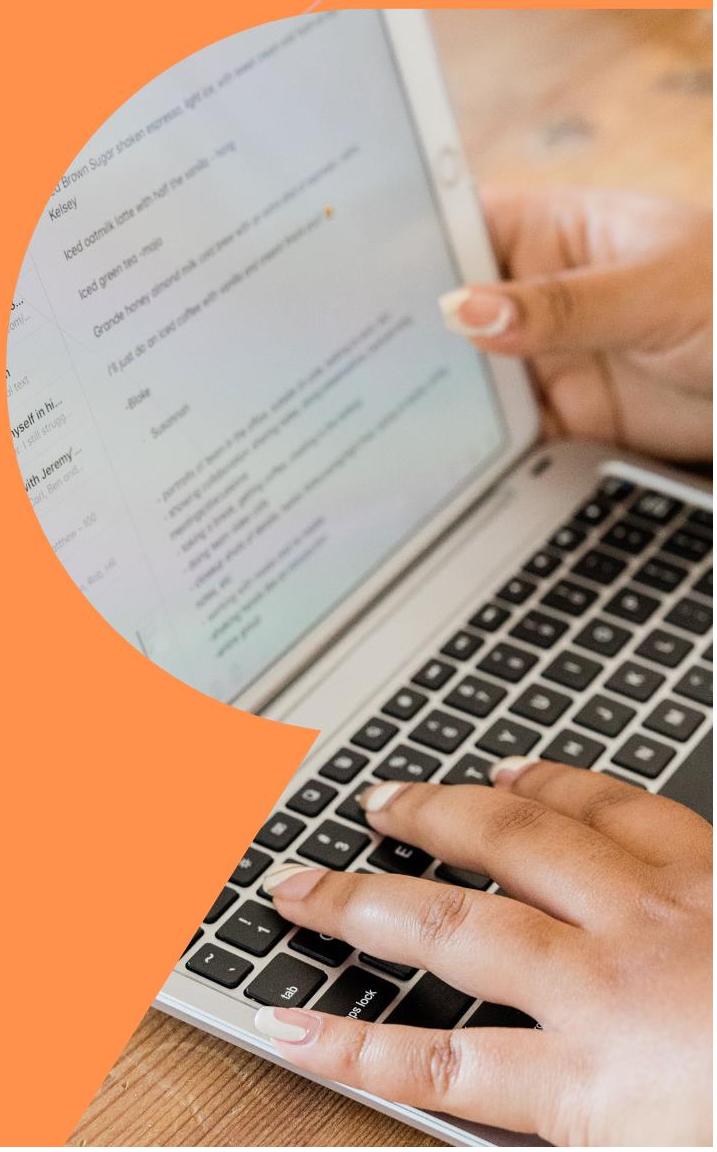
Epreuve E5

BTS SIO Session 2022

parcour SISR

Sécurisation d'un server
NAS Qnap ts-231P



PRÉSENTÉ PAR
Sandy Cerrato

2022

ÉPREUVE E4 : CONCEPTION ET MAINTENANCE DE SOLUTIONS INFORMATIQUES

PROJET PERSONNALISÉ ENCADRÉ

NOM PRENOM	N° CANDIDAT	PARCOURS
Cerrato Sandy		SISR

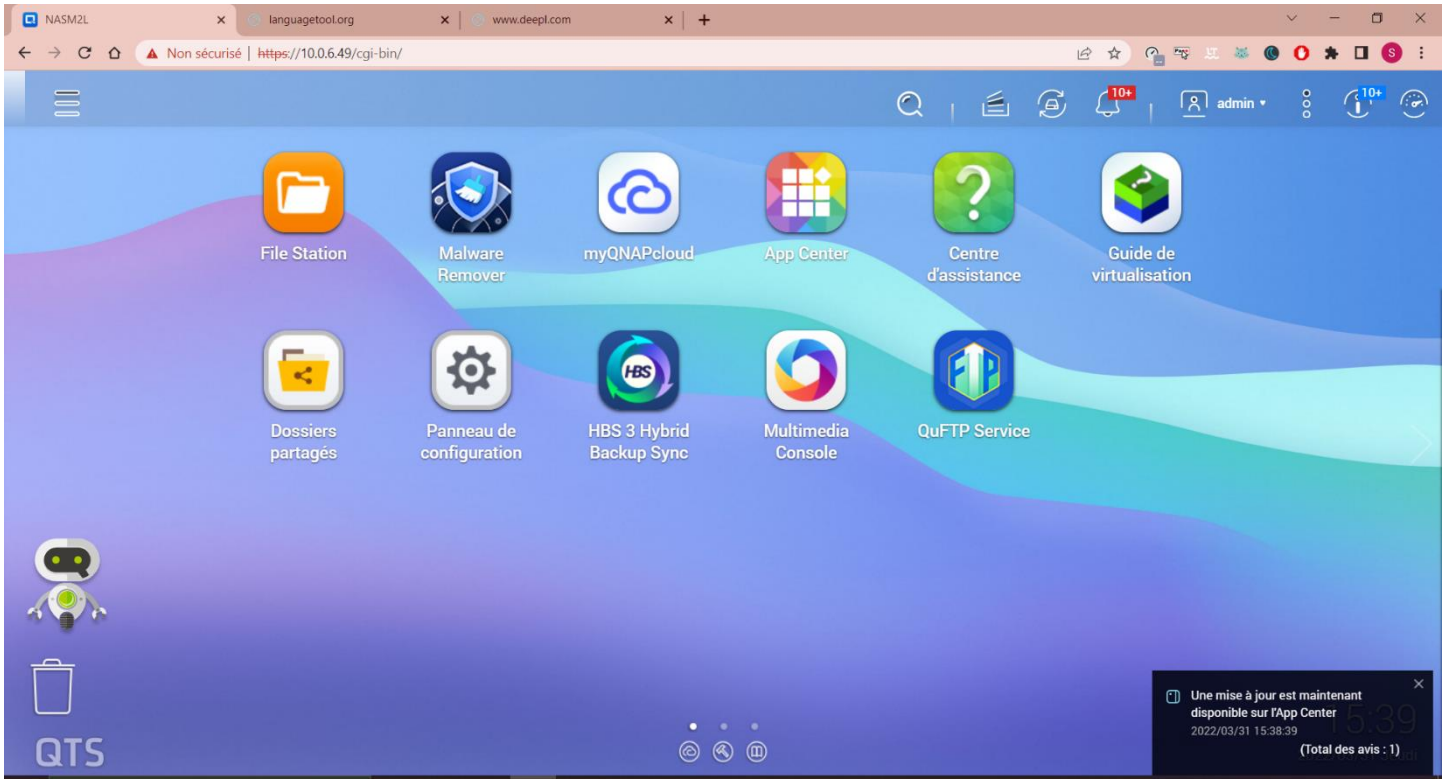
Augmentation du niveau de sécurité du server NAS

ÉPREUVE	⊗ Épreuve ponctuelle ◯ Contrôle en cours de formation			
MODALITÉS DE RÉALISATION	CONTEXTE BASÉ SUR LE CONTEXTE GÉNÉRAL DE LA : **M2L** MAISON DES LIGUES DE LORRAINE			
CONTEXTE GÉNÉRAL	**PÉRIODE**		**DURÉE ESTIMÉE**	
DESCRIPTION DE LA MISSION - DESCRIPTION DES BESOINS - RÉSULTATS ATTENDUS	Etudes des dispositions qui permettent de sécuriser le server NAS Rédaction d'un memento avec niveau d'importance Administration du server NAS Sauvegarde.			
RESSOURCES MOBILISÉES	➢ Server Nas QNAP TS-321P ➢ PC utilisateur windows 10 ➢ Protocole HHTPS			
PRINCIPAUX SAVOIR-FAIRE MOBILISÉS	➢ Gestion du patrimoine informatique. ➢ Gestion des sauvegardes. ➢ Étude des exigences liées à la qualité attendue d'un service ➢ Exploitation du référentiel. ➢ Déployer un service. ➢ Mise en place et vérification des niveaux d'habilitations ➢ Planification des sauvegardes et gestion des restauration ➢ Rédaction d'une documentation technique			
PRODUCTION ASSOCIÉES	Synoptique recto/verso, 7 annexes descriptives + screenshot , Mémento			
MODALITÉS D'ACCÈS AUX PRODUCTIONS EN LIGNE	https://editor.wix.com/website/builder?storyId=36572732-69f7-4d56-b7f2-05f02707d30b#!/builder/story/36572732-69f7-4d56-b7f2-05f02707d30b:c0b04378-533d-4a86-97e3-601082e95b9b			

RAPPORT D'ACTIVITE

ETAPE 1	Création de l'environnement de travail, définitions des objectifs		
OBJECTIF(S)	Avoir un environnement de travail fonctionnel et une vision clair de la marche a suivre		
RESSOURCE(S)	Connexion à l'interface NAS vérification de sa santé général		
CHRONOLOGIE DE RÉALISATION	➢ Analyse du niveau de sécurité du Server NAS ➢ Disposition applicable ➢ Rédaction mémento ➢ Back-up		
ETAPE 2	Analyse de la politique de sécurité		
OBJECTIF(S)	Etude des dispositifs de sécurité déjà présent		
RESSOURCE(S)	Interface NAS Réglages et sécurité		
CHRONOLOGIE DE RÉALISATION	➢ Etude des droits et privilèges des utilisateurs ➢ Etude de la sécurité des comptes ➢ Etudes des protocole en place		
ETAPE 3	Dispositif applicable		
OBJECTIF(S)	Mettre en lumière les amélioration applicable en termes de sécurité du NAS		
RESSOURCE(S)	Tableau de bord		
CHRONOLOGIE DE RÉALISATION	➢ Mise à jour ➢ Malware remover analyse ➢ Certificat a jour ➢ Double authentification ➢ Fail to ban ➢ Suppression de protocole non sécuriser ➢ Déconnexion automatique ➢ Renforcement de la politique des mot de passe ➢ fourchette IP ➢ Analyse programmé ➢ Quarantaine en cas d'infection d'un dossier ➢ Black-list ➢ Autoprotection du NAS ➢ Back up		
ETAPE 4	Rédaction du memento0		
OBJECTIF(S)	Fournir une solution détaillé de la réalisation du projet		
RESSOURCE(S)	Word et interface du NAS		
CHRONOLOGIE DE RÉALISATION	➢ Création du document Word ➢ Insertion des screen shot et explication ➢ Classement du niveau d'importance de chacun des éléments ➢ Rédaction et mise au propre		
ETAPE 5	Back up		
OBJECTIF(S)	Réaliser une sauvegarde la configuration		
RESSOURCE(S)	pc, Server NAS		
CHRONOLOGIE DE RÉALISATION	➢ Panneau de contrôle ➢ Système ➢ Sauvegarde ➢ Dossier back up dédier		

« 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.



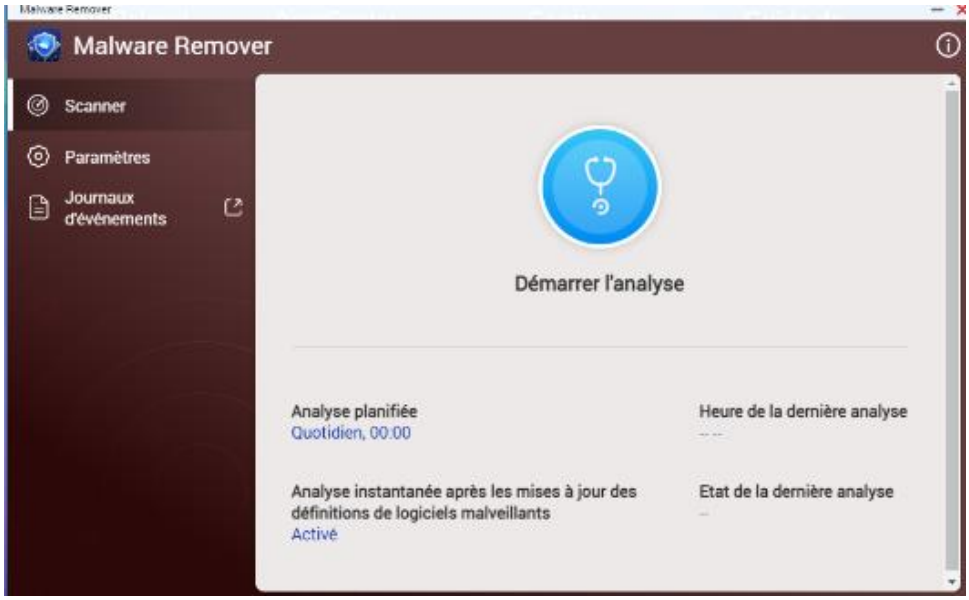
Présentation de l'interface de notre NAS QNAP TS-231P

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

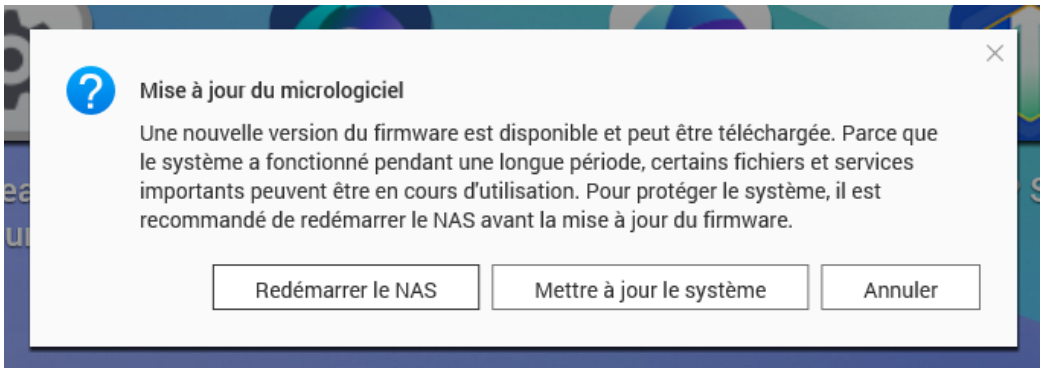
L'interface est très graphique ce qui rend son utilisation accessible.

Le NAS est lié au domaine de la M2L.

Analyse et mise a jour



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

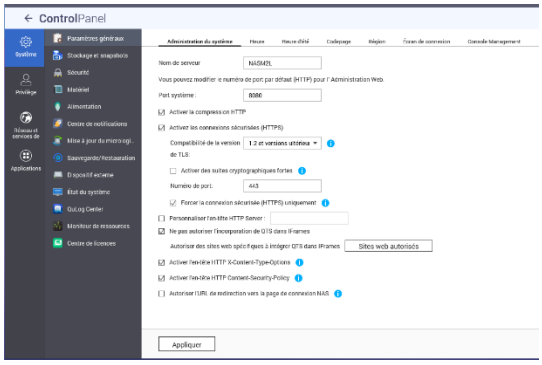


Vérifier si l'équipement est à jour , si non, lancer la mise à jour afin d'apporter d'éventuel correctif. 3

Administration à distance d'un NAS QNAP

Vérification des certificats SSL.et de leurs validité.

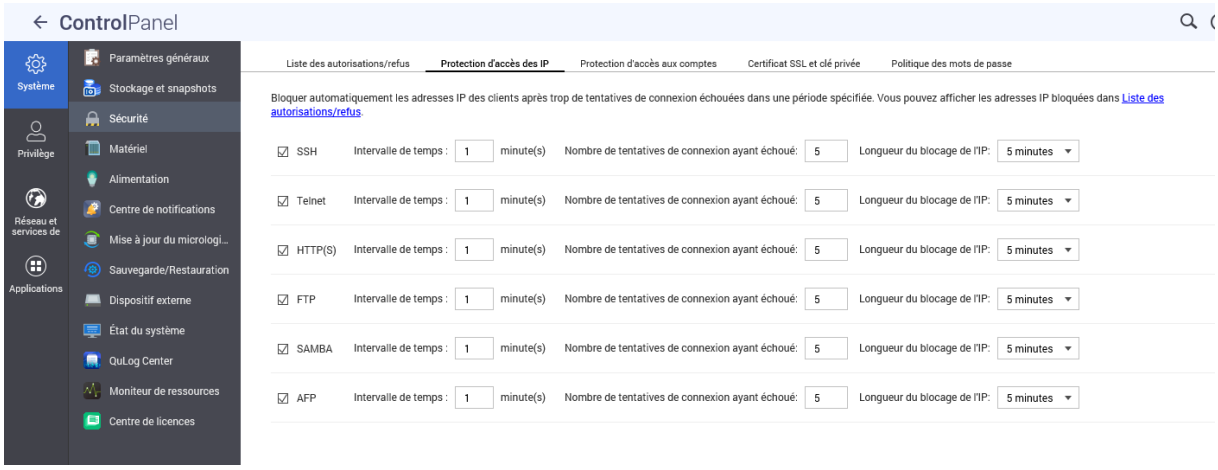
Les certificats SSL sont très important car c'est ce qui sécurise l'interface web ils sont indiqués par le petit cadenas en haut a gauche de l'adresse web. 3



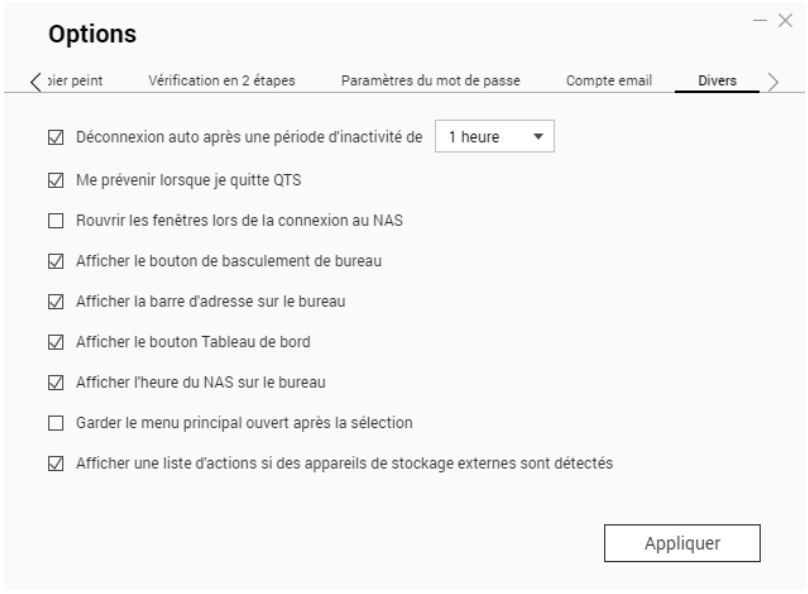
Modifier le numéro de ports http et activer les connexions sécuriser via https. 3

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

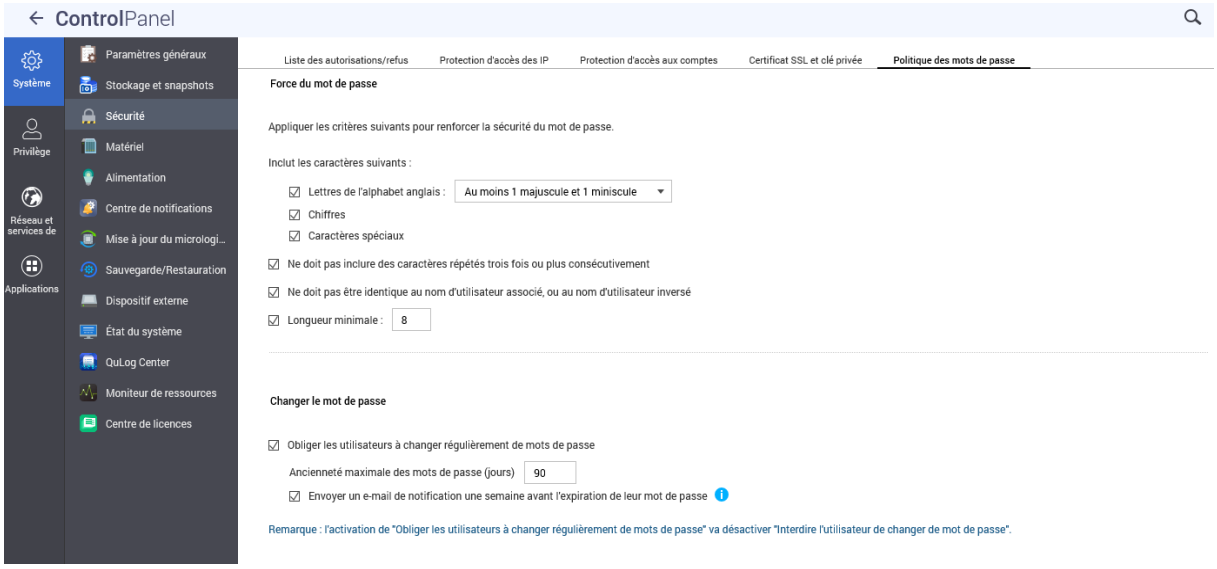


Fail to ban activé sur tous les protocoles proposés pour limiter au maximum les tentatives de connexions par force brute ou par dictionnaire via des bots. 1

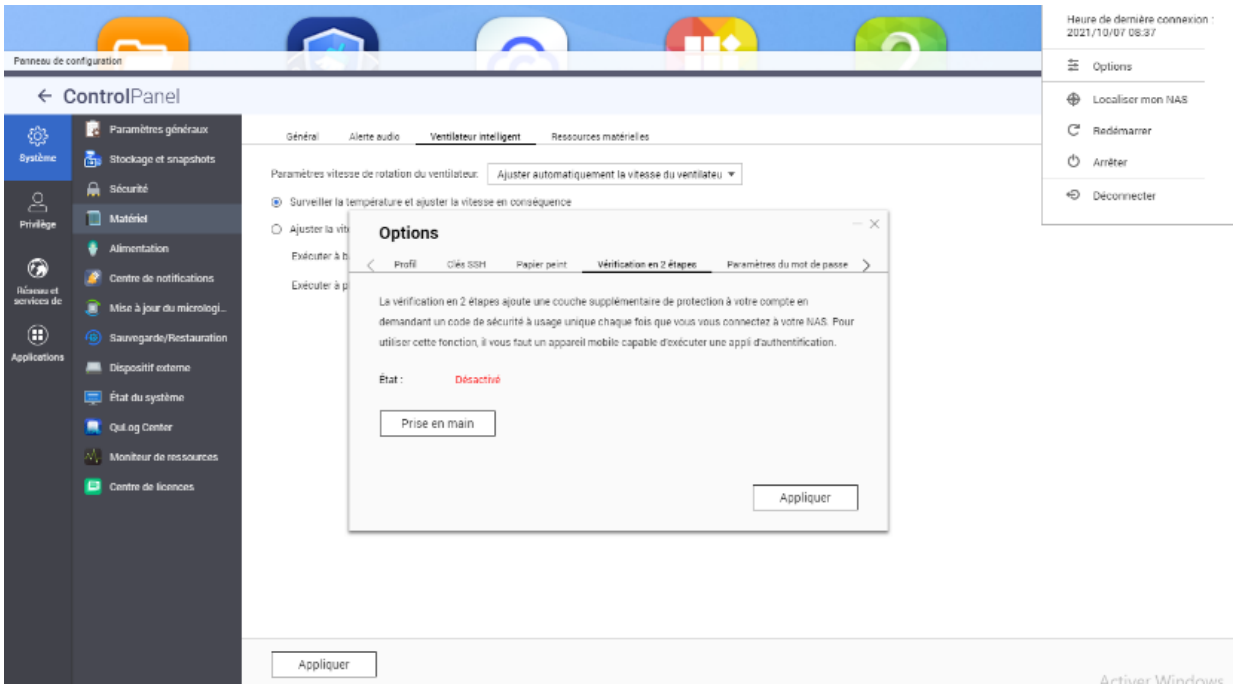


Mise en place de la déconnexion automatique après une période d'inactivité d'une heure, utile en cas de perte ou de vol de matériel avec une session ouverte dessus. 1

Politique des mots de passes

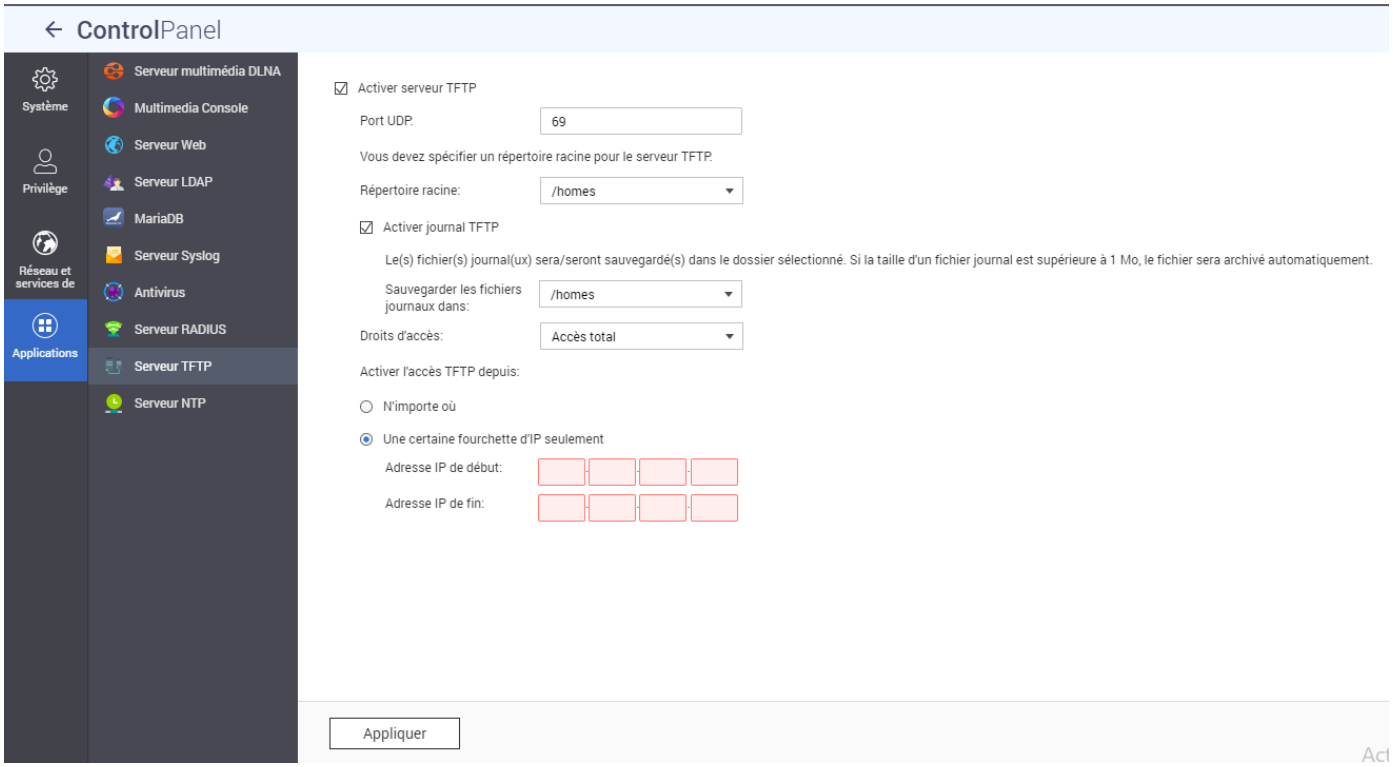


Renforcer l'exigence des mots de passes, obligé l'utilisateur à changer son mot de passe tous les 90 jours maximum . 3



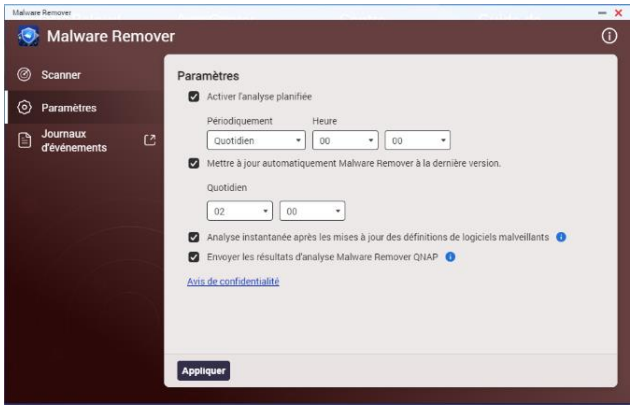
Mise en place de l'authentification en 2 temps. 2

Filtrage d'ip

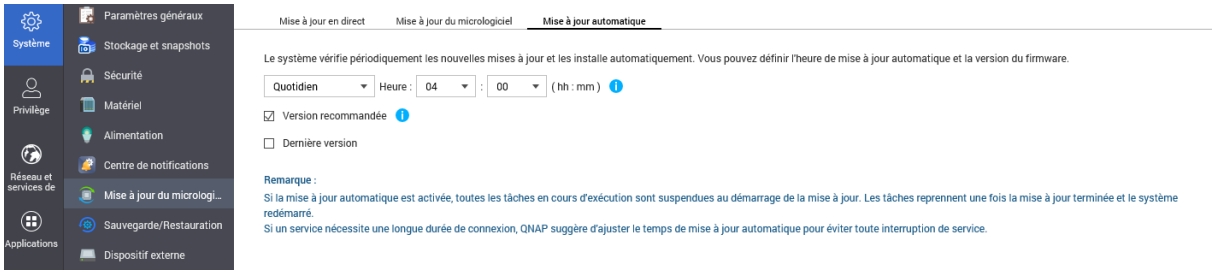


White List permet de définir une plage d'IP qui sera autorisé à se connecter sur le Nas . 2

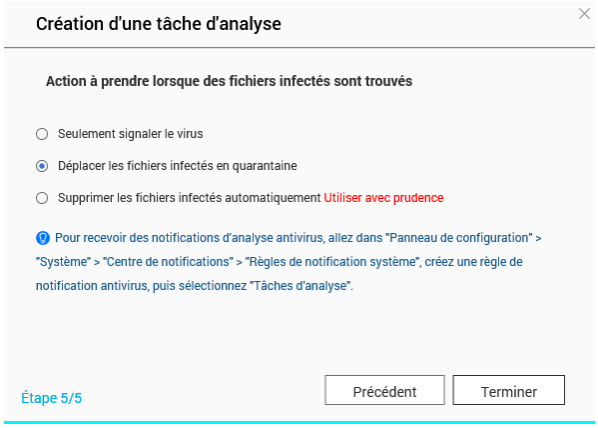
Mise à jour création des scan programmé et mise en quarantaine des malwares



Scan programmé de Malware Remover (quotidien) 2

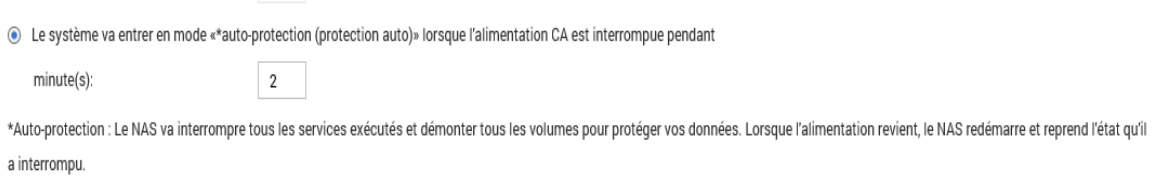


Mise à jour quotidienne du NAS automatique. 3



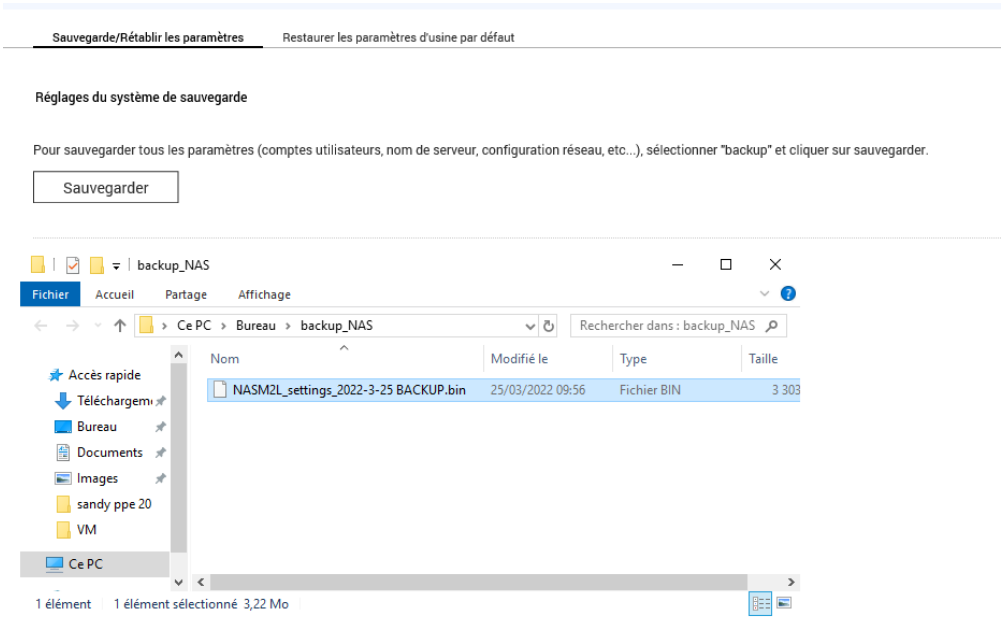
Création d'une tache d'analyse pour chercher d'éventuel virus et le cas échéant les mettre en quarantaine. 3

Sécurité matériel et back-up



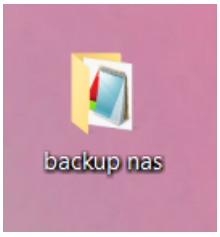
Mesure supplémentaire en cas de coupure électrique.

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 dédier 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 f nancières, 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 confier à des fournisseurs de services d'hébergement de données dont la sécurité est défaillante

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