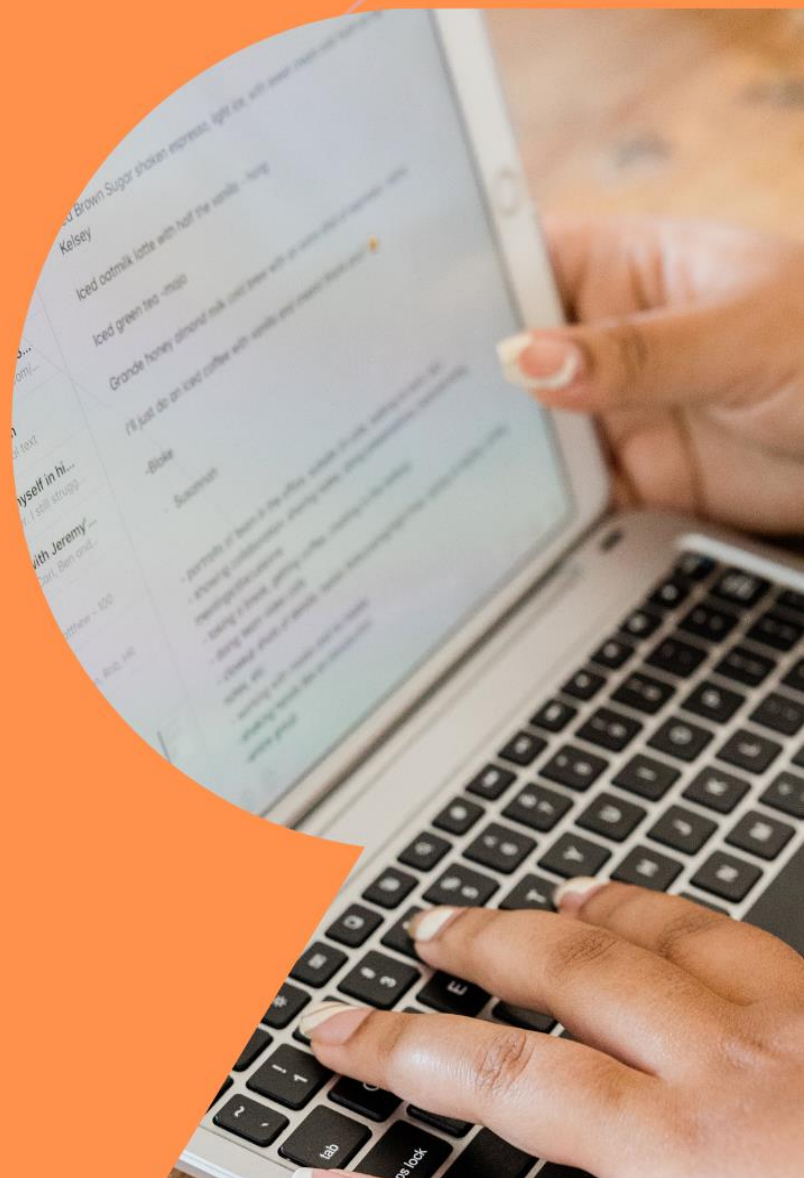


# Epreuve E5

## BTS SIO Session 2022 parcour SISR

Sécurisation d'un server  
NAS Qnap ts-231P

PRÉSENTÉ PAR  
Sandy Cerrato



ÉPREUVE E5 : CONCEPTION ET MAINTENANCE DE SOLUTIONS INFORMATIQUES  
**PROJET ENCADRÉ 2**

NOM PRENOM <b>Cerrato Sandy</b>	N° CANDIDAT <b>02145641463</b>	PARCOURS <b>SISR</b>
------------------------------------	-----------------------------------	-------------------------

**Augmentation du niveau de sécurité du server NAS**

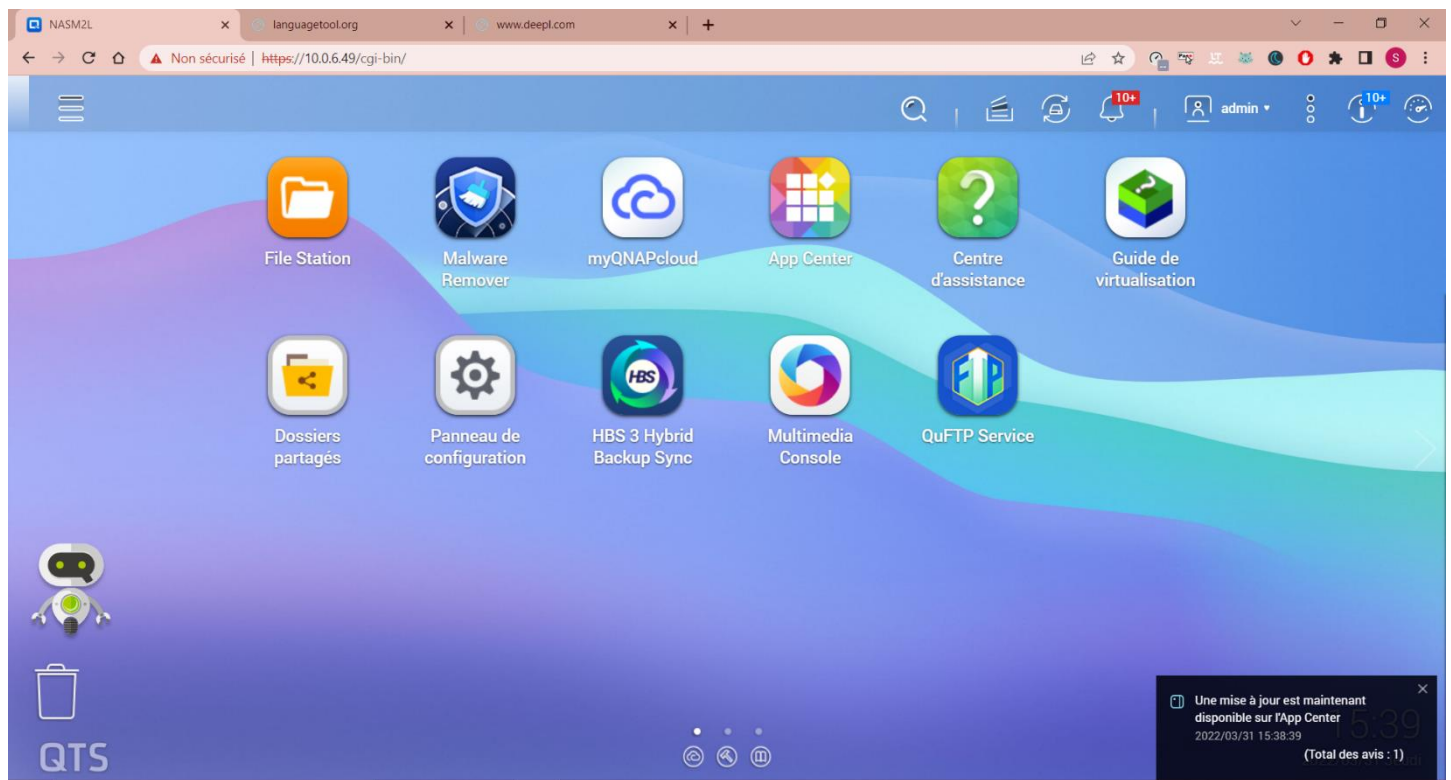
<b>ÉPREUVE</b>	<input checked="" type="radio"/> Épreuve ponctuelle <input type="radio"/> Contrôle en cours de formation			
<b>MODALITÉS DE RÉALISATION</b>	CONTEXTE BASÉ SUR LE CONTEXTE GÉNÉRAL DE LA : <b>M2L</b> MAISON DES LIGUES DE LORRAINE			
<b>CONTEXTE GÉNÉRAL</b>	<b>PÉRIODE</b>	Quatrième semestre	<b>DURÉE ESTIMÉE</b>	16 heures
<b>DESCRIPTION DE LA MISSION</b> - <b>DESCRIPTION DES BESOINS</b> - <b>RÉSULTATS ATTENDUS</b>	Etudes des dispositions qui permettent de sécuriser le server NAS Rédaction d'un memento avec niveau d'importance Administration du server NAS Sauvegarde.			
<b>RESSOURCES MOBILISÉES</b>	<ul style="list-style-type: none"> <li>➤ Server Nas QNAP TS-321P</li> <li>➤ PC utilisateur windows 10</li> <li>➤ Protocole HTTPS</li> </ul>			
<b>COMPETENCES MOBILISÉS</b>	<ul style="list-style-type: none"> <li>➤ Recenser et identifier les ressources numérique</li> <li>➤ Mettre en place et vérifier les niveaux d'habilitation associés à un service</li> <li>➤ Vérifier les conditions de la continuité d'un service informatique.</li> <li>➤ Traiter des demandes concernant les services réseau et système, applicatifs</li> <li>➤ Réaliser les tests d'intégration et d'acceptation d'un service</li> <li>➤ Déployer un service</li> </ul>			
<b>PRODUCTION ASSOCIÉES</b>	Synoptique recto/verso, 7 annexes descriptives + Screenshot , Memento			
<b>MODALITÉS D'ACCÈS AUX PRODUCTIONS EN LIGNE</b>	<a href="https://sandy-cerrato.herokuapp.com/">https://sandy-cerrato.herokuapp.com/</a>			

## RAPPORT D'ACTIVITE

<b>ETAPE 1</b>	Création de l'environnement de travail, définitions des objectifs		
<b>OBJECTIF(S)</b>	Avoir un environnement de travail fonctionnel et une vision clair de la marche à suivre		
<b>RESSOURCE(S)</b>	Connexion à l'interface NAS vérification de sa santé général		
<b>CHRONOLOGIE DE RÉALISATION</b>	<ul style="list-style-type: none"> <li>➤ Analyse du niveau de sécurité du Server NAS</li> <li>➤ Disposition applicable</li> <li>➤ Rédaction memento</li> <li>➤ Back-up</li> </ul>		
<b>ETAPE 2</b>	Analyse de la politique de sécurité		
<b>OBJECTIF(S)</b>	Etude des dispositifs de sécurité déjà présent		
<b>RESSOURCE(S)</b>	Interface NAS Réglages et sécurité		
<b>CHRONOLOGIE DE RÉALISATION</b>	<ul style="list-style-type: none"> <li>➤ Etude des droits et privilèges des utilisateurs</li> <li>➤ Etude de la sécurité des comptes</li> <li>➤ Etudes des protocole en place</li> </ul>		
<b>ETAPE 3</b>	Dispositif applicable		
<b>OBJECTIF(S)</b>	Mettre en lumière les amélioration applicable en termes de sécurité du NAS		
<b>RESSOURCE(S)</b>	Tableau de bord		
<b>CHRONOLOGIE DE RÉALISATION</b>	<ul style="list-style-type: none"> <li>➤ Mise à jour</li> <li>➤ Malware remover analyse</li> <li>➤ Certificat a jour</li> <li>➤ Double authentification</li> <li>➤ Fail to ban</li> <li>➤ Suppression de protocole non sécuriser</li> <li>➤ Déconnexion automatique</li> <li>➤ Renforcement de la politique des mot de passe</li> <li>➤ fourchette IP</li> <li>➤ Analyse programmé</li> <li>➤ Quarantaine en cas d'infection d'un dossier</li> <li>➤ Black-list</li> <li>➤ Autoprotection du NAS</li> <li>➤ Back up</li> </ul>		
<b>ETAPE 4</b>	Rédaction du memento0		
<b>OBJECTIF(S)</b>	Fournir une solution détaillé de la réalisation du projet		
<b>RESSOURCE(S)</b>	Word et interface du NAS		
<b>CHRONOLOGIE DE RÉALISATION</b>	<ul style="list-style-type: none"> <li>➤ Création du document Word</li> <li>➤ Insertion des screen shot et explication</li> <li>➤ Classement du niveau d'importance de chacun des éléments</li> <li>➤ Rédaction et mise au propre</li> </ul>		
<b>ETAPE 5</b>	Back up		
<b>OBJECTIF(S)</b>	Réaliser une sauvegarde la configuration		
<b>RESSOURCE(S)</b>	pc, Server NAS		
<b>CHRONOLOGIE DE RÉALISATION</b>	<ul style="list-style-type: none"> <li>➤ Panneau de contrôle</li> <li>➤ Système</li> <li>➤ Sauvegarde</li> <li>➤ Dossier back up dédié</li> </ul>		



« 1 - 2 - 3 » Ces numéros ajoutés à coter de chaque capture d'écran correspondent au niveau d'importances de chacune des propositions.  
1 étant la moins importantes et 3 la plus importantes.



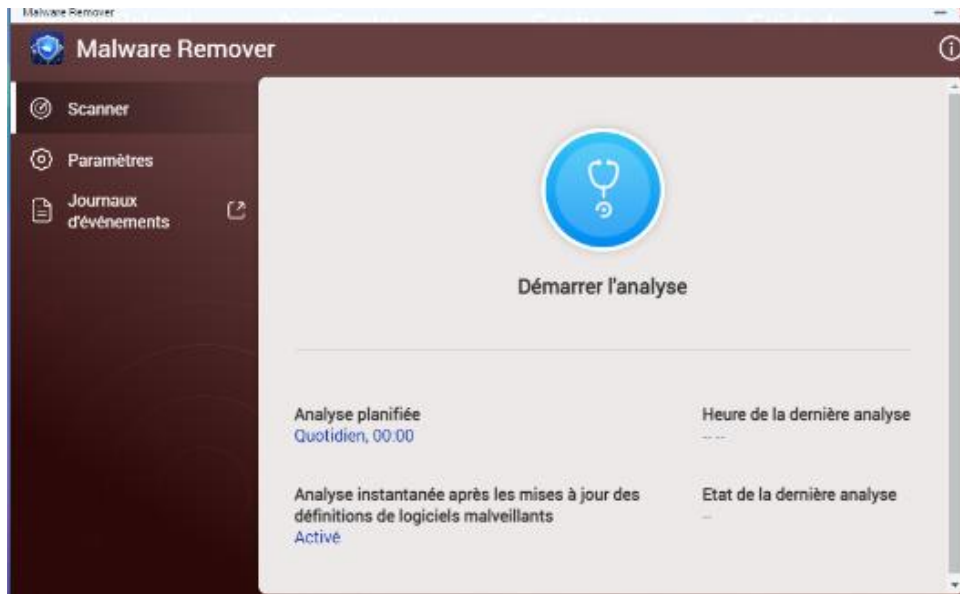
## Présentation de l'interface de notre NAS QNAP TS-231P

Pour me connecter j'utilise le navigateur chrome puis je rentre le protocole https suivie de l'IP du NAS.

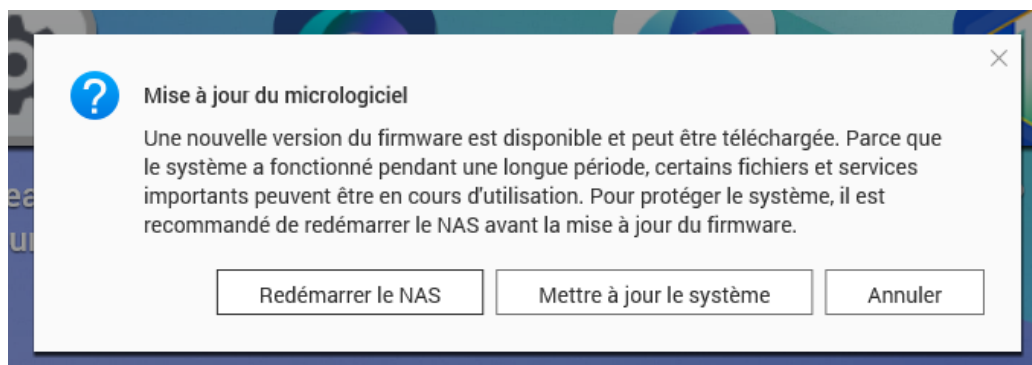
L'interface est très graphique ce qui rend son utilisation accessible.

Le NAS est lié au domaine de la M2L.

## Analyse et mise à jour



Analyse du matériel avec Malware Remover afin de scanner l'équipement et s'assurer qu'il soit sains. **2**



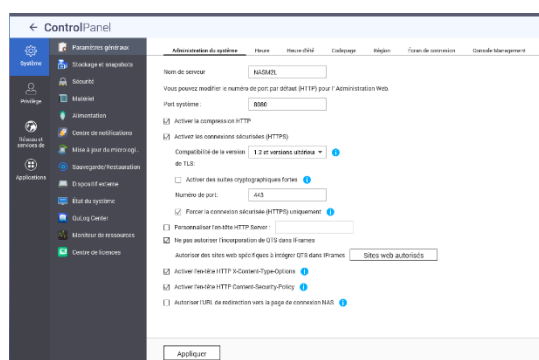
Vérifier si l'équipement est à jour, si non, lancer la mise à jour afin d'apporter d'éventuel correctif. **3**

## Administration à distance d'un NAS QNAP

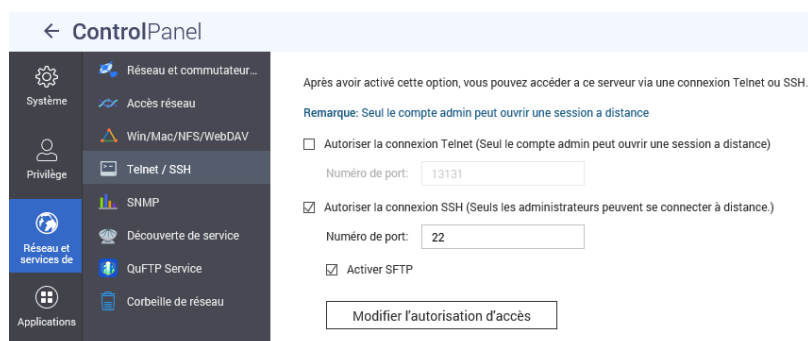


Vérification des certificats SSL et de leurs validité.

Les certificats SSL sont très important car c'est ce qui sécurise l'interface web ils sont indiqués par le petit cadenas en haut à gauche de l'adresse web. 3

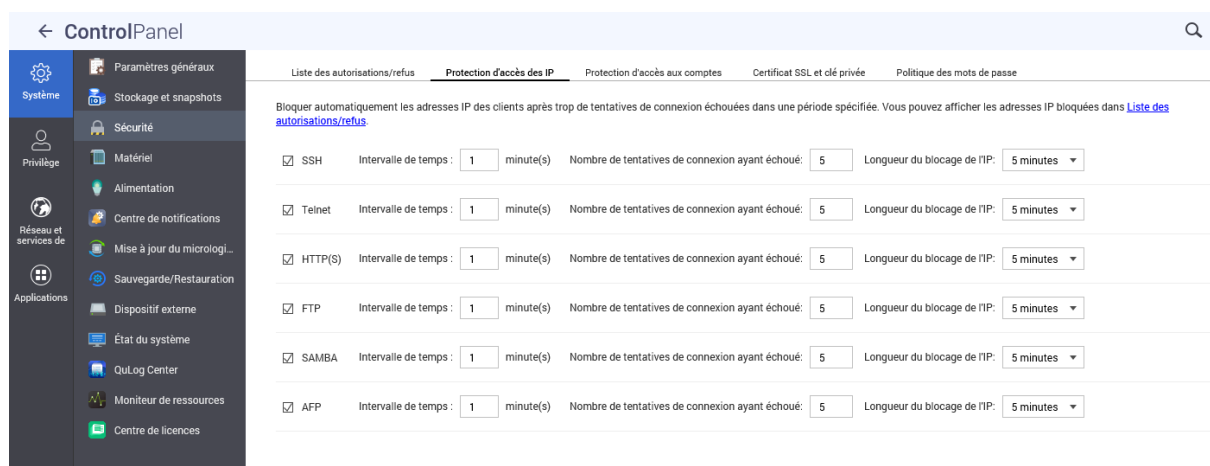


Modifier le numéro de ports http et activer les connexions sécuriser via https. 3

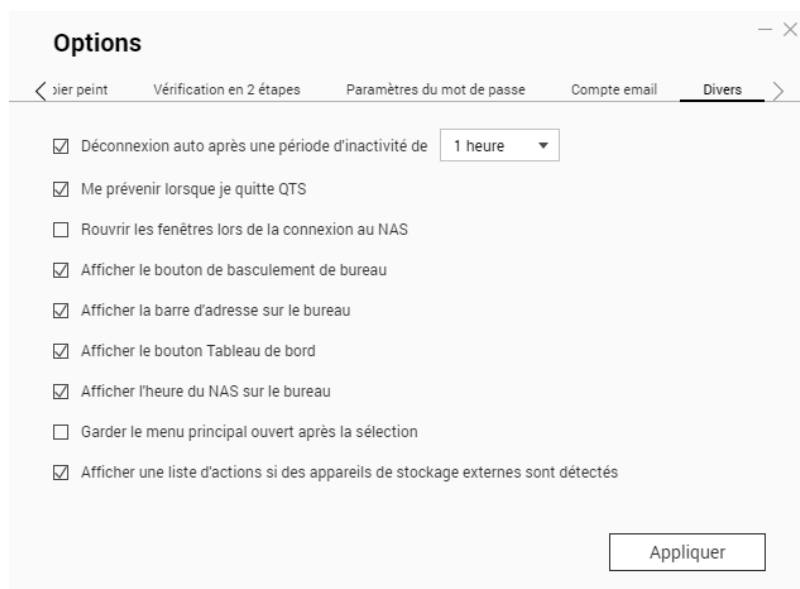


Bannir la connexion via le protocole Telnet car non chiffré et privilégier la connexion SSH chiffré de bout en bout. 3

## Sécurisation de l'accès au NAS

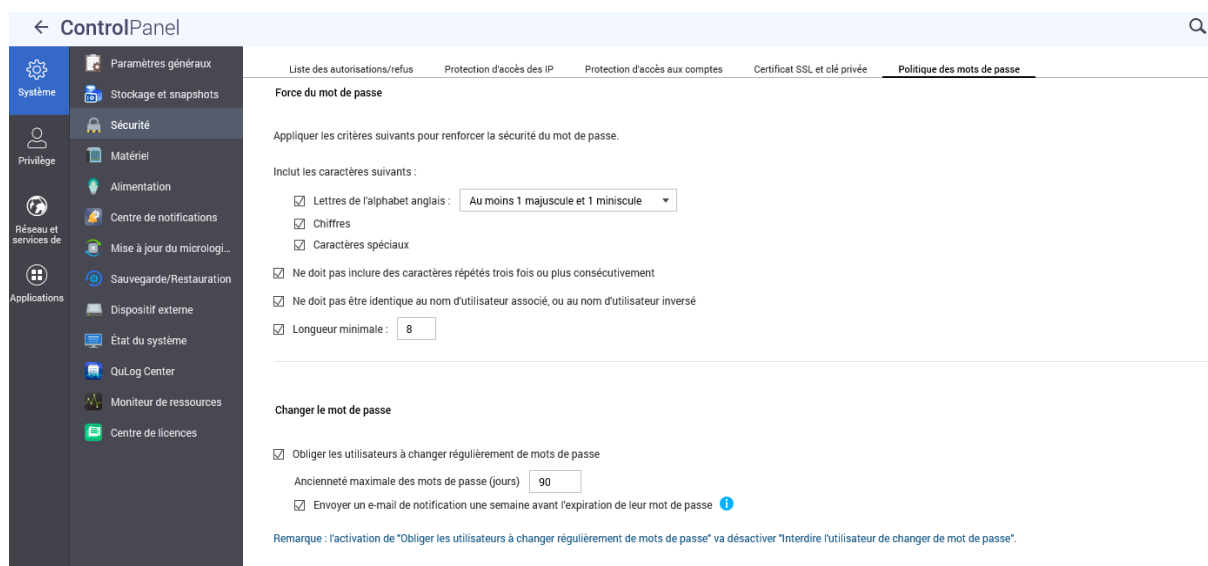


Fail to ban activé sur tous les protocoles proposés pour limiter au maximum les tentatives de connexions par force brute ou par dictionnaire via des bots. **1**

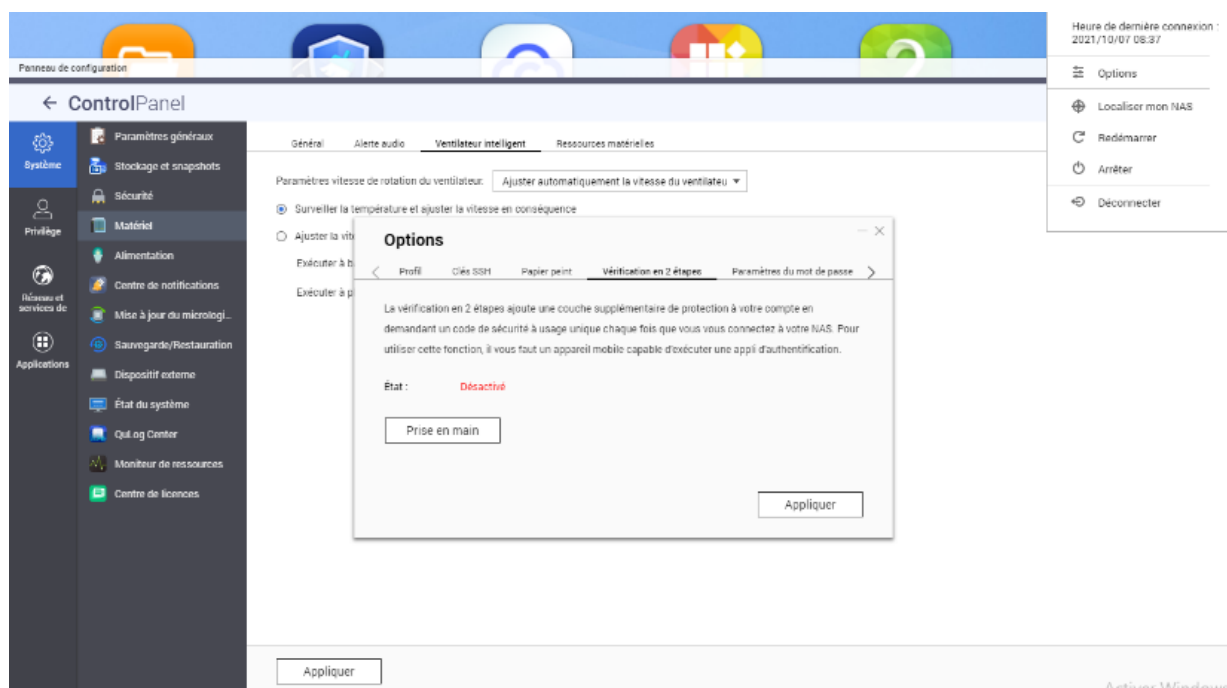


Mise en place de la déconnexion automatique après une période d'inactivité d'une heure, utile en cas de perte ou de vol de matériel avec une session ouverte dessus. **1**

## Politique des mots de passes



Renforcer l'exigence des mots de passes, obligé l'utilisateur à changer son mot de passe tous les 90 jours maximum . 3



Mise en place de l'authentification en 2 temps. 2



## Filtrage d'ip

← ControlPanel

Système

Privilège

Réseau et services de

Applications

Serveur multimédia DLNA

Multimédia Console

Serveur Web

Serveur LDAP

MariaDB

Serveur Syslog

Antivirus

Serveur RADIUS

Serveur TFTP

Serveur NTP

☒ Activer serveur TFTP

Port UDP:

Vous devez spécifier un répertoire racine pour le serveur TFTP:

Répertoire racine:

☒ Activer journal TFTP

Le(s) fichier(s) journal(ux) sera/seront sauvegardé(s) dans le dossier sélectionné. Si la taille d'un fichier journal est supérieure à 1 Mo, le fichier sera archivé automatiquement.

Sauvegarder les fichiers journaux dans:

Droits d'accès:

Activer l'accès TFTP depuis:

☐ N'importe où

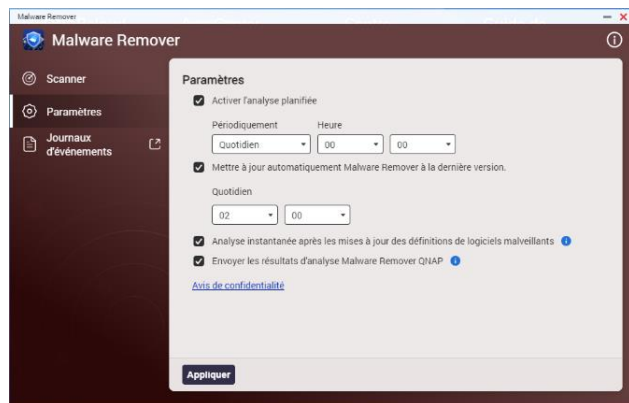
☒ Une certaine fourchette d'IP seulement

Adresse IP de début:

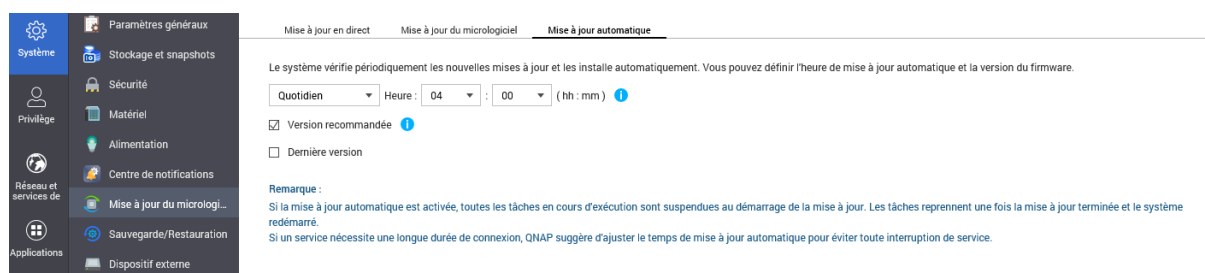
Adresse IP de fin:

White List permet de définir une plage d'IP qui sera autorisé à se connecter sur le Nas . 2

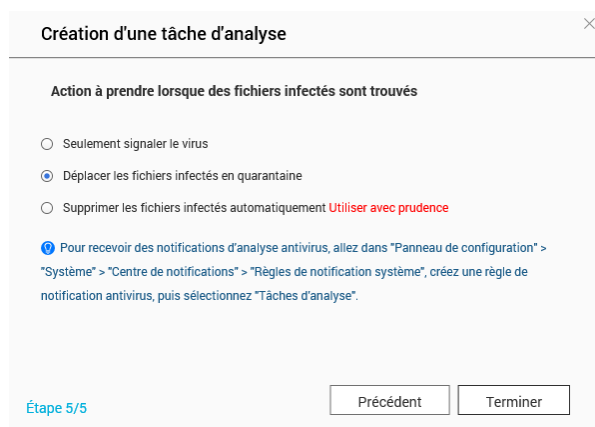
## Mise à jour création des scan programmé et mise en quarantaine des malwares



### Scan programmé de Malware Remover (quotidien) 2



### Mise à jour quotidienne du NAS automatique. 3



### Création d'une tâche d'analyse pour chercher d'éventuel virus et le cas échéant les mettre en quarantaine. 3

## Sécurité matériel et back-up

Le système va entrer en mode «\*auto-protection (protection auto)» lorsque l'alimentation CA est interrompue pendant

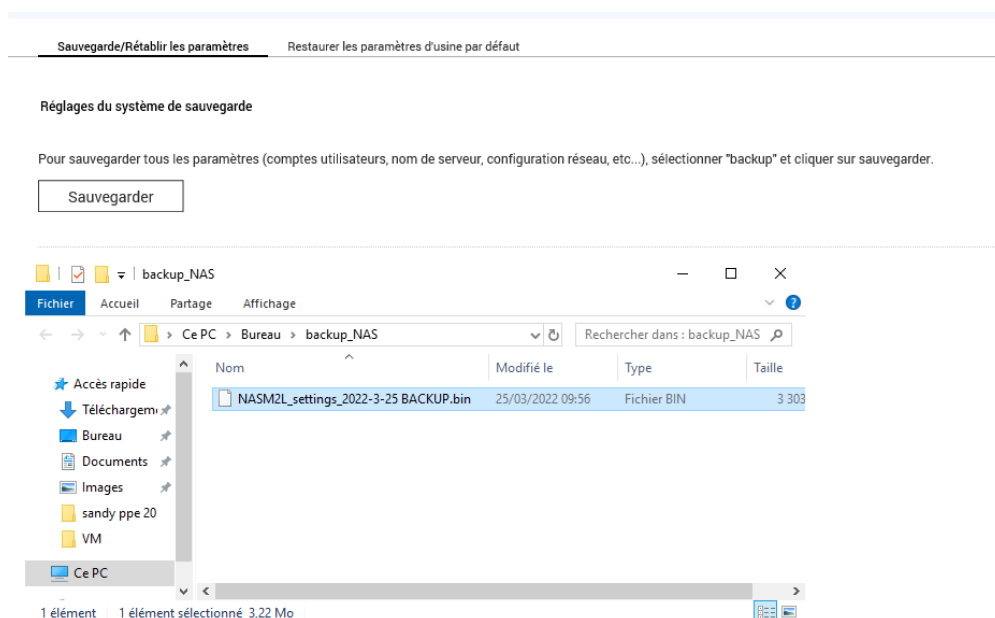
minute(s):

2

\*Auto-protection : Le NAS va interrompre tous les services exécutés et démonter tous les volumes pour protéger vos données. Lorsque l'alimentation revient, le NAS redémarre et reprend l'état qu'il a interrompu.

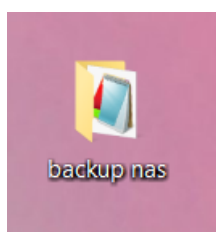
Mesure supplémentaire en cas de coupure électrique.

Ceci dit cela concerne d'avantage la sauvegarde des données que de la protection de celles-ci. **1**



Mise en place d'un backup de la configuration et création d'un dossier dédié pour celui-ci.

En cas de perte de la configuration ou de remplacement du matériels elle pourra être à nouveau injecté. **3**



## Mémento

Sécuriser un Sever Nas dans une organisation est un point stratégique primordiale.

En effet de nombreuses données sensible et importante sont stockés à l'intérieur, ce qui nécessite une politique de sécurité strict et régulièrement vérifié.

Par nature un NAS est un Server de stockage de données partagé ce qui implique que des utilisateurs y ont accès via des connexions depuis leurs pc.

Ils sont parfois client fixe ou bien nomades ce qui démultipliés les risques.

Afin de lutter au mieux contre les risque cités plus haut je vous invite à prendre toutes les mesures nécessaires que je vous ai présentés.

Les moyens informatiques, devenus essentiels à la qualité des services, se trouvent confrontés à des sources de menaces qui croissent en nature et en nombre. Cette informatisation rapide nécessite de tenir compte de nouveaux risques par rapport aux systèmes d'information papier. De nombreux exemples ont récemment mis en lumière ces menaces et la fragilité de moyens informatiques insuffisamment protégés :

- Certains virus détruisent très rapidement des volumes considérables de données ou mettent hors-service un ordinateur. Ces situations conduisent parfois à devoir réinstaller tout le parc informatique et à reconstituer les données, et ce avec un coût élevé pour un résultat souvent très partiel.

- Les vols de matériels informatiques se multiplient et conduisent trop souvent à la perte de volumes conséquents de données de santé. Les conséquences financières, de temps passé et de gêne professionnelle sont élevées et très comparables à celles évoquées dans le point précédent.

- Des altérations (effacement par erreur, modifications indues...) de données, parfois essentielles aux professionnels, se produisent régulièrement, par exemple dans le cas de suivi à partir d'informations issues de dispositifs implantés. Elles peuvent impacter très significativement la qualité du suivi des besoins et des données clients

- Des dossiers privée peuvent se retrouver accessibles sur Internet, par de simples requêtes à travers des moteurs de recherche tels que Google, Yahoo, Bing... Ils sont souvent publiés sur Internet soit par erreur, soit après avoir été confié à des fournisseurs de services d'hébergement de données dont la sécurité est défectueuse

Adhérer à la démarche sécurité permet de prévenir les incidents liés aux moyens informatiques et de limiter leurs impacts sur les données qu'ils peuvent contenir. Les menaces qui pèsent sur les moyens informatiques sont de nature technique, organisationnelle ou humaine. Elles peuvent résulter d'une volonté manifeste ou être fortuites

