Conception et déploiement d'une infrastructure réseau virtualisée redondée sous Proxmox (MFR)

Table des matières

Présentation de la situation professionnelle 3
Contexte technique 3
Architecture mise en place 3
Sécurisation et segmentation 4
Tests et validation 4
Apports professionnels 5
Bilan 5

Présentation de la situation professionnelle

Dans le cadre de ma formation en BTS SIO option SISR à la MFR, j'ai participé à la conception et au déploiement d'une infrastructure réseau complète entièrement virtualisée sous Proxmox VE.

L'objectif pédagogique était de reproduire une architecture d'entreprise réaliste, intégrant la redondance des services critiques et la sécurisation des flux réseau, tout en travaillant exclusivement dans un environnement virtualisé, sans matériel physique.

Cette situation m'a permis d'intervenir sur une architecture globale comprenant deux contrôleurs de domaine Active Directory avec DNS redondé, deux serveurs DHCP configurés en basculement, un cluster de deux pare-feux pfSense en haute disponibilité, ainsi qu'un serveur SFTP isolé en DMZ.

Contexte technique

L'infrastructure était hébergée sur un hyperviseur Proxmox VE. Plusieurs bridges virtuels ont été créés afin de simuler des segments réseau distincts : un réseau WAN, un réseau LAN interne, un réseau serveurs, une DMZ et un réseau dédié à la synchronisation des pare-feux.

L'objectif n'était pas seulement de faire fonctionner les services, mais de mettre en place une architecture cohérente et tolérante aux pannes. Dans un environnement professionnel physique, une telle architecture aurait reposé sur des équipements matériels redondés de type WatchGuard ou Zyxel. Dans notre cadre virtualisé, pfSense a été retenu pour reproduire ces mécanismes de haute disponibilité.

Architecture mise en place

L'infrastructure repose sur plusieurs niveaux de redondance.

Deux contrôleurs de domaine Windows Server ont été déployés. Chacun assure le rôle AD DS et DNS. La réplication Active Directory permet de synchroniser les objets (comptes utilisateurs, groupes, stratégies), tandis que le service DNS intégré garantit la résolution de noms même en cas d'indisponibilité d'un des serveurs. Les postes clients sont configurés avec les deux serveurs DNS afin d'assurer la continuité de l'authentification.

Deux serveurs DHCP ont également été mis en place en mode failover. Cette configuration permet de répartir la charge et d'assurer la distribution continue d'adresses IP même si l'un des serveurs devient indisponible. Les scopes ont été configurés de manière cohérente avec les différents segments réseau.

La couche de sécurité périmétrique repose sur deux pare-feu pfSense configurés en cluster haute disponibilité. Le protocole CARP permet de partager une adresse IP virtuelle utilisée comme passerelle par l'ensemble des machines du réseau interne. Le service pfsync assure la

synchronisation des états de connexion afin d'éviter toute interruption des sessions actives lors d'un basculement. La synchronisation XMLRPC garantit que les règles de pare-feu, les règles NAT et les paramètres système restent identiques sur les deux nœuds.

Un serveur SFTP unique a été déployé dans une zone DMZ distincte du réseau interne. Ce serveur permet le transfert sécurisé de fichiers tout en étant isolé des contrôleurs de domaine et des postes clients. Les règles de pare-feu autorisent uniquement les flux nécessaires vers ce serveur, conformément au principe du moindre privilège.

Sécurisation et segmentation

La segmentation réseau a été un élément central du projet. Le réseau LAN interne est isolé de la DMZ par le cluster pfSense. Les contrôleurs de domaine ne sont accessibles que depuis les segments autorisés. Les flux vers le serveur SFTP sont strictement filtrés.

La mise en place d'un réseau dédié à la synchronisation des pares-feux permet d'isoler le trafic de réplication CARP et pfsync du reste du réseau, garantissant stabilité et sécurité.

Cette organisation permet de limiter l'impact potentiel d'une compromission en DMZ et de préserver l'intégrité du cœur du système d'information.

Tests et validation

Plusieurs scénarios de panne ont été simulés afin de vérifier la robustesse de l'architecture.

L'arrêt volontaire d'un des pare-feux a entraîné un basculement automatique vers le second nœud, sans perte de connectivité pour les postes clients. Les sessions en cours ont été maintenues grâce à la synchronisation des états.

La désactivation d'un contrôleur de domaine n'a pas empêché l'authentification des utilisateurs, la réplication AD ayant déjà synchronisé les données et le second serveur DNS assurant la résolution des noms.

La coupure d'un serveur DHCP n'a pas interrompu la distribution d'adresses IP, le second serveur prenant le relais conformément à la configuration de basculement.

Des tests d'accès au serveur SFTP depuis le LAN et via les règles NAT ont également été réalisés afin de valider la configuration de la DMZ.

Apports professionnels

Cette situation m'a permis d'acquérir une vision globale d'une architecture d'entreprise structurée autour de la redondance et de la sécurité.

J'ai consolidé mes compétences en :

-administration Active Directory et réplication ;

-configuration DNS redondée ;

-mise en place de DHCP en failover ;

-configuration avancée de pare-feu pfSense en haute disponibilité ;

-gestion d'une infrastructure virtualisée sous Proxmox ;

-segmentation réseau et isolation DMZ.

Au-delà de la technique, ce projet m'a permis de comprendre l'importance de la planification d'architecture et de l'anticipation des points de défaillance.

Bilan

Même si l'environnement était pédagogique et entièrement virtualisé, l'architecture mise en place reproduit fidèlement les mécanismes utilisés en entreprise. Les principes de redondance, de segmentation et de continuité de service sont identiques à ceux rencontrés dans des infrastructures professionnelles.

Cette situation professionnelle démontre ma capacité à concevoir et déployer une infrastructure réseau complète, sécurisée et tolérante aux pannes, en intégrant plusieurs technologies complémentaires.

Elle constitue l'une des réalisations les plus représentatives de mes compétences en administration système et réseau dans le cadre du BTS SIO SISR.