

Rapport d'infrastructure réseau MuséoConnect

Introduction :

Le cahier des charges pour l'infrastructure réseau du Louvre expose les défis majeurs rencontrés avec leur système informatique datant des années 2000, engendrant des problèmes tels que des ralentissements, des pertes de données et une gestion inefficace du matériel. L'objectif principal est d'améliorer l'efficacité des collaborateurs en modernisant l'infrastructure pour répondre à l'augmentation des besoins en capacité et en performance, tout en améliorant la gestion du matériel et des données. Cela nécessite des méthodes de gestion plus efficaces pour réduire les erreurs et les pertes, ainsi que l'amélioration de la connectivité et l'adoption de solutions de stockage et de collaboration modernes pour favoriser la mobilité et la collaboration, tout en se conformant aux réglementations du RGPD. Ce rapport décrit l'infrastructure réseau mise en place, y compris la topologie et les configurations mis en œuvre. L'infrastructure est conçue pour être évolutive, sécurisée et fiable.

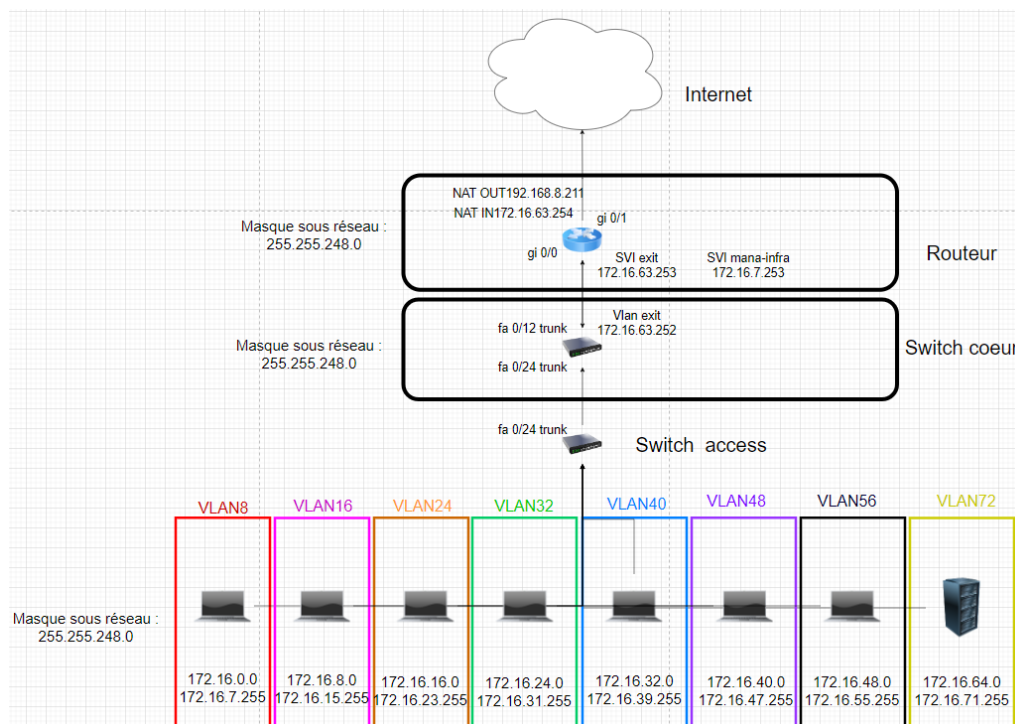
Topologie :

La topologie du réseau est en maillage, ce qui signifie que chaque périphérique est connecté à plusieurs autres périphériques. Cela permet de créer un réseau redondant et résilient, ce qui signifie que le réseau continuera à fonctionner même si un périphérique tombe en panne.

Le réseau est composé des équipements suivants :

- 1 routeur
- 1 switch cœur
- 1 switch d'accès
- Plusieurs Ordinateurs
- Plusieurs machines virtuel Windows 10 sur VirtualBox
- 1 serveur Proxmox
 - 1 Serveur ADDS, DHCP et DNS sous Windows serveur 2022
 - 1 Serveur de fichier sous Windows serveur 2022
 - 1 Debian 12 LAMP avec Apache pour le site web
 - 1 Debian 12 avec MariaDB pour la base de données

Architecture réseau :



Plan d'adressage des Vlan :

Adresse réseau	Masque	Première adresse réseau	première adresse dhcp	adresse de fin dhcp	Adresse broadcast	gateway	VLANs	Nom de VLAN
172.16.0.0	255.255.248.0	172.16.0.1	172.16.0.10	172.16.7.250	172.16.7.254	172.16.7.253	vlan 8	mana-infra
172.16.8.0	255.255.248.0	172.16.8.1	172.16.8.10	172.16.15.250	172.16.15.254	172.16.15.254	vlan 16	mana-systeme
172.16.16.0	255.255.248.0	172.16.16.1	172.16.16.10	172.16.23.250	172.16.23.254	172.16.23.254	vlan 24	employes
172.16.24.0	255.255.248.0	172.16.24.1	172.16.24.10	172.16.31.250	172.16.31.254	172.16.31.254	vlan 32	ateliers
172.16.32.0	255.255.248.0	172.16.32.1	172.16.32.10	172.16.39.250	172.16.39.254	172.16.39.254	vlan 40	conservations
172.16.40.0	255.255.248.0	172.16.40.1	172.16.40.10	172.16.47.250	172.16.47.254	172.16.47.254	vlan 48	conservateurs
172.16.48.0	255.255.248.0	172.16.48.1	172.16.48.10	172.16.55.250	172.16.55.254	172.16.55.254	vlan 56	compta/rh
172.16.56.0	255.255.248.0	172.16.56.1			172.16.63.254	172.16.63.254	vlan 64	exit
172.16.64.0	255.255.248.0	172.16.64.1			172.16.71.254	172.16.71.254	vlan 72	mana-serveurs

Chaque ports du switch access est attribué à un VLAN. Les VLANs permettent de segmenter le réseau en plusieurs réseaux logiques, ce qui permet d'améliorer la sécurité et la gestion du trafic.

Chaque Vlan possèdent les noms des services auxquelles elles sont attribuées.

- La vlan 8 est utilisé pour les administrateurs afin d'administrer les équipements sur le réseau (Routeur, switch cœur et switch access).
- La vlan 16 est utilisé les équipements systèmes (point d'accès wifi).
- La vlan 64 elle ne possède pas d'adressage IP en DHCP car elle permet uniquement de faire sortir les utilisateurs du réseau vers le réseau extérieur afin de pouvoir accéder à internet.
- La vlan 72 est utilisé pour le serveur Proxmox qui héberge différents serveurs. Elle ne possède pas d'adressage IP en DHCP car les serveurs se configurent en IP statique.

Configuration des équipements :

Le SSH est activé en local sur le routeur, le switch cœur et le switch access. Afin de se connecter en SSH l'adresse IP du routeur est 172.16.7.253, le switch cœur 172.16.7.252 et le switch access 172.16.7.251. Cependant, l'accès SSH est restreint aux utilisateurs du VLAN 8 uniquement. Cela est réalisé à l'aide d'une liste d'accès, qui est une liste d'adresses IP autorisées à accéder au SSH.

Routeur : Il est configuré avec une adresse IP statique et une passerelle par défaut. Le routeur est configuré en NAT pour permettre aux utilisateurs de notre réseau de pouvoir communiquer avec les réseaux extérieurs. Le routeur possède deux SIV, une sous interface exit de la vlan 64 et une sous interface mana-infra de la vlan 8. La SVI exit permet de faire sortir les utilisateurs du réseau vers le réseau extérieur, elle possède une interface avec un adresse IP afin de pouvoir communiquer avec la vlan exit qui est configuré sur le switch cœur. La vlan mana-infra permet aux administrateurs du réseau de pouvoir se connecter à distance au SSH du routeur afin de réaliser de la maintenance.

Switch cœur : Il est en mode IP routing afin de router les adresses IP envoyés par le serveur DHCP. La vlan exit est configuré afin de pouvoir communiquer avec la SVI exit du routeur. Certains ports sont attribués à un VLAN spécifique. Le port 12 est en mode trunk afin de faire passer la vlan exit et mana-infra vers le routeur. Le port 24 est en mode trunk vers le switch access.

Switch d'accès : Il est configuré avec des Vlan attribués aux ports. Cela permet aux équipements connectés à ce port de communiquer uniquement avec les autres équipements du même VLAN. La répartition des ports sur le switch a été réalisé en fonction du nombre d'utilisateur par Vlan. Certains services demandent plus de postes informatiques, plusieurs ports sont nécessaires pour relier le même service a plusieurs endroits.

Adressage des ports sur le switch d'access :

```
SWA1-DKRET#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/17, Fa0/23, Gig0/1, Gig0/2
8	mana-infra	active	Fa0/1, Fa0/2
16	mana-systeme	active	Fa0/3, Fa0/4, Fa0/5
24	employes	active	Fa0/6, Fa0/7, Fa0/8
32	ateliers	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13
40	conservations	active	Fa0/14, Fa0/15, Fa0/16
48	conservateurs	active	Fa0/18, Fa0/19, Fa0/20
56	compta/rh	active	Fa0/21, Fa0/22
64	exit	active	
72	mana-serveurs	active	Fa0/9
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Configuration du serveur Proxmox :

Le serveur Proxmox est attribué à la vlan 72 sur le port 9 du switch access. Son adresse IP est 172.16.64.1. Le serveur contient une template de Windows serveur 2022 et une Debian 12. Une template est une image de machine virtuelle préconfigurée et prête à être utilisée pour créer de nouvelles machines virtuelles.

Les différentes machines virtuelles sur le serveur :

- Un Windows serveur 2022 avec l'adresse IP 172.16.64.4. Le DHCP, l'ADDS et le DNS configuré et fonctionnel. Le DHCP a été configuré avec plusieurs étendu en fonction de chaque Vlan sur le réseau. L'ADDS est configuré en plusieurs Unité d'organisation en fonction des différents services du musée ainsi que les différents groupe utilisateur (administrateur, utilisateur, ordinateur utilisateur ...). Les utilisateurs peuvent se connecter aux postes sur le réseau avec comme nom d'utilisateur (première lettre du prénom suivi du nom de famille) ainsi qu'un mot de passe près-défini qui répond aux normes de la RGPD sur la gestion et la création de mot de passe. Il comprend au minimum douze caractères, une majuscule, deux chiffres, un caractère spécial ainsi que des lettres minuscules. Une rotation des mots des passes est mise en place pour changer tous les 30 jours.
- Un Windows serveur 2022 avec l'adresse IP 172.16.64.5. Il permet de stocker les sessions des utilisateurs ainsi que leurs fichiers. Un répertoire Z du serveur est partagé sur le réseau afin que les utilisateurs puissent se connecter à leurs sessions et enregistrer leurs documents.
 - Le répertoire HomeFolders est partagé aux utilisateurs afin qu'ils puissent enregistrer leurs documents. Celui-ci est segmenté en sous répertoire en fonction des utilisateurs qui enregistrent des documents. Seuls les utilisateurs de leurs répertoires peuvent accéder à son contenu.
 - Le répertoire Profiles est configuré pour enregistrer les configurations de Windows enregistré sur la session de l'utilisateur (Fond d'écran ...). Seul un administrateur peut accéder à ce répertoire.
- Une Debian 12 LAMP est configuré afin d'héberger la billetterie en ligne du musée et permettre aux utilisateurs de réserver une place pour visiter le musée.
- Une Debian 12 est configuré avec une base de données MariaDB. Elle permet de stocker les informations nécessaires aux bons fonctionnements de la billetterie (Compte utilisateur enregistré sur la billetterie, informations de paiements ...)

Configuration des postes informatiques :

Les postes sont en adressage IP automatique, le serveur DHCP attribue automatiquement les informations nécessaires au bon fonctionnement du poste sur le réseau. Les utilisateurs peuvent se connecter aux postes sur le réseau avec comme nom d'utilisateur (première lettre du prénom suivi du nom de famille) ainsi qu'un mot de passe prédéfini. Des droits administrateurs sont nécessaires pour installer des logiciels ou modifier certains paramètres dans Windows.

Tests réalisés :

Afin de tester le bon fonctionnement de notre infrastructure, nous avons réalisés les tests suivants :

- Pour tester le DHCP sur les postes : Les postes ont été mis en adressage IP automatique en DHCP. Ils reçoivent correctement une adresse IP ainsi que toutes les informations complémentaires au bon fonctionnement sur le réseau. Nous avons réalisé des pings entre différents postes se trouvant dans la même vlan afin de confirmer le bon fonctionnement.
- Pour tester les Vlan : Afin de tester que chaque vlan ne communique pas entre elle, des pings ont été réalisés entre différents postes se trouvant sur différentes vlan. Les requêtes ping n'aboutissent pas car les Vlan sont correctement configurés.
- Pour tester le bon fonctionnement de l'ADDS : Nous avons essayé de se connecter à un compte créé et configuré dans l'ADDS sur différents postes qui ont été ajoutés au domaine.
- Pour tester le NAT : Depuis les postes nous avons réalisé des pings vers des DNS public ainsi que des recherches sur les navigateurs web pour vérifier le bon fonctionnement et l'accès à internet.

Conclusion :

En tant que chef de mon groupe, j'ai distribué les tâches à réaliser à mon équipe. Toutes les tâches ont été réalisées équitablement par l'équipe. Chacune des personnes de l'équipe a pu contribuer à la réalisation de chacune des tâches citées précédemment afin d'apprendre à mettre en place une architecture réseau. De mon côté j'ai réalisé la configuration de la SVI exit, l'ajout d'adresse IP en guise de Gateway dans le switch cœur pour les Vlan. J'ai configuré sur le switch cœur, le IP Routing afin de router les vlan vers la vlan exit et le IP Helper-Address pour permettre au DHCP de se diffuser sur le réseau. J'ai installé le serveur Windows server et File-Server sur le serveur Proxmox. J'ai configuré une partie des étendu du DHCP ainsi que l'ADDS. J'ai aidé mon équipe dans leurs tâches afin de montrer et expliquer les configurations. À la suite d'un problème de dernière minute qui a rendu le serveur DHCP hors service, j'ai réalisé la reconfiguration totale du serveur DHCP et ADDS.

L'architecture réalisée par l'équipe apporte une meilleure évolutivité et bien plus sécurisé. Elle implémente la segmentation en VLANs qui permet une gestion efficace du trafic et renforce la sécurité, avec des attributions claires pour différents services et utilisateurs. La configuration des équipements, notamment l'activation du SSH restreint aux administrateurs,

montre une attention particulière à la sécurité. Le déploiement du serveur Proxmox, avec ses machines virtuelles dédiées permet de centraliser plusieurs services en un seul serveur Proxmox et ainsi réaliser des économies d'argent, de place dans le cas de notre petite infrastructure de test. Pour l'infrastructure réel, des serveurs seront utilisés afin de pouvoir subvenir aux besoins du nombre conséquent d'utilisateur. De la redondance sera mis en place avec plusieurs switch, switch cœur et routeur afin d'éviter toutes panne sur le réseau. Toutes les tâches ont été réalisées équitablement par l'équipe. Chacune des personnes de l'équipe a pu contribuer à la réalisation de chacune des tâches citées précédemment afin d'apprendre à mettre en place une architecture réseau.

Ci-joint l'architecture fonctionnelle sous le logiciel Cisco Packet Tracer.



infrastructure
réseau Théo Cabrell