BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2016

E5SR : PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES

Durée : 4 heures **Coefficient : 5**

CAMERA

Ce sujet comporte 16 pages dont 11 pages de documentation.
La candidate ou le candidat est invité.e à vérifier que le sujet qui lui a été remis est complet.

Conformément aux recommandations du Haut Conseil à l'Égalité entre les femmes et les hommes dans son guide publié en novembre 2015, l'expression du féminin et du masculin s'effectue en utilisant le point, par exemple, client.e.

Aucun matériel ni document autorisé

Documentation jointe :

DOCUMENTS COMMUNS 6

DOCUMENT 1: DESCRIPTION PARTIELLE DU RÉSEAU DE LA MAIRIE 6
DOCUMENT 2 : SCHÉMA LOGIQUE SIMPLIFIÉ DU RÉSEAU DE LA MAIRIE 10

DOCUMENTS POUR LE DOSSIER A 11

DOCUMENT A.1 : EXPRESSION DES BESOINS 11
DOCUMENT A.2 : PROCÉDURE DE CONFIGURATION D'UN ÉLÉMENT À SUPERVISER 12
DOCUMENT A.3 : ARCHITECTURE DE LA CONFIGURATION D'UN ÉLÉMENT AVEC SHINKEN 13

DOCUMENTS POUR LE DOSSIER B 15

DOCUMENT B.1 : DESCRIPTIF DU PROCESSUS DE DÉPANNAGE 15
DOCUMENT B.2 : COURRIEL DE DÉCLARATION D'UN INCIDENT 15
DOCUMENT B.3 : SCRIPT DE SAUVEGARDE 16
DOCUMENT B.4 : EXTRAIT DE DOCUMENTATION DU SCRIPT UTILISÉ 16
DOCUMENT B.5 : ÉVALUATION DU VOLUME DES SAUVEGARDES DES FICHIERS VIDÉO 16

Barème :

DOSSIER A : Intégration des nouveaux chantiers à l'infrastructure	50 points
DOSSIER B : Exploitation du réseau des caméras	50 points
Total	100 points

Présentation du contexte

L. est une ville touristique dont les fortifications, datant pour partie de l'époque gallo-romaine, attirent environ 30 000 visiteurs chaque année.

La mairie de la ville a récemment installé un système de vidéosurveillance sur une partie des espaces publics du territoire dont elle a la charge. La mise en route de l'ensemble du système date de moins de trois semaines.

Conformément à la loi et aux préconisations de la CNIL, ces dispositifs doivent exclusivement permettre de constater des infractions aux règles de la circulation, réguler les flux de transport, protéger des bâtiments et installations publics et leurs abords, prévenir des risques naturels ou technologiques, faciliter le secours aux personnes ou encore lutter contre les incendies et assurer la sécurité des installations accueillant du public dans les parcs d'attraction.

Une quinzaine de sites de la ville de L. sont équipés de 30 caméras fixes. Elles filment et enregistrent des images 24/24 qui sont sauvegardées pendant une durée maximum de 30 jours, conformément à l'autorisation préfectorale obtenue par la mairie de L.

Tous les équipements (caméras, postes de surveillances, ...) des sites distants sont reliés par fibre optique au cœur de réseau du service informatique de la ville, située à la mairie.

Trois chantiers concernant ces caméras sont actuellement en cours :

- le centre aquatique, qui a récemment ouvert ses portes, est le dernier site qui a été équipé de caméras. Il fait toujours l'objet d'aménagements extérieurs (nivellement du terrain, plantation d'arbres, installation de bordures, création d'une piste cyclable, etc.) ;
- l'intégration d'un réseau de caméras nomades permettant de couvrir certains événements provisoires : chantiers, salons, manifestations, périmètres non couverts ayant subi des dégradations, etc. Ces caméras, qui pourront être déplacées d'un endroit à l'autre de la ville, n'ont pas besoin pour fonctionner d'être raccordées au réseau de fibre optique municipal ;
- l'intégration du système de vidéosurveillance au logiciel de supervision de la mairie.

Vous êtes employé.e à la direction des systèmes d'information (DSI) de la mairie de L. et vos missions seront les suivantes :

- participer à l'intégration du réseau de caméras nomades à l'infrastructure du réseau de la mairie ;
- participer à la mise en place de la supervision du réseau des caméras ;
- participer à l'exploitation du réseau des caméras et au dépannage de l'ensemble des sites du réseau de vidéosurveillance ;
- assurer l'assistance aux utilisateurs.

DOSSIER A - Intégration des nouveaux chantiers à l'infrastructure

Vous participez à la mise en place des caméras nomades et à la consolidation du réseau des caméras.

Mission 1 : Intégrer les caméras nomades

Le technicien de la mairie doit procéder au paramétrage des différents matériels et à la mise à jour du serveur de noms (*DNS*). Vous réfléchissez à une configuration du nouveau réseau des caméras nomades qui soit compatible avec l'expression des besoins. À cet effet, le directeur du système d'information (DSI) vous demande de préparer les différentes actions à effectuer :

- sur les caméras ;
- sur les bornes *Wi-Fi* ;
- sur le commutateur cœur de réseau ;
- sur le serveur *DNS*.

Travail à faire

1.1	Proposer, en précisant le calcul, une segmentation du réseau des caméras afin de définir les deux sous-réseaux, l'un pour les caméras fixes, l'autre pour les caméras nomades (adresses réseaux et masques).
1.2	Donner un exemple de configuration IP pour une caméra fixe et une caméra nomade (adresse IP, masque, passerelle, *DNS*).
1.3	Rédiger un document décrivant les actions demandées sur les différents matériels et services (caméras, bornes *Wi*-Fi, commutateur cœur de réseau et serveur *DNS*).

Mission 2 : Superviser les caméras

Le réseau des caméras fixes et nomades doit être intégré au service de supervision. Le DSI a choisi de tester cette intégration avec les 4 caméras du centre aquatique.
Vous vous familiarisez avec l'outil *Shinken* qui est utilisé et vous prenez en charge la préparation de cette mission.

Travail à faire

2.1	Expliquer l'intérêt pratique de hiérarchiser les éléments à superviser (directive « parent » du fichier de configuration d'un élément). *Illustrer l'explication avec un exemple précis.*
2.2	Représenter une arborescence montrant les liens de dépendance « parent - enfant » des différents équipements physiques impliqués dans la surveillance des caméras du centre aquatique.
2.3	Lister les étapes nécessaires à l'intégration dans *Shinken* des 4 caméras. *Spécifier les fichiers à créer ainsi que les éléments à intégrer.*

DOSSIER B : Exploitation du réseau des caméras

Mission 3 : Gérer un incident

La procédure de déclaration d'un incident est décrite dans le dossier documentaire.

Le DSI de la mairie vous demande de prendre en charge le courriel reçu aujourd'hui par un technicien qui lui a relayé la demande. Celle-ci fait état d'un incident sur le nouveau site du centre aquatique : il est impossible d'accéder aux images de deux des caméras du centre aquatique.

Travail à faire

3.1 Rédiger la réponse à adresser au responsable sécurité du centre aquatique.

Vous constatez effectivement dans l'outil de supervision que les deux caméras en question sont à l'état « *DOWN* » et qu'aucune autre anomalie n'est signalée.

Travail à faire

3.2 Rédiger une note technique détaillée expliquant :

a) les raisons qui, d'après le courriel et la constatation de l'incident sur l'outil de supervision, vous font écarter un problème qui serait situé sur le commutateur fibre ou en amont de ce dernier ;

b) les causes possibles du problème rencontré ;

c) les éléments à tester et les tests à effectuer pour valider votre diagnostic.

Dans le but de rationaliser l'assistance auprès des utilisateurs du réseau de la mairie et en particulier celui du réseau de vidéosurveillance, il est envisagé d'utiliser, en complément du logiciel de gestion d'inventaireOCS, l'outil de gestion de configuration GLPI (« gestion libre de parc informatique »), qui intègre un module de gestion des incidents.

Chaque utilisateur devra utiliser ce logiciel aussi bien pour la déclaration d'un incident que pour son traitement.

Le DSI vous demande de préparer un argumentaire et une liste des tâches à destination des différents utilisateurs futurs.

Travail à faire

3.3 Citer les bénéfices d'un logiciel de gestion des incidents par rapport à la gestion actuelle. *Préciser l'intérêt supplémentaire lié à son intégration à un logiciel de gestion de parc.*

3.4 Lister les actions à entreprendre en direction des différentes catégories d'utilisateurs du logiciel de gestion des incidents pour qu'il soit utilisé dans de bonnes conditions.

Mission 4 : Sauvegarder les vidéos

Pour gérer plus facilement la consultation ultérieure des vidéos et pour des raisons de nécessité de sauvegarde, l'ensemble des vidéos est déplacé des serveurs *FTP* vers un dispositif de stockage réseau unique nommé NAS_ARCH. Cette action est effectuée automatiquement par un *script* lancé depuis la machine MASTER.

Depuis la mise en route des caméras du centre aquatique, le *script* de sauvegarde rencontre un problème et son exécution est interrompue. Voici le type d'erreur qui apparaît dans les journaux d'événements :

« mv: impossible de déplacer "VF_32A0988.ogv" vers "/stockage/videos/CentreAqua-Cam03/2016-05-10-0900.ogv": Aucun fichier ou dossier cible de ce type »

Un extrait du fichier `/root/admin/liste_sauvee.dat` a été conservé pour analyse :

```
Hopital-Cam02     172.16.150.30   VF_32A0968.ogv   2016-05-10-0900
Hopital-Cam02     172.16.150.30   VF_32A0978.ogv   2016-05-10-0908
CentreAqua-Cam03  172.16.150.30   VF_32A0988.ogv   2016-05-10-0900
```

Travail à faire

4.1 Rédiger une note à votre DSI expliquant le problème rencontré par le *script* et proposant une ou plusieurs solutions. Cette note doit comporter :

a) une explication du fonctionnement du script de sauvegarde des vidéos ;

b) une représentation de l'arborescence du disque dur de NAS_ARCH en prenant comme exemple l'extrait de fichier ci-dessus ;

c) la cause du problème ;

d) une ou plusieurs propositions de solutions.

Mission 5 : Respecter les contraintes légales

Conformément à l'autorisation préfectorale obtenue par la mairie de L., la contrainte réglementaire qui impose de ne conserver les vidéos qu'au plus 30 jours n'a pas encore été mise en œuvre puisque le fonctionnement du système ne date que de trois semaines.

À l'issue d'une réunion destinée à prendre en compte cette contrainte, deux questions sont posées :

1. Les éléments destinés à accueillir les vidéos sont-ils suffisamment dimensionnés ?
2. Comment mettre en place une purge automatique des données ?

Par mesure de simplification, seuls les calculs concernant les 30 caméras fixes sont pris en compte ici.

Travail à faire

5.1 Donner au DSI les éléments de réponse à la première question.

5.2 Donner au DSI les éléments de réponse à la deuxième question. *Préciser le nom des éléments du réseau à purger*.

DOCUMENTS COMMUNS

DOCUMENT 1: Description partielle du réseau de la mairie

1.1 - Architecture physique

Le **cœur de l'infrastructure du réseau de la mairie**, installé dans un local technique situé au sous-sol de la mairie est architecturé autour de :

- 2 commutateurs de niveau 3 empilés et dotés de 24 ports Ethernet Gigabit et de 24 ports fibre sur lesquels arrivent les brins de fibre des caméras et des points d'accès Wi-Fi ;
- 2 commutateurs de niveau 2 dotés de 24 ports Ethernet Gigabit ;
- 3 serveurs de virtualisation ;
- un câblage cuivre F/FTP en catégorie 6a.

Les caméras IP, actuellement au nombre de 30 (y compris celles du centre aquatique), permettent la numérisation et la compression vidéo. Le fichier contenant la vidéo est acheminé via les commutateurs réseau, pour être enregistré sur un serveur.

Les caméras sont toutes de marque Axis et répondent aux critères d'exigence suivants :

- une rotation sur 360° ;
- une étanchéité IP66 ;
- une caméra *PoE* (*Power over Ethernet*) ;
- un classement anti-vandale ;
- la gestion des alarmes ;
- une vision jour/nuit et la possibilité d'être mise en mode ronde (observation circulaire) ;
- l'intégration d'un serveur *HTTP*, *FTP*, d'un client *FTP* et de courriel.

Le protocole *SNMP* est activé sur les caméras. Celles-ci sont accessibles via le protocole *HTTP* avec l'URL *http://nom_hôte_dns/cam_connect*, en utilisant un nom d'utilisateur et un mot de passe. Ce nom et ce mot de passe sont actuellement ceux qui sont utilisés par défaut à la livraison, à savoir *admin/admin*.

Le réseau des caméras de la mairie intègre un système qui permet :

- de regarder en direct les flux vidéo des caméras de surveillance depuis les ordinateurs du réseau via les outils de gestion vidéos installés sur un serveur ;
- de créer des fichiers archives sur un groupe de quatre serveurs FTP pour une lecture en différé.

Les 4 serveurs *FTP* permettent de stocker les flux des caméras. Ils disposent chacun d'une capacité utile de 2 To.

Un **site distant,** s'appuyant lui aussi sur le réseau fibre de la ville, accueille notamment un **serveur *NAS* de sauvegarde** qui permet une sauvegarde à distance des fichiers archives. Il dispose d'une capacité utile de 4 To (extensible à 32 To).

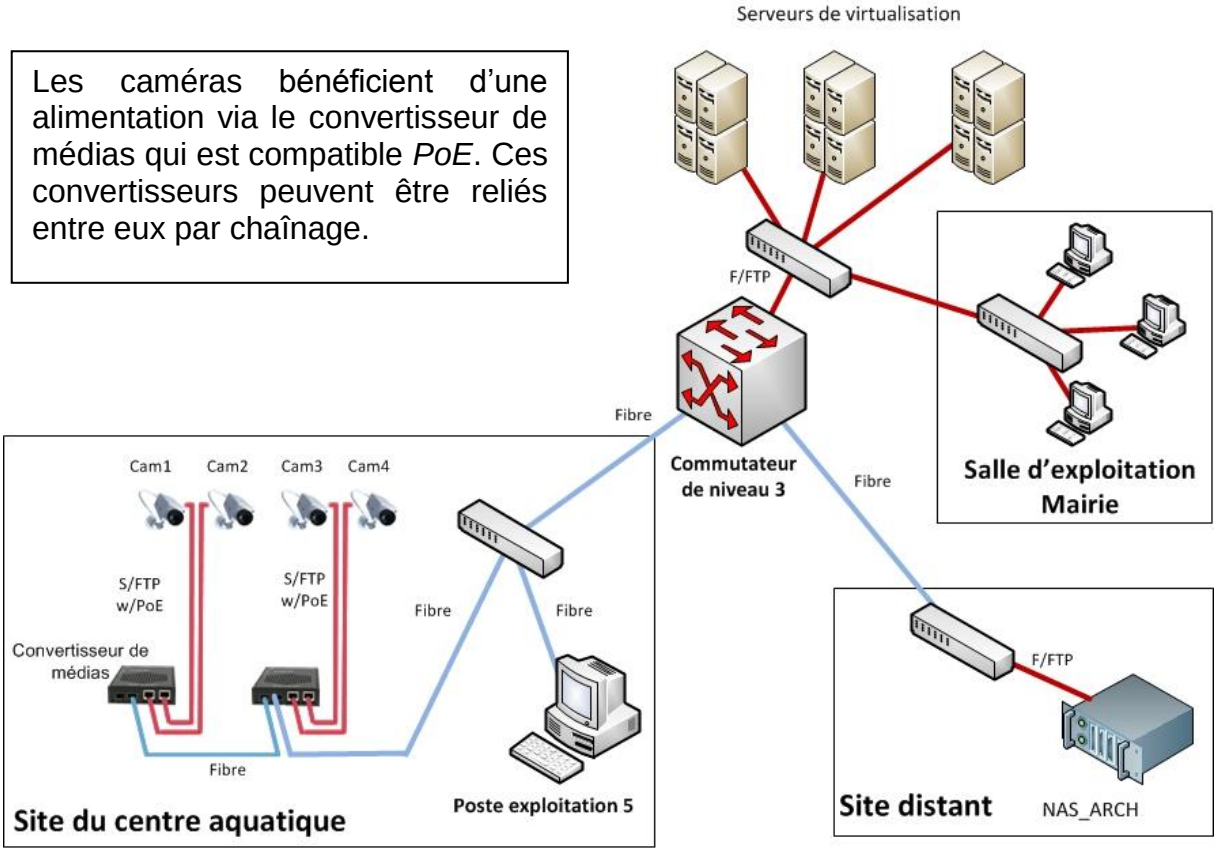
Les postes d'exploitation
80 % des postes d'exploitation sont regroupés dans un local de la mairie.
Mais quelques sites, comme celui du centre aquatique, bénéficient, notamment aux heures d'accueil du public, d'une surveillance des caméras sur place.

Le réseau Wi-Fi (non représenté ci-dessous)
La ville s'est appuyée sur son infrastructure (fibre et points d'accès Wi-Fi acceptant au maximum 8 *SSID*) pour la mise en place d'un réseau Wi-Fi urbain destiné au grand public et un réseau Wi-Fi sécurisé réservé aux élus et à l'administration municipale pour l'exercice de leurs fonctions.

Les points d'accès Wi-Fi sont directement connectés via la fibre sur le commutateur de niveau 3.

Le **site du centre aquatique intégrant 4 caméras** utilise, comme les autres sites, des convertisseurs de médias « cuivre-fibre ».

Les caméras bénéficient d'une alimentation via le convertisseur de médias qui est compatible *PoE*. Ces convertisseurs peuvent être reliés entre eux par chaînage.



Le lien fibre part d'une armoire d'équipements située près d'une prise d'alimentation. La source d'alimentation et le câble en fibre sont connectés sur un convertisseur de médias qui convertit le lien fibre en cuivre. Un lien Ethernet cuivre (câble S/FTP) est branché sur la caméra IP.

Le poste d'exploitation (N°5) du centre, installé sur place, est directement connecté au commutateur fibre.

1.2 - Architecture logique

Le réseau est segmenté en **6 *VLAN*** :

Fonction des *VLAN*	Support	Nom du *VLAN*	Numéro du *VLAN*	Adresse réseau
VLAN de la maintenance	Filaire	Maintenance	10	172.16.10.0/24
VLAN des usagers	Wi-Fi	Usagers	20	172.20.0.0/16
VLAN des élus	Wi-Fi	Elus	30	172.16.30.0/24
VLAN des employés	Filaire	Employés	40	172.16.40.0/24
VLAN des caméras	Filaire	CamérasFixes	100	172.16.100.0/24
VLAN des serveurs	Filaire	Serveurs	150	172.16.150.0/24

Sur les points d'accès :

- le *VLAN* 20 est associé au *SSID* « VilleL » diffusé ;
- le *VLAN* 30 est associé au *SSID* « ElusL » non diffusé.

Chaque *VLAN* géré par le commutateur de niveau 3, est associé à une adresse correspondant à l'adresse la plus haute dans chaque réseau IP. Ce principe fournit au commutateur des interfaces virtuelles qui lui permettent d'assurer le routage.

Description des serveurs

Serveur Physique	Fonction(s) des serveurs virtuels	Nom d'hôte du serveur	Adresse IP
Serveur Physique 1	Serveur d'authentification Serveur *DNS*	AD_DNS	172.16.150.20
	Serveur de gestion de parc	OCSNG	172.16.150.21
	Serveur de supervision	SHINKEN	172.16.150.22
	Serveur de gestion vidéo	MASTER	172.16.150.23
Serveur Physique 2	Serveur *FTP* (transfert de fichiers)	FTP_0	172.16.150.30
	Serveur *FTP* (transfert de fichiers)	FTP_1	172.16.150.31
	Serveur *FTP* (transfert de fichiers)	FTP_2	172.16.150.32
	Serveur *FTP* (transfert de fichiers)	FTP_3	172.16.150.33
Serveur Physique 3	Serveur *Proxy* – Portail captif	PROXY_NET	172.16.150.1
Serveur Physique 4	Serveur de sauvegarde	NAS_ARCH	172.16.150.10

Divers

- Les caméras disposent d'une configuration IP fixe : elles utilisent les 30 premières adresses de la plage.
- Les listes d'accès configurées sur le commutateur de niveau 3 permettent la communication entre n'importe quel *VLAN* et celui des serveurs.
- Les serveurs *FTP* n'acceptent des connexions en anonyme que depuis le serveur MASTER.
- Le logiciel de gestion vidéo se charge de répartir automatiquement les flux entre les 4 serveurs *FTP*.
- Les fichiers du serveur de stockage NAS_ARCH sont accessibles par l'intermédiaire du serveur MASTER via l'arborescence ***/*stockage**.

Description des services utiles

Afin d'assurer l'assistance et le dépannage des différents sites du réseau de vidéosurveillance, un **service de gestion d'inventaire** collecte automatiquement les informations concernant les matériels et logiciels de la mairie. Il est basé sur la solution libre *OCS Inventory NG (Open Computers and Software Inventory Next Generation),* et il a été installé sur le réseau.

Le serveur *DNS* intègre notamment l'ensemble des caméras car il est plus facile et rapide d'accéder à distance à une caméra via son nom plutôt que via son adresse IP. Le nom *DNS* d'une caméra fixe est de la forme : *NomSite*-Cam*NumCam*.mairie-l.fr. Par exemple : *CentreAqua-Cam01.mairie-l.fr*.

Le serveur de supervision avec l'outil *Shinken* (dérivé de *Nagios***)** est une solution libre permettant de surveiller des éléments actifs (commutateurs, routeurs, etc.), des hôtes (PC, imprimantes, caméras, etc.) et les services spécifiés. Les fonctionnalités principales de *Shinken* (dont les principes de fonctionnement sont présentés dans le **document A.3**) utilisées par le service informatique de la mairie sont les suivantes :

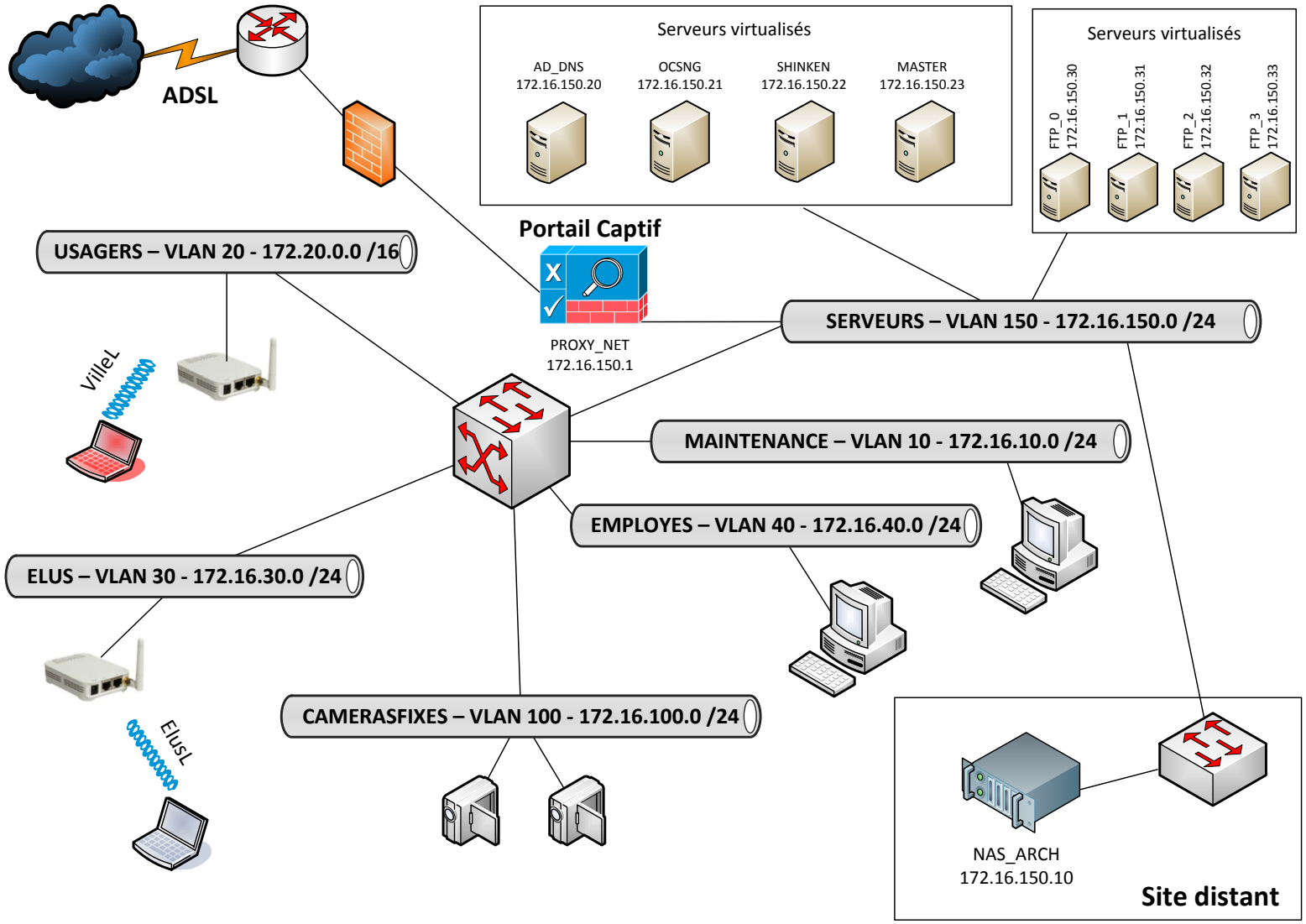
- la surveillance des serveurs avec les services associés (*SMTP*, *POP3*, *HTTP*, *FTP*, charge du processeur, espace disque...) ;
- la surveillance des éléments d'interconnexion et de leurs services ;
- la hiérarchisation des équipements composant le réseau ;
- la notification par courriel ;
- la journalisation des évènements ;
- la possibilité de développer ses propres dossiers de configuration (*packs)* et composants logiciels (*plugins)*.

Le serveur *Shinken* supervise actuellement :

- l'ensemble des serveurs dont chacun est identifié via la directive *host_name* par son nom d'hôte ;
- les services associés aux serveurs ;
- les éléments d'interconnexion (avec leurs services associés) comme :
    - le commutateur de niveau 3 : *host_name* = *comCoeurRéseau* ;
    - chaque commutateur fibre des sites dans lesquels se trouvent les caméras avec un nom d'hôte défini par la directive *host_name* qui a la structure suivante : *comFibre_nom*Site (par exemple pour le site du centre aquatique, *comFibre_centreAqua*).

En vue de la **supervision prochaine des caméras**, le service informatique a développé les modèles de configuration Shinken « webcam » et « webcam_générique ».

DOCUMENT 2 : Schéma logique simplifié du réseau de la mairie



DOCUMENTS POUR LE DOSSIER A

DOCUMENT A.1 : Expression des besoins

IMPORTANT : ce document fait référence à des éléments techniques expliqués dans le document A.3.

Intégration des caméras nomades

La ville a récemment acheté 10 caméras nomades *de deux type*s (6 caméras déplaçables et 4 caméras sur trépied) qui doivent pouvoir été intégrées de manière transparente et sécurisée dans l'infrastructure réseau de la mairie.

Les caméras déplaçables, à fixation temporaire, peuvent être placées sur n'importe quelle structure permanente, comme un poteau d'éclairage, par exemple. Elles seront utilisées lors d'événements ponctuels.
Les caméras nomades sur trépied seront utilisées lors d'événements ponctuels en l'absence de structure fixe disponible.

Ces caméras nomades s'appuieront sur l'infrastructure du réseau Wi-Fi urbain et devront être préalablement configurées en conséquence.

Pour des raisons de sécurité, il a été décidé de séparer les flux du réseau des caméras nomades s'appuyant sur l'infrastructure Wi-Fi de ceux du réseau des caméras fixes :

- un nouveau *VLAN* N° 101 « CamerasNomades » sera créé ;
- le *SSID* (non diffusé) associé à ce *VLAN* sera « CamNomades » ;
- la sécurisation des échanges sera assurée par un chiffrement *WPA2-TKIP* (*Wi-Fi protected Access -Temporal Key Integrity Protocol*) ;
- on restera sur un plan d'adressage commençant par 172.16.100 sachant que la ville prévoit encore d'acheter jusqu'à une quinzaine de caméras nomades supplémentaires et jusqu'à 80 caméras fixes supplémentaires ;
- le mot clé « nomade » remplacera « NomSite » dans la structure des noms *DNS*.

Intégration du réseau des caméras fixes et nomades au serveur de supervision

La supervision du réseau des caméras fixes et nomades doit être effectuée grâce au logiciel *Shinken*. La DSI a choisi de tester le système avec les 4 caméras fixes du centre aquatique.

Le modèle de configuration *Shinken* développé par le service informatique a été installé. Chaque caméra utilisera le modèle « webcam » :

```
define host {
name  webcam
use    webcam_generique
register 0
}
```

Chacun des services que l'on veut superviser au niveau d'une caméra a été défini dans ce modèle.

DOCUMENT A.2 : Procédure de configuration d'un élément à superviser

IMPORTANT : ce document fait référence à des éléments techniques expliqués dans le document A.3.

Pour configurer la supervision d'un élément via le logiciel *Shinken*, il est nécessaire de respecter les étapes suivantes (les éléments en gras doivent être remplacés par leur valeur réelle).

Étape 1 : installation éventuelle du ou des modèles de configuration nécessaires dans le répertoire : /usr/local/shinken/etc/packs

Étape 2 : création du fichier de configuration (***nom_hôte_dns.cfg***) dans le répertoire : /usr/local/shinken/etc/hosts

Étape 3 : configuration du fichier créé à l'étape 2

```
define host {
use                     nom_modèle_utilisé
contact_groups          admins
host_name               nom_hôte_dns
address                 adresse_IP
parents                 nom_hôte_dns
        …
}
```

La directive « parents » ne doit être intégrée que si nécessaire. Elle prend comme valeur le « host_name » de l'objet dont elle dépend.

Étape 4 (facultative) : définition des services

```
define service {
service_description     nom_service
use                     nom_modèle_utilisé
host_name               nom_modèle
check_command           commande
        …
}
```

La définition des services n'est en général pas utile si on utilise des modèles définissant déjà les services que l'on veut superviser.

DOCUMENT A.3 : Architecture de la configuration d'un élément avec Shinken

Cette documentation a été simplifiée.

Le serveur de supervision, équipé du logiciel *Shinken*, permet de surveiller des éléments actifs (commutateurs, routeurs, etc.), des hôtes (PC, imprimantes, caméras, etc.) et les services spécifiés.

Comment superviser un élément actif ?
Pour superviser un élément actif, par exemple le serveur « MASTER », il est nécessaire de disposer d'un fichier de configuration (par exemple *master.cfg*) dans le répertoire */usr/local/shinken/etc/hosts*.

La structure type d'un tel fichier commence par le mot clé "define" qui permet de définir un objet gérable par *Shinken*, ici un hôte (host) :

```
define host {
use linux
contact_groups admins
host_name master
address 172.16.150.23
}
```

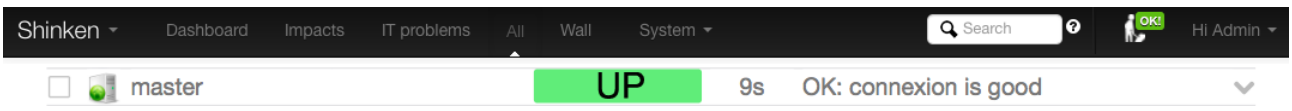
Cet hôte, « master » ici, utilise un **modèle prédéfini** (directive « use » qui a pour valeur « linux »). Il est **identifié par son nom** « master », son adresse « 172.16.150.23 » et le groupe à contacter « admins » en cas de problème (ce groupe est défini dans le fichier *contacts.cfg* qui contient notamment les adresses électroniques des personnes à alerter).

Le paramétrage est facilité par l'utilisation de modèles, eux aussi déclarés par les mots clés « define host ». Un modèle permet de définir l'ensemble des paramètres nécessaires à l'exécution des commandes associées à ce modèle.

```
define host {
name  linux
use    generic-host
register 0
}
```

Ce modèle est **identifié par le nom « linux »** et hérite lui-même d'un modèle plus général (generic-host). La directive « register » mise à la valeur 0 indique qu'il s'agit d'un modèle et non d'un hôte.

Par défaut, tous les modèles font référence à un modèle générique qui teste, via une commande *ping*, la présence d'un hôte sur le réseau. Ainsi, l'interface *web* de Shinken doit afficher au minimum le statut (*UP* ou *DOWN*) de chaque hôte déclaré dans le répertoire */usr/local/shinken/etc/hosts* :



De nombreux modèles sont disponibles en téléchargement sous forme de « packs » et chaque organisation peut développer ses propres modèles.

Comment superviser les services d'un élément actif ?

La supervision d'un service (au sens de *shinken*) se fait via une commande généralement de la forme « check_nom-commande » (par exemple, la commande « check_ping » va permettre de vérifier qu'un hôte est joignable).

De même, pour superviser la charge *CPU*, il est possible de définir dans un « pack » le service correspondant via un fichier *cpu.cfg* suivant :

```
define service {
service_description Cpu
use     linux-service
host_name    linux
check_command check_linux_cpu
register        0
}
```

Par conséquent, tous les hôtes utilisant ce modèle auront ce service supervisé.

L'image ci-dessous montre le rendu sur l'interface *web* de Shinken :

La gestion des dépendances entre les objets

Shinken permet de gérer les liens de dépendances qu'il peut y avoir entre les équipements de l'infrastructure réseau (hôtes, éléments actifs, etc …).
En effet, si par exemple, un commutateur ne répond plus, il n'est pas nécessaire de recevoir les notifications d'alertes concernant tous les équipements qui dépendent de lui.

La dépendance d'un objet est gérée dans son fichier de configuration via la directive « parents » qui prend comme valeur le nom d'hôte définie par la directive « host_name » de l'objet directement parent. Ici, le serveur est connecté sur le commutateur nommé « *comCoeurReseau* ».

```
define host {
use linux
contact_groups admins
host_name master
address 172.16.150.23
parents comCoeurReseau
}
```

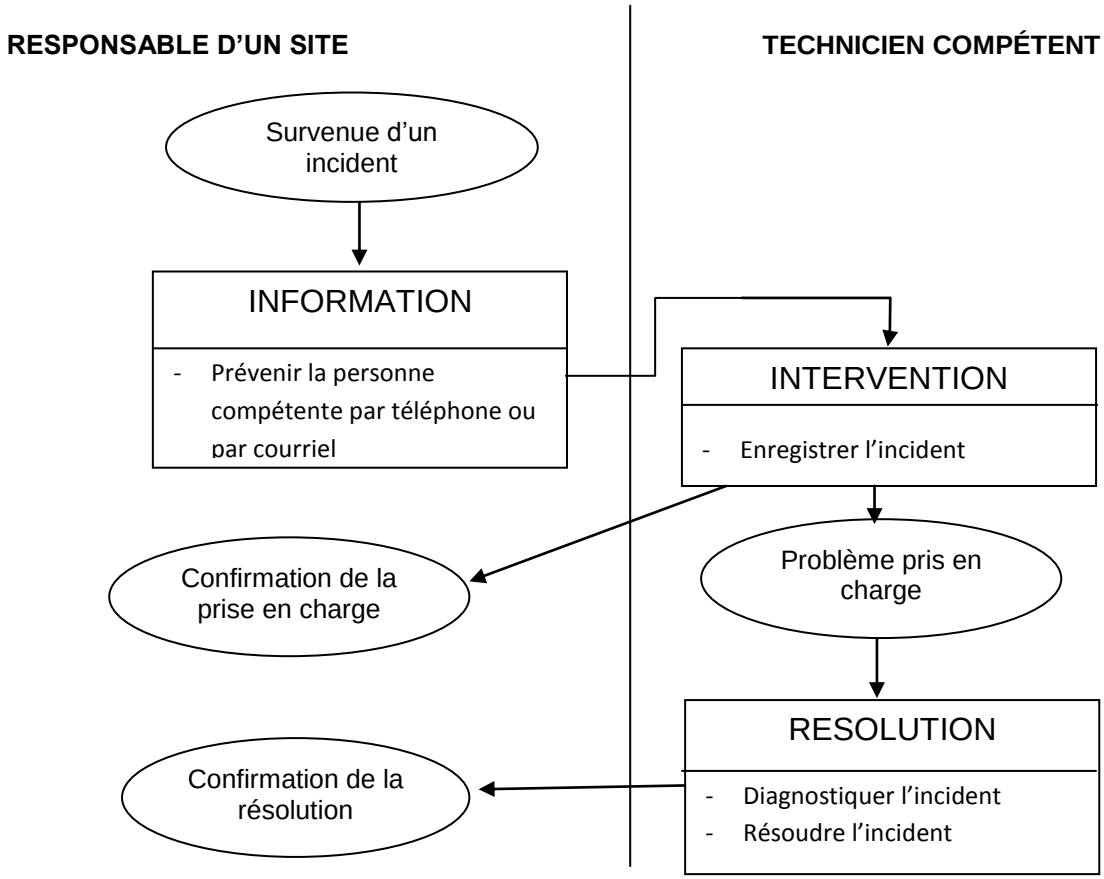
Les différents états gérés par *Shinken* sont les suivants pour un hôte (c'est-à-dire tout élément accessible par son adresse IP) :

- ***UP*** : l'hôte répond ;
- ***DOWN*** : l'hôte ne répond pas ;
- ***UNREACHABLE*** : l'hôte est injoignable car il se trouve derrière un autre hôte qui ne répond pas ;
- ***PENDING*** : l'hôte n'est pas encore testé (au démarrage généralement).

DOCUMENTS POUR LE DOSSIER B

DOCUMENT B.1 : Descriptif du processus de dépannage

Suivant la nature du problème (difficulté de connexion, images saccadées, caméra ne répondant plus, problème d'envoi de son rapport journalier,…), le technicien à contacter par le responsable d'un site est différent. Une page imprimée, avec les numéros de téléphone et les adresses électroniques de chaque technicien avec une description précise de leur compétence est collée sur chaque bureau disposant d'un poste de surveillance.



DOCUMENT B.2 : Courriel de déclaration d'un incident

De YYY@mairie-l.fr à XXX@mairie-l.fr
Le 10/05 à 8h45

Bonjour,

Je suis, depuis mon arrivée ce matin, dans l'incapacité de visionner les images des caméras n°1 et n°2 du centre aquatique, situées respectivement sur le parking et à l'entrée du centre.

Ces deux caméras paraissent intactes, elles sont alimentées et ne semblent pas avoir été endommagées.

A noter également que les deux autres caméras intérieures sont toujours opérationnelles et que je peux en visionner les images depuis mon poste de surveillance, qui porte le numéro 5.

Cordialement,
M. YYY
Responsable sécurité du centre aquatique.

DOCUMENT B.3 : Script de sauvegarde

```
#!/bin/sh
############################################################
# Description : script de sauvegarde des vidéos
# Nom : sauvvideos.sh
# Emplacement : /root/admin
# Planification :
#   ce script est lance par cron chaque jour pair à 23:59
#   voici la ligne à ajouter dans cron :
#   59 23 */2 * * /root/admin/sauvvideos.sh
############################################################

FIC_CAM_IP="/root/admin/liste_sauvee.dat"
# le fichier 'liste_sauvee.dat' contient
# -le nom de la camera
# -l'adresse IP du serveur FTP qui contient les vidéos de la camera
# -le nom du fichier vidéo sur le serveur FTP
# -la date et l'heure d'enregistrement du fichier vidéo
# Exemple de contenu :
# Hopital-Cam01   172.16.150.30   VF_32A0063.ogv   2016-02-14-1600
# Hopital-Cam02   172.16.150.30   VF_32A0068.ogv   2016-02-14-1600
# Hopital-Cam02   172.16.150.30   VF_32A0078.ogv   2016-02-14-1608

# lecture des informations du fichier
cat $FIC_CAM_IP | while read NOMCAM IPSRVFTP NOMFIC DATEVID
do
# on traite chacune des lignes de liste_sauvee.dat
# en utilisant chaque information nom de la caméra, son IP,
# le nom du fichier et la date de la vidéo.

# Connexion au serveur FTP et récupération du fichier sur MASTER
wget http://$IPSRVFTP/$NOMFIC
# enregistrement de la vidéo sur le stockage réseau NAS_ARCH
mv /root/admin/$NOMFIC /stockage/videos/$NOMCAM/$DATEVID.ogv
# /stockage est le répertoire qui permet d'accéder à la racine
# de NAS_ARCH
done
```

DOCUMENT B.4 : extrait de documentation du script utilisé

mv [OPTION...] SOURCE CIBLE
Déplace ou renomme des fichiers ou des répertoires.

cat [OPTION...] fichier
Affiche le contenu d'un fichier

wget [OPTION...] URL
Il s'agit d'une commande qui permet de télécharger un fichier depuis un serveur *HTTP* ou *FTP*.

DOCUMENT B.5 : Évaluation du volume des sauvegardes des fichiers vidéo

Le système de surveillance génère en moyenne 100 fichiers vidéo de 50 Mo (50.000.000 d'octets) par caméra fixe et par jour. Ils sont sauvegardés sur les différents serveurs FTP par le système de vidéosurveillance, puis répliqués sur le NAS par le script.