L'archive `wordpress_full_<date>.tar.gz` est créée dans le répertoire `/home/admin/backup/web-site`
- Le fichier `backup.snar` est créé dans le répertoire `/home/admin/backup/web-site`

III.1.2 Création d'une sauvegarde différentielle

Q2 : Donner la définition d'une sauvegarde différentielle

Soit les commandes suivantes

- Créer la sauvegarde différentielle

```
tar --create --gzip  
--listed-incremental=/home/admin/backup/web-site/backup.snar  
--file=/home/admin/backup/web-site/wordpress_diff_$(date +%F).tar.gz  
/var/www/wordpress
```

Q3 : Expliquer les options de la ligne de commande précédente

Préalable : Modifier un aspect du site web avant d'effectuer la sauvegarde différentielle

Tâche2. Créer la sauvegarde différentielle du répertoire `/var/www/wordpress` dans le répertoire `/home/admin/backup/web-site`

Résultats attendus

- L'archive `wordpress_diff_<date>.tar.gz` est créé dans le répertoire `/home/admin/backup/web-site`
- Le fichier `backup.snar` a été mis à jour



III.1.3 Restaurer les sauvegardes

Vous allez vérifier que les sauvegardes puissent être correctement restaurées.

Soit les commandes suivantes

```
tar -xzf /home/admin/backup/web-site/wordpress_full_<date>.tar.gz -C  
/home/admin/test_restore  
  
tar -xzf /home/admin/backup/web-site/wordpress_diff_<date>.tar.gz -C  
/home/admin/test_restore
```

Q3 : Expliquer les options des lignes de commandes ci-dessus.

Tâche3. Restaurer la sauvegarde complète et différentielle dans le répertoire
/home/admin/test_restore

Résultats attendus

- Le répertoire /var/www/wordpress est correctement restauré dans
/home/admin/test_restore
- Les modifications sont également restaurées une fois l'archive différentielle
également restaurée.

III.1.4 Chiffrer les archives

Vous allez chiffrer l'archive avec un mot de passe interactif

Soit les commandes suivantes

```
gpg --batch --yes --passphrase "mlp-ciel" --symmetric --cipher-algo AES256  
/home/admin/backup/web-site/wordpress_full_<date>.tar.gz
```

Q3 : Expliquer les options des lignes de commandes ci-dessus.

Tâche4. Chiffrer l'archive complète avec un mot de passe interactif (*ne pas oublier de
détruire ensuite le fichier à chiffrer en production*)

**Résultats attendus**

- Le fichier `wordpress_full_2024-09-25.tar.gz.gpg` est créé dans le répertoire `/home/admin/backup/web-site/`
- Avec le mauvais mot de passe, l'archive n'est pas déchiffrée
- Avec le bon mot de passe, l'archive est déchiffrée (fichier `apache2_full_restored.tar.gz`)

III.1.5 Automatiser les sauvegardes

Vous allez automatiser les sauvegardes en utilisant un script bash et la crontab

Ressources

<https://doc.ubuntu-fr.org/cron>

<https://opensource.com/article/17/11/how-use-cron-linux>

Procédure

Vous avez déjà créé des scripts bash dans une séquence précédente. Ici votre script doit reprendre les éléments précédents du TP (création d'une archive chiffrée différentielle)

Vous allez utiliser cron et la crontab pour automatiser les sauvegardes.

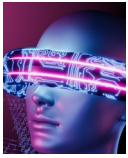
Conseils

- Procéder par étapes successives
- Créer la sauvegarde chiffrée en utilisant un fichier contenant le mot de passe

Tâche5. En utilisant un script bash, automatiser la création des sauvegardes complètes et différentielles.

Résultats attendus

- Le script `/home/admin/backup-web-site-test.sh` est créé et contient la configuration de test
- Le script est exécutable
- Le script est appelé dans la crontab toutes les 5 minutes
- Au bout de 15 minutes, le répertoire `/home/admin/backup/web-site` contient une sauvegarde complète et 2 sauvegardes différentielles



III.2 Sauvegarde RDS

Ressource

https://docs.aws.amazon.com/fr_fr/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

Tâche6. Suivre les recommandations d’AWS pour activer les sauvegardes automatiques de votre base de données

Résultats attendus

- Les sauvegardes automatiques sont programmées, tous les jours, avec une période de rétention de 7 jours.