ARCANES
VIDEO TECHNOLOGY

VX Core

ADMINISTRATION DU SYSTÈME

Version 7.0

août 2023

Ce document décrit l'administration des systèmes VXCORE.

Table des matières

1 Connexion sur l'interface

Cette documentation décrit l'administration d'un système VXCORE via l'espace d'administration accessible uniquement au super utilisateur "root" ou aux administrateurs qui ont les bonnes permissions.

VXCORE est un système d'exploitation dédié qui permet de transformer un serveur informatique en appliance de vidéosurveillance professionnelle.

Par conséquent, le système Linux servant de base au système ne dispose d'aucun accès utilisateur ou administrateur sur la console. La seule interface de configuration et d'utilisation du système est l'interface graphique, accessible via le réseau TCP/IP et le protocole HTTPS (protocole HTTP désactivé par défaut).

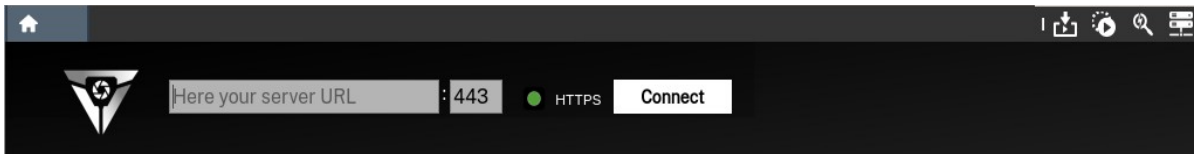
Vous devez installer l'application VXCORE-ACCESS pour consulter et configurer le système. Cette application native a été spécialement conçue et optimisée pour la consultation des systèmes VXCORE.

Toutes les applications (PC/Mobile) sont signées afin de garantir un contrôle des accès au serveur VXCORE : toute connexion non autorisée sera automatiquement bloquée (exemple : via un simple navigateur Web).

Le système nécessite la connexion d'un clavier et d'un écran directement sur le serveur seulement pour la configuration des interfaces réseau.

La configuration complète du système se fait via son interface graphique, accessible avec une des adresses IP que vous avez configuré à la fin de l'installation.

Utilisez le logiciel VXCORE-ACCESS et saisissez l’adresse IP du serveur VXCORE pour y accéder (ou utilisez la fonctionnalité de recherche réseau située à droite).



Utilisez les identifiants qui ont été générés lors de l’installation du système pour vous connecter sur l’interface (par sécurité, chaque nouvelle installation créera un mot de passe administrateur root différent).

Remarque : le protocole HTTP est désactivé par défaut, il est nécessaire d’utiliser HTTPS.

Si vous avez perdu votre mot de passe root, il sera nécessaire de le restaurer : cette opération est décrite dans la section "Maintenance" de ce manuel.

Si vous ne retrouvez plus l’adresse IP du système ou que vous n'y accédez plus via le réseau, il sera nécessaire de connecter un écran et un clavier sur votre serveur. Vous pourrez ensuite modifier la configuration réseau avec l’utilitaire intégré en ligne de commande en appuyant sur la combinaison de touche < CTRL + C >.

Remarque sur les connexions HTTPS :

VXCORE utilise un certificat SSL "auto-signé" qui permet de garantir la même confidentialité des échanges et la même sécurité que les certificats signés par un organisme de certification officiel.

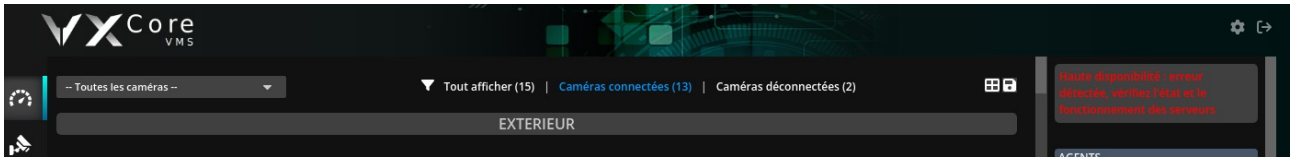
La seule différence est le coût : un certificat officiel doit être acheté et renouvelé tous les ans par l'utilisateur final. Consultez le chapitre "Configuration du réseau et des certificats SSL" de ce manuel si vous souhaitez installer un certificat SSL officiel.

Si vous configurez des adresses IP statiques ou une adresse DNS publique dans les paramètres réseaux, alors un certificat SSL sera automatiquement généré pour chaque IP et/ou adresse DNS.

2 Interface d’administration du système

Après la connexion au système, vous serez placé automatiquement dans l’interface de consultation du système vidéo (interface vide si système vidéo non configuré).

Selon la version de l’OS VXCORE installée, il est possible que vous n’ayez accès qu’a l’interface d’administration (pas de visualisation ou configuration de caméras).



 Cliquez sur le bouton d’accès aux paramètres de configuration et d’administration système, accessible en haut à droite de l’interface.

A gauche, vous verrez un menu regroupant l’ensemble des sections : PERSONNALISATION, CONFIGURATION, ADMINISTRATION et JOURNAUX.

Ces sections s’afficheront en fonction des permissions du compte utilisateur/administrateur utilisé.

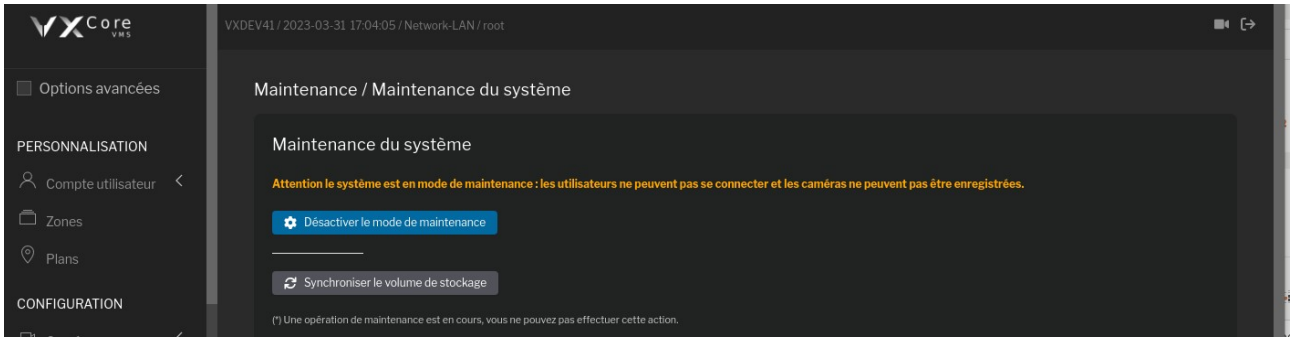
Le menu ADMINISTRATION permet de configurer tous les paramètres du système/OS (licence, stockage, réseau …) et de contrôler l’état de fonctionnement du serveur vidéo (graphiques d’état, consommation cpu/ram, journaux systèmes …).

L’interface dispose de deux modes de consultations : mode simple ou avancé. Cliquez sur le bouton « Options avancées » situé en haut à gauche pour afficher tous les menus disponibles.

La plupart des opérations de configuration du serveur nécessiteront d’activer le mode de maintenance du système : tous les services systèmes/ vidéo seront coupés et les utilisateurs ne pourront plus se connecter.

Pour placer le serveur en mode maintenance, cliquez sur le menu « Maintenance » et appuyez sur le bouton « Activer le mode maintenance ».

Le système vous signalera que le mode est bien activé avec un message d’avertissement.



Pour quitter le mode de maintenance et ré-activer le système vidéo, cliquez sur le bouton « Désactiver le mode de maintenance ».

3 Installation / mise à jour de licence

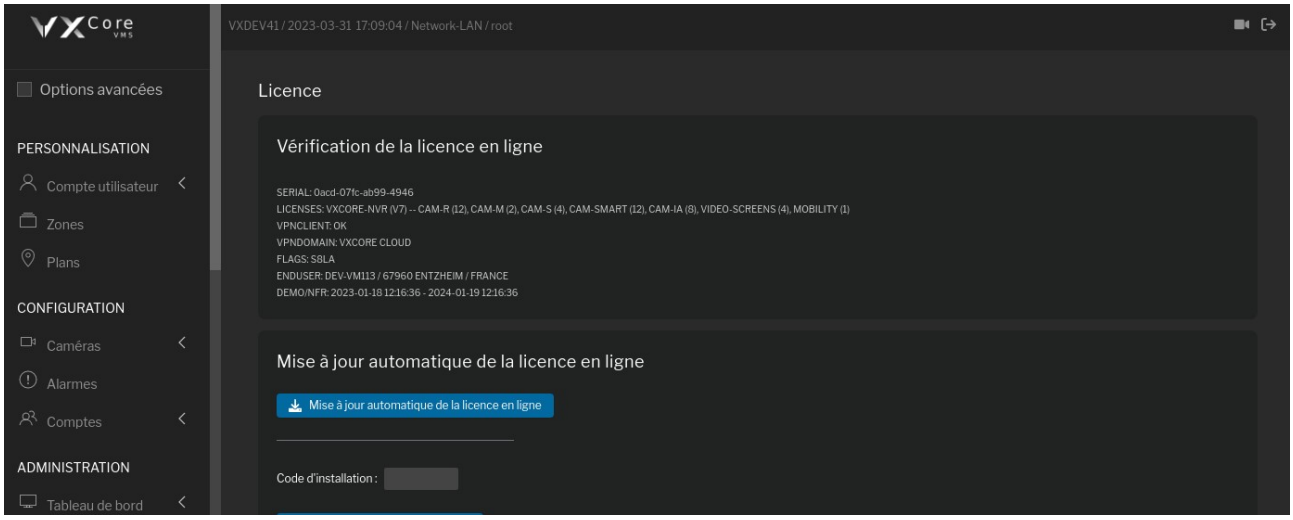
Avant de configurer votre serveur vidéo, vous devez installer une nouvelle licence ou une licence existante. Lors d'une nouvelle installation de serveur, cette étape se fait directement après le premier démarrage et la configuration réseau de base (ou vous pouvez également copier le mot de passe administrateur root).

L'installation d'un fichier de licence fait automatiquement via une connexion Internet, mais il est également possible de le faire en mode « hors-ligne ».

Afin d'installer ou mettre à jour une licence, vous devez placer votre serveur en maintenance via la section administration/maintenance. Configurez ensuite la connexion Internet sur le système, en utilisant la section administration/réseau (si vous ne l'avez pas fait avec l'utilitaire en ligne de commande après l'installation).

Remarque : si vous ne disposez pas d'une connexion Internet sortante, vous pouvez utiliser la procédure d'installation de licence en mode "hors-ligne". Contactez votre distributeur pour plus d'informations.

Cliquez sur le menu « Licence » pour afficher l'interface de gestion.



Si votre système VXCORE est connecté sur Internet, cliquez sur le bouton « Rechercher la licence en ligne ». Le système procédera à une recherche automatique en ligne afin de vérifier son état : installée, mise à jour possible, licence corrompue ou détournée …

3.1 Installation d'une nouvelle licence

Pour installer une nouvelle licence, vous devez disposer d'un code d'installation, fourni par un distributeur officiel de la solution.

Le code d'installation est unique et généré pour une seule installation de système VXCORE (un fichier de licence ne fonctionnera que sur un seul et unique serveur ou machine virtuelle). Toute nouvelle installation ou changement de serveur nécessitera donc un nouveau code d'installation.

Remarque : il existe une procédure d'installation de licence en mode "hors-ligne", si vous ne disposez pas d'une connexion Internet sortante. Contactez votre distributeur pour plus d'informations.

Après le téléchargement et l'installation de la licence, le système profitera de la connexion Internet pour synchroniser la date et l'heure du serveur via un serveur de temps et vérifiera si des correctifs de versions sont disponibles.

3.2 Ré-installation ou mise à jour d'une licence existante

Si vous avez ré-installé votre serveur suite à la casse du disque système (sans changer la carte mère ou d'architecture), ou que vous avez rajouté des licences dans votre système, vous pouvez ré-installer très simplement le fichier de licence.

Il existe deux possibilité de ré-installation d'une licence existante : soit directement en ligne, soit en transférant manuellement le fichier de licence dans le serveur (si vous n'avez pas de connexion Internet).

Contactez votre distributeur si vous avez besoin de transférer votre fichier de licence manuellement.

3.3 Migration d'une licence existante

Le système de licence est suffisamment souple et sécurisé pour vous permettre de faire évoluer votre serveur sans devoir ré-installer une nouvelle licence.

Le seul cas ou vous ne pourrez pas utiliser le même fichier de licence d'un serveur est celui d'un changement d'architecture physique (comme le remplacement de la carte mère par exemple).

Contactez votre distributeur afin d'obtenir la procédure de migration de licence dans le cas d'un changement ou d'une évolution de serveur.

4 Maintenance logicielle (SMA)

VXCORE intègre une gestion des mises à jours automatique, au travers d'un contrat de maintenance logicielle (SMA).

La SMA est un contrat de maintenance logiciel souscrit directement entre l'éditeur de la solution VXCORE et l'utilisateur final de la licence. Il est donc nécessaire de préciser les coordonnées complètes de l'utilisateur final lors de la création de la licence VXCORE. L'éditeur du logiciel se réserve le droit de refuser toute demande de maintenance logicielle si ces conditions ne sont pas respectées, même avec une SMA en cours de validité.

Tout système VXCORE peut bénéficier d'un contrat SMA que l'utilisateur final peut choisir de renouveler ou non via son distributeur.

La SMA est le seul moyen de se protéger contre l'évolution des technologies et les failles de sécurité (cyber-menaces).

La SMA est disponible sur l'ensemble des logiciels et solutions VXCORE et permet d'inclure un suivi complet des logiciels avec leurs évolutions, comprenant :

- les correctifs logiciels mineurs (exemple : 6.0.X).
- les correctifs de sécurité de l'OS ou des librairies systèmes.
- les mises à jour de versions avec nouvelles fonctionnalités (exemple : 6.X.0).
- les nouvelles générations des OS (exemple : 7.0.0 / 8.0.0).

- l'intégration et le suivi des nouveaux modèles de caméras (après tests validés en labo, flux vidéo et contrôle PTZ).
- les nouvelles images d'OS incluant les drivers et librairies les plus récentes pour les nouvelles plate-formes hardware (serveurs et/ou PC).
- les diagnostiques à distance et l'assistance des problématiques complexes aux distributeurs (Support Technique Niveau 3).

La SMA est souscrite et renouvelée pour des périodes de 12 à 48 mois avec un tarif dégressif selon la durée souscrite. Il est aussi possible de souscrite à une SMA pour un parc de serveurs VXCORE, contactez votre distributeur pour plus d'informations.

Tout ajout de licences et/ou options sur un système existant avec une SMA nécessitera aussi une mise à niveau de la SMA (au prorata du temps restant).

Exemple : pour un ajout de caméra sur un système dont la SMA expire dans 2 mois, on calculera la SMA pour le nombre de caméras ajouté seulement sur les 2 mois restants.

Toute expiration de SMA entraînera l'arrêt des mises à jour et du suivi des logiciels VXCORE (installation de patch automatiquement et/ou manuellement).

La SMA n'est pas obligatoire pour un système, mais dans ce cas, il sera figé en fonctionnalité, non évolutif en terme de licences et options, et ne disposera d'aucun suivi ou support logiciel (aucun correctifs ou mises à jour).

Après la date d'expiration de la SMA, il sera encore possible de la renouveler durant un délais de 36 mois. Le renouvellement prendra effet à la date d'expiration de la SMA du système et non à partir de la date du renouvellement.

Exemple : si un système dispose d'une SMA expirée depuis 6 mois, et que l'on choisi un renouvellement de 12 mois : le système n'aura qu'un renouvellement SMA effectif de 6 mois.

Au delà de 36 mois d'expiration de la SMA, il ne sera plus possible d'effectuer un renouvellement. Pour disposer des dernières versions des logiciels VXCORE, il sera nécessaire d'acquérir un nouveau logiciel complet avec ses licences et options.

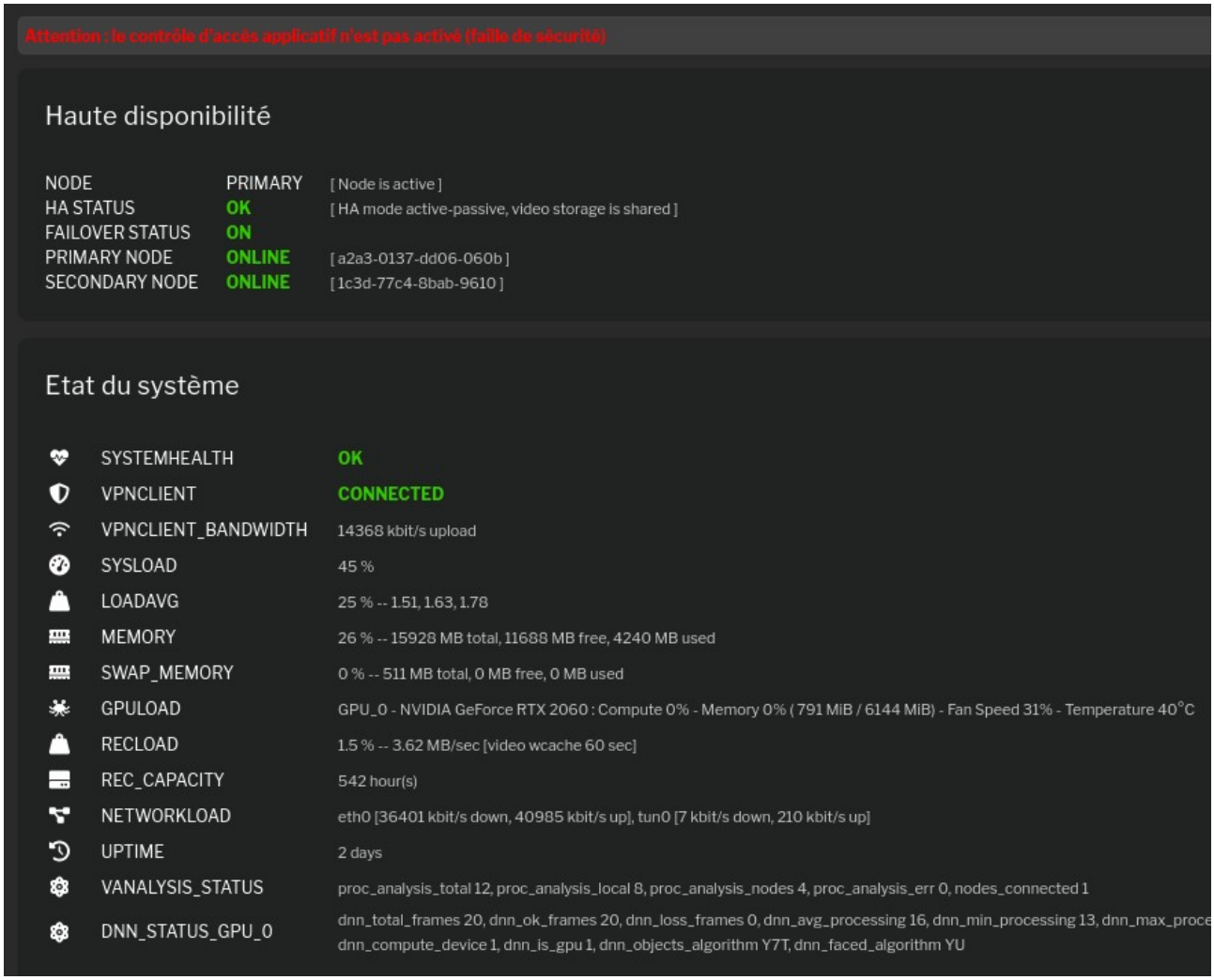
5 Tableau de bord

Le tableau de bord d'administration va regrouper toutes les informations systèmes importantes et l'état de fonctionnement général du serveur vidéo.

5.1 État du système

Cette interface va regrouper toutes les informations systèmes détaillées du système vidéo, ainsi que l'état de la haute disponibilité si vous l'avez configuré.

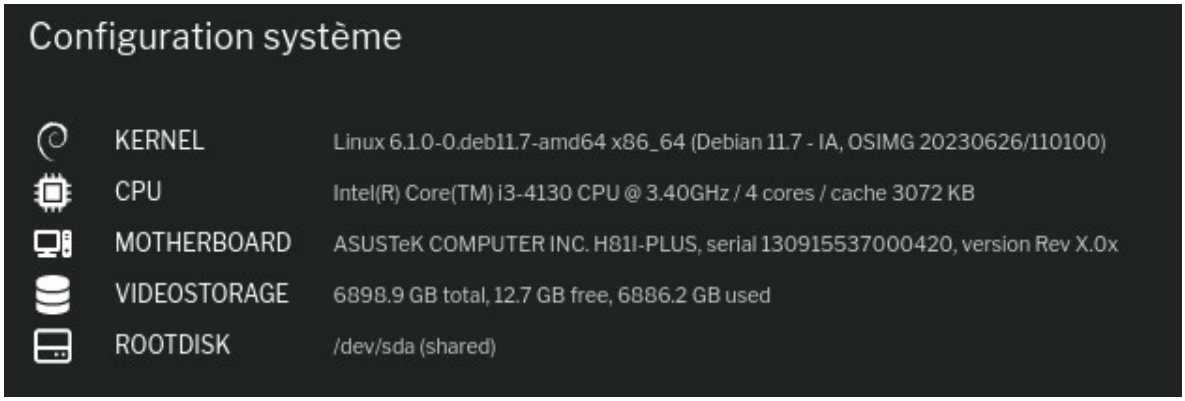
Les messages d'erreurs, d'avertissements ou de supervision systèmes seront tous visibles en haut.



Les informations systèmes sont très complètes : état de santé, état de connexion VPN, charge du système (CPU/IO), consommation mémoire (RAM/SWAP), charge du/des GPU, charge de l'enregistrement vidéo et du réseau, statistiques d'analyse vidéo, etc.

Ces informations systèmes seront également synchronisées dans le cas du raccordement du système sur un serveur de centralisation, pour une supervision globale de tous les systèmes vidéo.

Après l'état du système, vous verrez l'affichage de la configuration système : Noyau linux et OSIMG, CPU, carte mère, stockage vidéo, disque système, etc



Après la configuration système, vous verrez l'affichage des détails de la version et de la licence installée sur le serveur (numéros de série, licences, client final, date de validité SMA, etc)

5.2 État du réseau

Ce menu affichera les résultats des commandes de l'OS Linux pour afficher l'état du réseau de manière détaillé :

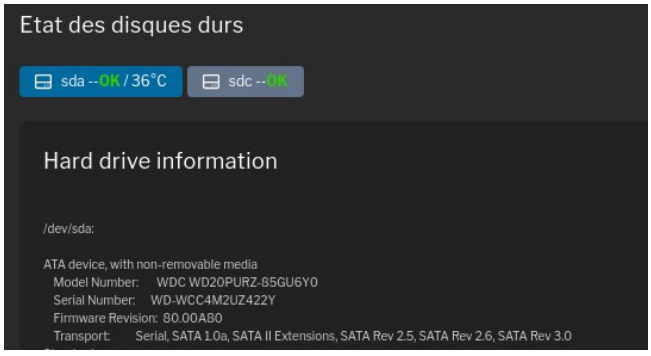
- Interfaces réseau
- Routes du serveur
- Liste des serveurs DNS

Ces informations peuvent être utiles aux administrateurs système/réseau pour vérifier la configuration du serveur vidéo ou identifier un problème.

5.3 État des disques durs / SMART

Ce menu affichera tous les disques durs connectés dans le serveur, ainsi que leur température de fonctionnement (si disponible).

Cliquez sur chaque onglet identifiant un disque dur pour afficher tous les détails.

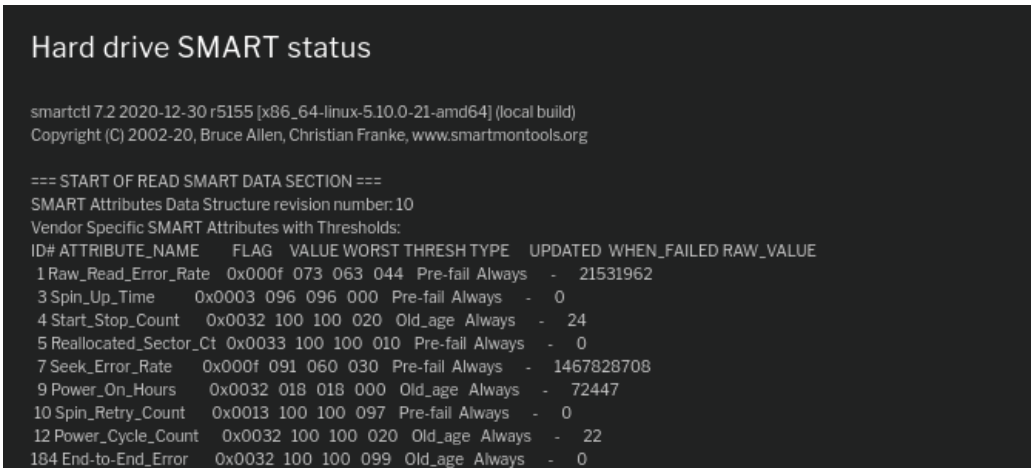


La technologie S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology, ou littéralement Technique d'auto-surveillance, d'analyse et de Rapport) est un système de surveillance permettant de diagnostiquer l'état de fonctionnement et la fiabilité des disques dur, dans le but d'anticiper les erreurs et les défaillances.

VXCORE intègre un client S.M.A.R.T. qui supervisera automatiquement tous les disques durs compatibles, afin d'alerter l'administrateur en cas de défaillance imminente. Si le disque est compatible, sa température de fonctionnement sera aussi indiquée.

Seuls les disques durs physiques connectés directement aux contrôleurs de stockage seront supervisés, et non ceux connectés derrière une carte RAID.

Le système lancera une procédure d'auto-test des disques durs tous les jours à Minuit, afin de déceler des éventuels problèmes (test rapide).



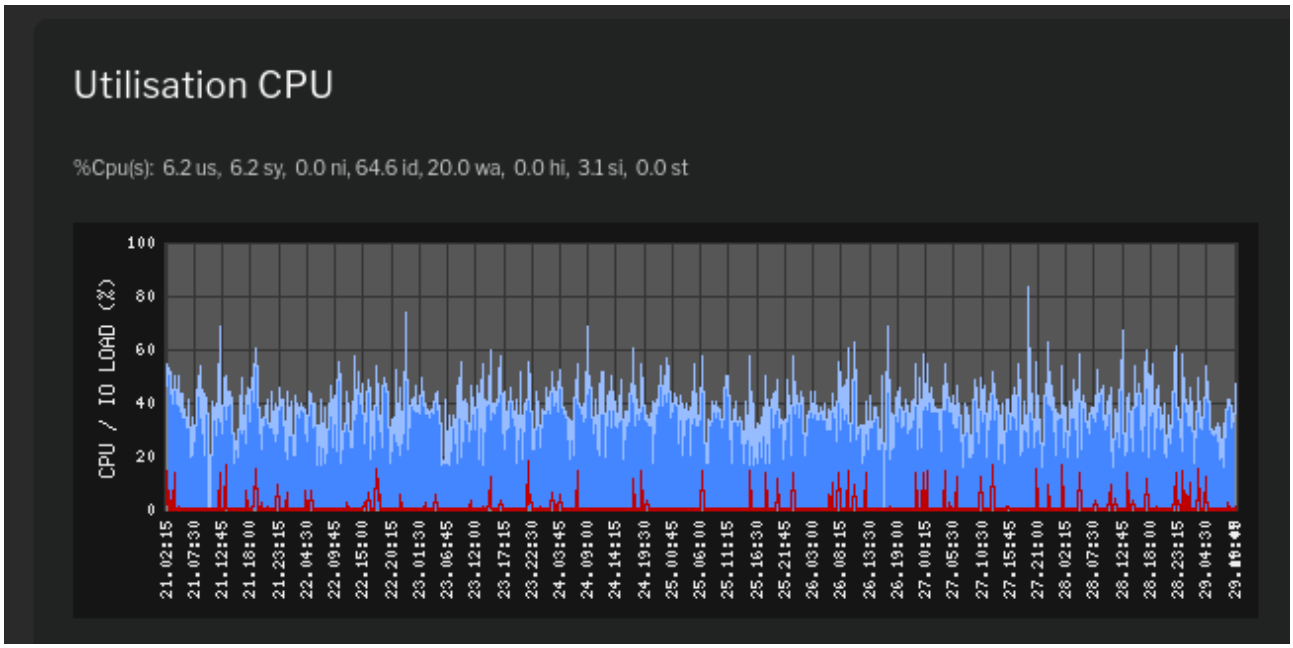
Les constructeurs ne disposant pas tous de la même implémentation du S.M.A.R.T., il vous est possible de désactiver la supervision dans les options systèmes si jamais vous rencontrez des problèmes ou des fausses alertes (notamment avec l'utilisation de certaines carte mémoires mSata ou SataDom non compatibles).

5.4 Ressources systèmes

VXCORE va générer automatiquement différents graphiques sur l'état de fonctionnement du système.

Les graphiques seront mis à jours et générés toutes les 15 minutes.

L'utilisation du CPU est une donnée importante, elle détermine la puissance de calcul disponible du système vidéo. Avec certains serveurs récents et multi-cœurs, il n'est pas rare d'avoir une utilisation très basse du CPU malgré la gestion d'un nombre important de caméras (sans analyse vidéo SMART/IA).



Codes couleurs du graphique d'état :

- **Graphique Bleu**
  Graphique de consommation CPU, correspond à la puissance de calcul utilisée par le système.
- **Graphique Rouge**
  Graphique de délais I/O, correspond au temps des ralentissements systèmes liés aux périphériques de stockage (disque système, base de données, volume RAID, etc).
  Si ce graphique dépasse les 10 % régulièrement, cela signifie que votre serveur est mal dimensionné.

De manière générale, VXCORE fonctionnera mieux avec un processeur de type « PC multimédia » puissant et rapide (fréquence élevée, type core i7 4 Ghz avec 8 cœurs) plutôt qu'un processeur « serveur » lent avec beaucoup de cœurs (type intel Xeon serveur 2,2 Ghz avec 24 cœurs).

Voici dans un ordre de priorité les processus qui consommeront le plus de CPU dans un système VXCORE :

- Analyse vidéo avec IA
- Affichage vidéo sur écran connecté au serveur (sortie vidéo du serveur)

- Algorithmes de détection de mouvement simples et avancés

  (configurez toujours un flux vidéo secondaire pour l'analyse vidéo, exemple 640x480 à 15 img/s)

- Exportation vidéo intégré avec transcodage
- Gestion des alarmes

  (en cas de journalisation importante si temps de réarmement des alarmes est trop petit, si pas besoin de notification ou de scénarios agents/actions, utilisez plutôt la recherche intelligente pour retrouver des évènements)

- Transcodage vidéo temps réel

  La consommation CPU peut être grandement affectées selon le codec vidéo choisi (exemple : H.265 beaucoup plus gourmand en ressource que MPEG4).

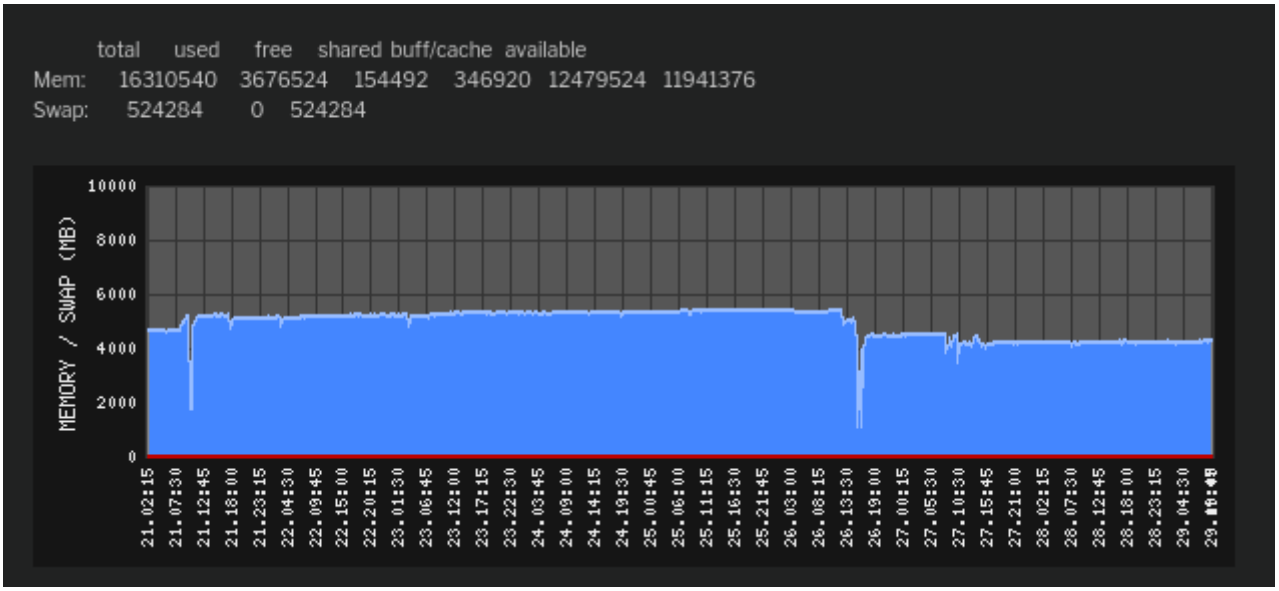
- Proxy vidéo multi-flux

  (avec des images 4K ou Mégapixels, évitez de configurer 3 flux vidéo sur les caméras, 2 flux vidéo sont suffisant dans la majorité des cas)

- Enregistrement vidéo (en fonction de la rapidité du stockage, attention aux cartes RAID bas de gamme)
- Visualisation des flux vidéo en mode chiffré (en protocole HTTPS ou via le VPN)

Le graphique d'utilisation mémoire représentera l'utilisation de la mémoire physique (RAM) et de la mémoire virtuelle (SWAP) du serveur.

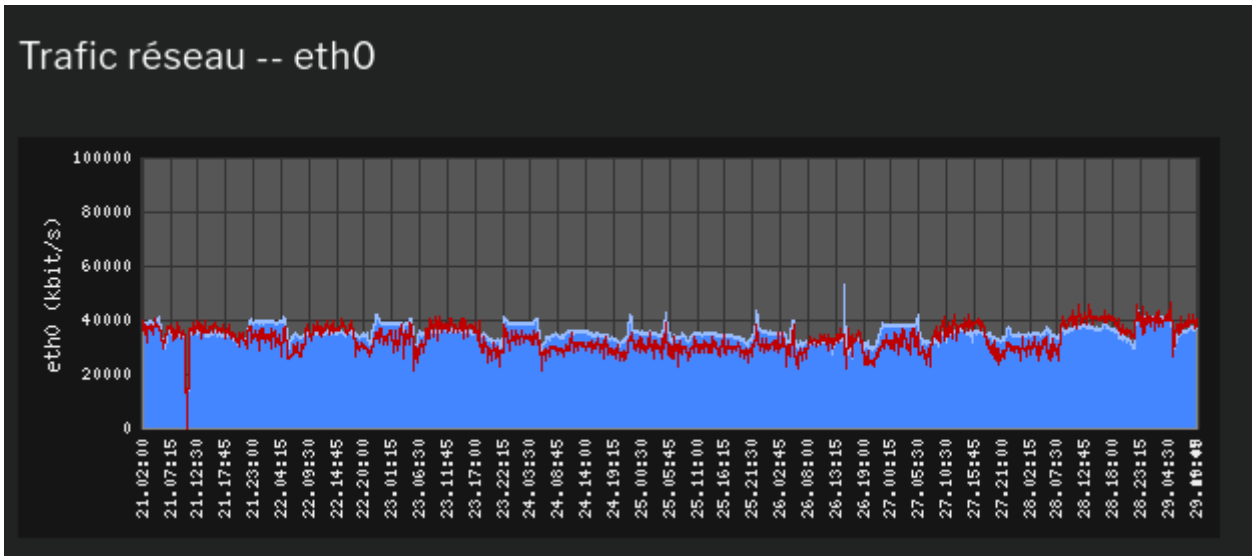
La mémoire RAM sera représentée avec le graphique bleu et la mémoire SWAP avec le graphique rouge.



Normalement, le graphique rouge devrait rester proche de zéro, donc sans aucune utilisation de la mémoire SWAP. Si ce n'est pas le cas, cela signifie que votre serveur ne dispose pas d'assez de mémoire physique RAM. L'intégralité du système pourrait en être fortement ralenti.

5.5 Trafic réseau

Ce menu va représenter les graphiques d'état de toutes les interfaces réseau configurés dans le système, ainsi que l'interface réseau VPN.



Pour chaque interface réseau, le graphique de couleur bleu représente le trafic entrant (download), et le graphique rouge représente le trafic sortant (upload).

6 Configuration réseau

VXCORE est une appliance basée sur un système Linux réputé pour sa fiabilité et sa richesse de fonctionnalité de mise en réseau.

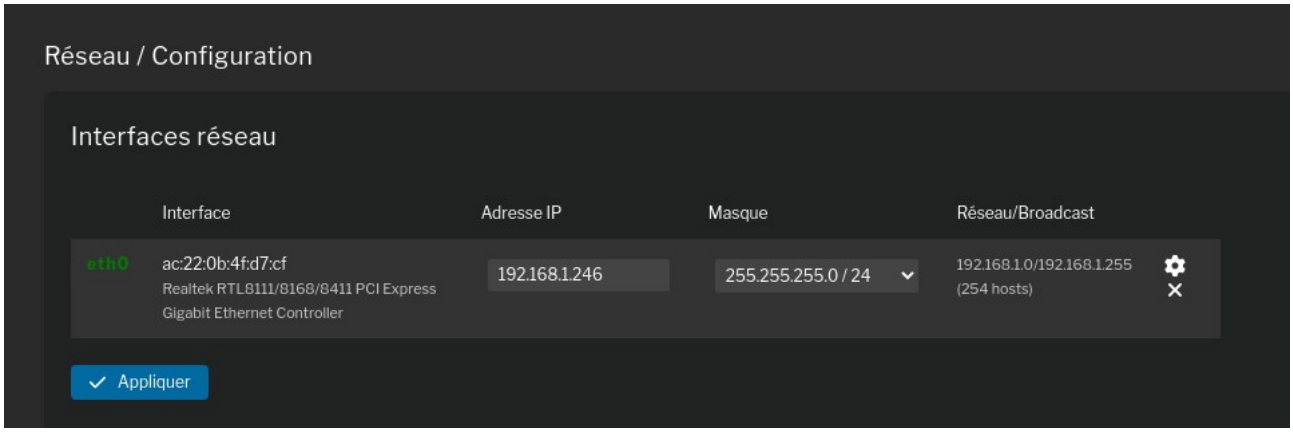
6.1 Paramètres réseau

6.1.1 Interfaces réseau

On appelle une interface réseau une "porte" vers un réseau extérieur. Schématiquement, une carte réseau est considérée comme une interface réseau, qui sera nommée sous Linux en eth0, eth1, eth2, ethx ...

Il n'y a pas de limite dans la gestion du nombre d'interfaces réseaux sous VXCORE, ou du moins pas de limite atteignable facilement dans l'intégration d'un serveur. Il n'est pas rare que certains serveurs utilisent jusqu'à 4 cartes réseaux pour répartir la charge ou s'intégrer dans une configuration réseau complexe.

Les interfaces listées dans la page de configuration sont celles qui ont été configurées en ligne de commande, à l'aide de l'utilitaire de configuration. Si vous rajoutez une nouvelle carte réseau dans votre serveur, elle sera automatiquement détectée dans l'interface après le redémarrage. Si ce n'est pas le cas, vous devrez utiliser l'utilitaire en ligne de commande sur la console Linux pour détecter et ajouter la nouvelle interface.



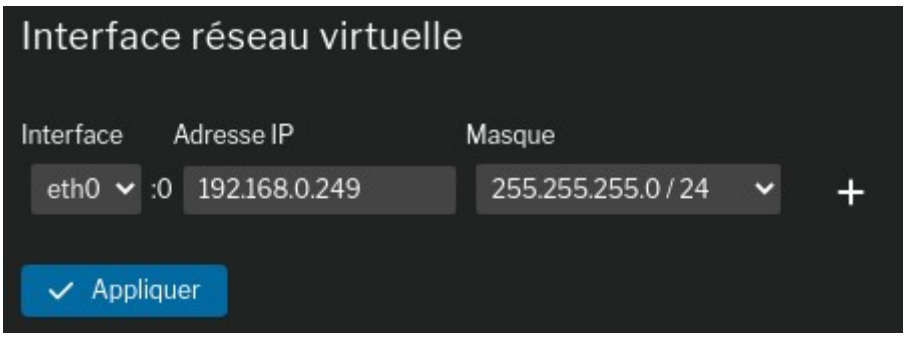
VXCORE garde en mémoire le nommage des interfaces réseaux, en fonction de l'adresse physique de la carte (adresse MAC). Cette fonctionnalité vous assure que les interfaces ne seront jamais mélangées même en cas d'ajout ou de suppression physique d'une ou plusieurs cartes.

Remarque : le système dispose d'un contrôle de la configuration réseau qui vous indiquera si vous faites une erreur de configuration (comme par exemple la configuration de deux interfaces réseaux accédant au même réseau physique).

Vous pourrez également choisir de configurer une interface réseau automatiquement via le protocole DHCP (attribution automatique de l'adresse IP, de la passerelle et des DNS par un routeur).

6.1.2 Interface réseau virtuelle

Le système permet de configurer une adresse IP virtuelle dans les paramètres réseau, afin de "simuler" une nouvelle carte/interface réseau.



Cette fonctionnalité peut être très utile si votre serveur ne dispose que d'une seule carte réseau : vous pourrez quand même ajouter virtuellement une deuxième carte pour un créer un réseau dédié aux caméras.

Exemple de cloisonnement réseau pour simuler un réseau privé et un réseau caméra:

1. **Configurez l'interface eth0 en DCHP**

   Le routeur/box internet présent sur le réseau attribuera automatiquement une adresse IP au serveur VXCORE, ainsi que la passerelle et les DNS.
   La connexion internet sortante du serveur sera opérationnelle (éventuellement pour initier la connexion VPN au serveur central).

2. **Créez une interface réseau virtuelle nommée "eth0:0"**

Configurez une adresse IP statique du type : 10.10.20.14 / 255.255.255.240 correspondant au réseau caméra. Ce sous-réseau virtuel sera composé de 14 adresses IP : de 10.10.20.1 à 10.10.20.14 (10.10.20.14 étant le serveur VXCORE).

3. **Raccordez vos caméras sur le même réseau** que le serveur VXCORE et le routeur / box Internet
4. **Configurez une adresse IP du réseau virtuel pour chaque caméra** : de 10.10.20.1 à 10.10.20.13 (avec le masque de sous-réseau 255.255.255.240)

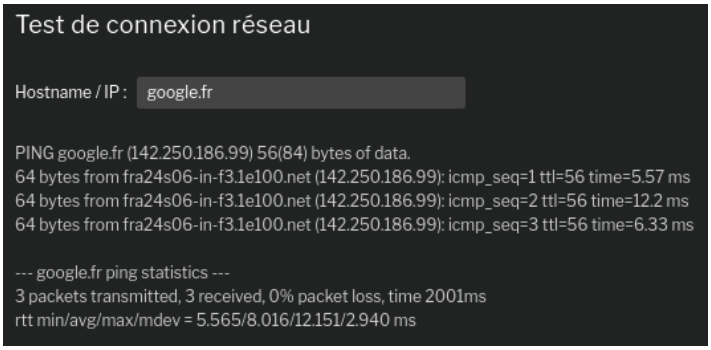
Dans cet exemple, tous les éléments du réseau sont bien connectés sur le même switch : serveur, caméras, routeur/box internet, PC(s) utilisateurs, etc. Mais les caméras seront bien sur un réseau IP séparé, non accessible directement par les PC(s) utilisateurs (sans configuration réseau spécifique).

Important : un réseau virtuel doit toujours être dissocié du réseau principal en utilisant un masque de sous-réseau différent, sinon il y aura forcément des problématiques de communications réseaux.

6.1.3 Test de connexion

Cette interface permet de lancer la commande « ping » à partir du serveur VXCORE.

Cela peut être utile dans la vérification de la configuration ou dans les diagnostiques des problèmes réseau.



6.1.4 Paramètres réseau

Passerelle / DNS

Si vous souhaitez que votre système se mettre à jour automatiquement ou que les utilisateurs puissent se connecter à distance, vous devez configurer la passerelle par défaut et l'adresse d'un serveur DNS. Ces paramètres ne sont pas nécessaires si vous avez configuré une de vos interfaces en DHCP.

Nom du serveur

Le nom du serveur est utilisé pour identifier votre système VXCORE dans l'interface web, dans l'envoi des alertes email (alarmes ou de maintenance) ou dans une configuration multi-site.

Adresse publique

L'adresse publique du serveur correspond à l'adresse accessible via l'extérieur (si existant).

Par exemple, cela peut être un nom de domaine ou une adresse IP. Cette adresse représente une URL absolue HTTPS, en tenant compte du port de connexion, s'il est spécifié.

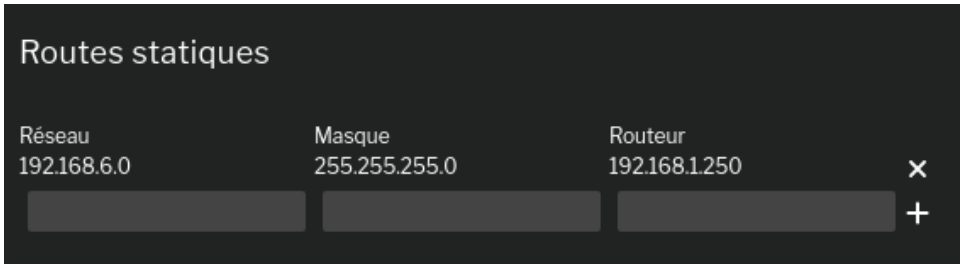
Exemple : https://demo.vxcore.fr:4431

L'adresse publique sera utilisée dans les alertes Email ou les notifications Push envoyées par le système, afin de simplifier la connexion aux utilisateurs. Elle sera également utilisée pour la génération du certificat SSL, afin de sécuriser les accès Web/SSL sur le bon nom de machine (hostname/dns).

6.1.5 Routes statiques

Utilisez l'interface de configuration des routes statiques pour ajouter des routes vers d'autres réseaux, qui n'utiliseraient pas la passerelle par défaut.

Pour chaque route, vous devez spécifier l'adresse d'un réseau, son masque et l'adresse du routeur qui fera la communication.

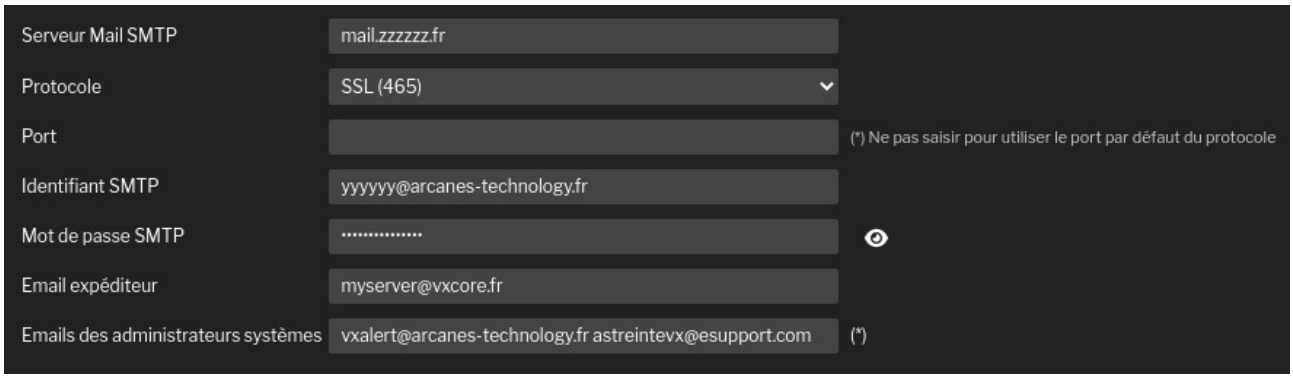


6.2 Paramètres SMTP

Si vous souhaitez que votre serveur puisse envoyer des alertes emails, vous devez configurer les paramètres SMTP du système.

VXCORE est capable d'envoyer des Emails via des serveurs SMTP classiques (port 25) ou sécurisés par SSL (port 465) ou TLS (port 587), avec authentification ou non (mot de passe normal).Dans certaines configurations, il sera peut être nécessaire de modifier l'adresse d'envoi des emails (par défaut vxcore@vxcore.fr).

Si vous renseignez les adresses emails des administrateurs systèmes, VXCORE sera capable de leur envoyer des alertes emails en cas d'erreur ou de problème détecté dans le fonctionnement du système.



Ces alertes emails seront envoyés au format HTML pour plus de lisibilité et incluront un état du fonctionnement et les logs du système.

Vous pouvez utiliser le bouton de test d’envoi des alertes mails pour vérifier la configuration.

6.3 Redirections réseau

VXCORE intègre une fonctionnalité de redirection de port automatique permettant de communiquer avec des périphériques IP situés sur le même réseau que le serveur.

Cette fonctionnalité est appelée proxy TCP : un port du serveur sera ouvert (dynamique ou statique) pour être redirigé sur un port d'une autre adresse IP du réseau (exemple : port 10001 du serveur redirigé vers le port 80 de la caméra 1).

6.3.1 Redirections réseau systèmes

Les redirections réseau systèmes permettent de se connecter aux interfaces des caméras ou des serveurs vidéo clients (dans le cas d'un serveur central).

Ces redirections sont gérées de manière automatique par le système.

Concrètement, elle permet aux utilisateurs de se connecter directement sur les interfaces des caméras IP, en utilisant VXCORE comme passerelle, même si elles sont situées sur un réseau complétement différent. Le port de connexion de la caméra qui sera utilisé sera celui configuré dans les paramètres de la caméra IP (en général le port Web 80).

Ces redirections TCP sont "dynamiques" car le Firewall ouvrira ces ports "à la volée" en fonction des demandes utilisateurs (authentification préalable).

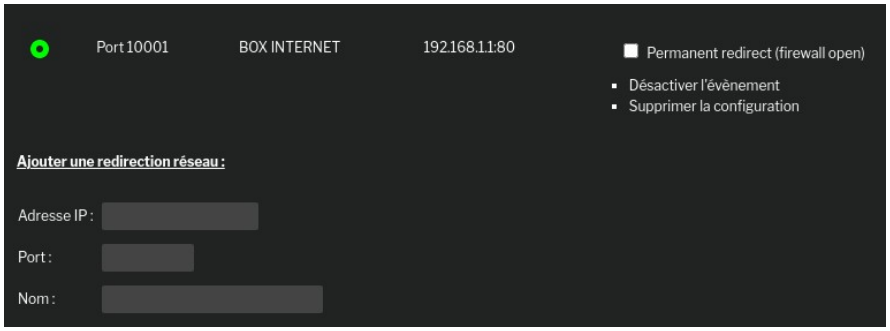
Les ports par défauts sont de 8000 à 8999 pour les redirections caméras et les de 9000 à 9999 pour les serveur vidéo clients VPN.

Remarque : dans la majorité des cas, il n'est pas nécessaire de modifier ces ports.

6.3.2 Redirections réseau externes

Les redirections réseau externes vous permettent rajouter des ports pour communiquer avec des éléments présents sur le même réseau que le système (routeur 3G/4G, centrale d'alarme, baie de stockage NAS, etc).

Ces redirections sont personnalisables par les administrateurs et peuvent ensuite être utilisées par les utilisateurs (permission requise dans le compte).



Exemple : redirection du port 10001 vers l'adresse IP 192.168.1.1 port 80, correspondant à l'interface Web d'un routeur Internet

*Important : ces redirections sont **statiques** : soit ouvertes, soit fermées. Vous devez les activer/désactiver selon vos besoins. Une redirection active implique que le port est ouvert en permanence sur le réseau, pour tout le monde.*

Redirections réseau centralisée (VPN) :

Sur un système central multi-site VXCORE-CORPORATE / VXCORE-ENTERPRISE, il est possible de chainer les redirections réseau au travers du tunnel VPN.

Concrètement, cela permet de créer une « porte d'accès » sécurisée vers un périphérique IP située sur le réseau d'un client VPN.

Exemple : accès à l'interface du routeur 4G situé derrière un serveur VXCORE nomade raccordé en VPN sur un serveur central.

Pour cela, il vous faudra créer deux règles de redirection : une sur le serveur VXCORE "distant" et une sur le serveur VXCORE "central" :

1. **Connectez-vous sur le serveur VXCORE "distant" (client VPN)**

   Dans les redirections réseau, ajouter la règle vers l'adresse IP/port du périphérique IP local, comme par exemple : port 10001 vers adresse IP 192.168.0.254, port 80 (interface Web routeur 4G).

   Le serveur local ouvrira le port "10001" qui pointe vers l'interface située sur le port 80 de l'adresse IP 192.168.0.254 (interface Web routeur 4G)

2. **Connectez-vous ensuite sur le serveur VXCORE "central" (serveur VPN)**

   Dans les redirections réseau, ajouter une règle de redirection VPN, qui pointe vers le client VPN et le port que vous venez de configurer (10001).

   Le serveur central ouvrira un nouveau port "10012" (par exemple), qui pointera de manière transparente vers l'interface du routeur 4G situé sur le réseau du serveur VXCORE "distant" (communication encapsulée dans le tunnel VPN).

Important : ces redirections sont statiques : soit ouvertes, soit fermées. Vous devez les activer/désactiver selon vos besoins. Une redirection active implique que le port est ouvert en permanence sur le réseau, pour tout le monde.

6.4 Firewall

VXCORE communique directement avec le module firewall du noyau Linux en créant ses propres règles. Ce firewall est suffisamment véloce et sécurisé pour permettre une installation d'un serveur directement sur un accès réseau public tel qu'Internet ou dans une DMZ (*).

(*) DMZ "Zone démilitarisée" : sous-réseau isolé du réseau local par un pare-feu contenant tous les serveurs susceptibles d'être accédés depuis Internet.

Remarque : dans la majorité des cas, il n'est pas nécessaire de modifier la configuration par défaut du firewall de VXCORE.

Si néanmoins votre système serait installé dans un environnement réseau sensible, il vous est possible de modifier sa configuration en sélectionnant quels services seront accessible sur les différentes interfaces réseaux.

Liste des ports et des services du système :

HTTPS	TCP port 443	Service Web sécurisé, utilisé pour accéder à l'interface du système *Activé par défaut*
HTTP	TCP port 80	Service Web non sécurisé, utilisé pour accéder à l'interface du système *Désactivé par défaut*
RTSP	TCP port 554	Service de streaming vidéo non sécurisé, utilisé pour accéder aux flux vidéo des caméras via des systèmes externes (live/playback) *Désactivé par défaut*
FTP	TCP port 20/21	Service de transfert de fichier, utilisé pour réceptionner les images ou les alarmes envoyées par les caméras *Désactivé automatiquement si aucune alarme FTP (recommandé uniquement en réseau local)*
SSH	TCP port 22	Service utilisé pour la maintenance distante d'un système, uniquement par l'éditeur *Désactivé par défaut*
VX	TCP port 73	Service propriétaire de synchronisation et de diffusion des flux vidéo en SSL/TLS (utilisé pour visualiser un trafic important de données vidéo sur le réseau) *Toujours activé*
VX	TCP port 79	Service propriétaire de synchronisation et de diffusion des flux vidéo (utilisé pour visualiser un trafic important de données vidéo sur le réseau) *Toujours activé*
NTP	UDP port 123	Service de synchronisation du temps (utilisé pour synchroniser les horloges des caméras IP avec celle du

		serveur VXCORE, par exemple) *Activé uniquement si firewall ouvert (recommandé uniquement en réseau local)*
SNMP	UDP port 161	Service de supervision système (utilisé pour superviser les ressources du serveur VXCORE : CPU, mémoire, etc) *Activé uniquement si firewall ouvert (recommandé uniquement en réseau local)*
VPN	TCP port 1194	Service utilisé sur les systèmes VXCORE de centralisation, permettant le raccordement des systèmes vidéo clients (VPN) *Activé uniquement si configuration VPN*
PING	ICMP	Service utilisé pour diagnostiquer la connectivité réseau *Activé par défaut*

Remarque : si vous avez bloqué votre accès réseau suite à une mauvaise configuration du firewall, il sera nécessaire de connecter un écran et un clavier sur votre serveur pour utiliser l'utilitaire de configuration réseau en ligne de commande.

6.5 Supervision SNMP

VXCORE intègre un service SNMP qui peut être activé depuis la configuration système/firewall (Simple Network Management Protocol).

Ce service expose des OIDs SNMP qui peuvent êtres interrogés pour une éventuelle intégration dans un système de supervision d'entreprise. Par ce billet, il est alors possible de superviser le LOAD, l'usage CPU, l'usage mémoire et l'usage réseau du serveur vidéo.

La mib est accessible en lecture simple et version 2c du protocole.

Communauté v2c: **vxsnmp**

Adresses d'OID :

```
Load
1 minute Load: .1.3.6.1.4.1.2021.10.1.3.1
5 minute Load: .1.3.6.1.4.1.2021.10.1.3.2
15 minute Load: .1.3.6.1.4.1.2021.10.1.3.3
CPU
percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
raw user cpu time: .1.3.6.1.4.1.2021.11.50.0
percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
raw system cpu time: .1.3.6.1.4.1.2021.11.52.0
percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0
raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0
Memory Statistics
Total Swap Size: .1.3.6.1.4.1.2021.4.3.0
Available Swap Space: .1.3.6.1.4.1.2021.4.4.0
Total RAM in machine: .1.3.6.1.4.1.2021.4.5.0
Total RAM used: .1.3.6.1.4.1.2021.4.6.0
Total RAM Free: .1.3.6.1.4.1.2021.4.11.0
Total RAM Shared: .1.3.6.1.4.1.2021.4.13.0
Total RAM Buffered: .1.3.6.1.4.1.2021.4.14.0
Total Cached Memory: .1.3.6.1.4.1.2021.4.15.0
Networking
1.3.6.1.2.1.2.2.1.10 - ifInOctets returns the total number of octets received on
the interface, including framing characters.
1.3.6.1.2.1.2.2.1.16  -  ifOutOctets  returns  the  total  number  of  octets
transmitted out of the interface, including framing characters.
```

Remarque : pour plus de détails sur les OIDs - https://oidref.com

Exemple d'usage : la commande Linux "SNMPWALK" permet de dumper la liste des OIDs accessibles :

snmpwalk -v 2c -c vxsnmp ADRESSE_IP_VXCORE

6.6 Certificats SSL

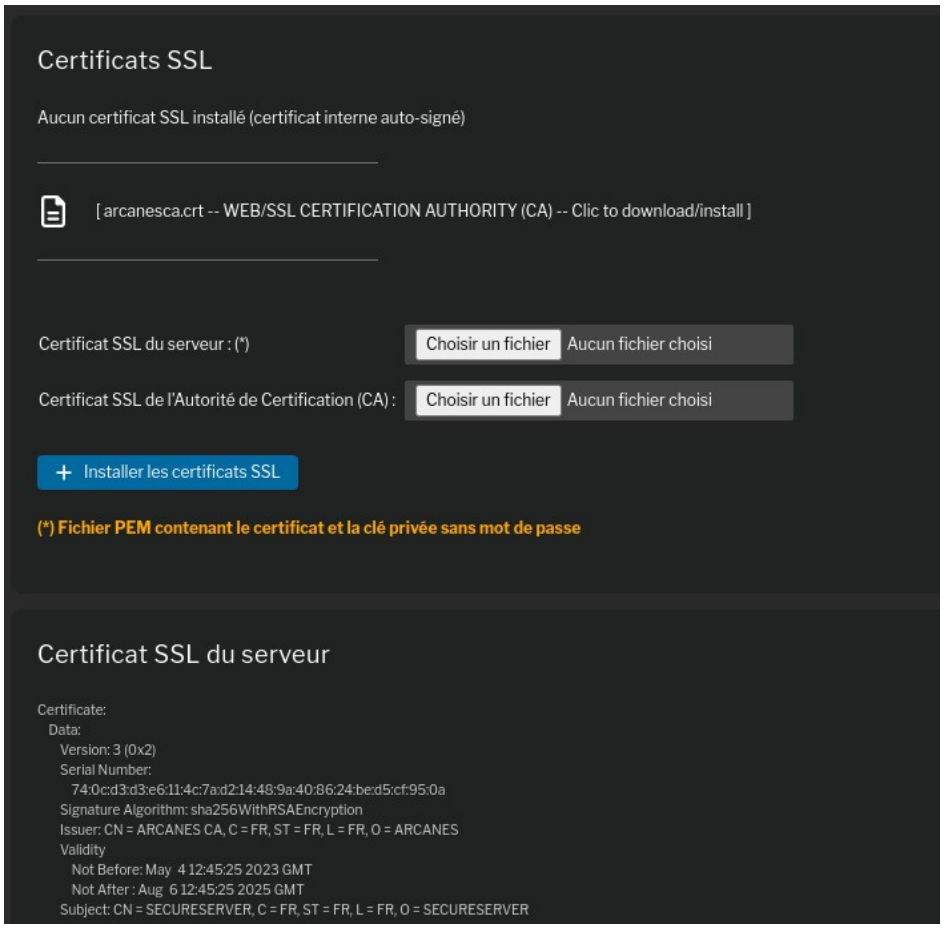
VXCORE intègre un certificat SSL "auto-signé" permettant de sécuriser les accès sur le port HTTPS / 443 par défaut.

Ce type de certificat permet de garantir la même confidentialité des échanges et la même sécurité que les certificats signés par un organisme de certification officiel. La seule différence est le coût : un certificat officiel doit être acheté et renouvelé régulièrement par l'utilisateur final.

Si vous vous connectez sur un serveur VXCORE sur Internet, comme un serveur central multi-site par exemple, il est préférable de **ne jamais utiliser le protocole HTTP**. Ce protocole n'est pas chiffré et tous les échanges seront en clair, comme l'authentification et le transfert de votre mot de passe.

Si vous configurez des adresses IP statiques ou une adresse DNS publique dans les paramètres réseaux, alors le certificat SSL sera automatiquement généré pour chaque IP et/ou adresse DNS.

Cela signifie que le client PC ou le navigateur Web pourra certifier la connexion réseau avant toute tentative de connexion utilisateur sur l'interface du système.



Vous pouvez également choisir d'installer votre propre certificat SSL dans VXCORE.

Pour cela, vous devez passer par une autorité de certification officielle qui vous délivrera un certificat SSL signé.

Vous pourrez ensuite importer votre certificat dans le système, au format PEM (composé de la clé privée RSA et du certificat public CRT).

Il sera quelque fois nécessaire d'importer le certificat intermédiaire de l'Autorité de Certification (CA).

Vous pouvez également utiliser un service en ligne pour tester et valider votre configuration SSL, toutes les autorités de certifications le propose (SSL CHECKER).

Dans le cas de l'installation d'un certificat SSL externe, le système supervisera la date d'expiration du certificat et affichera un message d'avertissement lorsque celui ci arrivera a échéance (90 jours).

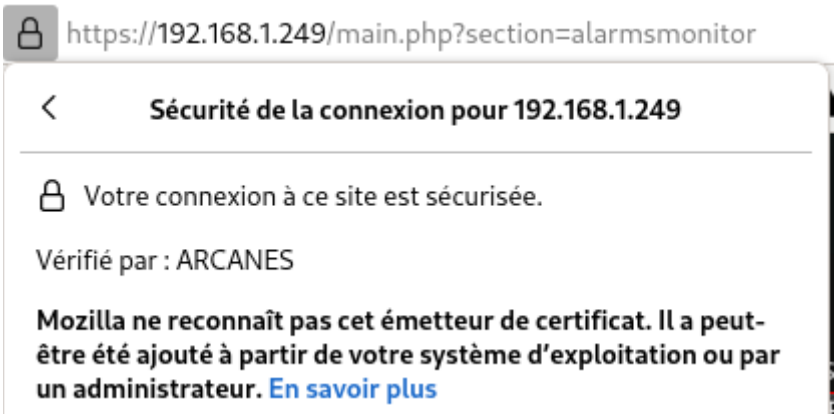
Le certificat interne auto-généré par le système sera automatiquement renouvelé tous les 825 jours.

Consultation de l'interface du système avec un navigateur Web :

Si vous décidez de consulter l'interface du système avec un navigateur Web, vous devez d'abord désactiver le contrôle d'accès applicatif dans les paramètres de sécurité.

Ensuite, vous devez télécharger et installer le certificat d'autorité «arcanesca.crt » directement dans le magasin des certificats du navigateur Web (ou de l'application mobile). Ce certificat est téléchargeable directement depuis l'interface de configuration SSL du système.

De cette manière, le navigateur aura tous les éléments pour vérifier et certifier la connexion HTTPS vers le système.



6.7 LDAP / Active Directory

La fonctionnalité LDAP/AD permet aux systèmes VXCORE d'authentifier les utilisateurs de manière externe sur un serveur LDAP ou Microsoft Active-Directory.

Remarque : le module LDAP/AD n'est pas disponible sur toutes les versions des systèmes VXCORE.

6.7.1 Fonctionnement

VXCORE utilise sa propre base de données interne pour stocker les utilisateurs et les mots de passe.

Le module d'authentification LDAP/AD permet de faire l'authentification des utilisateurs via un serveur LDAP externe ou un service Microsoft Active-Directory.

Une correspondance est ensuite faite entre des « groupes de sécurité » et des « rôles VXCORE » afin d'attribuer des droits et permissions.

Une fois la configuration en place, l'utilisateur pourra alors se connecter au système via son couple "login / mot de passe MS-AD" (le login étant l'attribut LDAP "*sAMAccountName*", a l'image de ce que Microsoft utilise pour la connexion à un poste de travail Windows).

Lors de la première connexion d'un compte utilisateur LDAP, l'utilisateur sera créé dans la base de données du système VXCORE. Les informations disponibles dans l'annuaire seront utilisées pour créer le compte (login, nom et email de l'utilisateur).

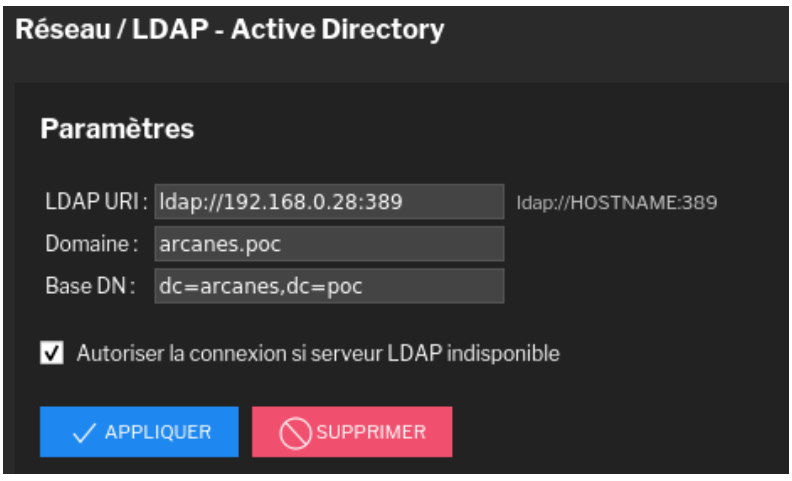
Lors qu'un utilisateur existant se connectera a nouveau, le système vérifiera et synchronisera les informations de l'annuaire.

Si aucun rôle n'est affecté au compte utilisateur : le compte sera automatiquement désactivé.

Remarque : le système ne supprimera pas automatiquement les comptes utilisateurs périmés de sa base de données interne. Vous devrez le faire manuellement.

6.7.2 Définition de l'annuaire

Dans le menu administration, cliquez sur Réseau / LDAP – Active Directory pour définir l'accès à l'annuaire/serveur externe (options avancées).

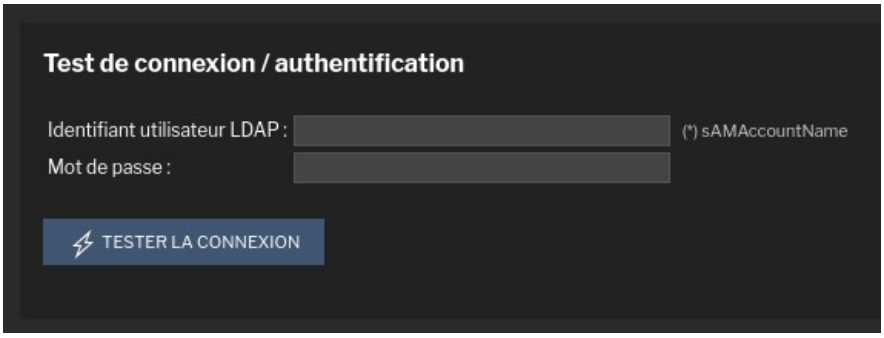


Saisissez ensuite les paramètres de connexion de votre serveur LDAP/AD.

L'option « *Autoriser la connexion si serveur LDAP indisponible* » permet à un compte LDAP précédemment authentifié avec succès sur le système, de se connecter malgré que l'annuaire LDAP soit indisponible (ex: maintenance AD/panne réseau…).

Pour cela, il faudra que l'utilisateur se soit connecté une première fois, afin que le compte ait bien été synchronisé dans la base de données interne.

Après votre saisie, vous pouvez utiliser le test de connexion d'authentification afin de vérifier que les paramètres LDAP/AD sont corrects.



6.7.3 Liaison entre groupe MS-AD et rôles

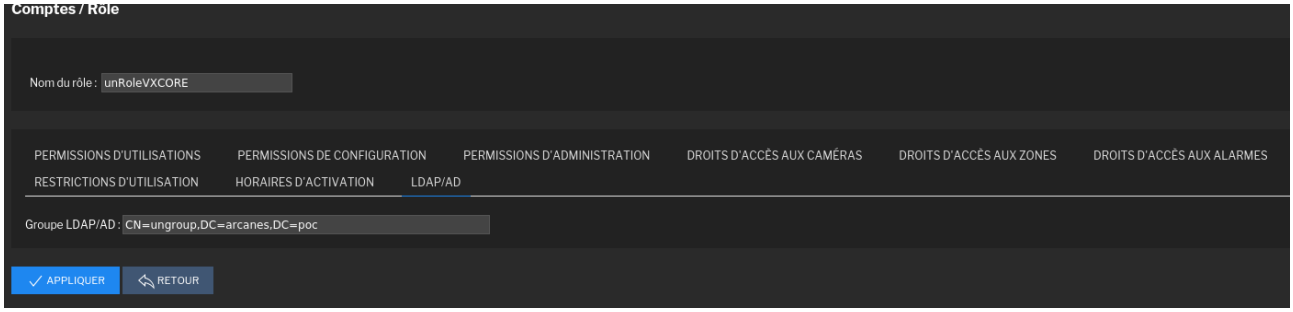
Cette étape de configuration est nécessaire afin de lier un groupe LDAP/AD à un rôle VXCORE.

Si un utilisateur LDAP n'est lié a aucun rôle, il ne pourra pas se connecter au système (compte automatiquement désactivé).

Depuis le menu configuration du système, cliquez sur le menu Comptes / Rôles.

Créer ensuite un rôle, en définissant tous les droits d'accès et les permissions systèmes.

Pour terminer, il faut lier ce rôle au groupe LDAP/AD en cliquant sur l'onglet correspondant.



Renseignez bien le « DN » (Distinguished Name) complet du groupe Active-Directory : le chemin LDAP qui permettra de trouver le groupe dans l'annuaire.

6.8 HA / Haute disponibilité

La fonctionnalité de haute disponibilité ou high availability (HA) permet aux systèmes VXCORE de concevoir une architecture redondante des services vidéo, tolérante aux pannes les plus courantes.

Afin de concevoir un système vidéo redondant avec le module HA, il sera nécessaire de disposer de deux serveurs physiques parfaitement dimensionnés (ressources CPU suffisantes, quantité de mémoire RAM, stockage vidéo, disque système et formatage équivalent, etc)

Chaque serveur doit être capable de fonctionner sans problème avec le parc caméra et les utilisateurs en cas de reprise d'activité (pas de sous dimensionnement du serveur de secours).

Par exemple, attention au dimensionnement de l'analyse vidéo avec IA : il sera préférable d'utiliser un ou plusieurs serveurs d'analyses vidéo externes pour répartir la charge (VXNODE).

Remarque : le module HA n'est pas disponible sur toutes les versions des systèmes VXCORE et nécessite un module de licence spécifique.

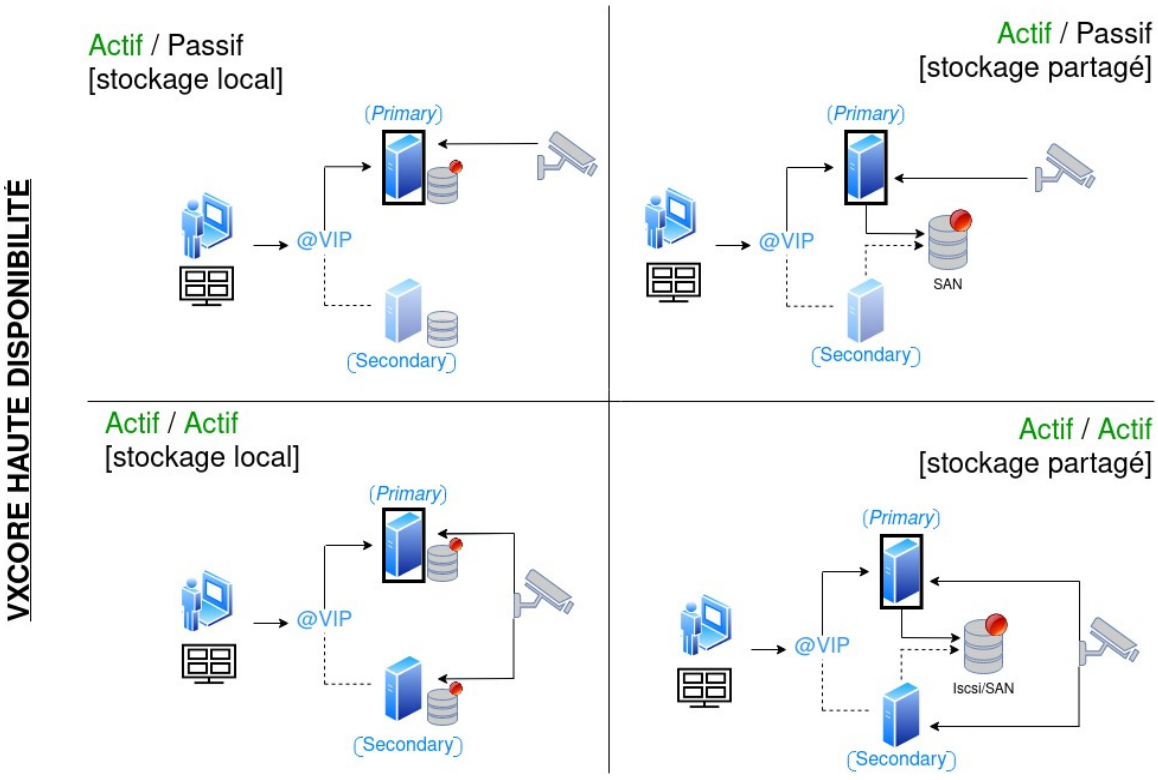
6.8.1 Fonctionnement

Un système VXCORE configuré pour la haute disponibilité va disposer d'un fichier de licence spécial qui pourra être installé sur deux serveurs physiques : un **node primaire** et un **node secondaire**.

Seul un de ces nodes pourra activer les adresses IP failover, qui seront utilisées pour accéder aux ressources vidéo par les utilisateurs, les murs d'images, etc

Les données seront automatiquement synchronisées entre les deux serveurs/nodes, afin qu'ils disposent toujours d'une configuration identique.

Le module permet de concevoir des architectures Haute Disponibilité de type **Actif/Passif** ou **Actif/Actif**, avec une stratégie de stockage indépendante ou partagée.



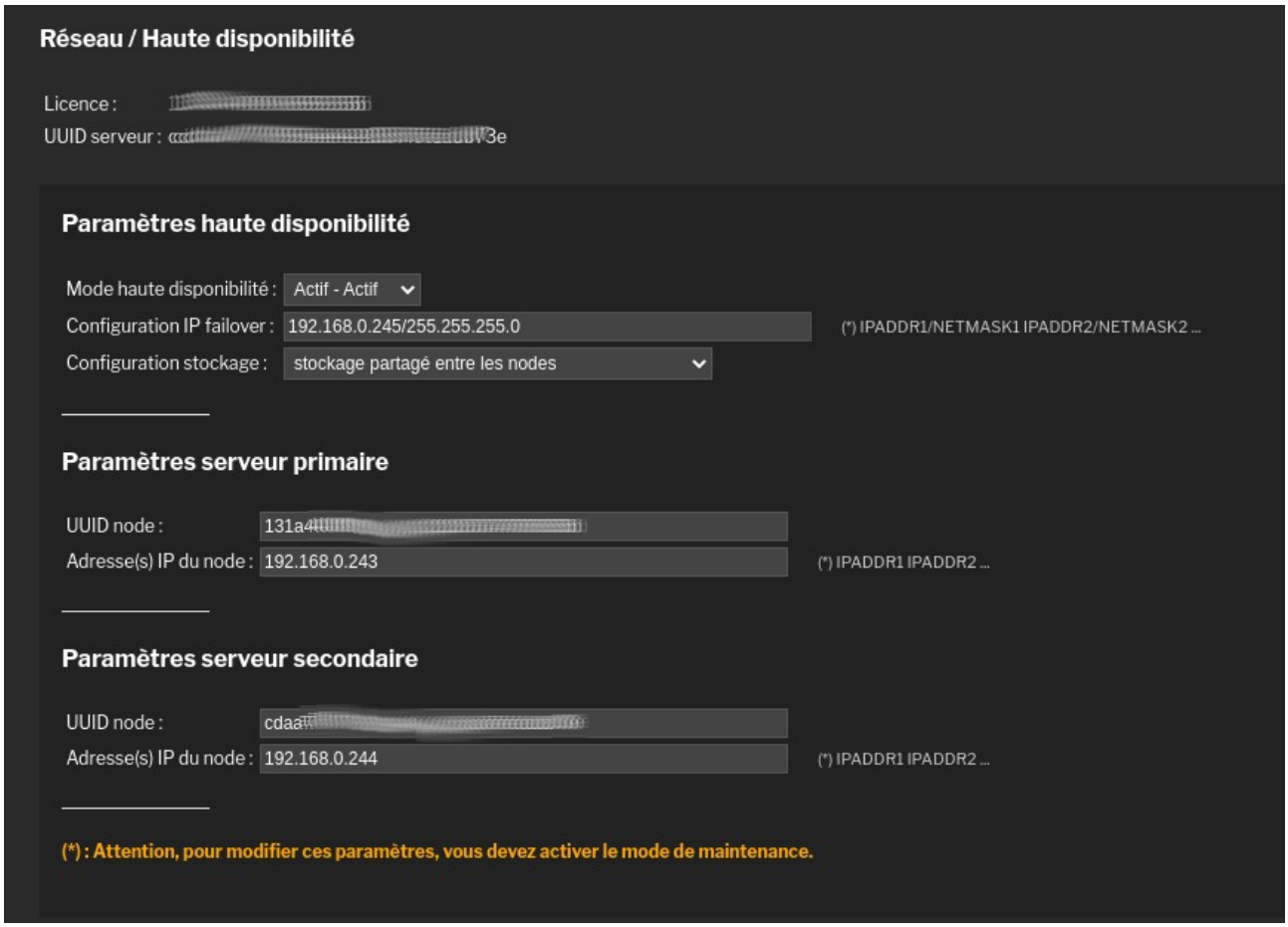
6.8.2 Configuration

Après avoir correctement installé les serveurs primaire et secondaire avec leur fichier de licence commun, vous pourrez configurer le module HA.

Dans le menu administration, **activez le mode de maintenance** sur les deux serveurs primaire et secondaire.

Dans le menu administration, cliquez sur Réseau / Haute disponibilité pour afficher l'interface de configuration (options avancées).

Important : la configuration est à renseigner à l'identique sur les nodes primaire et secondaire



Renseigner ensuite toutes les informations concernant le mode Haute disponibilité, la configuration des IP failover et la stratégie de stockage (locale ou partagée).

La stratégie de stockage partagée nécessite une baie de stockage commune et accessible par les deux serveurs (iSCSI ou Fibre channel).

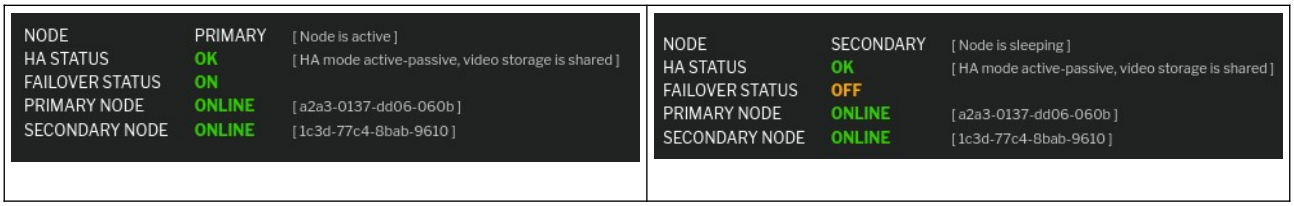
Dans la partie suivante, saisissez les identifiants uniques de chaque node (UUID), que vous pourrez récupérer sur l'interface de configuration de chaque serveur.

Vous devez également saisir les adresses IP statiques de chaque node, afin qu'ils puissent bien communiquer entre eux (synchronisation).

Remarque : il est fortement recommandé de saisir plusieurs adresses IP pour avoir une synchronisation fiable entre les nodes (plusieurs chemins réseau utilisant des équipements différents ou même un câblage direct pour lier une interface réseau de confiance).

Après avoir configuré les différents éléments, vous pouvez **désactiver le mode maintenance sur les deux serveurs**.

Vous verrez l'état de la configuration Haute Disponibilité directement dans le tableau de bord administration **de chaque serveur** (chaque node disposera de son propre état) :



NODE : indique sur quel serveur on est actuellement connecté, et si le node est en activité ou non

HA STATUS: indique l'état de la configuration haute disponibilité (ainsi que le mode HA et la stratégie de stockage configurée).

FAILOVER STATUS: indique si la ou les adresses IP Failover sont actives sur le node

PRIMARY/SECONDARY NODE : indique l'état et l'identifiant unique de chaque serveur

Important: si le node secondaire reprend l'activité suite à un crash du serveur principal, la rebascule n'est pas automatique. Après avoir remis en état le serveur principal, il sera nécessaire de redémarrer le node secondaire pour y rebasculer l'activité.

Avant de faire un redémarrage de serveur, et pour éviter toute perte de données, vérifiez bien dans le tableau de bord de chaque node que tout est opérationnel (pas d'erreurs ou de problèmes de synchronisation après au moins 15 minutes d'activité).

Le service de haute disponibilité intègre une sécurité interne pour éviter le mode « split-brain » en utilisant le réseau des caméras.

Un *split-brain* se produit lorsque les deux nodes ne peuvent plus communiquer ensemble, chacun croyant que l'autre ne fonctionne plus.

Avant de faire une bascule lorsque le serveur primaire ne répond plus, le serveur secondaire va vérifier qu'il arrive bien a communiquer avec le réseau des caméras afin de vérifier qu'il n'est pas isolé dans le réseau.

6.9 Connexion du système sur Internet

Pour vous connecter au système vidéo par Internet, il existe deux méthodes :

- soit en connexion directe
- soit via un serveur central VXCORE-CORPORATE/ENTERPRISE en VPN

Dans les deux cas, vous devez configurer l'adresse de la passerelle par défaut et l'adresse d'un serveur DNS. Votre système doit pouvoir "sortir" sur Internet (test de PING).

6.9.1 Connexion à distance directe

Pour permettre une connexion directe sur un serveur VXCORE, vous devez configurer votre routeur/firewall afin de rediriger le trafic réseau correctement.

Vous devez aussi posséder une adresse publique accessible en permanence de l'extérieur, comme une adresse IP fixe ou un nom de domaine fixe ou dynamique (type dynDNS).

Classiquement, il existe deux méthodes de configuration du routeur.

Configuration en DMZ :

Cette méthode consiste à configurer votre routeur pour placer le serveur VXCORE dans la DMZ.

Tout le trafic entrant sera donc automatiquement redirigé vers VXCORE qui se chargera de répondre ou non aux requêtes, en utilisant son propre firewall (que vous devez configurer, afin de fermer les ports non utilisés).

Ouverture et redirections des ports :

Cette méthode consiste à configurer votre routeur pour qu'il redirige le trafic entrant de certains ports vers le serveur VXCORE.

Le seul port à rediriger pour accéder au système vidéo est le port **HTTPS / 443 (tcp)**.

Si vous souhaitez accéder à l'interface de vos caméras ou équipements réseaux externes, pour les configurer par exemple, vous devrez également rediriger les ports (ceux qui ont été configurés).

Pour les caméras, les ports par défaut sont de 8000 à 8xxx ("xxx" représentant le nombre total de caméras).

Dans tous les cas, il sera nécessaire de vous référer à la documentation de votre routeur/firewall pour définir la configuration la plus adaptée.

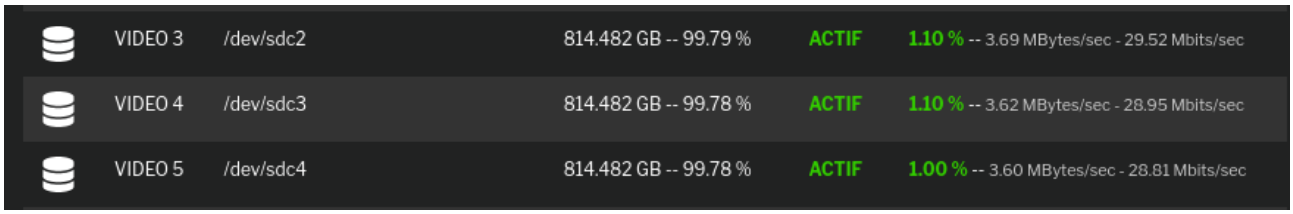
6.9.2 Connexion à distance via serveur de centralisation

L'autre méthode pour se connecter sur un serveur VXCORE à distance est de le rattacher à un serveur central VXCORE-CORPORATE/ENTERPRISE (VPN dédié).

Cette méthode est décrite plus en détail dans la section "Extensions/VPN" de ce manuel.

7 Stockage vidéo

VXCORE a été conçu pour gérer des gros volumes de stockage et l'enregistrement de débits extrêmes de flux vidéo, tout en utilisant des systèmes de fichiers standards et fiables du monde Linux.



Le système inclut la technologie propriétaire "VXSYNC" permettant de bufferiser l'ensemble des données vidéo afin de procéder à une écriture intelligente sur les disques durs, en fonction de la stratégie de stockage et de l'état des périphériques connectés. Cette technologie permettra d'obtenir des débits très important d'enregistrement vidéo en continu, sans en altérer les performances du système (jusqu'à 1 Gbit/s - avec un serveur et une architecture adapté).

Quelque soit la dimension de votre architecture vidéo, il est conseillé d'utiliser des disques durs adaptés à l'enregistrement vidéo continu. Les constructeurs proposent des produits réservés à cet usage, il existe maintenant des disques durs "série serveur" ou "vidéo surveillance" (vitesse minimale 7200 tr/min).

VXCORE utilise le système de fichier XFS pour ses LUNs vidéo, conçu par Silicon Graphics, Inc. (SGI). XFS combine la technologie de journalisation avancée avec un adressage full 64-bit et des structures et algorithmes scalable. La taille maximale d'un système de fichier XFS est de 9 HEXABYTES.

7.1 Configuration du volume de stockage

Le volume de stockage vidéo n'est pas configuré lors de l'installation du système VXCORE, vous devez le configurer dans la section administration/stockage de l'interface Web (sauf en mode installation « shared »).

VXCORE détecte automatiquement les disques durs, les volumes logiques RAID ou les volumes logiques externes connectés au serveur (SAN/Fibre Chanel). Il est possible de configurer des volumes en réseau via le protocole iSCSI ou NFS, mais vous devriez dédier une interface réseau à cet usage pour éviter les engorgements (dissocier réseau caméra et réseau stockage).

Les périphériques connectés en USB ne sont pas utilisés pour le stockage interne du système, mais il existe un module d’enregistrement vidéo externe adapté à cet usage (double enregistrement vidéo avec extraction des données).

Le système dispose d'une fonctionnalité d'importation de LUN vidéo existant, qui détectera et ajoutera tout volume précédemment configuré par un système VXCORE (sauf la partition réservée d'un disque système). Après l'importation d'un LUN vidéo, il sera important de procéder à une synchronisation du volume de stockage pour reconstituer la nouvelle base de données (section administration/maintenance).

Il existe deux modes de configuration pour le volume de stockage vidéo :

normal ou **séquentiel**

Le choix du mode de stockage ne sera possible que lorsque le volume n'est pas configuré (aucun LUN vidéo). Si vous souhaitez changer de mode en cours de fonctionnement, vous devez obligatoirement réinitialiser complétement votre volume de stockage.

Configuration normale (par défaut)

Ce mode permet d'utiliser un ou plusieurs disques de stockage vidéo et d'activer toutes les fonctionnalités du système VXCORE.

Configuration séquentielle (HSR)

Ce mode est utilisé par les systèmes nécessitant une gestion de gros débits d'enregistrement vidéo, comme dans une configuration de plus de 50 caméras en RAID ou avec des résolutions d'images Full-HD ou 4K. Nécessite 4 volumes au minimum pour fonctionner et limite certaines fonctionnalités de VXCORE.

Quelque soit la configuration et la stratégie de stockage vidéo, VXCORE identifiera et utilisera chaque disque ou volume logique de manière indépendante, avec son propre système de fichier, appelé "LUN vidéo".

Le système ne créera pas de volume global constitué comme un RAID 0 ou une configuration LVM (logical volume manager). Les volumes pourront être de taille et de type différents (SATA, IDE, RAID, ...).

VXCORE utilisera tous les LUNs disponibles pour constituer un volume de stockage vidéo solide, performant et résistant à la perte d'un ou plusieurs LUNs (tolérance de panne).

Exemple d'une configuration de LUNs vidéo (hétéroclite, non réelle) :

video1 - /dev/sda6	800 MB	Partition réservée du disque système (mode installation «shared»)
video2 - /dev/sdb1	2 TB	Disque dur SATA entier
video3 - /dev/sdc1	3 TB	Volume RAID 5 interne via carte LSI constitué de 4 disques SATA 1 TB
video4 - /dev/sdd1	6 TB	Volume logique RAID d'une baie de stockage externe Fibre Channel

Capacité de stockage vidéo totale : video1 + video2 + video3 + video4 = 11,8 TB

7.1.1 Stockage normal (par défaut)

Dans la configuration par défaut, le système utilise les disques durs comme des systèmes de fichiers classiques. Dans un cycle permanent, des nouveaux fichiers seront créés et d'autres plus anciens seront supprimés, lorsque le volume de stockage vidéo sera plein. La limite d'enregistrement vidéo sera alors fixée par la capacité totale du volume de stockage et les quotas d'enregistrement configurés dans le système.

Dans cette configuration de stockage, il sera possible de supprimer des fichiers vidéo ciblés, comme les enregistrements hors alarmes ou les enregistrements non sécurisés. La rétention des données vidéo est optimisée au maximum.

Le système va enregistrer de manière cyclique des données sur tous les LUNs vidéo, jusqu'à ce que l'ensemble du volume soit plein. Dans ce cas, le système procédera à la suppression des anciennes données pour ensuite les remplacer par les nouvelles données. Les données vidéo seront donc découpées en petits blocs, et réparties sur l'ensemble des LUNs de stockage.

Ce mode de configuration ne formatera jamais les LUNs vidéo, les systèmes de fichiers seront préservés : on travaillera uniquement les fichiers. Il y aura potentiellement un risque d'erreurs liés à des déconnexions violentes des LUNs et de la perte de la mémoire cache des contrôleurs de stockage (coupures de courant, déconnexions des baies externes ...). Ces erreurs ne pourront être corrigées qu'en réparant manuellement ou en reconfigurant à zéro le LUN vidéo endommagé (nouveau formatage, perte des données).

Ce mode de configuration aura cependant ses limites, il sera effectivement impossible de dépasser certains débits d'enregistrements vidéo (par exemple dans le cas de l'enregistrement de plus de 50 caméras 4K en 8 Mégapixels). En général, dans les systèmes de fichier informatique, il est toujours plus gourmand en ressource de supprimer un fichier que de le créer. Le système rencontrera donc un point d'encombrement ou les données enregistrées n'arriveront plus à se supprimer correctement, ce qui provoquera des surcharges et des coupures dans les enregistrements vidéo. Dans ce cas, il sera nécessaire d'activer le mode séquentiel (HSR).

7.1.2 Stockage séquentiel (HSR)

La stratégie de stockage séquentielle à été conçue pour créer des grosses architectures d'enregistrement vidéo, avec des débits très importants, tout en utilisant du matériel standard.

Attention : pour fonctionner correctement, l'enregistrement séquentiel nécessite la configuration d'au moins 4 LUNs vidéo.

Dans cette configuration de stockage, chaque LUN vidéo sera considéré comme un bloc entier, et sera entièrement rempli avant que le système n'utilise un autre LUN. Lorsque tous les LUNs seront pleins, le système formatera entièrement le premier LUN avant d'y enregistrer les nouvelles données.

Afin d'optimiser les performances des accès I/O aux périphériques de stockage, le système ne procédera à aucune création, modification ou suppression de fichier ou donnée stockée sur un LUN vidéo plein.

En enregistrement séquentiel, certaines options du système seront donc automatiquement désactivées :

- **Enregistrement sur alarme**

  deviendra identique à un enregistrement permanent (plus d'optimisation du stockage en supprimant les vidéo hors alarme.

- **Enregistrement sécurisé**

  deviendra identique à un enregistrement permanent (qui est par défaut un enregistrement sécurisé).

- **Quota d'enregistrement vidéo par caméra**

  les enregistrements vidéo seront supprimés de la base de données, mais pas physiquement des LUNs vidéo.

Comme l'enregistrement sur alarme sera automatiquement désactivé, le calcul du stockage vidéo sera fait comme pour un enregistrement continu 24h/24.

Pour optimiser la gestion séquentielle, il est recommandé de "découper" chaque LUN vidéo dont la taille excède 2 TB (partitionnement physique). En effet, un gros système de fichier de plus de 6 TB aura plus de chance d'être corrompu qu'un système fichier de 2 TB et sera aussi beaucoup plus lourd à gérer par le système d'exploitation (gros système de fichier = grosse structure de données).

Lors de la création des LUNs vidéo, VXCORE vous proposera de partitionner automatiquement vos périphériques de stockage. Ce partitionnement sera calculé pour obtenir des LUNs vidéo proches de 2 TB.

Si vous disposez d'un très gros volume de stockage vidéo, nous vous recommandons de partitionner les volumes manuellement pour obtenir un total de **16 LUNs vidéo maximum** (ce n'est pas une limite physique, mais une recommandation pour la gestion des systèmes de fichiers).

Lorsque tous les LUNs vidéo seront partitionnés et le formatage terminé, VXCORE procédera à une réorganisation des ID des LUNs, afin d'optimiser la répartition des enregistrements vidéo (perte d'un périphérique de stockage = perte de toutes ses partitions).

L'avantage de la gestion du stockage séquentiel est sa robustesse à l'utilisation, même dans un environnement sensible. Comme chaque bloc vidéo sera entièrement formaté avant d'être utilisé, les éventuelles erreurs présentes sur les systèmes de fichiers seront automatiquement éliminées à chaque cycle.

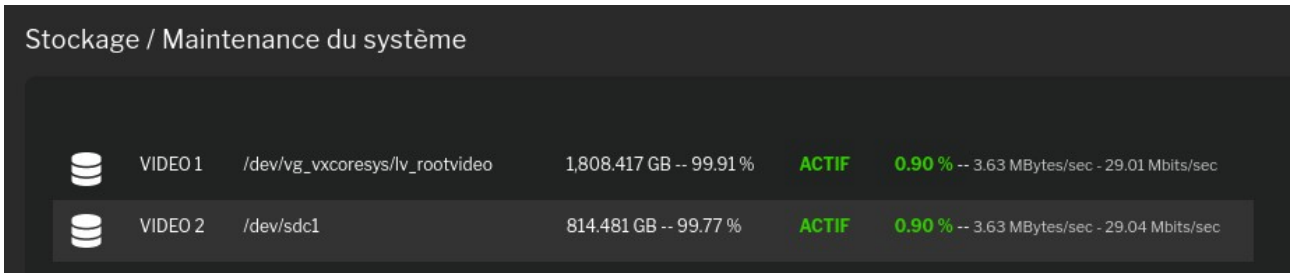
Il est recommandé d'activer le mode d'enregistrement séquentiel avec l'utilisation de baies de stockage externes ou avec des gros volumes logiques RAID hardware (type LSI/3WARE).

7.2 Maintenance du volume de stockage

VXCORE dispose d'une interface spécifique pour observer et contrôler la gestion du volume de stockage vidéo, située dans l'espace d'administration/stockage.

7.2.1 État des LUNs vidéo

Cette page représente l'ensemble des LUNs vidéo configurés et leur état de fonctionnement (systèmes de fichiers, et non forcément périphériques physiques).



Remarque : lors d'un démarrage du serveur, les LUNs vidéo ne seront pas immédiatement attachés. VXCORE testera d'abord l'accès aux LUNs vidéo avant de monter et d'activer les périphériques de stockage.

Il existe 5 états de fonctionnement pour chaque LUN vidéo :

- **Actif**

  LUN vidéo opérationnel et utilisé par le système

- **Initialisation / Maintenance**

  LUN vidéo en cours d'initialisation ou opération de maintenance système (formatage, réparation, ...).

- **Absent**

  LUN vidéo non trouvé ou impossible à monter dans le système (disque dur ou baie de stockage déconnectée, système de fichier corrompu).

- **Erreur**

  LUN vidéo en erreur, le système a rencontré un problème lors de l'écriture ou la lecture de données.

- **Surcharge (Overload)**

  Surcharge du périphérique lors de l'écriture des données (lorsque le temps d'écriture des données a dépassé le temps d'acquisition).

LUN vidéo absent

Lorsqu'un LUN vidéo est marqué "absent", c'est que le système ne le détecte plus et qu'il lui est impossible de l'attacher.

Un système de fichier peut être marqué absent pour plusieurs raisons : le disque dur ou la baie de stockage n'est pas connecté physiquement ou le système de fichier a été trop endommagé et n'est même plus détecté.

Si après un redémarrage du serveur le LUN est toujours dans le même état, essayez de le détruire et de le reconfigurer dans le volume de stockage. Si le système ne détecte plus ce périphérique dans la liste, c'est qu'il est endommagé ou déconnecté physiquement.

LUN vidéo en erreur

Lorsqu'un LUN vidéo est marqué en "erreur", c'est que le système a rencontré un problème lors de l'écriture ou la lecture de données sur le périphérique.

Cette erreur est en général liée à l'état de santé du périphérique de stockage, et n'apparait que dans le cas d'un réel problème physique d'écriture des données. VXCORE teste les LUNs vidéo en erreur en lecture/écriture avant de le signaler défectueux.

Si après un redémarrage du serveur le LUN réapparait en erreur, vous pouvez tenter une réparation du système de fichier (procédure qui pourra être longue selon le type et la taille du périphérique). Sinon essayez de le détruire et de le reconfigurer dans le volume de stockage. Si le système ne détecte plus ce périphérique dans la liste, c'est qu'il est physiquement endommagé. Consultez également les logs du système Linux pour vérifier qu'il n'y a pas de remontées d'erreurs I/O du périphérique de stockage.

LUN vidéo en surcharge

Lorsqu'un LUN vidéo est marqué en "surcharge" ou "overload", c'est que le système n'a pas réussi à écrire les données dans le temps imparti, impliquant une surcharge du périphérique de stockage. En général, la charge d'un LUN vidéo doit rester en dessous de 30% en moyenne et 50% en pointe.

Pendant chaque seconde de fonctionnement, VXCORE réceptionne des données vidéo dans sa mémoire interne (VxSync) et procède à son écriture sur le LUN vidéo actif. Si le temps d'écriture dépasse le temps de réception plusieurs fois de suite, le LUN vidéo sera marqué en surcharge.

La surcharge d'un LUN vidéo peut être liée à plusieurs causes : panne ou vieillissement du périphérique de stockage, mauvaise configuration du système, charge trop importante d'enregistrement vidéo ou encore périphérique de stockage trop lent en écriture (cas de certains volumes RAID lorsque le cache d'écriture est désactivé).

Si vous avez régulièrement des problèmes de surcharges sur vos LUNs vidéo, essayez d'augmenter le cache d'écriture de l'enregistrement vidéo ou d'activer l'enregistrement séquentiel pour soulager les volumes. Si cela ne résout pas le problème, vous n'aurez d'autres choix que de changer la configuration de stockage ou de réduire le débit des flux vidéo enregistrés.

7.2.2 Cache d'écriture du volume de stockage

VXCORE intègre une fonctionnalité de cache d'écriture logicielle, qui permet de compenser les ralentissements des périphériques de stockage physique en stockant temporairement les données dans la mémoire vive du serveur (RAM).

Il est plus facile et moins onéreux d'augmenter la quantité de mémoire vive d'un serveur que d'accélérer son volume de stockage (mémoire cache et débit des cartes RAID, vélocité et mémoire cache des disques durs ...).

Le cache d'écriture est par défaut réglé en mode automatique, ce qui signifie qu'il va s'adapter en fonction de la mémoire disponible du serveur.

Par exemple, un cache d'écriture de 30 secondes signifie que le système dispose de ce même temps pour écrire les données avant de perdre les suivantes (dans le cas d'un ralentissement

du volume de stockage). La valeur peut sembler importante mais les disques durs de grande capacité sont souvent très lents, surtout lorsqu'ils synchronisent leur mémoire cache.

Vous pouvez régler ce paramètre manuellement et augmenter le cache d'écriture jusqu'à 60 secondes maximum (en plaçant le système en mode maintenance). Le système calculera d'abord la quantité de mémoire vive requise et disponible avant d'appliquer le nouveau réglage.

7.2.3 Réparation des LUNs vidéo

VXCORE intègre une fonction de test et réparation des systèmes de fichiers des LUNs vidéo. Si vous avez des erreurs sur un volume de stockage, vous pouvez tenter de le réparer.

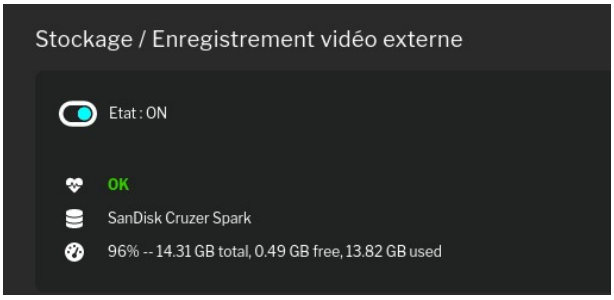
Cette réparation peut se faire à chaud si le LUN n'est pas utilisé en enregistrement (système en fonctionnement), mais il est conseillé de placer le serveur en maintenance pour cette opération. La réparation d'un système de fichier peut être très longue et gourmande en ressources, surtout avec des volumes de stockage importants.

7.3 Enregistrement vidéo externe

VXCORE dispose d'une fonctionnalité d'enregistrement vidéo externe sur périphérique USB amovible.

Cette fonctionnalité permet d'ajouter un deuxième volume de stockage supplémentaire amovible, en plus stockage vidéo interne statique du système. Le système l'utilisera en parallèle du stockage vidéo principal, afin d'y enregistrer les caméras et les photos des déclenchements d'alarmes.

Attention : cette fonctionnalité est un module optionnel nécessitant une mise à jour de la licence. Contactez votre distributeur pour plus de précisions.



Ce stockage vidéo sera géré de manière indépendant, et disposera de sa propre rétention d'enregistrement vidéo, directement lié à la capacité du périphérique configuré (attention : tout l'espace disque sera utilisé).

Il disposera de sa propre supervision d'erreur, et comme avec le stockage vidéo interne, le système pourra envoyer des alertes email en cas de problème ou de dysfonctionnement du périphérique de stockage.

Lorsqu'un périphérique de stockage externe est activé, toutes les caméras et les flux vidéo y seront automatiquement enregistrés de manière permanente (24h/24), ainsi que toutes les photos d'alarmes (on ne peut pas choisir quelles caméras seront enregistrées ou non, ou le mode d'enregistrement vidéo).

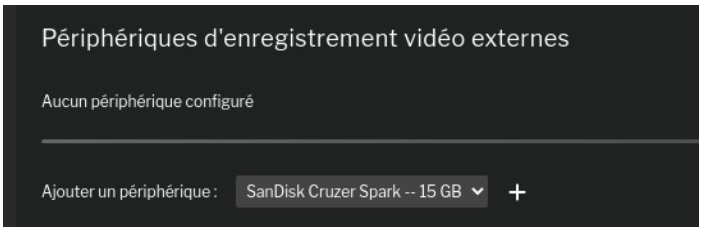
Toute nouvelle caméra ou alarme configurée dans le système sera donc automatiquement enregistrée sur le stockage vidéo externe.

Ce périphérique de stockage pourra ensuite être totalement déconnecté du système (proprement, éviter les arrachages à chaud) pour ensuite être consulté sur un PC avec le lecteur vidéo intégré du logiciel VXCORE-ACCESS ou VXPLAYER. Consultez la documentation utilisateur pour plus de précisions.

Par mesure de sécurité, tout nouveau périphérique USB doit d'abord être « tagué » par le système pour ensuite être utilisé comme volume de stockage vidéo externe. Cette procédure assurera qu'aucun autre périphérique USB connecté par erreur ne sera effacé par le système.

Avant d'ajouter ou supprimer des périphériques de stockage externes, vous devez désactiver la fonctionnalité en appuyant sur le bouton « OFF » de l'interface.

Pour taguer un nouveau périphérique USB, connectez le au système et cliquez sur l'onglet « Enregistrement vidéo externe » : il devrait apparaître dans la liste des périphériques disponibles. Cliquez ensuite sur le bouton « ajouter » situé à droite pour qu'il soit utilisé par le système pour l'enregistrement vidéo.

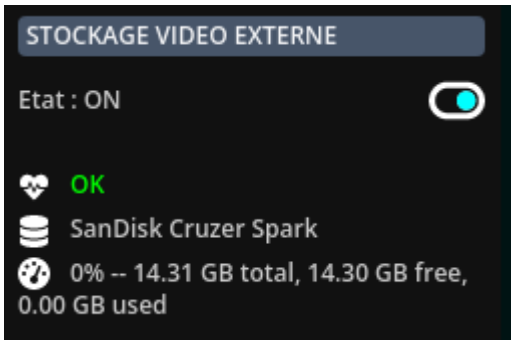


Pour supprimer un périphérique USB tagué, cliquez simplement sur le bouton « suppression » situé à droite.

Important : tout ajout ou suppression de périphérique USB pour l'enregistrement vidéo externe implique un formatage complet du périphérique (suppression de toutes les données).

Remarque : un périphérique USB tagué pour l'enregistrement vidéo externe ne sera plus visible ailleurs dans le système, comme dans les exportations vidéo ou les sauvegardes sur périphériques USB (vous devrez d'abord le supprimer pour le « dé-taguer »).

Lorsqu'un périphérique de stockage externe est activé, vous pourrez le voir dans le tableau de bord du système.



L'interface dispose d'un bouton ON/OFF permettant de désactiver l'enregistrement vidéo et de démonter proprement le périphérique de stockage USB (avant de le retirer ou de le remplacer par un autre).

Important : si vous ne désactivez pas le stockage vidéo externe avant de le déconnecter, vous risquez d'endommager irrémédiablement le système de fichier et donc de perdre toutes vos données vidéo.

Lorsque l'enregistrement vidéo est en état « OFF » (et que vous disposez de la permission dans votre compte utilisateur), vous trouverez également un bouton qui vous permettra de formater le volume de stockage externe (suppression totale des données).

Un reformatage est utile lorsque l'on souhaite réinitialiser proprement un volume ayant rencontré des erreurs au fonctionnement.

7.4 Maintenance du RAID hardware

VXCORE dispose d'une interface spécifique pour la maintenance du RAID hardware, située dans l'espace d'administration/stockage.

Le système supervise automatiquement les contrôleurs RAID hardware : en cas de problème, des alertes email seront envoyées aux administrateurs "root" et un message d'erreur sera affiché dans l'interface du système (casse disque dur, reconstruction des volumes, ...).

Comme expliqué dans la documentation d'installation/intégration VXCORE, les seuls constructeur de carte RAID entièrement compatibles avec Linux Debian et dont les utilitaires de maintenance ont été intégrés dans VXCORE sont BROADCOM/MEGARAID (anciennement LSI) et DELL/PERC.

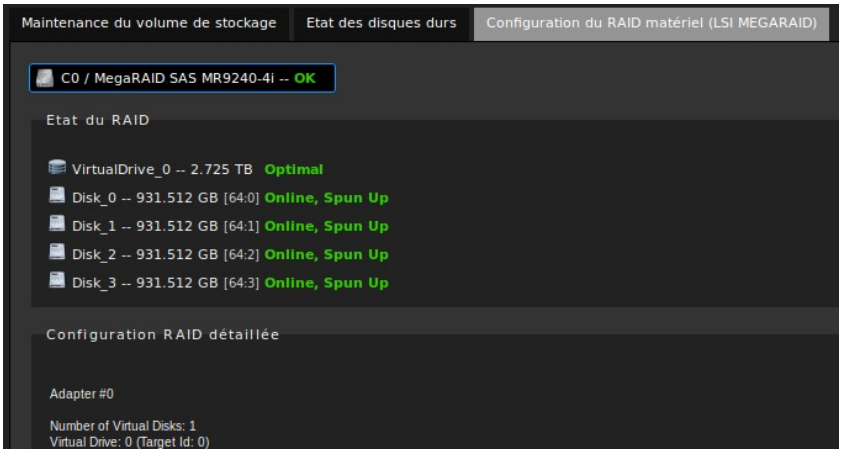
Le système dispose d'interfaces bien distinctes pour la supervision du RAID Hardware : une pour chaque constructeur.

7.4.1 RAID hardware BROADCOM/MEGARAID et DELL/PERC

Si votre serveur intègre une ou plusieurs cartes contrôleurs BROADCOM/MEGARAID ou DELL/PERC, le système affichera automatiquement les menus pour afficher l'état détaillé de chaque contrôleur RAID.

L'interface de gestion du RAID hardware vous apportera les fonctionnalités suivantes :

- Visionner l'état de fonctionnement de tous les volumes RAID répartis sur l'ensemble des cartes contrôleurs
- Détecter et ajouter un disque de secours (spare) : ce disque sera automatiquement utilisé par le contrôleur pour remplacer un disque défectueux sur l'un de ces volumes RAID



Interface de maintenance du RAID hardware

Remarque : La gestion des contrôleurs RAID Hardware a été intégré dans un objectif de supervision des erreurs. Si vous souhaitez activer ou utiliser des fonctionnalités avancés des contrôleurs RAID, vous devez utiliser les outils fourni par le constructeur (Interface, BIOS, ...)

7.4.2 RAID hardware 3WARE (obsolète)

Si votre serveur intègre une ou plusieurs cartes contrôleurs 3WARE, le système affichera automatiquement le menu pour accéder a l'ancienne interface de gestion.

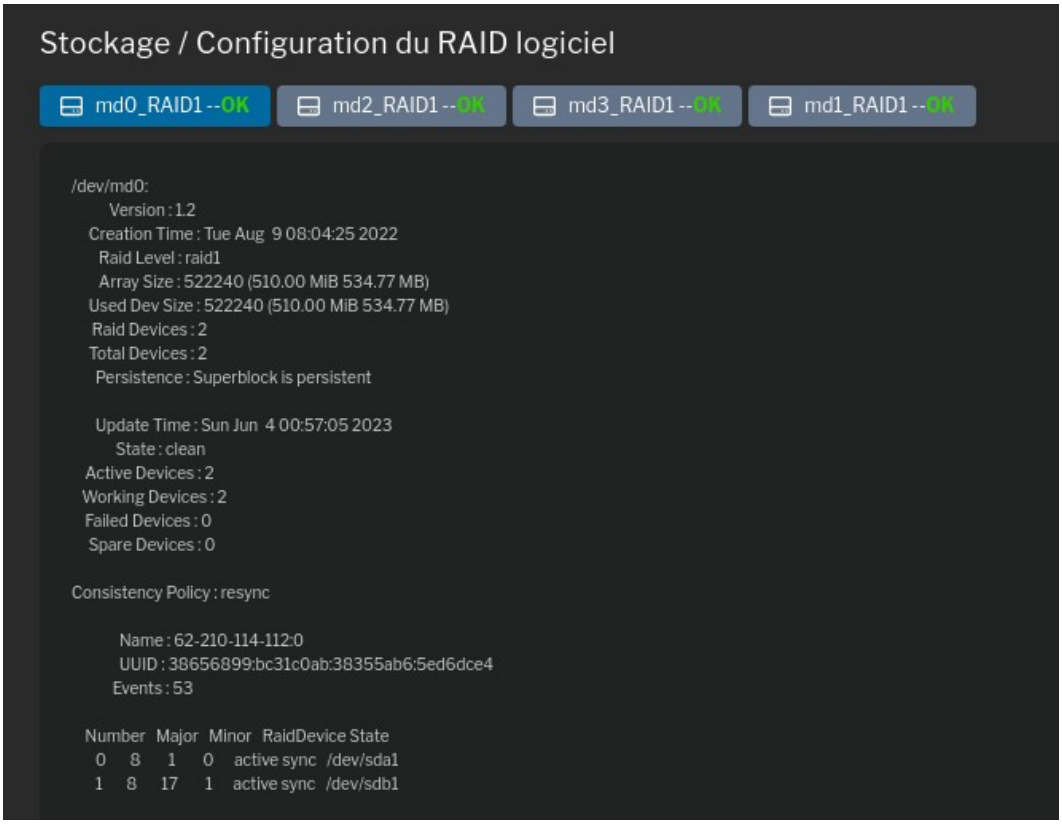
L'interface de gestion du RAID hardware 3WARE vous apportera les fonctionnalités suivantes :

- Visionner l'état de fonctionnement de tous les volumes RAID répartis sur l'ensemble des cartes contrôleurs
- Détecter et ajouter un disque de secours (spare) : ce disque sera automatiquement utilisé par le contrôleur pour remplacer un disque défectueux sur l'un de ces volumes RAID
- Lancer un test de la batterie (BBU) (Battery Backup Unit) : Batterie connectée en option sur un contrôleur RAID, utilisée pour conserver les données présentes dans la mémoire cache en cas de coupure de courant

Important : les cartes 3WARE ne sont plus supportées et plus maintenues dans VXCORE.

7.5 Maintenance du RAID software

VXCORE dispose d'une interface de supervision du RAID software Linux, située dans l'espace d'administration/stockage. Elle permet le monitoring des erreurs comme avec le RAID hardware.



Remarque : cette fonctionnalité ne vous permettra pas de créer des périphériques RAID software directement, elle vous permettra juste de superviser des volumes créés avec via un autre système Linux.

Par exemple, il est tout à fait possible de configurer un volume multi-voie (multipath I/O) avec une autre distribution Linux et de le configurer en LUN vidéo dans VXCORE . Un tel périphérique

permet de profiter du matériel prenant en charge plusieurs voies d'E/S vers des LUNs individuels, afin de garantir une disponibilité continue des données dans le cas d'un échec matériel ou d'une saturation de voie de communication.

VXCORE vous permettra de configurer tous les périphériques de type "/dev/md" en LUN vidéo. Par contre, l'utilisation de ce type de périphérique étant réservé aux administrateurs systèmes Linux chevronnées, nous n'assurerons aucun support sur l'utilisation, la configuration ou la maintenance de ceux-ci.

7.6 Stockage iSCSI

Le protocole iSCSI (Internet Small Computer System Interface) est un protocole de stockage en réseau fiable, performant et peu couteux, permettant de déporter le stockage des données via le réseau IP.

VXCORE intègre un client iSCSI qui permettra d'attacher des baies de stockage externes en réseau afin de créer des infrastructures performantes pour des volumes importants de données.

Il sera également possible d'utiliser une partie d'une baie de stockage existante afin de mutualiser les couts et la maintenance.

Pour ajouter un volume de stockage en iSCSI, vous devez d'abord configurer une cible dans le système (iSCSI target). Vous devez également disposer d'une baie ou d'un serveur de stockage correctement configuré et accessible sur le réseau.

Cliquez sur le bouton «Rechercher» et saisissez l'adresse IP de votre baie de stockage iSCSI. Le système lancera une requête de « scan » afin de lister les cibles iSCSI disponibles sur la baie de stockage.

Cliquez ensuite sur le bouton « Ajouter » situé à droite d'une cible iSCSI pour l'ajouter au système.

Vous pourrez vérifier dans l'interface le status de la cible : une session iSCSI sera automatiquement créée pour le volume de stockage. Le nouveau périphérique de stockage sera alors visible par le système, comme n'importe quel autre disque dur local. Il vous suffira de le choisir pour le formater et l'ajouter dans le volume de stockage vidéo.

Remarque : VXCORE ne gère pas l'authentification des cibles iSCSI, elles doivent être configurées en mode anonyme dans la baie de stockage. Ce protocole est recommandé uniquement en réseau local dédié.

8 Réglages et options systèmes

Cette interface regroupe tous les réglages possibles de la configuration globale du système.

8.1 Options systèmes et sécurité

Cette section vous permettra de régler différents paramètres du système.

8.1.1 Options système

- **Sauvegarde automatique des paramètres systèmes** (activé par défaut)

  VXCORE dispose d'une fonctionnalité de sauvegarde automatique et journalière vers tous les périphériques de backup ou le serveur FTP configuré (tous les jours à minuit).

- **Prévenir de l'expiration de la maintenance logicielle (SMA)** (activé par défaut)

  La maintenance logicielle doit être renouvelée régulièrement pour assurer un suivi constant des mises à jour de sécurité du système. Le système indiquera automatiquement un message d'avertissement précédant 3 mois avant la date d'expiration. Vous pouvez désactiver ce message si vous disposez d'un suivi SMA en gestion de parc.

- **Mises à jour systèmes automatiques** (activé par défaut)

  Le système dispose d'une fonctionnalité de mise à jour automatique en ligne, permettant de corriger les éventuelles failles de sécurité ou d'ajouter des fonctionnalités (tous les jours à minuit).
  Vous pouvez désactiver cette fonctionnalité (bien que cela ne soit pas recommandé).

- **Langue par défaut**

  VXCORE est développé et maintenu en Français et Anglais. Il est possible de changer la langue par défaut du système, principalement pour le login du système et dans la création des comptes utilisateurs.

8.1.2 Options de l'interface

Ces options permettent de personnaliser l'interface de la solution pour adapter son usage, spécifiquement pour les grandes installations ou les centres de sécurité.

- **Recherche des caméras par identifiant/numéro** (désactivé par défaut)

  Cette option permet de rechercher directement les caméras par leur identifiant numérique (exemple : 44). Dans les grands sites, il est quelque fois plus utile d'identifier par leurs numéros que par un nom complexe. Cette option permet d'inclure l'ID caméra dans tous les champs de recherche du serveur. Cette option ne devrait pas être activée dans un serveur ou une configuration mutualisée.

- **Archives partagées pour tous les utilisateurs** (désactivé par défaut)

  En mode normal, les archives et les données exportées sont propres à chaque utilisateur. Cette option permet d'activer un mode collaboratif ou tous les utilisateurs pourront gérer toutes les archives du système ensemble (cas de plusieurs opérateurs vidéo dans un centre de sécurité par exemple).

- **Écrans vidéo partagés pour tous les utilisateurs** (désactivé par défaut)

  En mode normal, les écrans vidéo et les murs d'images sont personnalisables pour chaque utilisateur. Cette option permet d'activer un mode collaboratif ou tous les utilisateurs pourront gérer ensemble le mur d'image (profils, personnalisation, rondes, etc).

8.1.3 Sécurité

Ces options permettent de régler plusieurs paramètres liés à la sécurité du système. Si vous activez ou désactivez un point sensible, le système vous l'indiquera par un message d'avertissement.

- **Force des mots de passes utilisateurs** (mot de passe fort par défaut)

  Option permettant de choisir la stratégie de mot de passe du système : soit fort, soit faible. La stratégie de mot de passe fort est fortement recommandée, notamment pour les systèmes accessibles à distance (basée sur les recommandations de l'ANSSI Agence nationale de la sécurité des systèmes d'informations).

  Mot de passe fort : 12 caractères minimum : au moins une lettre minuscule, au moins une lettre majuscule, au moins un chiffre, au moins un caractère spécial

  Mot de passe faible : 8 caractères minimum

- **Masquer l'identité/version du système sur la page de connexion** (activé par défaut)

  Cette option permet d'anonymiser totalement le système, notamment sur la page de connexion accessible de manière publique (sans authentification). Cela permet d'éviter les recherches automatiques de systèmes vidéo sur Internet par des robots ou des scripts malveillants, et des tentatives de connexions non désirées.

- **Activer l'authentification sécurisée (HTTPS)** (activé par défaut)

  Cette option permet de forcer les connexions utilisateurs via le protocole HTTPS uniquement. Le protocole HTTP pourra être activé via le firewall, mais aucune connexion utilisateur ne sera possible via la page de login. Seule la connexion HTTPS permettra de garantir la sécurité des échanges des identifiants et du mot de passe entre le serveur et le logiciel de visualisation.

- **Activer le contrôle d'accès applicatif** (activé par défaut)

  Le contrôle d'accès applicatif permet de sécuriser toutes les connexions au systèmes vidéo avec des signatures applicatives fortes. Seules les applications signées officielles pourront être utilisées pour la consultation du système, ce qui sécurisera tous les accès externes ou internes (par exemple : tous les navigateurs Web publics seront automatiquement bloqués).

  Important : vous ne devriez jamais désactiver cette option (le système pourrait être vulnérable à des attaques automatisées par des robots ou des scripts malveillants de hackeurs).

- **Connexion utilisateurs uniquement en réseau local** (désactivé par défaut)

  Lorsque cette option est activé, le système va filtrer toutes les demandes de connexion et exclure toutes les requêtes non « locales ». Une connexion sera considérée comme locale uniquement si elle provient d'une plage d'adresse IP privée (10.0.0.0/8 – 172.16.0.0/12 - 192.168.0.0/16).

8.1.4 Supervision du système

VXCORE intègre plusieurs modules de supervision pour contrôler l'état de fonctionnement du système. Vous pouvez les désactiver si vous n'en avez pas l'utilité ou si vous rencontrez des problèmes.

- **Supervision des disques durs (S.M.A.R.T.)** (activé par défaut)

  VXCORE intègre un client S.M.A.R.T. et supervisera automatiquement tous les disques durs compatibles, afin d'alerter l'administrateur en cas de défaillance imminente. Vous pouvez désactiver cette option si vous rencontrez des erreurs de supervision liés à la compatibilité de vos disques durs. Les tests des disques durs seront fait au démarrage du serveur et tous les jours à Minuit

- **Supervision du RAID matériel** (activé par défaut)

  VXCORE supervise automatiquement l'état des contrôleurs RAID Hardware compatibles, afin d'alerter l'administrateur en cas de défaillance.

- **Supervision de l'horloge matérielle** (activé par défaut)

  Le système indiquera s'il rencontre un problème pour sauvegarder ou restaurer l'horloge système dans l'horloge matérielle de la carte mère ou du serveur (RTC). Désactivez cette option si votre serveur ou architecture matérielle ne dispose pas d'horloge matérielle (exemple : raspberry PI).

  Remarque : cette option ne permet pas d'indiquer un problème de pile ou de batterie de l'horloge matérielle.

- **Supervision de l'enregistrement réel des caméras** (désactivé par défaut)

  VXCORE peut superviser l'enregistrement réel des caméras. Le système déclenchera une erreur et alertera les administrateurs si une ou plusieurs caméras programmées en enregistrement ne sont plus enregistrées physiquement (Exemple : 4 caméras programmées dans l'agenda, mais seulement 3 enregistrées réellement).

  Les erreurs peuvent être multiples : déconnexion ou plantage de la caméra, perte du flux vidéo, engorgement réseau, ...

- **Supervision des erreurs critiques du système Linux** (activé par défaut)

  VXCORE intègre un système de monitoring des erreurs remontées par le noyau Linux (manque de mémoire physique, incompatibilité de périphérique ou de driver, ...).

  Ne désactivez cette option que si les erreurs remontées par le noyau Linux sont bénignes, comme dans le cas de message d'informations et non d'erreurs réelles (le noyau informe, mais corrige automatiquement en désactivant un driver, par exemple).

- **Supervision de l'analyse vidéo** (activé par défaut)

  VXCORE intègre un système de monitoring des erreurs de l'analyse vidéo, notamment si aucun flux vidéo n'est disponible pour lancer l'analyse. Ces erreurs sont visibles dans le tableau de bord détaillé des caméras avec le message « video analysis ~ Error : no video stream available »

  Ces erreurs indiquent que l'analyse vidéo n'est pas fonctionnelle et donc indirectement, de tous les problèmes qui peuvent en découler (en fonction de la configuration système) : aucun déclenchements d'alarmes et donc agents de sécurité ou scénarios d'actions non fonctionnels, pas de recherche intelligente, pas d'enregistrement vidéo sur alarme, etc

8.1.5 Limites de stockage vidéo

Ces options permettent de régler la rétention des différentes données du système.

- **Enregistrement des caméras** (30 jours par défaut)

  Permet de régler le quota de stockage maximal pour l'enregistrement vidéo des caméras.

  Par défaut, la rétention des enregistrements vidéo est fixée à 30 jours.

- **Journal des alarmes** (automatique par défaut)

  Permet de régler le quota de stockage maximal du journal des alarmes et des photos d'alarmes.

  Par défaut, la rétention du journal des alarmes est automatiquement réglée sur la rétention des caméras. Par exemple : si votre caméra ne dispose que de 5 jours d'enregistrements vidéo, alors le journal des alarmes associé sera aussi de 5 jours.

- **Archives vidéo exportées** (illimité par défaut)

  Permet de régler la rétention des fichiers exportées des utilisateurs. Le système supprimera automatiquement toute archive ou fichier vidéo exporté dont la date sera dépassée0

  Par défaut, le stockage des données exportées des utilisateurs n'est pas limitée dans le temps.

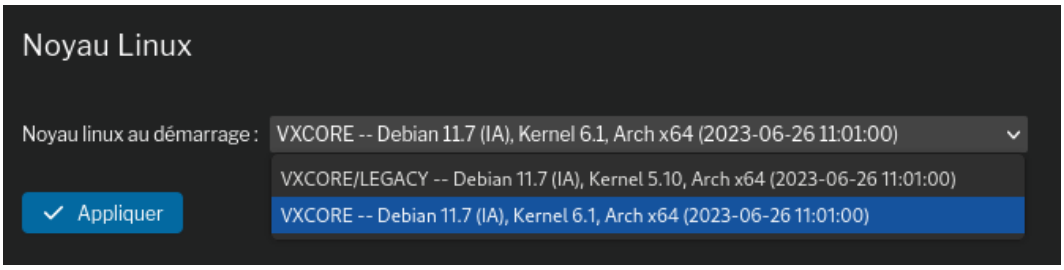
- **Rétention des journaux systèmes** (30 jours par défaut)

  Permet de régler de régler la rétention totale de tous les journaux du système (connexions utilisateurs, notifications, configuration, système ...)

  Par défaut, la rétention des journaux systèmes est fixée à 30 jours.

8.1.6 Noyau Linux

Selon la version de l'OS VXCORE utilisée, le menu de choix du Kernel Linux peut s'afficher.



Il permettra de choisir le noyau Linux qui sera utilisé au démarrage du système : VXCORE (DEFAULT) ou VXCORE/LEGACY.

Le kernel VXCORE/LEGACY est un noyau Linux légèrement plus ancien, avec moins de drivers et donc de compatibilité matérielle.

Il est quelque fois nécessaire de le choisir si votre serveur rencontre des soucis de compatibilité hardware ou des plantages inexplicables de type «FREEZE» ou « KERNEL PANIC » (blocage complet de l'OS lié à de la corruption mémoire, mauvaises instructions cpu ou incompatibilité matérielle).

8.2 Réglages options vidéo

Cette section vous permettra de régler différents paramètres du système vidéo.

8.2.1 Options vidéo

- **Utiliser le service de streaming en réseau local** (activé par défaut)

  VXCORE intègre un service spécifique pour la diffusion des flux vidéo pour les sessions utilisateurs et/ou les murs d'images (port 79 et port 73). Ce service a été conçu pour ne pas faire transiter la vidéo dans les services WEB du système (le service est limité en nombre de connexions persistantes). Ce service permettra de diffuser un nombre illimité de flux vidéo sur le réseau local, sans saturer l'utilisation de l'interface du système (hors ressources serveur).

  Ne désactivez cette option que si vous rencontrez des problèmes d'accès aux flux vidéo sur le réseau local.

- **Autoriser l'exportation/encodage vidéo sur le serveur** (activé par défaut)

  La fonctionnalité d'exportation vidéo intégrée permet de créer des séquences vidéo directement dans l'espace exportation du serveur (et en fonction des archives utilisateurs). Dans certains cas, et avec un dimensionnement trop léger du serveur en ressources de calculs, ce processus peut s'avérer extrêmement gourmand à cause de l'encodage vidéo. Cette option vous permettra de désactiver la fonctionnalité, afin que les utilisateurs utilisent une autre méthode pour exporter les données vidéo (exemple : téléchargement/encodage direct sur le PC d'exploitation).

- **Autoriser l'exportation/extraction des données audio** (désactivé par défaut)

  Cette option permettra d'inclure automatiquement les éventuelles données audio enregistrées dans les fichiers vidéo qui seront exportés par le serveur. Dans certains cas, et selon la législation en vigueur ou sera installé le système vidéo, les extractions audio ne sont pas autorisées.

- **Autoriser l'exportation des données vidéo sur des périphériques externes USB** (désactivé par défaut)

  VXCORE dispose d'une fonctionnalité de copie automatique ou manuelle des fichiers exportés sur des périphériques USB connectés directement sur le serveur (clé USB ou disque externe USB). Si cette option est activée et que l'utilisateur dispose du droit d'accès spécifique, le système détectera et affichera tous les périphériques USB dans l'interface d'exportation du système. L'utilisateur sera alors capable d'y copier des fichiers exportés de manière sécurisé (contrôle automatique de l'intégrité des fichiers).

- **Autoriser l'exportation des données vidéo par le réseau** (désactivé par défaut)

  VXCORE dispose d'une fonctionnalité d'extraction des données vidéo brutes qui permet une exportation instantanée de l'ensemble des données vidéo (tous les flux disponibles) sans aucune perte de qualité (pas de transcodage vidéo), ainsi que toutes les photos d'alarmes associées.

  Cette option doit être activée pour permettre aux utilisateurs de l'utiliser (chaque utilisateur devra aussi disposer de la permission dans son compte).

- **Autoriser la suppression de données vidéo ou alarmes** (désactivé par défaut)

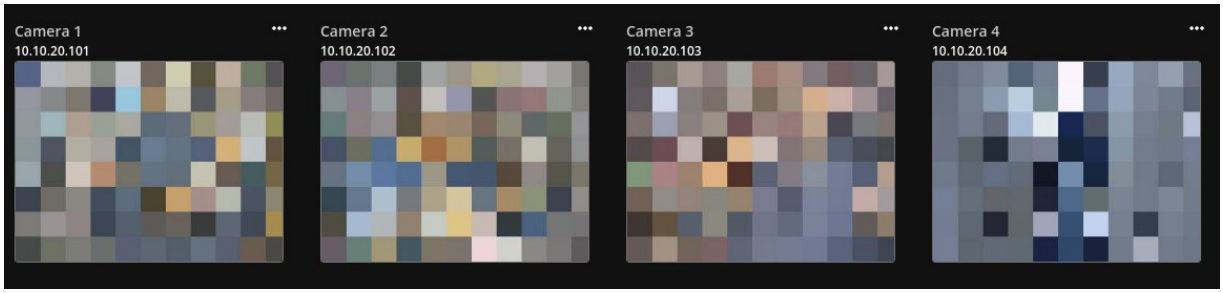
  Cette option permet d'activer la fonctionnalité de suppression ciblée des données vidéo/alarmes stockées sur le serveur vidéo (chaque utilisateur devra aussi disposer de la permission dans son compte).

- **Autoriser l'armement/désarmement des alarmes du système** (désactivé par défaut)

  Cette option permet d'activer la fonctionnalité d'armement/désarmement de toutes les alarmes du système. Via un contrôle API externe, il est possible de contrôler les alarmes pour les désactiver automatiquement afin qu'elle ne génèrent plus de notifications ou encore d'actions avec les agents de sécurité. Par exemple, ce contrôle API externe peut être fait depuis une centrale d'alarme ou un autre système de contrôle d'accès.

- **Activé la confidentialité du compte root** (désactivé par défaut)

  Cette option permet d'activer le mode de confidentialité du compte root : il ne pourra plus voir aucune données vidéo (vignettes caméras/alarmes brouillées, flux vidéo live/playback désactivés, exportations vidéo bloquées, etc).



  Selon la législation en vigueur ou sera installé le système vidéo, l'admin système root ne doit quelque fois pas pouvoir consulter les données vidéo (confidentialité des images).

  Attention : si vous activez cette option, vous ne pourrez plus la désactiver via l'interface (option à sens unique). Il sera nécessaire de réinstaller complétement le serveur.

8.2.2 Enregistrement vidéo automatique

VXCORE dispose d'une option globale permettant de définir le mode d'enregistrement vidéo par défaut de l'ensemble des caméras du système (sans devoir configurer un évènement dans l'agenda). Cela signifie que toute nouvelle caméra connectée et correctement configurée dans le système sera automatiquement enregistrée.

- **Désactivé**

  Lorsque l'option est désactivée, le système n'enregistrera pas les caméras automatiquement. Il sera nécessaire de programmer un évènement dans l'agenda système pour activer l'enregistrement vidéo.

- **Enregistrement vidéo permanent** (activé par défaut)

  Lorsque ce mode est activé, les caméras seront enregistrées de manière permanente dans le système (24h/24 et 7j/7), quelque soit l'état des alarmes ou de la détection intelligente.

- **Enregistrement vidéo sur alarme (sécurisé)**

  Ce mode d'enregistrement permet d'activer un enregistrement vidéo sur alarme et/ou sur détection d'activité de manière sécurisé (analyse vidéo et/ou détection de mouvement). Toutes les caméras seront enregistrées en continu, mais le système procédera à une

suppression intelligente des données, en fonction des états d'alarmes et de la détection intelligente (si aucun évènement associé pendant la période). La suppression des données ne sera effective qu'après la période d'enregistrement sécurisée du système (réglable).

- **Enregistrement vidéo sur alarme (en mémoire cache)**

  Ce mode d'enregistrement vidéo permet d'activer un enregistrement vidéo sur alarme avec une optimisation importante de l'écriture sur les disques durs. Les données vidéo ne seront enregistrées que dans le cas du déclenchement d'un évènement associé à la caméra (alarme / détection de mouvement / analyse vidéo). Les données vidéo seront stockées environ 10 secondes dans la mémoire vive du serveur avant de conserver une période pré-alarme en cas d'activation de l'enregistrement vidéo.

Remarque : lorsqu'un enregistrement vidéo sera activé sur alarme/détection, le système fonctionnera de manière inversé ; c'est a dire que l'enregistrement vidéo sera continu, mais que les données ne seront supprimées que si aucun événement n'est associé (pas d'activité dans l'analyse vidéo et aucun déclenchement d'alarme).

Cela signifie que s'il y a un soucis quelconque avec l'analyse vidéo (erreur flux vidéo, problème décodage des images, etc) ou les alarmes internes ou même externes (exemple : caméra IA déconnectée) : les enregistrements vidéo seront continu et qu'il n'y aura pas de suppression automatique.

8.2.3 Enregistrement vidéo sur alarme

Ces options modifient directement la stratégie de stockage des enregistrements vidéo sur alarme.

- **Enregistrement pré alarme**

  Seulement pour l'enregistrement sur alarme : permet de régler la période pré-enregistrement des caméras. Cette période correspond à la rétention forcée des enregistrements vidéo avant le déclenchement d'une alarme. La période post-enregistrement est directement liée aux alarmes et à la détection d'activité : tant qu'au moins une alarme sera active, l'enregistrement vidéo de la caméra sera maintenu (remarque : une caméra peut être associée à plusieurs alarmes). De la même manière : tant que l'analyse vidéo détectera de l'activité, l'enregistrement vidéo de la caméra sera maintenu.

- **Enregistrement sécurisé**

  Seulement pour l'enregistrement sur alarme : permet de régler la période de rétention sécurisée des enregistrements vidéo. Le système ne procédera a aucune suppression de fichiers vidéo dans cette période sécurisée, même si aucune alarme ne s'est déclenchée. La suppression des éventuels enregistrements hors alarme se ferra après cette période.

8.2.4 Séquences vidéo d'alarmes

Cette option permet de définir la durée par défaut des séquences vidéo d'alarmes pour les levées de doute.

8.2.5 Mémoire vidéo (Live)

Les applications PC/Mobile peuvent utiliser le buffering vidéo pour un affichage et une visualisation plus confortable des caméras, afin de préserver la fluidité d'image tout en compensant les latences ou les ralentissements réseau.

Les images seront pré-chargées et conservés en mémoire tampon coté application avant leur affichage, impliquant une petite latence avec le temps réel.

Ces options permettent de régler la taille de la mémoire vidéo des applications en consultation réseau local ou à distance par Internet.

8.2.6 Transcodage vidéo

VXCORE dispose d'une fonctionnalité de transcodage vidéo, permettant de ré-encoder en temps réel les flux vidéo des caméras pour ensuite les transmettre au travers de connexions Internet limitées en bande passante.

Avec cette fonctionnalité, le système créera un 4ème flux vidéo totalement dédié à la consultation à distance, entièrement personnalisable selon les installations, et sans devoir configurer un flux vidéo dédié dans la caméra. Le système supporte 3 formats de transcodage vidéo pour optimiser les ressources du serveur : H.265/H.264/MPEG4.

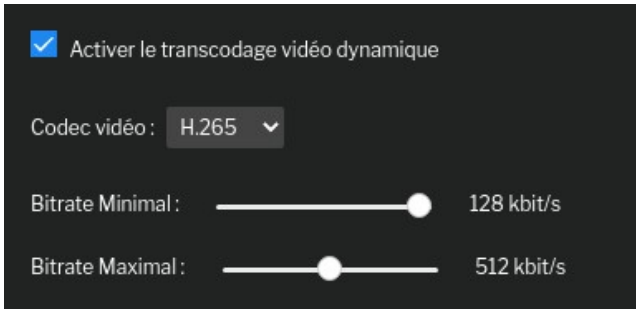
Avec le format de transcodage vidéo H.265 intégré, il est possible de visualiser n'importe quelle caméra malgré des bandes passantes inférieures à 32 kbit/s et sans aucune latence (sur le logiciel PC et/ou les applications mobiles).

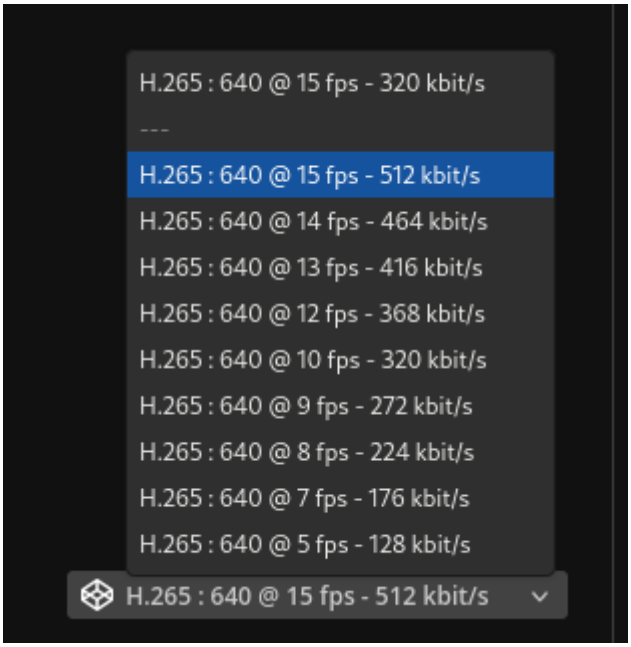
Cette fonctionnalité est compatible avec tous les modèles de caméras du système, et quel que soit leur format vidéo d'origine.

Remarque : selon la configuration de votre système, il est possible que l'encodage vidéo H.265 ne soit pas disponible (ressources CPU limitée du serveur).

La fonctionnalité de transcodage vidéo dynamique permet de rajouter 8 flux vidéo dans un menu déroulant spécifique, qui sera affiché lors de la consultation du flux vidéo transcodé (dans le Live caméra).

Les débits de ces flux vidéo seront automatiquement calculés en fonction des valeurs minimales et maximales que vous aurez configurés.





Cette fonctionnalité sera très utile pour ajuster très précisément l'affichage vidéo lorsque la bande passante réseau est limitée ou fluctuante.

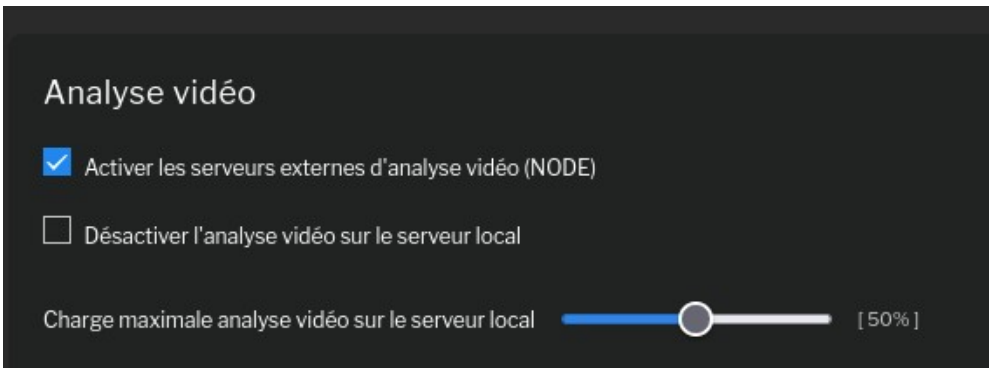
8.2.7 Analyse vidéo

Ces options permettront de régler les paramètres de l'analyse vidéo.

L'analyse vidéo et notamment l'IA consomment énormément de ressources et de puissance de calcul. Il est fortement recommandé d'utiliser une carte GPU intégrée au serveur, ou lorsque cela n'est pas possible, de connecter un ou plusieurs serveurs externes « NODE » sur le réseau pour augmenter les capacités de calcul.

Un serveur externe NODE est un système VXCORE spécifique et allégé qui sera dédié uniquement à l'analyse vidéo. Il sera connecté sur le même réseau que le serveur VXCORE principal pour traiter l'analyse vidéo des caméras et lui envoyer les résultats en temps réel. Selon les configurations, il est possible de raccorder les serveurs NODE au travers du réseau VPN pour créer des configurations multi-sites ou centralisées.

Dans les grandes infrastructures de plusieurs centaines de caméras, il est déconseillé de faire l'analyse vidéo directement sur les serveurs de gestion et d'enregistrement des caméras. Les serveurs externes NODE seront utilisés pour créer un cluster de calcul totalement dédié à l'analyse, ce qui va optimiser les ressources de toute l'installation (tout en étant également compatible avec une configuration Haute Disponibilité).



- **Activer les serveurs externes d'analyse vidéo (NODE)**

  Lorsque cette option est active, le système va utiliser tous les serveurs externes disponibles pour délester et répartir les traitements de l'analyse vidéo des caméras. Cela aura pour effet de soulager directement les ressources du serveur vidéo principal. Les serveurs NODE devront être installés a part et ensuite raccordés au serveur vidéo principal.

- **Désactiver l'analyse vidéo sur le serveur local**

  Lorsque cette option est active, plus aucun processus d'analyse vidéo ne sera lancé sur le serveur vidéo principal. Il sera donc nécessaire d'utiliser des serveurs externes « NODE » pour faire l'analyse vidéo. Cette option est utile pour préserver les ressources du système vidéo principal et ne pas le saturer avec l'analyse vidéo.

- **Charge maximale analyse vidéo sur le serveur local**

  Si vous ne désactivez pas l'analyse vidéo sur le serveur local, et que vous utilisez un ou plusieurs serveurs externes « NODE », vous pouvez régler la répartition de la charge de l'analyse vidéo des caméras.

Par exemple, si vous disposez de 100 caméras et que vous choisissez de ne pas dépasser 50% de charge sur le serveur local : alors 50 processus d'analyses vidéo seront lancés sur le serveur local, et les 50 autres seront lancés sur les serveurs externes.

Remarque : si aucun serveur externe « NODE » n'est connecté au système, alors l'intégralité des processus d'analyse vidéo seront lancés sur le serveur local (100%), quelque soit le réglage de votre répartition. Dès lors qu'un ou plusieurs serveurs externes NODE seront à nouveau connectés, la répartition reviendra automatiquement au réglage défini.

- **Activer le décodage vidéo hardware (GPU)**

  Cette option permettra d'activer le décodage Hardware pour les flux d'analyse vidéo en utilisant le GPU (type Nvidia/Cuda). Cela permettra d'optimiser les ressources CPU du système vidéo (environ 10~25% selon les configurations).

- **Activer l'analyse IA hardware (GPU)**

  Cette option permettra d'activer l'analyse vidéo IA Hardware pour les flux d'analyse vidéo en utilisant le GPU (type NVidia/Cuda). Cela permettra d'optimiser les ressources CPU du système vidéo de manière significative. Il est fortement recommandé d'utiliser un GPU pour les traitements IA, car il est nettement plus optimisé pour ce type de calculs qu'un processeur CPU. Les traitements IA peuvent d'ailleurs faire très facilement « surcharger » les systèmes vidéo qui ne sont pas correctement dimensionnés.

  Remarque : vous ne pouvez pas activer les options de décodage Hardware GPU et d'analyse vidéo IA GPU en même temps.

- **Activer la détection des visages**

  Cette option permettra d'activer le réseau de neurones IA pour faire de la détection de visages. Cet algorithme IA supplémentaire sera lancé en même temps que l'algorithme de reconnaissance des objets (traitement IA parallélisé).

  Lorsque cette option est active, une nouvelle classe « FACE » sera disponible dans les filtres pour faire des recherches intelligentes ou configurer des alarmes sur détection de visages.

  Remarque : attention aux ressources de calculs, il est fortement recommandé d'utiliser un GPU intégré au système ou des serveurs NODE pour l'analyse vidéo IA multiple (détection objets + détection visages)

- **Réseau neuronal de reconnaissance d'objets**

  Cette option permettra de modifier l'algorithme de reconnaissance des objets IA (« simple » par défaut). Le mode optimisé sera nettement plus efficace dans la détection des objets car il utilise un réseau neuronal plus important et mieux entrainé (donc avec moins de faux positifs).

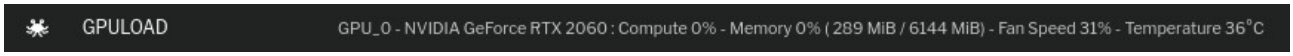
  Le mode optimisé est fortement recommandé dans la configuration de systèmes vidéo pour faire de l'anti-intrusion avec des déclenchements d'alarmes fiables avec IA.

  Remarque : attention aux ressources de calculs, il est fortement recommandé d'utiliser un GPU intégré au système ou des serveurs NODE pour utiliser le réseau neuronal optimisé (environ 30~50% plus consommateur en ressources que le mode simple).

- **Détection des cartes GPU compatibles**

En bas des options de configuration, vous verrez apparaitre la liste des GPU compatibles qui ont été détectés par le système :

Dans le tableau de bord du système, vous verrez également les statistiques d'utilisation du/des GPU installés dans le serveur :



"Compute" correspond à la charge du GPU et "Memory" a l'occupation mémoire du GPU.

Remarque : ces statistiques ne sont pas forcément pertinentes, car elle nécessite une actualisation temps réelle (ce qui ne coïncide pas forcément au moment ou l'IA est utilisée)

- **Statistiques de charge de l'analyse vidéo IA**

Dans le tableau de bord du système, vous verrez une ligne spéciale qui affichera les statistiques de l'analyse vidéo IA : DNN_STATUS_GPU ou DNN_STATUS_CPU (selon le mode d'activation de l'IA).

Ces statistiques permettront de vérifier le dimensionnement ou les réglages de l'analyse vidéo IA :

- dnn_avg_processing : temps de traitement moyen par image en millisecondes (valeur basse = peu de latence)

- dnn_avg_fps_processing : temps de traitement moyen par image en FPS (capacité de calcul en Images/seconde)

- dnn_avg_cameras_processing : moyenne estimée du nombre de caméras en simultané que le système pourra analyser (cette donnée est la plus pertinente pour vérifier le dimensionnement de votre serveur)

- dnn_avg_delay : moyenne du délais de traitement de l'analyse vidéo en secondes (idéalement cette valeur doit rester à zéro, en cas de dépassement de plus de 3 secondes, les images seront droppées pour préserver l’intégrité système)

- dnn_loss_frames : nombre d'images qui ont été droppées de l'analyse vidéo, par manque de ressources

En cas de drop/overload de l'analyse vidéo IA/DNN, vous verrez une ligne spécifique apparaitre dans les journaux systèmes :

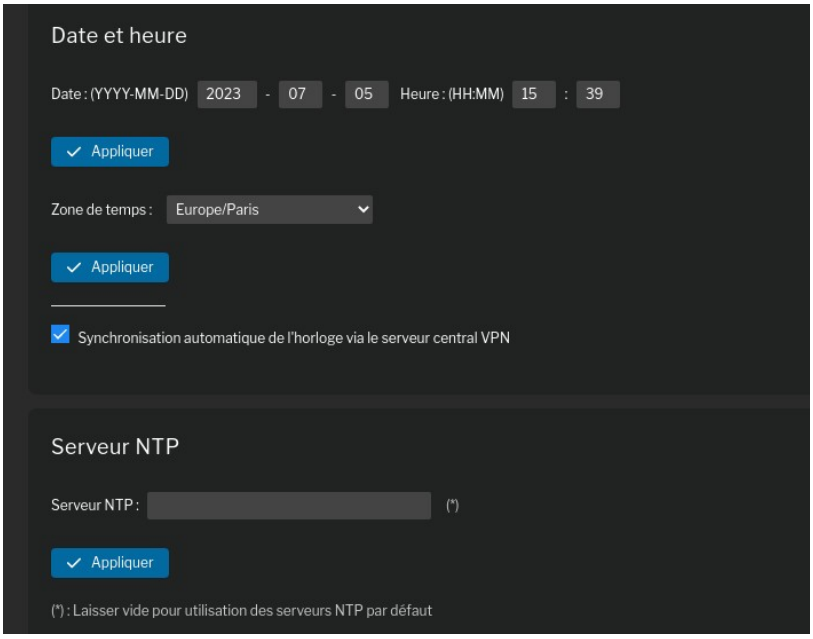
Si votre système remonte trop d'erreurs de ce type, vous pouvez :

- utiliser le réseau neuronal par défaut (et non pas le mode optimisé)
- désactiver la détection de visages
- réduire le nombre de caméras IA ou configurer des zones de masquages plus restrictives
- investir dans un GPU plus performant
- délester l’analyse vidéo IA sur des serveurs externes VXNODE

8.3 Réglage de l'heure système

Le réglage de la date et l'heure du système est très importante dans un système d'enregistrement vidéo. En effet, tous les enregistrements vidéo et tous les évènements d'alarmes seront archivées selon l'horloge interne du système.

Remarque : si vous n'utilisez pas l'overlay vidéo des caméras, vous pouvez d'ailleurs désactiver totalement le timestamp des caméras, il ne sera pas utilisé.



Si le système est connecté sur Internet, l'horloge se mettra automatiquement à jour via le protocole réseau NTP.

Le serveur NTP par défaut est celui de la distribution Linux Debian.

Il vous est possible de configurer un autre serveur NTP, situé sur votre réseau interne par exemple. Pour supprimer le serveur NTP personnalisé, laissez le champ de configuration vide et appliquez la configuration.

Chaque serveur utilise son propre fuseau horaire, selon la zone de la surface terrestre où il sera utilisé. Par défaut le fuseau horaire du système est celui de **Europe/Paris**. Pour changer le fuseau horaire du système, vous devez placer le serveur en maintenance.

Si votre serveur vidéo est raccordé sur un serveur de centralisation, l'horloge sera automatiquement synchronisée.

Attention néanmoins aux serveurs clients situés dans une autre zone de temps, ils seront tous synchronisés à l'heure du serveur central (même en réglant l'heure manuellement). Dans ce cas, vous devez désactiver la synchronisation automatique de l'heure par le serveur central.

VXCORE peut aussi jouer le rôle de relais NTP en répondant aux requêtes des équipements sur le réseau.

Par exemple : chaque caméra peut aller synchroniser son horloge avec celle de VXCORE.

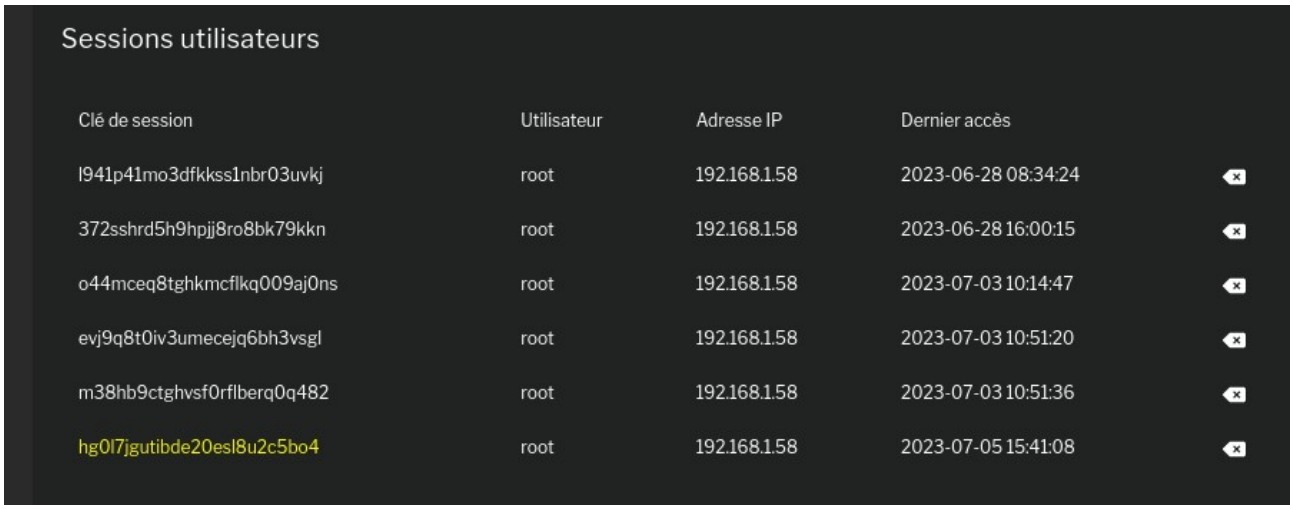
Pour activer le service relais NTP, il suffit d'ouvrir le firewall et le port NTP (uniquement sur le réseau local de préférence).

8.4 Sessions utilisateurs

Pour utiliser le système, chaque utilisateur doit ouvrir une session en s'authentifiant. Cette session est identifiée par une clé unique, qui sera différente à chaque connexion utilisateur.

Une session utilisateur est limitée dans le temps, et l'utilisateur sera automatiquement déconnecté du système en cas d'inactivité prolongée **supérieure à 15 minutes**. L'utilisateur peut mettre fin à sa session manuellement en cliquant sur le bouton "déconnexion/logout" du système.

En tant qu'administrateur "root", vous pouvez visualiser les sessions utilisateurs actives et forcer leur déconnexion en détruisant manuellement leurs sessions.



Le système dispose d'une sécurité bloquant automatiquement l'accès utilisateur en cas de trop d'erreurs d'authentification.

Si un utilisateur persiste avec trop d'erreur de login/mot de passe, l'adresse IP de connexion de l'utilisateur sera automatiquement placée en quarantaine, pendant un temps incompressible (de 2h à 48h selon la configuration, 24h par défaut pour 5 tentatives de connexions).

L'accès au système sera alors impossible, et l'utilisateur devra patienter pendant toute la durée de la quarantaine avant de débloquer l'accès et pouvoir tenter une nouvelle connexion au système.

En tant qu'administrateur "root", vous pouvez débloquer toutes les adresses IP placées en quarantaine, en cliquant sur le bouton adéquat. Les utilisateurs bloqués auront à nouveau accès au système.

9 Extensions

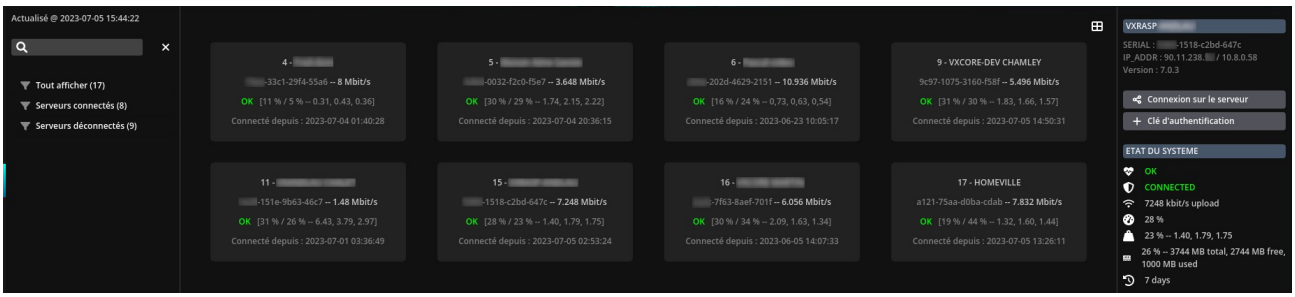
Une extension est un module supplémentaire permettant d'étendre les fonctionnalités du système.

Les extensions disponibles dépendent de la version de l'OS VXCORE installée (serveur d'enregistrement ou de centralisation, etc) et de la configuration de la licence (module complémentaires).

9.1 Centralisation / Accès VPN

Toutes les solutions VXCORE utilisent un mécanisme de centralisation basé sur une technologie VPN dédiée (*Virtual Private Network : interconnexion de réseaux locaux via une technique de "tunnel" sécurisée).*

Les systèmes d'enregistrements vidéo "clients" peuvent être rattachés en VPN sur un serveur vidéo "central" multi-sites.



Le serveur central disposera alors d'un accès quasi transparent aux données des systèmes vidéo clients (caméras, alarmes, enregistrements, ...). Toutes les données pourront être consultées via l'interface unique du serveur central, en utilisant des connexions chiffrées et optimisées (réactivité variable en fonction de la bande passante entre le PC utilisateur / le serveur central et le système vidéo client).

- **Système vidéo client** (client VPN)
  Système vidéo qui se raccordera automatiquement sur un serveur central
- **Serveur vidéo central** (serveur VPN)
  Serveur central qui centralisera toutes les données des systèmes vidéo clients

Cette technique a été conçue pour interconnecter de manière sécurisée des systèmes vidéo "distants" via des accès Internet mobiles (type 3G/4G) et/ou fixes (type ADSL/Fibre). La connexion Internet coté client ne nécessite aucune configuration spécifique du routeur (ouverture de ports) et pas d'adresse IP fixe : la connexion entrante reste donc "fermée" et sécurisée.

Tous les systèmes vidéo clients se connecteront automatiquement au serveur central de manière automatique (connexion VPN automatique et persistante, dès que la connexion Internet est active).

La connexion VPN est sécurisée via les protocoles SSL/TLS (chiffrage AES 256) et utilise un mécanisme de certificats partagés (clés 2048 bits) avec double authentification et signature numérique pour assurer une authentification robuste : aucun client non déclaré ne pourra se connecter à un serveur central.

Le mécanisme de centralisation utilise deux ports sur le serveur central : le port **443/HTTPS** pour le contrôle/heartbeat de la connexion et le port **1194/VPN** pour le tunnel de communication. Ces deux ports utilisent des communications chiffrées.

Cette technologie de centralisation est aussi utilisée pour concevoir d'importantes architectures vidéo en réseau local : un serveur central sera utilisé pour communiquer et fédérer plusieurs systèmes vidéo (et chaque système vidéo enregistrera son propre réseau dédié de caméras).

Ce modèle d'architecture distribuée permettra d'optimiser les ressources afin d'installer des infrastructures avec plusieurs milliers de caméras :

- **Systèmes vidéo clients**
  Gestion et enregistrements des caméras, analyse vidéo, gestion des alarmes et des évènements, stockage des enregistrements vidéo
- **Serveur vidéo central**
  Centralisation des données, gestion des utilisateurs et des permissions, centralisation des évènements, recherches intelligentes multi-sites, synchronisation/backup des enregistrements vidéo sur stockage vidéo secondaire

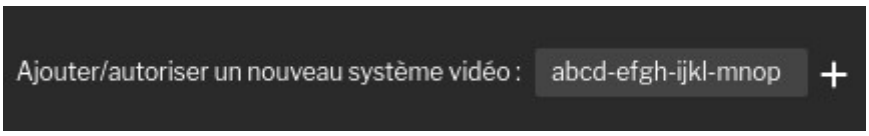
Dans ce modèle d'architecture distribué réseau local, il est possible d'activer des options spécifiques qui éviteront de faire transiter les flux vidéo par le serveur central.

9.1.1 Licences et domaines VPN

L'utilisation de la centralisation nécessite une licence supplémentaire dans chaque système vidéo client.

La licence client VPN permettra au système vidéo de se connecter sur n'importe quel serveur central, sans limitation de durée.

Pour autoriser les nouvelles connexions de systèmes vidéo clients, il sera nécessaire d'activer les accès sur le serveur central, soit pour tous les nouveaux clients, soit en pré-enregistrant le numéro de série du système vidéo.



Afin de sécuriser les connexions VPN, il est possible de spécifier un domaine VPN pour les systèmes vidéo clients et les serveurs de centralisation (paramètre supplémentaire directement dans la licence). Un domaine VPN assurera une sécurité supplémentaire : seuls les systèmes/serveurs vidéo du même domaine pourront communiquer ensemble.

Par exemple : un système vidéo du domaine A ne pourra pas se connecter sur un serveur central du domaine B (et inversement).

Il est également possible de sécuriser les applications (PC/Mobile) en incluant le domaine VPN, afin de forcer l'utilisation d'applications signées pour consulter les systèmes/serveurs vidéo.

Par exemple : l'application du domaine A ne pourra pas se connecter sur un système vidéo du domaine C ou encore sur un serveur central du domaine B (et inversement).

Contactez votre distributeur de licence pour étudier les possibilités de sécurité et de cloisonnement VPN de vos systèmes et serveurs vidéo.

9.1.2 Sécurité et compatibilité

Le système de centralisation de VXCORE est en développement permanent afin de garantir une sécurité maximale des échanges entre les systèmes vidéo clients et les serveurs.

VXCORE fonctionne avec une notion de version sur la partie centralisation, ce qui signifie qu'un système vidéo trop ancien ne pourra pas se connecter sur un serveur vidéo central récent. Dans ce cas précis, vous n'aurez pas d'autre moyen que de procéder à une mise à jour de votre système vidéo client.

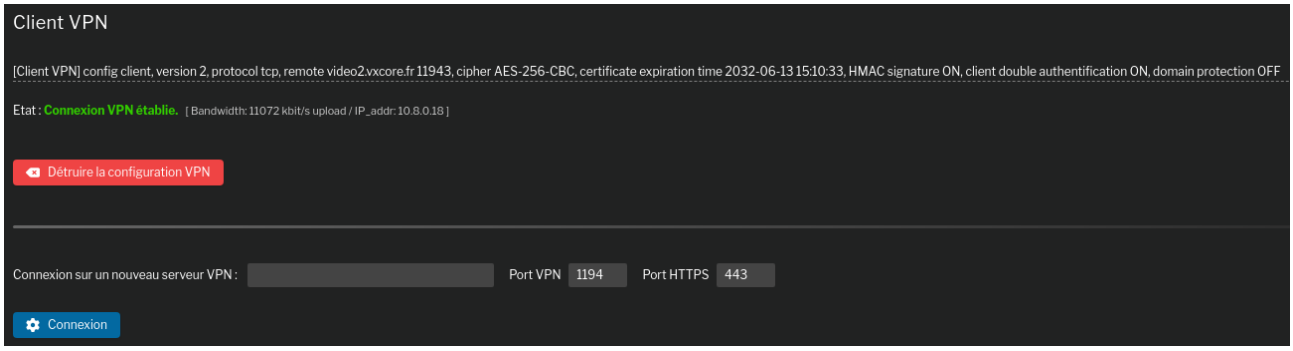
Les dernières versions de la centralisation utilisent un mécanisme de signature hardware+licence, des échanges de certificats entre les clients/serveurs, une triple authentification client et un chiffrage AES-256.

Par ailleurs, les OS/VXCORE trop anciens ne disposeront pas toujours des bonnes versions de librairies Linux pour activer la connectivité VPN (obsolescence des algorithmes de chiffrage/hash).

9.1.3 Configuration système vidéo client

Pour connecter un systèmes vidéo client « NVR » sur un serveur de centralisation, vous devez connaître son adresse IP fixe publique ou son hostname.

Afin de simplifier votre configuration VPN, il est conseillé de bien nommer votre système vidéo, en spécifiant un nom identifiant dans les paramètres réseau (hostname). Sinon c'est le nom du End User déclaré dans la licence qui sera utilisé pour identifier le système vidéo.



Configuration de la connexion Internet "sortante" du système vidéo :

Votre système vidéo client doit disposer d'une connexion Internet "ouverte" vers le serveur central pour télécharger les certificats et se connecter au VPN.

Le serveur client utilisera le port **VPN 1194** (TCP) et le port **HTTPS 443** (TCP) du serveur central. Le port 443 sera utilisé pour le contrôle/heartbeat de la connexion et le port 1174 sera utilisé pour créer le canal de communication chiffré.

Important : ces deux ports sont nécessaires pour assurer le fonctionnement de la centralisation

Si ces deux ports ont été redirigés coté serveur de centralisation et ne sont plus les ports par défaut, vous devez les spécifier lors du raccordement du système vidéo client.

Lors d'une nouvelle connexion sur un serveur central, le système testera d'abord les deux ports pour vérifier qu'ils sont bien accessibles.

Configuration de la connexion Internet "entrante" du système vidéo :

Comme expliqué précédemment, la connexion Internet du système vidéo client pourra rester fermée en trafic entrant.

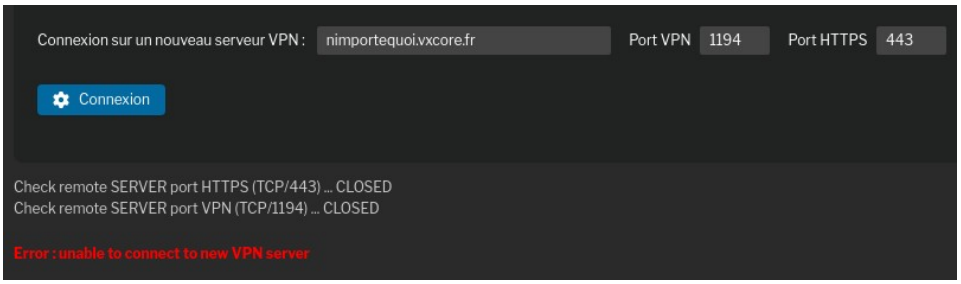
En effet, le mécanisme de centralisation ne nécessite aucune configuration particulière du routeur ou de la Box Internet : **aucun port ne devra être ouvert ou redirigé sur le système vidéo**.

Par ailleurs, l'accès Internet ne nécessite aucune adresse IP fixe, l'adresse IP de la connexion pourra être renouvelée régulièrement.

Changement/migration de serveur central :

Il est également possible de changer de serveur central « à chaud », c'est à dire si le système vidéo client est déjà raccordé sur un serveur central.

Chaque nouvelle tentative de raccordement sur un serveur central va tester toute la chaine de communication avec le nouveau serveur, avant de remplacer la connexion VPN actuelle.

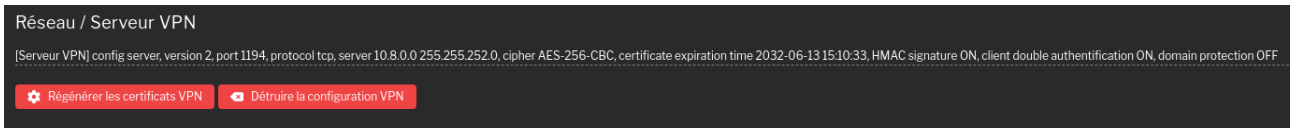


Vous pourrez donc utiliser cette fonctionnalité tout en étant connecté à distance sur le système vidéo client.

9.1.4 Configuration serveur vidéo central

Pour configurer le système en serveur central VPN, vous devez disposer d'une version d'OS VXCORE spécifique. Il est possible de centraliser des systèmes vidéo clients et/ou de gérer/enregistrer un parc de caméra en plus (comme un serveur d'enregistrement NVR). Contactez votre distributeur pour connaître la gamme produit disponible.

Dans le menu administration du système, menu Extensions / VPN : cliquez sur le bouton "Activer le serveur VPN" pour créer une nouvelle configuration VPN et autoriser les raccordements de systèmes vidéo clients.

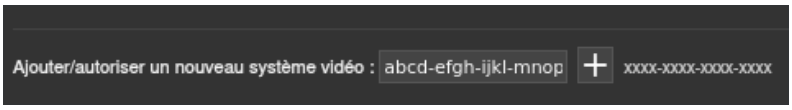


Le bouton « Régénérer les certificats VPN » permet de recréer une nouvelle configuration VPN de zéro (certificats serveur et clients, clés privées, etc). Les systèmes vidéo clients devront donc télécharger une nouvelle version des certificats pour se connecter. Ce bouton aura pour effet de déconnecter temporairement tous les systèmes vidéo clients, le temps qu'ils se resynchronisent et se reconnectent automatiquement. Cette action ne modifiera pas la configuration des caméras ou les alarmes actuelles, ou encore les données stockées. Vous pouvez utiliser cette fonctionnalité si la date d'expiration de votre certificat VPN est atteinte.

Le bouton « Détruire la configuration VPN » va supprimer toute la configuration VPN du serveur et des systèmes vidéo clients. Les clients ne pourront plus se connecter au serveur central tant qu'une nouvelle configuration n'aura pas été créée. Cette action nécessitera une reconfiguration de chaque système vidéo client pour le reconnecter a nouveau sur le serveur central. Attention : cette action est définitive et irrémédiable.

Ajouter/autoriser un nouveau système vidéo :

Pour permettre le raccordement d'un nouveau système vidéo, celui-ci devra disposer d'une licence client VPN. Le serveur central devra ensuite être configuré pour autoriser le raccordement du client, soit en activant l'option « Autoriser les connexions de nouveaux clients VPN », soit en ayant préalablement enregistré le numéro de série du système vidéo.



Le serveur central VPN utilisera les ports **1194** (TCP) et **443** (HTTPS) pour raccorder les clients VPN. Il sera peut être nécessaire de configurer votre firewall pour autoriser les connexions entrantes.

Ces deux ports sont nécessaire pour le fonctionnement du système de centralisation.

Le port HTTPS sera utilisé par les systèmes clients pour la communication et le contrôle de la connexion VPN (heartbeat). Le port VPN sera utilisé pour la synchronisation des données entre les systèmes vidéo et le serveur central.

Remarque : le raccordement effectif d'un nouveau client VPN est toujours plus long lors de la première connexion (initialisation des certificats VPN).

Options globales de centralisation :

Ces options affecteront la configuration de l'ensemble des raccordements ou du comportement des systèmes vidéo clients sur le serveur central.

- **Autoriser les connexions de nouveaux clients VPN**

  Cette option permet d'autoriser les raccordements de tous les systèmes vidéo qui disposent d'une licence client VPN.

  Important : lorsque cette option est activée, tous les systèmes vidéo pourront se connecter au serveur central (serveur central « ouvert »).

  Pour garantir une meilleure sécurité, vous devriez plutôt autoriser chaque système vidéo client en pré-enregistrant son numéro de série.

- **Superviser les erreurs systèmes des clients VPN**

  Si cette option est activée, le serveur central supervisera l'état de fonctionnement de tous les systèmes vidéo clients, et enverra des alertes email aux administrateurs root en cas d'erreur détectée (comme si tous les systèmes connectés faisaient parti du même système)

- **Autoriser l'exportation vidéo des clients VPN**

  Lorsque cette option est activée, les utilisateurs seront capable de lancer des ordres d'exportation sur les systèmes vidéo clients. Les fichiers seront ensuite synchronisés automatiquement dans l'espace de stockage des archives du serveur central.

  Remarque : la taille maximale des fichiers exportés sur les systèmes vidéo client sera fonction du quota de stockage du compte utilisateur sur le serveur central et de l'option « Taille maximale des fichiers exportés ».

- **Autoriser la synchronisation des enregistrements vidéo des clients VPN**

  Lorsque cette option est activée, les utilisateurs pourront synchroniser les données vidéo directement dans l'espace de stockage du serveur central. Cette fonctionnalité permet de conserver une copie des enregistrements vidéo directement sur le serveur central, qui pourront ensuite être consultés et exportés, même si le système vidéo client est déconnecté.

  Remarque : cette fonctionnalité nécessite un module supplémentaire dans la licence du serveur central.

- **Taille maximale des fichiers exportés**

  Cette option globale permet de définir une taille de fichier maximale pour les ordres d'exportations qui seront donnés aux systèmes vidéo clients. Ces fichiers exportés seront ensuite synchronisés automatiquement dans les archives du serveur central.

Options des systèmes vidéo :

Ces options permettent de définir la configuration de synchronisation de chaque système vidéo lorsqu'il sera raccordé au serveur central. Ces options peuvent être définies de manière globales ou individuellement pour chaque système vidéo.

- **Serveur LAN**

  Si cette option est activée, le serveur central considérera que le système vidéo client est situé sur le même réseau physique que lui (réseau de confiance).

  Cela permettra de ne pas encapsuler les flux vidéo dans le tunnel VPN lors de la consultation (ce qui peut être très gourmand en ressources CPU dans le cas d'un affichage multiple et totalement inutile dans un réseau privé local).

  Remarque : il existe la même option pour les serveurs externes (murs d'image ou node d'analyse vidéo)

- **Synchronisation automatique caméras/alarmes**

  Lorsque cette option est cochée, le serveur central va automatiquement vérifier et synchroniser les nouvelles caméras/alarmes du système vidéo client (et supprimer celles qui n'existent plus).

  Cette synchronisation automatique sera faite toutes les 15 minutes environ.

  Remarque : si vous disposez d'un système vidéo centralisé « statique » qui n'est pas soumis à modification sur les systèmes vidéo clients, vous devriez plutôt utiliser les fonctionnalités de synchronisation manuelles.

- **Synchronisation du journal des alarmes hors-ligne**

  Lorsque cette option est cochée, le serveur central va automatiquement vérifier et synchroniser les nouveaux déclenchements d'alarmes du système vidéo client (lorsqu'il était déconnecté d'internet par exemple). Cela permet d'avoir une copie parfaite du journal des alarmes entre le serveur central et le système vidéo client.

  Remarque : attention à la consommation de la bande passante du système vidéo, surtout si vous disposez d'une connexion internet à trafic limité, comme par exemple une connexion mobile via 3G/4G.

- **Synchronisation des redirections réseau externes**

  Lorsque cette option est cochée, le serveur central va automatiquement synchroniser les redirections réseaux configurés sur les systèmes vidéo clients (toutes les redirections seront synchronisées). Ces redirections pourront ensuite être ré-affectés aux utilisateurs dans les permissions de leur compte.

- **Synchronisation des journaux systèmes**

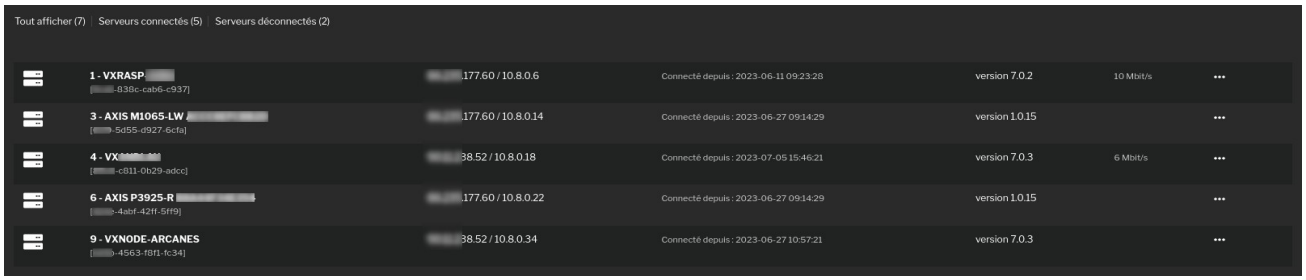
  Lorsque cette option est cochée, le serveur central va automatiquement vérifier et synchroniser les journaux du système vidéo client (journaux de connexions, consultations, exportations, etc).

  Cela permettra de disposer sur le serveur central d'un historique complet des journaux des systèmes vidéo clients, consultable même si les systèmes vidéo clients sont déconnectés.

  Remarque : la rétention maximale des journaux systèmes des systèmes vidéo clients sera fonction de la configuration de la rétention globale du serveur central.

Liste des systèmes vidéo clients :

Après le raccordements des clients VPN, vous verrez apparaître une liste d'état, que vous pouvez filtrer par état de connexion « connectés/déconnectés » :



Chaque système vidéo client sera représenté sur une ligne avec son nom, numéro de série, adresse IP distante et VPN, date/heure dernière connexion/déconnexion et bande passante montante (upload).

Bande passante des systèmes vidéo :

Le serveur central procédera à un calcul instantané de la bande passante montante "upload" pour chaque système vidéo connecté (capacité du système vidéo à envoyer des données au travers de sa connexion internet).

Si la valeur de bande passante montante (upload) est trop faible, le système vous l'indiquera avec une couleur orange ou rouge :

- **Couleur normale** - Bande passante suffisante (> 256 kbit/s)

  Toutes les fonctionnalités de centralisation seront actives, mais dépendante de la bande passante disponible.

- **Couleur orange** - Bande passante limitée (< 256 kbit/s)

  Les fonctionnalités de synchronisation des séquences vidéo seront automatiquement désactivées

- **Couleur rouge** - Bande passante insuffisante (< 128 kbit/s)

  Les fonctionnalités de synchronisation des séquences vidéo seront automatiquement désactivées, le système vidéo client passe en mode connexion dégradé (vous ne pourrez pas consulter ses données correctement).

Les bandes passantes inférieures fonctionneront pour une synchronisation automatique des données sur le serveur central, mais ne permettront pas une consultation optimisée des données à distance (live, enregistrements, contrôle PTZ, séquences vidéo, etc).

Par exemple : il sera impossible de consulter une vidéo live 4K (environ 4Mbit/s) avec une bande passante montante de 256 kbit/s (cela risque même de provoquer des coupures du tunnel VPN).

Remarque : la bande passante minimale conseillée en upload d'un système vidéo client pour un système 4 caméras est de 512 kbit/s.

Options/réglages/actions sur les systèmes vidéo clients :

- **Gestion de la sortie audio**

  Lorsque cette option est activée, il sera possible d'utiliser les sorties vidéo des systèmes vidéo clients dans la programmation ou dans l'interface du serveur central. Chaque système vidéo client pourra donc être utilisé comme un « haut-parleur » distant pour diffuser des messages audio.

  Remarque : la sortie audio de chaque système vidéo client devra d'abord avoir été configurée.

- **Synchroniser automatiquement les caméras et les alarmes du client VPN**

  Utilisez cette fonctionnalité pour synchroniser automatiquement toutes les nouvelles caméras et les nouvelles alarmes du client VPN. Tout ajout de nouvelles caméras ou alarmes sur le client VPN nécessiteront une nouvelle synchronisation.

  Le nom des caméras et des alarmes seront automatiquement synchronisés par le serveur central.

  Si vous avez coché l'option « synchronisation automatique caméras/alarmes » il ne sera pas nécessaire de procéder à des synchronisation manuellement.

- **Configurer automatiquement la zone du client VPN (root)**

  Utilisez ce bouton pour créer ou mettre à jour automatiquement la zone d'affichage du système vidéo client en y rangeant ses caméras et ses alarmes (Exemple : site1, site2, site3, ...).

  La zone d'affichage sera configurée pour le super-utilisateur root, vous pourrez ensuite la faire hériter directement aux administrateurs, puis aux utilisateurs.

  Attention : cette option va détruire toute configuration de zone existante.

- **Supprimer la synchronisation du client VPN**

  Utilisez ce bouton pour supprimer les caméras et les alarmes qui ont été configurées sur le serveur central pour un système vidéo client. Cette action ne supprimera pas la connexion VPN du système vidéo client mais supprimera toutes caméras et des alarmes du serveur central.

- **Supprimer le client VPN**

  Utilisez cette fonctionnalité pour supprimer définitivement un système vidéo client du serveur central.

  Cette option nécessitera que le système vidéo client soit déconnecté du serveur central pour supprimer les certificats d'authentification. Si le système vidéo client tente à nouveau de se connecter alors qu'il a été supprimé, le serveur central indiquera un problème de configuration et désactivera la connexion VPN du client.

  Remarque : pour réactiver la connexion VPN d'un système vidéo supprimé, il sera nécessaire de procéder à un nouveau raccordement depuis le système vidéo, après avoir détruit l'ancienne configuration VPN.

9.2 Synchronisation / Hypervision

VXCORE dispose d'un module complémentaire permettant à un serveur central d'automatiser, pour un même domaine VPN, la gestion des systèmes vidéo clients ainsi que les comptes utilisateurs/administrateurs et l'ensemble des droits d'accès.

La configuration de l'ensemble des éléments du domaine se feront fait via la solution d'hypervision « VXHUB » qui se chargera de tout centraliser, automatiser et synchroniser.

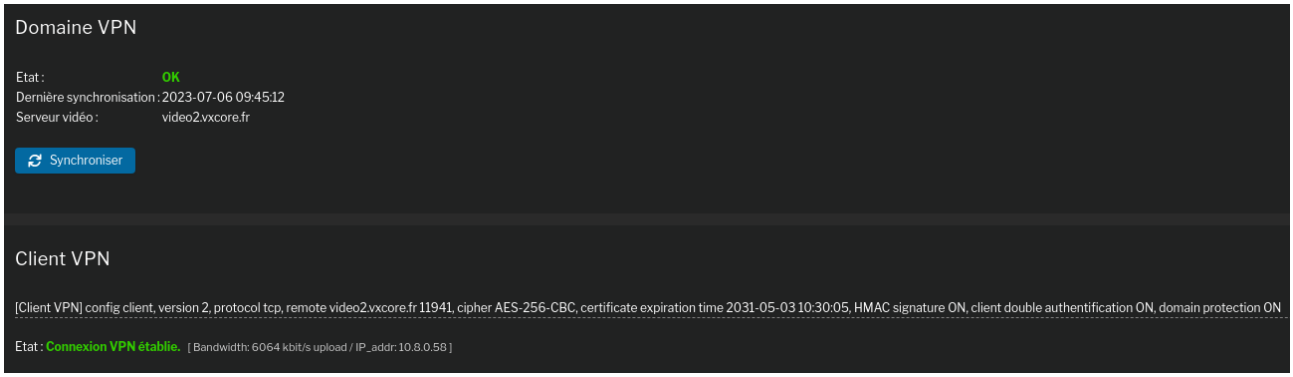
Cette solution sera indispensable dans la gestion d'un environnement CLOUD VIDEO avec un grand nombre de systèmes et d'utilisateurs, notamment pour la gestion des droits d'accès aux images (confidentialité et propriété).

Remarque : ce module nécessite également que la SMA du serveur central et des systèmes vidéo connectés soit à jour pour garantir un fonctionnement optimal (mises à jour des versions et de sécurité).

Les systèmes et les serveurs vidéo seront enregistrés dans un domaine VPN identique, qui sera intégralement géré par l'hyperviseur VXHUB (cloisonnement VPN et/ou applicatif).

Configuration des systèmes vidéo clients :

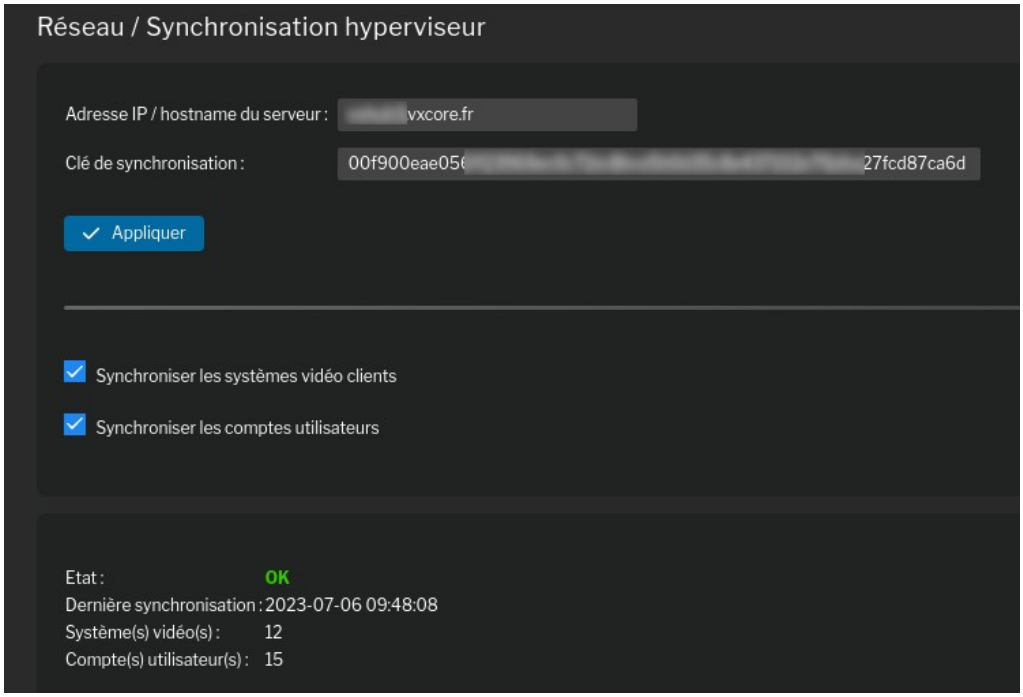
Tous les systèmes vidéo du domaine iront interroger régulièrement l'hyperviseur pour connaître l'adresse de leur serveur vidéo central, pour ensuite s'y raccorder automatiquement. Il n'y aura donc plus aucune configuration à faire coté système vidéo client : ils géreront automatiquement leur connexion VPN.



L'hyperviseur vous permettra de raccorder automatiquement les systèmes vidéo aux différents serveurs de centralisation et également de gérer les migrations des systèmes entre eux, sans perte de données.

Configuration des serveurs de centralisation :

Les serveurs de centralisation se synchroniseront automatiquement avec l'hyperviseur. Vous n'aurez aucune configuration à faire pour enregistrer/configurer les systèmes vidéo ou encore dans la création des comptes utilisateurs/administrateurs et leurs droits d'accès.



Les comptes utilisateurs pourront être affectés a des rôles, ce qui permettra de gérer les permissions et droits d'accès de manière groupées, sans devoir aller modifier chaque utilisateur dans le cas d'ajout/suppression d'un droit.

Confidentialité des images :

L'hyperviseur permettra également de gérer la confidentialité des images et des flux vidéo. Il sera possible d'attribuer un droit de confidentialité supplémentaire, qui autorisera un utilisateur ou un administrateur à accéder à la configuration des caméras ou des alarmes, mais sans pour autant pouvoir afficher un flux vidéo ou une image.

Dans ce cas, il sera impossible de visualiser les flux vidéo des caméras (live/playback) et toutes les vignettes images caméras/alarmes seront brouillées.

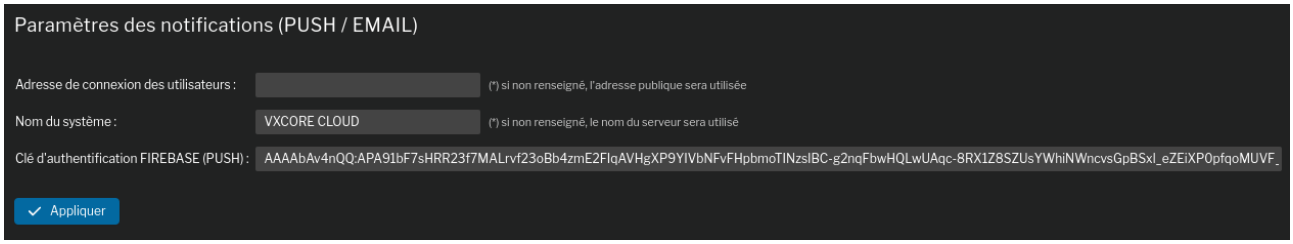
9.3 Notifications

VXCORE dispose d'un module spécifique pour envoyer des notifications temps réel en fonction des déclenchements d'alarmes du système.

Les notifications seront au format push/smartphone (iOS/Android) et/ou email. Une notification contient un identifiant de système vidéo et le nom de l'alarme qui s'est déclenchée, ainsi qu'une vignette image de prévisualisation.

La différence entre ces notifications et celles des agents de sécurité du système, qui peuvent aussi envoyer des alertes emails, est que ce sont les utilisateurs qui activent directement leurs notifications via l'application Mobile, alors qu'un agent de sécurité doit d'abord être configuré dans le système.

Remarque : pour configurer les notifications, vous devez disposer du module additionnel dans la licence du système. Ce module n'est disponible que sur les serveurs de centralisations.



Le système vidéo qui émet une notification devra également être accessible depuis une adresse publique, via le protocole HTTPS/443 (port personnalisable). Il ne sera pas obligatoire d'installer un certificat SSL officiel sur le système vidéo, car le certificat interne auto-signé apportera le même niveau de sécurité (chiffrage des communications).

Adresse de connexion des utilisateurs

Ce paramètre permet de spécifier une adresse de connexion personnalisée, qui sera différente de l'adresse publique du serveur configurée dans les paramètres réseaux (cas d'un centralisateur/hyperviseur de domaine par exemple).

Cette adresse sera celle qui sera utilisée par les utilisateurs et les applications mobiles pour consulter l'interface du système lorsqu'ils cliqueront sur une notification de leur smartphone. Elle devra donc être accessible sur le port HTTPS.

Une adresse publique est toujours au format : https://HOSTNAME{:PORT}
(le port est optionnel, mais vous devez le spécifier s'il est différent de 443).

Nom du système

Le nom du système sera utilisé si vous souhaitez remplacer le nom qui est configuré dans les paramètres réseau du serveur (hostname). Ce paramètre est utile dans une configuration Cloud ou plusieurs serveurs de centralisations sont utilisés : le nom de la notification sera normalisé quel-qu'en soit l'émetteur (serveur de centralisation).

Clé d’authentification FIREBASE

Les notifications utilisent l’API FIREBASE (GOOGLE) pour transmettre les données sur les applications mobiles des smartphones (iOS/Android).

Vous devez donc utiliser une clé API qui aura été liée à l’application Mobile que vous utiliserez (application Mobile officielle ou application spécifique en marque blanche).

CLÉ API <=> VERSION APPLICATION MOBILE

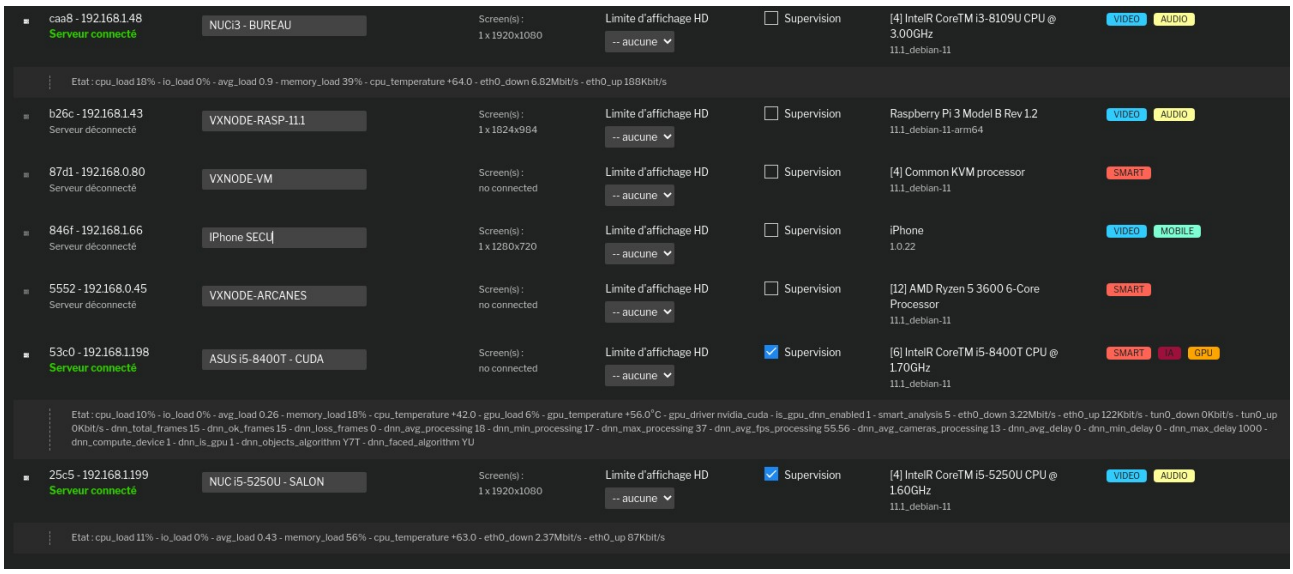
Si vous configurez une clé API qui n’est pas enregistrée dans l’application mobile des utilisateurs, les notifications ne fonctionneront pas.

9.4 Serveurs externes

VXCORE peut centraliser un ou plusieurs serveurs externes pour étendre les fonctionnalités du serveur vidéo principal.

Ces serveurs externes auront plusieurs rôles possibles (cumulatifs) :

- Affichage vidéo pour concevoir des murs d'images
- Diffusion audio pour créer des haut-parleurs connectés
- Cluster de calculs pour de l'analyse vidéo (augmentation/délestage des capacités de calculs Smart/IA du serveur principal)



Ces serveurs externes seront installés avec n'importe quel PC compatible et en utilisant l'installateur officiel disponible en ligne (OS VXVIEW ou OS VXCORE-NODE selon les cas).

Trois OS/versions sont disponibles selon les infrastructures a déployer :

- VXVIEW – OS simplifié pour faire de l'affichage vidéo et/ou de la diffusion audio
- VXVIEW-MOBILE - Application mobile pour smartphone, permettant de faire de la diffusion vidéo mobile
- VXCORE-NODE – OS avancé pour faire de l'affichage vidéo et/ou de la diffusion audio et/ou de l'analyse vidéo Smart/IA

Un OS VXVIEW pourra s'installer sur une clé USB bootable ou un disque dur système (aucune clé de de licence nécessaire pour l'installation)

L'application mobile VXVIEW-MOBILE pourra s'installer sur smartphone récent iOS/ANDROID (aucune clé de de licence nécessaire pour l'installation)

Un OS VXCORE-NODE aura la particularité de s'installer sur un disque système comme un système VXCORE classique. Il nécessitera également l'utilisation d'une clé de licence. Cet OS disposera de fonctionnalités avancées, comme l'accès à une interface d'administration via le réseau, un client VPN pour de la centralisation, de la journalisation, et la possibilité de mettre à jour l'OS et le système à distance avec la SMA).

Après l'installation de l'OS sur le serveur externe, vous devez procéder à sa configuration :

- **Configuration réseau**
  Choix de l'interface réseau, adressage IP, passerelle par défaut.
- **Configuration serveur vidéo** (serveur principal ou sera connecté le serveur externe)
  Adresse IP ou nom du serveur vidéo et protocole de transport des flux vidéo (auto/HTTP/HTTPS)
- **Configuration graphique** (ou désactivé)
  Sélection des cartes graphiques, choix du driver, résolution des écrans.
- **Configuration audio** (ou désactivé)
  Choix de la sortie audio pour faire de la diffusion audio depuis le serveur principal

Lorsqu'un serveur externe d'affichage vidéo est correctement configuré, il affichera l'image/logo de la solution sur tous les écrans connectés. Cela signifie que l'écran vidéo est disponible pour afficher des caméras.

Si vous avez désactivé l'affichage vidéo du serveur externe, il affichera un simple message sur la console Linux et restera en attente.

Vous pourrez appuyer sur la combinaison de touches < CTRL + C > pour revenir au menu de configuration.

Remarque : pour connecter vos serveurs externes sur le serveur vidéo principal, vous devez d'abord avoir coché l'option pour autoriser les nouvelles connexions.

Dans l'interface de configuration des serveurs externes, vous verrez des badges à droite permettant de visualiser facilement les capacités du serveur connecté :

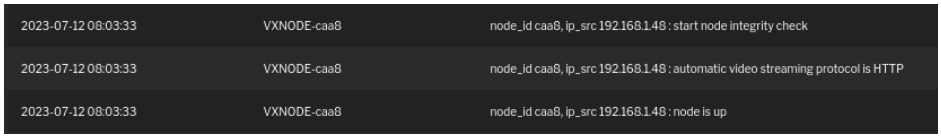
- VIDEO : le serveur externe peut faire de l'affichage vidéo
- AUDIO : le serveur externe peut faire de la diffusion audio
- MOBILE : le serveur externe est un terminal de diffusion vidéo mobile (application mobile)
- SMART : le serveur externe a des capacités d'analyse vidéo (analyse vidéo simple ou avancé)
- IA : le serveur externe a des capacités d'analyse vidéo IA
- GPU : le serveur externe dispose d'un GPU compatible pour l'analyse vidéo IA

Pour chaque serveur externe connecté, vous verrez un état système détaillé qui sera remonté régulièrement sur le serveur principal (charge cpu, utilisation mémoire, charge analyse vidéo, trafic réseau, etc)

Pour les écrans d'affichages vidéo, vous pourrez sélectionner une limite d'affichage HD pour restreindre l'affichage vidéo du serveur et contrôler les ressources (par exemple : 50 images/secondes maximum pour l'ensemble des flux vidéo du serveur externe). Les flux vidéo concernés ne seront que ceux qui auront une résolution supérieure à 1024 pixels (exemple 1920x1080).

La case a cocher « Supervision » permettra d'activer la supervision du serveur externe et d'envoyer une alerte email aux administrateurs systèmes en cas de déconnexion.

Les serveurs externes enverront des messages dans les journaux systèmes du serveur principal, ce qui permettra de bien tracer les différentes actions.



9.5 Écrans d’affichages vidéo

VXCORE peut centraliser un ou plusieurs serveurs d’affichage vidéo pour créer des murs d’images en réseau (entièrement pilotables à distance).

Ces serveurs externes dédiés a l’affichage pourront gérer plusieurs sorties vidéo (multiples sorties sur les cartes graphiques et/ou plusieurs cartes graphiques).

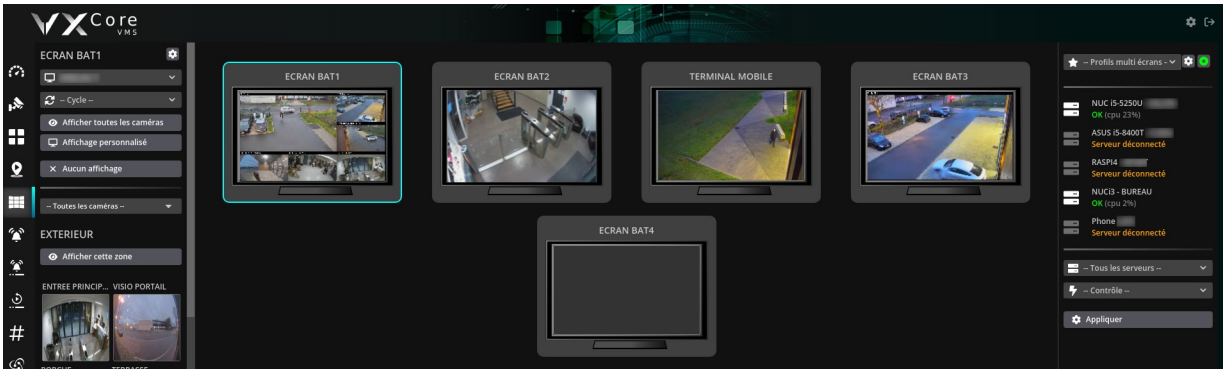
Les écrans vidéo fonctionnent avec des licences : 1 licence pour chaque écran de visualisation

Exemple de configuration pour 4 licences :

Licence Écran 1 - sortie Vidéo n°1 du serveur A (carte graphique double écran)
Licence Écran 2 - sortie Vidéo n°2 du serveur A (carte graphique double écran)
Licence Écran 3 - sortie Vidéo n°1 du serveur B (carte graphique simple écran)
Licence Écran 4 - licence disponible pour un futur écran

L’ordre de configuration des écrans/licences déterminera aussi leur ordre d’affichage dans l’interface de contrôle du système. Vous devez affecter les sorties vidéo dans le menu Admin > Extensions > Écrans de visualisation (Options avancées).

Dès lors que les écrans d’affichages vidéo seront affectés aux différents serveurs d’affichage, le menu de contrôle spécifique apparaitra dans l’interface de visualisation du système.



L’affichage et le contrôle des écrans vidéo sera aussi dépendant des droits d’accès configurés pour chaque utilisateur/administrateur du système.

Choix d’un serveur d’affichage vidéo :

Un serveur externe dédié à l’affichage vidéo sera capable de gérer plusieurs cartes graphiques et les sorties multi-écrans (si matériel compatible avec l’OS). Il est tout à fait possible de créer un serveur d'affichage avec 4 cartes graphiques double écran, pour une gestion totale de 8 écrans.

En pratique, il est cependant plus performant et plus économique de concevoir plusieurs petits serveurs d’affichage vidéo avec un ou deux écrans maximum, plutôt qu'un gros serveur centralisant toutes les cartes graphiques (saturation du processeur, quantité de mémoire, ventilation des cartes graphiques, puissance de l'alimentation, maintenance, ...).

9.6 Configuration de l'affichage vidéo intégré

VXCORE peut utiliser la sortie graphique du serveur pour afficher des caméras (carte graphique dédiée ou carte graphique intégrée). Cette fonctionnalité est limitée à un seul et unique écran (pas de dual-screen) et dépendra également de la version de l'OS VXCORE (licence).

Remarque : pour activer cette fonctionnalité, vous devrez disposer d'un serveur vidéo bien dimensionné avec un processeur puissant multi-cœur (et des possibilités d'affichage graphique chipset/carte vidéo).

Les performances d'affichages intégrées au système vidéo sont limitées pour ne pas compromettre le fonctionnement de base du système : **20 images/secondes** maximum par flux vidéo et **50 images/secondes** maximum sur la totalité de l'écran.

Par exemple :

- affichage de 1 caméra en plein écran => 20 images/secondes.

- affichage de 4 caméras (mode quadview) = 50 / 4 => 12 images/secondes par flux vidéo.

Pour activer la sortie vidéo du serveur, cliquez sur l'option d'activation, et redémarrer votre serveur vidéo.

A la fin du redémarrage, le système activera l'affichage graphique après avoir procédé à la détection automatique de la carte graphique et de la résolution de l'écran.

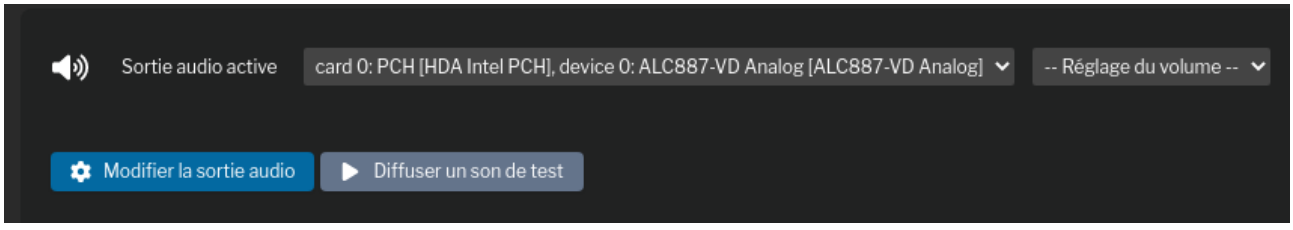
Lorsque l'écran d'affichage est chargé et affiche bien l'image et le logo, cela signifie qu'il est prêt à être configuré pour l'affichage de caméras, comme n'importe quel écran vidéo du système.

Remarque : VXCORE dispose d'une sécurité qui coupera l'affichage des flux vidéo en cas de surcharge processeur, afin de ne pas compromettre la tache principale du système d'enregistrer les caméras (si utilisation CPU > 85%).

9.7 Sortie / diffusion audio

VXCORE dispose d'une fonctionnalité de diffusion de messages audio en utilisant la sortie audio du serveur vidéo (carte audio ou sortie son intégrée, selon la compatibilité matérielle).

Grâce a cette fonctionnalité, n'importe quel serveur vidéo pourra diffuser des messages audio, aussi bien en configuration locale, qu'à distance via l'interface d'un serveur de centralisation. Chaque système vidéo pourra donc jouer un rôle de haut-parleur IP connecté au travers du réseau sécurisé VXCORE.



Pour activer la sortie audio du serveur, vous devez choisir quelle carte et/ou sortie audio utiliser par défaut (un seul choix possible). Vous pouvez également définir un niveau de volume de sortie audio, qui sera restauré a chaque redémarrage du serveur. Pour vérifier que la sortie audio fonctionne correctement, utilisez le bouton « Jouer un son de test ».

Si aucune sortie audio n’est détectée, vérifiez la compatibilité de votre matériel avec Linux/Debian ou utilisez une image de l’OS VXCORE plus récente.

Lorsque la sortie audio est configurée, la fonctionnalité apparaitra automatiquement dans le système : les utilisateurs pourront diffuser des messages audio et les administrateurs pourront programmer des agents/actions pour de la diffusion automatique.

9.8 Accès API / CGI

VXCORE dispose d’une API/WEB/CGI qui permet a des systèmes tiers d’interroger le serveur et d’accéder aux flux vidéo des caméras (live et enregistrement).

L’API Web du système communique au format CGI/JSON, via les protocoles HTTPS en réseau local ou à distance.

Les fonctionnalités disponibles seront les mêmes quelque soit la taille du système vidéo : un petit enregistreur vidéo local avec une ou deux caméra, ou un gros serveur ce centralisation multi-site avec des centaines de caméras distantes.

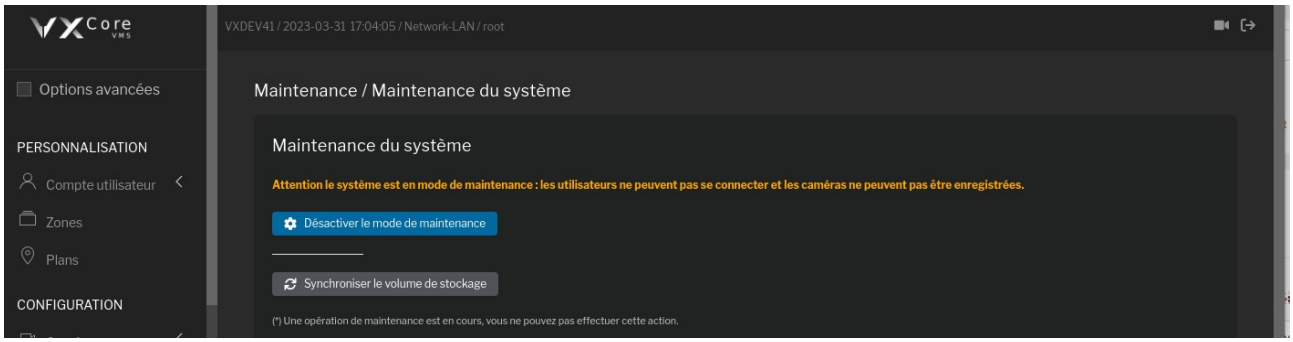
Le principe de l'API est de créer une clé de connexion unique pour chaque système tiers. Cette clé unique se comportera comme une session utilisateur simplifiée, en spécifiant des droits d'accès aux fonctionnalités et aux caméras.

Exemple de clé de connexion : ea817f1c1507dc59fcb1c0349fb60715

Consultez la documentation spécifique à l'API du système pour le détail des fonctionnalités implémentées.

10 Maintenance

Avant de procéder aux opérations de maintenance, il sera nécessaire "d'activer le mode de maintenance" du serveur. Ce mode permet de couper tous les services et les processus liés au système vidéo et de bloquer toutes les connexions utilisateurs pendant les opérations (sauf super-user root).



10.1 Opérations de maintenance courantes

Lorsque le mode de maintenance est activé, vous aurez accès aux différentes actions de réparation ou de diagnostique du système.

- **Activer/désactiver le mode de maintenance**

  Permet d'activer ou désactiver le mode de maintenance du système.

- **Synchroniser le volume de stockage**

  Permet de forcer la synchronisation des données présentes sur tous les volumes de stockage vidéo (enregistrement vidéo, photos d'alarmes et métadonnées d'analyse). Cette fonctionnalité peut être utile en cas de crash système ou pour resynchroniser la base de données après une importation d'un volume de stockage existant.
  Cette synchronisation à pour avantage d'être exécutable lorsque le système est en fonctionnement, sans devoir activer le mode de maintenance. Chaque périphérique de stockage vidéo sera entièrement scanné et les données vidéo seront testées et indexées dans la base de données au fur et à mesure.

Remarque : cette synchronisation peut être très longue avec les gros volumes de stockage.

- **Effacer toutes les données vidéo, alarmes et archives**

  Cette opération permet de supprimer l'ensemble des données du serveur vidéo, mais en gardant toute la partie configuration. Tous les enregistrements vidéo, images d'alarmes ou séquences vidéo exportées seront automatiquement supprimés.

Attention : cette action de suppression globale est irréversible.

- **Réparer la base de données**

  Cette opération de maintenance permet de vérifier et éventuellement de réparer les tables de la base de données système. La base de données peut être endommagée suite à la coupure violente d'un serveur ou lorsque le disque système rencontre des problèmes (secteur défectueux, perte mémoire cache ...)

- **Générer le rapport de fonctionnement du système**

  Le rapport de fonctionnement permet de générer une archive compressée contenant un état complet du système (charge, mémoire, logs, graphiques d'états, etc). Il est en général utilisé afin d'être envoyé à l'éditeur pour diagnostiquer un problème.
  Ce rapport de fonctionnement détaillé sera aussi automatiquement envoyé dans les alertes emails aux administrateurs en cas de détection d'erreurs système.

- **Éteindre / redémarrer**

  Utilisez ces boutons pour éteindre ou redémarrer le système. Ces actions peuvent être effectuées de manière normale « software » ou forcé « hardware ». En mode normal, le système/OS sera éteint proprement après envoi des signaux d'extinction à tous les services/programmes. En mode forcé « HARD » le kernel Linux va faire un reboot/extinction instantané, comme si on éteignait le serveur de manière forcé via la carte mère (reset/power). Le mode Hard est surtout utilisé quand un périphérique ou un volume de stockage bloque le redémarrage normal du serveur (attention aux corruptions de données avec cette méthode).

10.2 Mise à jour du système

La mise à jour du système se fait en installant un patch de mise à jour au format « .veox7 » et ne concerne que les programmes ou services du système vidéo (et non les librairies ou les services liés à l'OS Linux).

Ce fichier patch peut être installé de manière automatique par le système de mise à jour intégré ou manuellement via l'interface du système.

Remarque : il n'est pas toujours possible d'installer un patch de mise à jour selon le degré d'évolution d'une version à une autre (compatibilité de l'image OS, nouvelles librairies ...).

Avant de procéder à une mise à jour, il est fortement recommandé de faire une sauvegarde des paramètres afin de pouvoir restaurer le système en cas de problème.

Le système utilise une numérotation précise pour ses évolutions de version, avec 3 chiffres X.Y.Z (exemple : VXCORE - version 7.0.3).

Pour une version X.Y.Z :

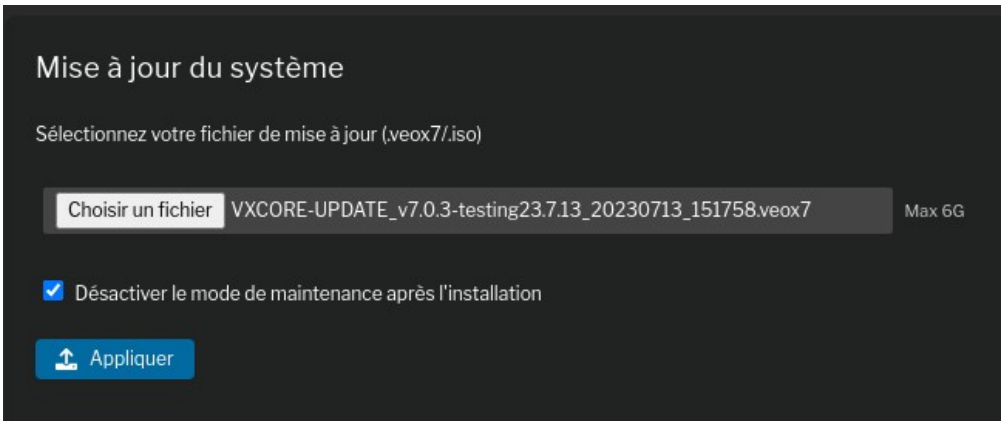
- **X -** Indication de la génération du système (exemple V6, V7)

  Un changement de génération inclut une nouvelle interface graphique et des changements importants.
  La licence devra également être mise à jour pour utiliser la nouvelle génération du système.

- **Y -** Version majeure du système, incluant des nouvelles fonctionnalités importantes ou des évolutions de l'interface graphique. Ces versions ne sont pas installés automatiquement, car elles peuvent nécessiter de revoir certains éléments dans la configuration (deprecated).

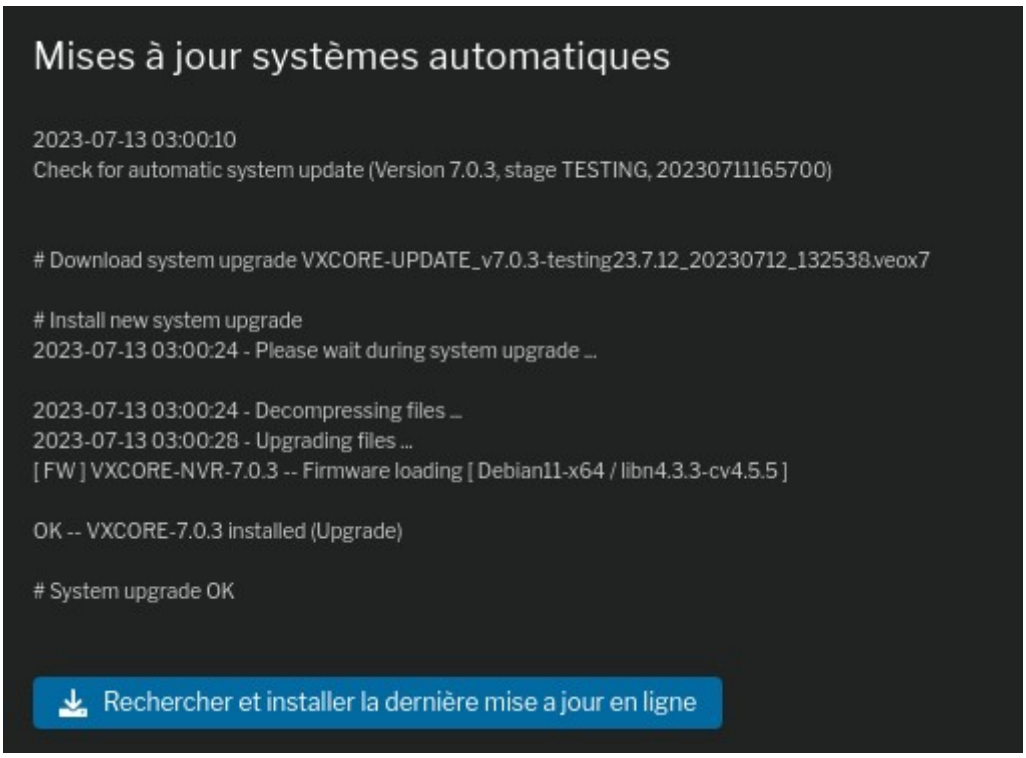
- **Z -** Correctif mineur du système, incluant des correctifs de BUG ou d'optimisations des fonctionnalités, qui n'impacte pas ou très légèrement l'interface graphique. Ces correctifs sont en général déployés automatiquement si le système vidéo est connecté sur Internet.

Pour installer un patch de mise à jour, vous devez placer votre serveur en maintenance, puis choisir le fichier à installer via l'interface.



Après la mise à jour, il est recommandé de se reconnecter au système pour réinitialiser la session utilisateur (login).

Lorsque le système est connecté sur Internet, vous pouvez utiliser le bouton de recherche/mise à jour automatique : il permet de vérifier en ligne si une nouvelle version est disponible, de la télécharger et de l'installer automatiquement.



10.3 Mise à jour de l'OS Linux

La mise à jour de l'OS Linux se fait en téléchargeant une nouvelle image système, qui permettra « d'héberger » les programmes et services VXCORE.

Important : la mise à jour régulière de l'OS est nécessaire pour installer tous les correctifs de sécurité du système Linux et ses composants (SSL, VPN, KERNEL ...). La plupart des failles de sécurités sont corrigées rapidement, mais si elles ne sont jamais installées, le risque peut devenir très important, notamment sur les systèmes vidéo exposés en ligne (serveurs de centralisation).

Par ailleurs, selon la mise à jour que vous souhaitez installer, il sera quelques fois nécessaire de respecter un pré-requis de l'image de l'OS (exemple : la version 7.0 nécessite une image de l'OS Debian 11 minimum).

VXCORE utilise un système de mise à jour de l'OS inédit et entièrement automatisé, qui permet d'installer une nouvelle image Linux intégralement à distance, sans aucune intervention physique (comme lors de la procédure d'installation).

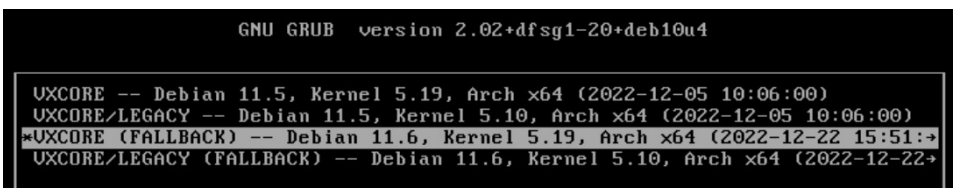
Si une mise à jour est disponible, vous pouvez cliquez sur le bouton « installer la mise à jour » :

Lorsque les nouveaux fichiers auront été téléchargés et installés, il sera nécessaire de redémarrer le serveur sur la nouvelle image de l'OS. Vous pourrez cliquez sur l'option « Redémarrer automatiquement après la mise à jour » pour que le redémarrage soit immédiat après l'installation de l'OS.

Remarque : la procédure de mise à jour de l'OS se fait totalement en tâche de fond, pendant que le système vidéo est en cours de fonctionnement (sauf pour le redémarrage du serveur).

Après l'installation d'un nouvel OS, vous verrez apparaitre un nouveau menu au démarrage du système (BIOS) qui sera nommé « FALLBACK ». Cette entrée correspond à l'ancienne image de l'OS, qui a été remplacée par la nouvelle fraichement installée.

Si vous rencontrez des problèmes au redémarrage avec la nouvelle image de l'OS, vous pouvez sélectionner l'entrée FALLBACK pour revenir a l'ancienne version de l'OS.



10.4 Sauvegarde et restauration des paramètres

VXCORE intègre plusieurs fonctionnalités d'import/export des paramètres systèmes essentiels pour la maintenance.

Quelque soit votre type de serveur et la sécurité des données mise en place, vous n'êtes jamais à l'abri d'une corruption du système de fichier suite à un arrêt brutal du serveur (comme une coupure de courant). Il est fortement recommandé de mettre en place une stratégie de sauvegarde des paramètres systèmes (manuelle ou automatique).

L'exportation des paramètres créera une archive compressée contenant toute la configuration du système (réseau, caméras, utilisateurs, plans, ...).

Par défaut, l'importation des paramètres ne s'applique pas aux paramètres réseaux pour éviter les erreurs et surtout la perte de l'accès au système (adresse IP, passerelle, DNS, VPN, ...). Il est néanmoins possible de forcer l'importation des paramètres réseaux en cochant la case correspondante dans l'interface.

Remarque : si vous importez les paramètres d'un système disposant de plus de licences dans un système sous dimensionné, comme par exemple l'importation d'un système 16 caméras dans un système 4 caméras, seules les premières caméras seront importées.

VXCORE procédera à l'exportation automatique de sa configuration système tous les jours entre 00h00 et 03h00, sur l'ensemble des solutions de sauvegardes mises en place (FTP, périphériques de backup...)

10.4.1 Import/export manuel par le réseau

Cette fonctionnalité vous permet d'exporter les paramètres systèmes manuellement, en téléchargeant l'archive et en la sauvegardant sur votre PC pour une ré-importation ultérieure.

Pour restaurer une configuration système, vous devez d'abord placer votre serveur en maintenance.

10.4.2 Export automatique sur serveur externe S/FTP

Cette fonctionnalité permet de sauvegarder la configuration sur un serveur de backup externe accessible sur le réseau (local ou distant). Un répertoire sera automatiquement créé sur le serveur de backup en utilisant le numéro de série du système, pour ensuite y transférer l'archive.

Exemple : sftp://server/aaaa-f02d-7965-c160/VXCORE-CONFIG_20200212000008.veox

Le backup des paramètres pourra être fait via le protocole SFTP/SSH ou le protocole FTP (protocole non sécurisé, a éviter).

Chaque procédure de backup sera testée et relancée jusqu'à 5 essais en cas de problème (timeout réseau, serveur backup surchargé, etc).

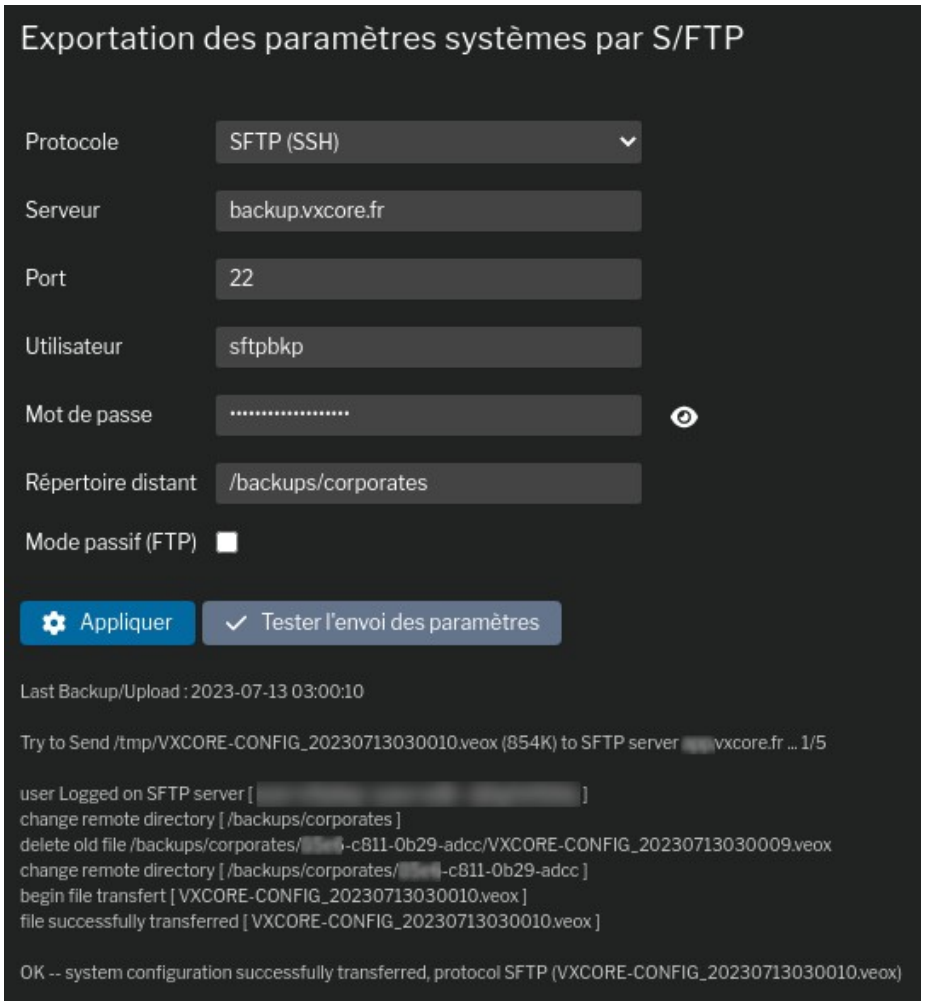
Vous pourrez également spécifier un chemin de répertoire distant sur le serveur de backup pour ranger vos archives.

A chaque sauvegarde, le système nettoiera automatiquement ce répertoire pour y stocker la nouvelle archive des paramètres.

Après avoir sauvegardé les paramètres, vous pouvez utiliser le bouton « Test l'envoi des paramètres » pour lancer un test du backup.

Le backup automatique des paramètres sera lancé tous les jours entre 00h00 et 03h00, selon la version et la charge du système.

Remarque : pour importer une archive stockée sur le serveur de backup, vous devrez d'abord la télécharger manuellement sur votre poste.



10.4.3 Import/export automatique sur périphérique de backup

VXCORE dispose d'une fonctionnalité de sauvegarde des paramètres systèmes sur un ou plusieurs périphériques de backup USB connectés en permanence au serveur (une petite clé USB, de préférence à l'intérieur).

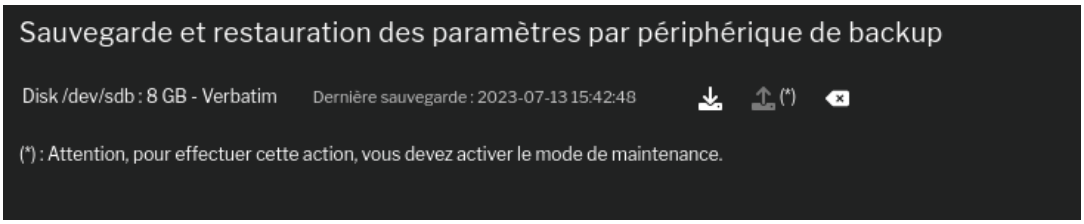
Une capacité de 1 GB est largement suffisante pour enregistrer toute la configuration d'un système vidéo (toute capacité supérieure ne sera pas utilisée).

Grâce à cette fonctionnalité, vous serez capable de réinstaller un serveur très rapidement, puisque toute la configuration du système sera stockée sur un périphérique totalement indépendant du disque système ou vidéo.

Un périphérique de backup n'est pas forcément associé à une licence ou un serveur. Il est donc possible de migrer les paramètres d'un système à un autre.

Pour restaurer une configuration système stockée sur un périphérique de backup, vous devez d'abord placer votre serveur en maintenance.

Attention : la création d'un périphérique de backup détruit intégralement toutes les données présentes sur le périphérique.



Si vous souhaitez supprimer un périphérique de backup, le système créera une nouvelle table de partition sur le périphérique. Il vous sera alors possible de le formater pour le réutiliser avec un autre système d'exploitation.

10.5 Heartbeat

VXCORE intègre une fonctionnalité de heartbeat qui va générer une requête WEB (HTTP/HTTPS) ou un upload S/FTP vers un serveur externe automatiquement toutes les 15 minutes.

Elle peut être utile pour vérifier la connectivité et l'état de fonctionnement d'un ou plusieurs serveur vidéo en utilisant un serveur externe comme « récepteur ». Par exemple, cette fonctionnalité pourra être utilisée pour récupérer automatiquement et maintenir à jour dynamiquement les adresses IP des systèmes distants.

Remarque : pour fonctionner correctement, cette fonctionnalité nécessite que la SMA du système vidéo soit en cours de validité (non expirée).

Le hearbeat pourra fonctionner avec deux protocoles différents : soit par HTTP/S, soit par S/FTP, soit les deux. Et pour chaque protocole, différents formats seront disponibles pour envoyer les données.

Les données qui seront envoyées seront dépendantes du système VXCORE utilisé (OS/licences/version) et de sa configuration (données visibles dans le tableau de bord).

Pour le format JSON, les données envoyées correspondront à la requête/route API :

https://IP_VXCORE/ctrl/system/status?token=XXX

```
{"vxreturncode":0,"system_time":"2023-07-13 16:07:57","system_serial":"abcd-
efgh-ijkl-mnop","system_version":"7.0.3","system_uptime":"1
day","system_status":"ERROR","video_storage_status":"OK"}
```

Référez-vous à la documentation API/REST du système pour avoir plus d'informations.

Lorsque vous avez saisi et sauvegarder les paramètres Heartbeat, vous pouvez utiliser le bouton « Tester » en bas de l'interface. Les détails complets et les éventuelles erreurs de chaque requête/upload seront indiquées.

10.5.1 Heartbeat HTTP/S

Le heartbeat HTTP/S permet de générer une requête Web HTTP ou HTTPS en incluant les paramètres selon le format défini :

- **JSON** : Requête POST / Content-type « application/json » / JSON du status système
- **OLD/TEXT/LEGACY** : Requête POST / Content-type « application/x-www-form-urlencoded »

Le format OLD/TEXT/LEGACY ne devrait pas être utilisé, il n'est disponible que pour assurer la compatibilité avec les anciennes intégrations (anciennes versions VXCORE). Il sera supprimé dans les prochaines versions du système.

Remarque : les requêtes HTTP non sécurisées sont fortement déconseillées.

10.5.2 Heartbeat S/FTP

Le heartbeat S/FTP permet de générer un upload de fichier en utilisant les protocoles SFTP/SSH ou FTP.

Si vous spécifiez un préfixe dans la configuration, tous les fichiers uploadés seront nommé avec le préfixe en début de fichier : PREFIX_FILE.EXT

Différents formats d'upload sont disponibles :

- **JSON** : Fichier JSON du status système
- **Alarm Video (MPEG4/AVI)** : fichier d'alarme vidéo généré aléatoirement
- **Alarm Picture (jpeg)** : fichier d'alarme image généré aléatoirement

Les fichiers vidéo et images sont très utilisés par les centres/logiciels de télésurveillances pour vérifier que le système vidéo est toujours « ONLINE ».

Ces fichiers seront toujours générés avec le code d'alarme spécial « 0602 » :

- Fichier VIDEO : PREFIX_TIMEID_cam-0_alarm-0602_videosize-320x240_fps-1.0_prealarm-0.avi

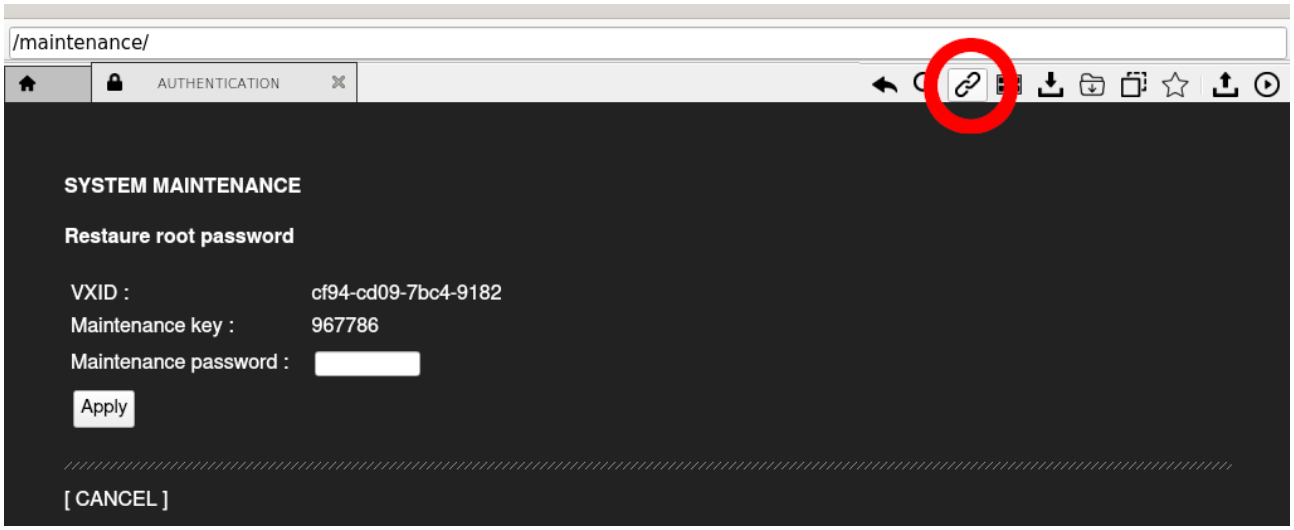
- Fichier IMAGE : PREFIX_TIMEID_alarm-0602.jpg

Remarque : les transferts utilisant le protocole FTP non sécurisé sont fortement déconseillés.

10.6 Opérations de maintenance spéciales

Le système intègre une interface spéciale qui permet de réaliser des opérations de maintenance spécifiques avec un mécanisme de clés partagées (sans avoir les droits d'accès root).

Pour y accéder, il suffit d'utiliser le bouton spécial du logiciel VXCORE-ACCESS pour afficher l'URL du serveur vidéo, puis de taper l'adresse « /maintenance ».



Liste de opérations de maintenance :

- **Restaure root password**
  Restauration du mot de passe du super-utilisateur root (le mot de passe restauré par cette interface sera toujours « vxcore7! »)
- **Deleting users quarantine**
  Supprimer tous les utilisateurs bloqués en quarantaine
- **System clock setup**
  Réglage de l'horloge du système
- **Enable remote maintenance**
  Activer le tunnel de maintenance distant (uniquement pour l'éditeur)

Pour obtenir la clé de maintenance relative à une opération, contactez votre distributeur de la solution et communiquez lui les informations suivantes : type d'opération de maintenance, numéro de série de licence et clé de maintenance.

11 Journaux systèmes

VXCORE dispose d'un système de journalisation de plusieurs évènements liés au système ou à la configuration vidéo.

Chaque journal sera conservé pour une durée de 30 jours par défaut. Il est possible de régler la rétention des journaux dans les paramètres systèmes.

Sur les serveurs de centralisation VXCORE, le système dispose d'une fonctionnalité de synchronisation des journaux des serveurs vidéo clients VPN. Tous les journaux seront alors consultables directement dans l'interface du serveur central.

- **Journaux des connexions utilisateurs**

  Retrace chaque tentative de connexion utilisateur (login, erreur d'authentification, quarantaine, type et version d'application ...)

- **Accès vidéo**

  Retrace toutes les consultations vidéo des utilisateurs, aussi bien en visualisation direct (live) qu'en relecture d'enregistrement (playback).
  Si l'utilisateur supprime une ou plusieurs données vidéo, cela apparaitra aussi dans ce journal.

- **Caméras externes**

  Retrace toutes les importations vidéo des caméras externes (données vidéo, audio, métadonnées, etc). Ces importations pourront être fait avec le logiciel PC VXCORE-ACCESS, l'application mobile VXSHARE encore via un upload/API intégré dans un système tierce.

- **Journaux des exportations utilisateurs**

  Retrace toutes les extractions de séquences vidéo des utilisateurs (exports vidéo, téléchargement, consultation, séquence vidéo d'alarmes ...)

- **Journaux des alertes emails**

  Retrace toutes les alertes emails qui ont été envoyés par le système

- **Journaux des agents de sécurité**

  Retrace tous les évènements liés aux agents de sécurité virtuels (début et fin d'alerting, activation d'actions, déplacements PTZ, ...)

- **Journaux des modifications de configuration**

  Retrace tous les évènements liés aux modifications de configuration du système vidéo (modification ou suppression de caméra, ...)

- **Journaux des déconnexions caméras**

  Retrace tous les évènements liés aux connexions et déconnexions des caméras

- **Journaux du système (VXCORE)**

  Retrace tous les évènements liés au fonctionnement du système vidéo (services, serveur externes, haute disponibilité, erreurs, avertissements, etc).

- **Journaux du système (Linux)**

  Donne accès au journal physique du système Linux (journalctrl), qui retrace tous les évènements du système d'exploitation Linux

- **Journaux du noyau (Linux)**

  Donne accès au journal physique du noyau Linux (dmesg), qui retrace tous les messages liées au hardware

12 Gestion des erreurs

VXCORE intègre plusieurs modules de supervision systèmes, capables de détecter de multiples erreurs ou dysfonctionnements du système d'exploitation ou à la configuration vidéo.

Ces erreurs seront signalées par un message dans l'interface graphique et aussi envoyées via des alertes emails aux administrateurs.

Pour recevoir les alertes Email, il faudra configurer la partie "SMTP" qui se trouve dans le menu Administration > Réseau > SMTP. Il sera également nécessaire de renseigner une ou plusieurs adresses emails des administrateurs systèmes.

En cas d'erreur, vérifiez bien dans les journaux des services vidéo tous les messages pour investiguer et corriger les problèmes. Les journaux du système Linux ou du Kernel permettent quelque fois d'avoir des indications supplémentaires (erreurs I/O disques durs, corruptions mémoires, drivers matériels défectueux, etc).

12.1 Erreurs de licence

- **Licence non trouvée**

  La clé de licence n'a pas été installée ou elle ne correspond pas au bon matériel (une licence/numéro de série est associée à un serveur unique).

- **Problème de génération de licence**

  La licence installée ne correspond pas à la génération du système VXCORE installée. Contactez votre distributeur pour une mise à jour de licence (exemple : mise à jour version 4.x à 5.x).

- **Licence invalide ou corrompue**

  La licence installée a été déclarée invalide ou a été détournée par un revendeur ou un installateur.
  Contactez votre distributeur de toute urgence pour ne pas être poursuivi pour piratage.

- **Licence expirée**

  La licence installée a expirée et ne peut plus être utilisée (uniquement pour les licences de démo).
  Contactez votre distributeur pour une mise à jour ou une réactivation de la licence.

- **SMA expirée**

  La licence installée dispose d'une SMA expirée (maintenance logicielle), le système vidéo n'est plus suivi en terme de mise à jour de sécurité ou de fonctionnalité.
  Contactez votre distributeur pour une mise à jour de licence.

12.2 Erreurs services vidéo

- **Analyse vidéo**

  Le système a détecté que l'analyse vidéo n'est pas active sur une ou plusieurs caméras (alors que la configuration a été faite). Cela signifie que des éventuelles alarmes, des enregistrements vidéo sur détection ou encore des agents de sécurité pourraient être inopérants. Vérifiez dans le tableau de bord quelles caméras sont concernées et dans les journaux systèmes les causes (caméra déconnectée, problème flux vidéo, etc).

- **Surcharge analyse vidéo IA/DNN**

  Des images ont été perdues dans le processus d'analyse vidéo IA/DEEP LEARNING. Cela est en général dû a un mauvais dimensionnement hardware : le serveur ne peut pas assumer la quantité d'image a analyser. Pour rappel, l'analyse vidéo IA est très consommatrice en ressources et nécessite l'installation d'un GPU dans le serveur ou l'utilisation de serveurs externes pour optimiser les ressources (OS VXCORE-NODE configuré en analyse vidéo).

  Si votre système remonte trop d'erreurs de ce type, vous pouvez :

  - utiliser le réseau neuronal par défaut (et non pas le mode optimisé)
  - désactiver la détection de visages
  - réduire le nombre de caméras IA ou configurer des zones de masquages plus restrictives
  - investir dans un GPU plus performant
  - délester l'analyse vidéo IA sur des serveurs externes VXNODE

- **Enregistrement vidéo désactivé**

  Si ce message d'erreur est affiché, cela signifie que l'horloge du système n'est pas réglée correctement (cas d'un problème de pile carte mère ou de module RTC inexistant ou défectueux). Dans ce cas, le système désactivera la fonctionnalité d'enregistrement vidéo automatiquement pour éviter d'écraser des données existantes avec un horodatage faussé.

12.3 Erreurs de stockage vidéo

- **Aucun volume de stockage**

  Le volume de stockage vidéo n'a pas été configuré ou tous les LUNs vidéo sont endommagés ou absents. Dans ce cas de figure, il sera impossible d'enregistrer les caméras.

- **Volume de stockage endommagé**

  Une erreur a été détecté sur un des LUNs vidéo. Essayez de le réparer via le bouton de l'interface et consultez les logs du système Linux a la recherche d'éventuelles erreurs I/O du périphérique.
  Si le périphérique est physiquement endommagé, remplacez le, puis ré-créez un nouveau LUN vidéo.

- **LUN vidéo absent**

  Un ou plusieurs LUN vidéo n'ont pu être monté : soit les volumes sont endommagés, soit ils sont déconnectés physiquement ou alors les systèmes de fichiers sont corrompus. Redémarrer physiquement votre serveur et essayez de réparer les périphériques de stockage vidéo.

- **Surcharge en écriture (overload)**

  Le système à détecté un ralentissement inquiétant sur un ou plusieurs LUN vidéo lors de l'enregistrement et l'écriture des données vidéo. Les volumes sont trop lent ou la configuration du système vidéo est inadaptée à l'architecture (sous-dimensionnée).

- **Problème sur le RAID**

  Un ou plusieurs volumes RAID (hardware ou software) sont en état dégradé ou en erreur. Utilisez l'interface spécifique du RAID pour diagnostiquer le problème, située dans l'administration/stockage.

- **Erreur S.M.A.R.T.**

Le système a détecté une panne imminente d'un ou plusieurs disques durs compatibles avec la supervision S.M.A.R.T. Identifiez le disque défectueux dans l'interface d'administration/stockage et remplacez le.

- **Erreur d'écriture des données physiques**

  Le système ne parvient plus a écrire les données vidéo sur le volume de stockage. Cette erreur peut survenir dans le cas d'une corruption des systèmes des fichiers ou d'un blocage d'une carte contrôleur. Redémarrer physiquement votre serveur et essayez de réparer les périphériques de stockage vidéo.

- **Erreur stockage vidéo persistant**

  Si ce message est affiché, cela signifie que le système utilise un volume de stockage vidéo mémoire RAM, et donc que les données enregistrées seront perdues en cas de coupure de courant ou de redémarrage du serveur. Lorsqu'aucun volume vidéo physique n'a été configuré, le système va créer un volume de stockage vidéo virtuel en utilisant une partie de la mémoire RAM disponible. Cette fonctionnalité permettra de disposer d'un système vidéo opérationnel, avec toutes les fonctionnalités d'enregistrements vidéo, les alarmes ou encore la recherche intelligente.

12.4 Erreurs systèmes

- **Système corrompu / intégrité non vérifiée**

  L'image système/OS semble avoir été corrompue avec une tentative d'attaque/intrusion externe. Vous devez restaurer le système en démarrant sur le Kernel Fallback ou réinstaller le serveur.

- **Base vidéo endommagée**

  La base de données vidéo est endommagée, le fichiers vidéo ne peuvent plus y être indexés. Essayez de réparer la base de données en utilisant le bouton situé dans la section administration/maintenance

- **Surcharge du système**

  Le système à détecté une charge active trop importante et a interrompu automatiquement ses processus internes pour éviter une casse du matériel ou des pertes de données irréversibles. Les surcharges peuvent être liées à une mauvaise configuration du système vidéo ou des problèmes hardware.

- **Problème d'horloge matérielle**

  Le système n'arrive pas à accéder ou à mettre à jour l'horloge matérielle du serveur. En cas de coupure de courant ou de redémarrage du serveur, l'heure sera déréglée. Vérifiez la compatibilité de votre carte mère avec le système Linux ou installez une version plus récente de l'OS VXCORE.

- **Manque de mémoire (RAM)**

  Le système a détecté un dimensionnement insuffisant de la mémoire physique du serveur par rapport à la configuration vidéo (nombre de caméras, détection de mouvement, ...). Augmentez la mémoire physique en vous référant aux pré-requis technique disponibles dans la documentation d'installation du système.

- **Erreur de noyau Linux**

  Le système a détecté un problème dans les journaux du noyau Linux. Cette erreur peut identifier un problème de compatibilité hardware ou software de votre matériel. Vérifiez la compatibilité de votre matériel avec le système Linux ou installez une version plus récente du système.

- **Erreur d'espace disque des partitions systèmes**

  Une ou plusieurs partitions systèmes sont anormalement pleines. Cette erreur peut arriver sur les systèmes de plusieurs centaines de caméras, ou la base de données et la gestion du système occuperont plus d'espace disque. Pour éviter cela, choisissez bien le dimensionnement lors de l'installation du système : mode normal (NVR < 50 caméras) ou mode large (NVR > 50 caméras ou serveur de centralisation).
  Vous trouverez plus de détails dans la documentation d'installation du système.

- **Erreur d'espace disque mémoire virtuelle**

  La mémoire virtuelle de synchronisation des flux vidéo arrive presque à saturation, le proxy vidéo peut rencontrer des erreurs. Augmentez le cache d'écriture du volume de stockage pour étendre l'espace de la mémoire virtuelle tampon.

- **Erreur certificat SSL**

  Le système préviendra de l’expiration proche du certificat SSL installé dans le serveur (90 jours). Si le système utilise son propre certificat Interne, il sera automatiquement renouvelé et vous ne devriez jamais voir ce message (sauf en cas de problème). Si vous utilisez votre propre certificat SSL, il sera nécessaire de réimporter une nouvelle version du certificat dans le serveur. Dès que la date du certificat SSL aura expiré, le système l’indiquera avec un message d’erreur dans l’interface.

- **Erreur serveurs externes déconnectés**

  Cette erreur sera affichée si vous avez coché la supervision d’un ou plusieurs serveurs externes, et qu’ils sont en état déconnectés.

- **Erreur haute disponibilité**

  La configuration haute disponibilité rencontre une erreur, vous devez vérifier l’état et la connectivité des deux serveurs (primaire et secondaire). Vous trouverez tous les détails des erreurs haute disponibilité dans les journaux systèmes de chaque serveur.