Plan de Reprise d'Activité (PRA) et Plan de Retour à la Normale (PRASN)

SCÉNARIO 1 : Panne réseau totale

PRA (Actions immédiates)

- **Contexte :** Plus aucune communication entre les 3 VMs.
- **Impacts :** AD inaccessible, site web HS, client Windows inutilisable.
- **Actions :**
  1. Vérifier la configuration réseau des VMs (IP, passerelle, connexion active).
  2. Tester la connectivité avec un ping entre les machines.
  3. Redémarrer les interfaces réseau si nécessaire.
  4. Restaurer un snapshot récent si la panne persiste.

PRASN (Retour à la normale)

1. Corriger la configuration réseau et noter les paramètres corrects.
2. Sauvegarder la configuration fonctionnelle.
3. Documenter l'incident et créer un guide de résolution rapide.
4. Tester la connexion après reboot des VMs.

SCÉNARIO 2 : Intrusion sur l'Active Directory

PRA

- **Contexte :** Un compte administrateur compromis.
- **Impacts :** Fuite de données, risque de propagation de l'attaque.
- **Actions :**
  1. Déconnecter la VM AD du réseau.
  2. Analyser les logs de sécurité (Event Viewer) pour identifier l'attaque.
  3. Restaurer un snapshot avant l'intrusion (si disponible).
  4. Changer les mots de passe des comptes sensibles.

PRASN

1. Mettre en place l'authentification forte (MFA) pour l'admin AD.
2. Créer un script de sauvegarde automatique des GPOs et utilisateurs.
3. Tester la connexion sécurisée au domaine.
4. Former l'équipe aux bonnes pratiques de sécurité sur AD.

SCÉNARIO 3 : Coupure d'alimentation prolongée

PRA

- **Contexte :** Coupure électrique impactant les VMs.
- **Impacts :** Toutes les machines sont arrêtées brutalement.
- **Actions :**
  1. Vérifier si la machine physique redémarre correctement.
  2. Démarrer les VMs dans l'ordre : AD → Client Windows 10 → Serveur Web.
  3. Tester l'accès aux services (connexion AD, accès site web).

PRASN

1. Vérifier l'intégrité des VMs après redémarrage.
2. Mettre en place des snapshots réguliers avant chaque TP.
3. Sauvegarder les données critiques en local et sur un stockage externe.

SCÉNARIO 4 : Panne de sauvegarde réseau

PRA

- **Contexte :** Impossible d'accéder aux snapshots et backups.
- **Impacts :** Risque de perte définitive des données.
- **Actions :**
  1. Vérifier l'état du stockage contenant les sauvegardes.
  2. Tester l'accès à une ancienne sauvegarde manuelle.
  3. Si nécessaire, recréer un snapshot de secours immédiatement.

PRASN

1. Automatiser les sauvegardes vers un stockage externe (USB, NAS).
2. Tester la restauration d'un snapshot chaque semaine.
3. Créer un document de procédure de récupération rapide.

SCÉNARIO 5 : Crash du service Web

PRA

- **Contexte :** Le serveur Web ne répond plus.
- **Impacts :** Site web inaccessible.
- **Actions :**
  1. Vérifier l'état du service Web (Apache/IIS/MySQL).
  2. Redémarrer les services impactés.
  3. Restaurer un snapshot si nécessaire.

PRASN

1. Tester la montée en charge avant chaque mise en production.
2. Mettre en place des sauvegardes automatiques de la base de données.
3. Créer un script de redémarrage automatique en cas de crash.

SCÉNARIO 6 : Base de données compromise

PRA

- **Contexte :** Injection SQL ou suppression accidentelle des données.
- **Impacts :** Données corrompues, site web inutilisable.
- **Actions :**
  1. Restaurer une sauvegarde froide de la base de données.
  2. Isoler la machine pour éviter la propagation.
  3. Appliquer un correctif de sécurité (ex : validation des entrées SQL).

PRASN

1. Vérifier les permissions sur la base pour éviter les accès non autorisés.
2. Appliquer un pare-feu applicatif (WAF) pour protéger contre les injections SQL.
3. Tester la restauration de la base chaque semaine.

SCÉNARIO 7 : Version logicielle non fonctionnelle

PRA

- **Contexte :** Une mise à jour fait planter l'application.
- **Impacts :** Site web ou application inutilisable.
- **Actions :**
  1. Revenir au snapshot précédent (rollback).
  2. Analyser les logs pour comprendre l'erreur.
  3. Corriger et tester la mise à jour avant un nouveau déploiement.

PRASN

1. Utiliser un environnement de test avant la mise en production.
2. Automatiser les tests pour détecter les erreurs avant le déploiement.
3. Documenter les mises à jour pour éviter les erreurs similaires.

SCÉNARIO 8 : Attaque par ransomware

PRA

- **Contexte :** Chiffrement des données sur toutes les VMs.
- **Impacts :** Perte totale d'accès aux fichiers.
- **Actions :**
  1. Éteindre immédiatement toutes les VMs pour limiter la propagation.
  2. Restaurer un snapshot sain des VMs.
  3. Analyser l'origine de l'attaque et corriger la faille.

PRASN

1. Mettre en place des sauvegardes hors ligne (stockage externe).
2. Former l'équipe à la détection des menaces (emails, sites frauduleux).
3. Tester la résistance aux attaques via des simulations.

SCÉNARIO 9 : Inondation des locaux

PRA

- **Contexte :** Dommages matériels sur la machine physique.
- **Impacts :** Serveurs HS, perte de données potentielles.
- **Actions :**
  1. Transférer les snapshots et backups sur un autre stockage.
  2. Utiliser un PC de secours pour accéder aux sauvegardes si possible.

PRASN

1. Mettre les équipements en hauteur pour limiter les dégâts.
2. Planifier un PRA externe (hébergement des VM sur un autre serveur).
3. Tester la récupération de données sur un autre PC.