GDPR
LIVRE BLANC

QNAP

Le nouveau Règlement européen sur la protection des données personnelles (GDPR - Règlement général sur la protection des données) : Toute l'équipe QNAP propose son soutien pour aider les Sociétés pendant et après les adaptations nécessaires afin de se conformer au Règlement.

Qu'est-ce que le GDPR ?

Le GDPR (Règlement général sur la protection des données) est le Règlement européen 2016/679 qui couvre la protection des personnes physiques à l'égard du traitement des données personnelles et de la Portabilité de celles-ci. Le présent Règlement remplace la Directive européenne sur la protection des données personnelles (Directive 95/46/EC) adoptée en 1995 et abroge les règles en conflit établies dans le Code sur la protection des données personnelles (décret législatif n°196/2003). Le Règlement a été adopté le 27 avril 2016 et sera entièrement mis en application dans les pays de l'UE à partir du 25 mai 2018 après une période de transition de deux ans et en dehors des Directives, aucune loi d'application n'est requise par les États membres.

Le GDPR vise à unifier et à normaliser, au sein de l'Union européenne, les différentes règles régissant le traitement des données à caractère personnel, déterminant de façon définitive comment les Sociétés doivent stocker, protéger et rendre accessible les données et les informations. Le GDPR s'applique aux Sociétés non UE si elles fournissent des biens ou des services à des particuliers résidant dans l'Union européenne.

Il faut souligner que les règles du GDPR sont applicables à tous et qu'il ne faut pas prévoir d'exigences spécifiques ou différentes en fonction de la taille, du type ou du secteur dans lequel la Société exerce.

Selon la Commission européenne, les données personnelles représentent toutes les informations sur un individu, relatives à sa vie privée, professionnelle ou publique. Elles peuvent concerner tout type d'informations : les noms, photos, adresses e-mail, coordonnées bancaires, messages sur des sites Web de réseaux sociaux, des dossiers médicaux ou des adresses IP d'ordinateurs.

Les étapes à effectuer : depuis le Registre des activités de traitement au Plan d'adaptation pour être en conformité

Le principal objectif du GDPR est de garantir que les données personnelles ne soient pas divulguées ; mais qu'elles soient protégées et surveillées. Les modifications introduites par le GDPR, pouvant impliquer des modifications dans la manière d'organiser les traitements, nécessitent que les sociétés planifient rigoureusement sur une période très limitée ; car le délai pour l'adaptation est désormais très proche (environ six mois).

Les sociétés doivent définir un Plan d'adaptation afin de se conformer aux exigences du GDPR. Dans cette étape, il est nécessaire d'évaluer le modèle actuel de l'organisation afin de définir un plan avec un ensemble d'actions détaillées à mettre en application dans la Société.

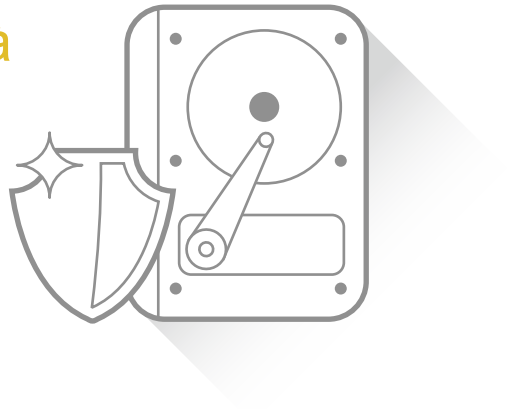
Le Plan d'adaptation, à mettre en application suite à une approche structurée, doit prendre en considération deux domaines importants dans la Technologie et l'informatique :

• Le domaine des Traitements et des règles. Ceci représente certainement l'un des domaines les plus touchés par les exigences en matière d'adaptation dans le GDPR. Par exemple la portabilité des données, la gestion des violations de données, l'enregistrement des activités de traitement et les droits des personnes concernées. La vie privée dès la conception constitue un autre aspect crucial : en d'autres termes, une nouvelle approche requise par le GDPR qui a établi l'obligation pour les sociétés de commencer un projet, en planifiant dès le début les outils pour protéger les données personnelles.

• Le domaine de la Technologie et des outils. Il s'agit d'un domaine crucial, même à envisager la budgétisation des investissements dans le Plan d'adaptation. Les mesures de sécurité informatique (antivirus, récupération après sinistre, par-feu, pseudonymisation des données, chiffrement des données, prévention et détection de la violation de données, Gestion des identités, etc.), Sécurité physique (par ex. Contrôles d'accès), adoption d'outils GRC informatiques (Gouvernance, risque et conformité).

Le GDPR établit un cadre légal axé sur les tâches et la responsabilité du Contrôleur de données. Les nouvelles règles exigent que le Contrôleur garantisse la conformité avec les principes établis dans le Règlement, et qu'il soit en mesure de prouver ladite conformité, en adoptant un certain nombre d'outils spécifiés dans le GDPR.

Comment QNAP peut vous aider à protéger vos données



Le NAS QNAP vous permet de chiffrer toutes vos données, ou tous vos dossiers individuels à l'aide du chiffrement AES 256 bits. D'autres mécanismes de protection des données comprennent les configurations RAID, les snapshots et S.M.A.R.T. (Technologie d'auto-surveillance, d'analyse et de rapport).

• Configuration RAID flexible

Le NAS QNAP prend en charge les types de RAID complets, dont le RAID 1/5/6/10/50/60 5+ échange à chaud, le 6 + échange à chaud et le 10+ échange à chaud. Vous pouvez activer la configuration RAID la plus adaptée pour réduire efficacement le risque de perte de données causé par une panne de disque dur inattendue tout en conservant des performances système optimales.

• Protection par snapshot

Les snapshots permettent à tout moment à votre NAS QNAP d'enregistrer l'état du système. Si une défaillance imprévue affecte votre système, vous pouvez restaurer son état précédent enregistré dans le snapshot. Le Gestionnaire de stockage ajoute un outil de snapshot web simple d'utilisation pour que vous puissiez sauvegarder et restaurer des données à n'importe quel point dans le temps pour empêcher la perte de données importantes.

• Vérification de la santé des disques durs avec S.M.A.R.T.

S.M.A.R.T. (Technologie d'auto-surveillance, d'analyse et de rapport) affiche l'état des disques durs installés dans le NAS QNAP, vous permettant de prendre des actions préalables si des valeurs S.M.A.R.T sont signalées comme anormales et réduire le risque de perte de données causée par une panne des disques durs physiques.

• Chiffrement AES 256 bits de la totalité du NAS

Le NAS QNAP prend en charge le chiffrement basé sur le volume afin de protéger les données sensibles. Un code de sécurité et un mot de passe sont nécessaires pour monter un volume encodé au démarrage du NAS QNAP. Toutes les données ne sont pas accessibles sans la clé de chiffrement qui protège contre l'accès non autorisé et la violation de données sensibles sur le NAS QNAP, même si les disques durs et le NAS sont volés. Certains modèles de NAS prennent en charge le chiffrement matériel accéléré qui supprime les données encodées de la charge de travail du processeur, offrant des performances plus rapides tout en assurant une protection des données sécurisée.

• Chiffrement des lecteurs externes

Le NAS QNAP peut également chiffrer des appareils de stockage externes afin de protéger contre l'accès non autorisé. Le personnel informatique a la possibilité de chiffrer des volumes de disque sur une partition spécifique de l'appareil externe à l'aide de l'AES-128, l'AES-192 ou de l'AES-256.

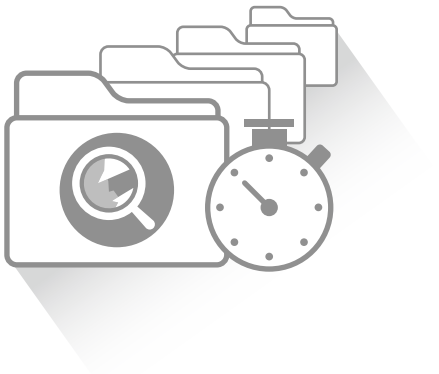
• Protection de niveau militaire

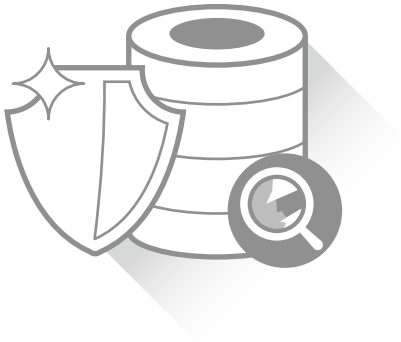
Pour chiffrer des unités de stockage internes et externes, on utilise la méthode de chiffrement AES 256 bits de niveau militaire. Cette méthode est validée par le programme FIPS 140-2 CAVP (Programme de validation des algorithmes de chiffrement) et aide à empêcher l'accès aux données professionnelles sensibles si les disques durs de tout le système NAS ont été volés.

Comment QNAP peut vous aider à gérer vos données

• Qsirch est un puissant moteur de recherche sur NAS

Il existe de nombreux avantages pour les sociétés, en particulier la possibilité de récupérer des documents et des fichiers afin de créer des propositions, des rapports, des contrats et plus encore. Grâce à Qsirch, il est possible d'accroître fortement la productivité et l'efficacité.

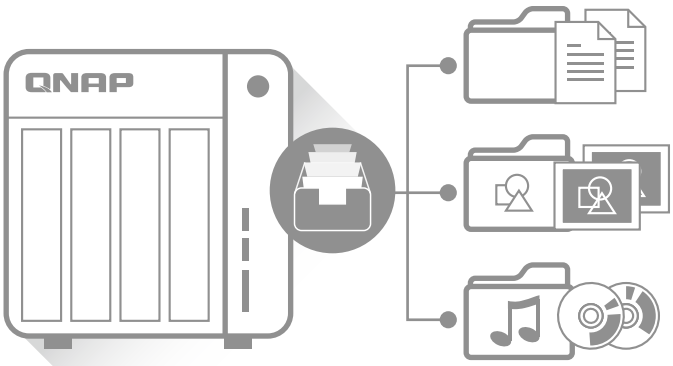




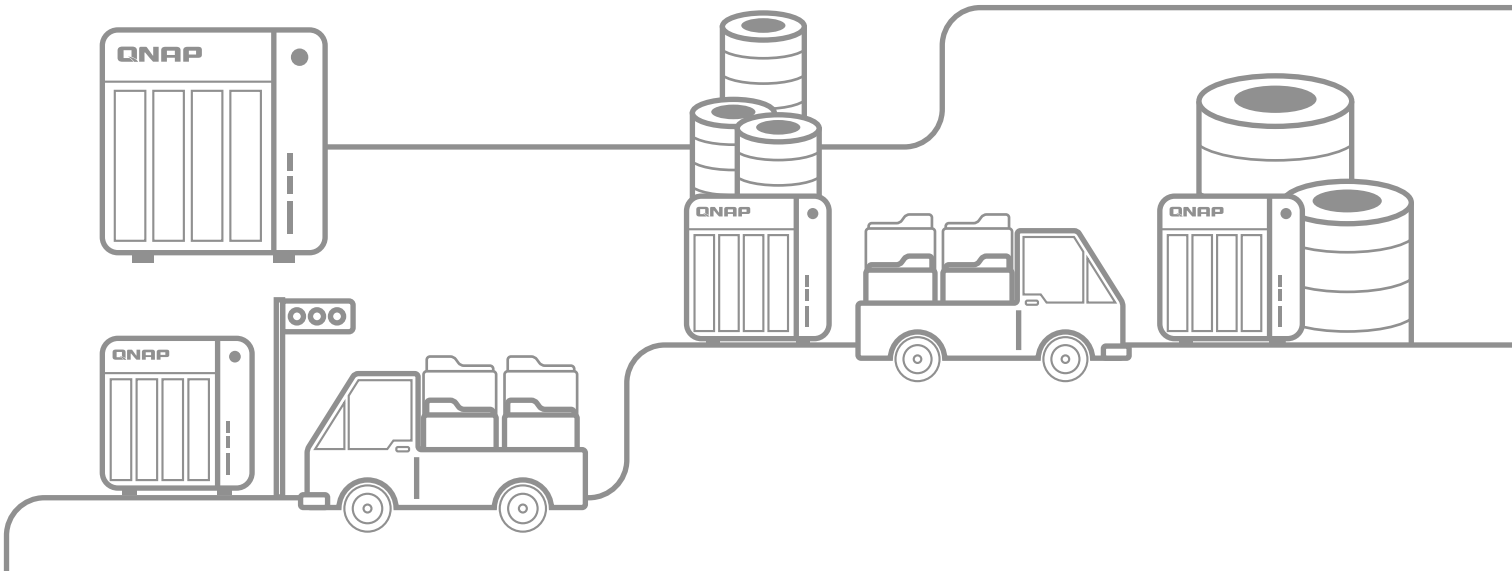
Qsirch travaille en suivant les droits d'accès des dossiers partagés et des comptes d'utilisateurs. Qsirch protège efficacement la confidentialité des données et les résultats des recherches affichent uniquement les fichiers auxquels cet utilisateur peut accéder. Les administrateurs peuvent facilement ajouter et supprimer des dossiers partagés spécifiques pour Qsirch. Les dossiers partagés peuvent être exclus de l'indexation de manière sélective afin de garantir la sécurité des données.

• Qfiling automatise efficacement l'organisation des fichiers

Lorsque le NAS QNAP est utilisé comme stockage de fichiers centralisé, la possibilité d'organiser correctement les fichiers représente un point clé dans la gestion et l'utilisation des fichiers. Néanmoins, lorsque nous sommes confrontés à un très grand nombre de fichiers répartis dans beaucoup de dossiers, les classer et les stocker peut s'avérer difficile, chronophage et fatiguant. Avec Qfiling, l'organisation des fichiers est automatisée et efficace.
Les principales caractéristiques de Qfiling sont :



- Vitesse ▶ Qfiling peut être configuré en quelques clics.
- Organisation ▶ Les fichiers sont organisés en fonction des paramètres utilisateur.
- Productivité accrue ▶ L'organisation des fichiers est automatique et à des intervalles réguliers, sans perte de temps ou effort.
- Gestion optimisée ▶ Conserve les fichiers organisés pour que les utilisateurs les retrouvent facilement.



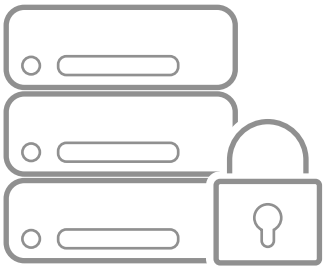
Comment QNAP peut vous aider à gérer vos utilisateurs

Le NAS QNAP prend en charge plusieurs fonctionnalités de sécurité pour le système, l'accès aux données et les fichiers stockés. L'accès chiffré protège le système et les connexions de communication, le blocage des IP empêche l'accès des utilisateurs suspects, et le chiffrement des appareils de stockage externes réduit le risque de détournement des données si les disques durs sont volés. Les paramètres de privilège avancés tels que Windows ACL, Windows Active Directory (AD), et le service d'annuaire LDAP sont pris en charge pour simplifier la gestion du contrôle d'accès. Les solutions anti-virus sont également prises en charge. Toutes ces mesures font du NAS QNAP un emplacement sûr pour les fichiers importants.

Protection d'accès au réseau

Les administrateurs informatiques peuvent définir une liste de connexions autorisées et non autorisées pour permettre l'accès au NAS QNAP à plusieurs utilisateurs à l'aide d'une adresse IP. Elle fonctionne comme un bloc automatique d'IP basé sur des critères, et protège l'accès réseau. Par exemple, cette commande peut être définie comme « dans 1 minute après 5 tentatives échouées, bloquer l'IP pendant 1 heure, 1 jour ou pour toujours ».
Si une adresse IP est refusée, l'hôte ne peut plus se connecter au serveur, peut importe les ports de connexion utilisés.

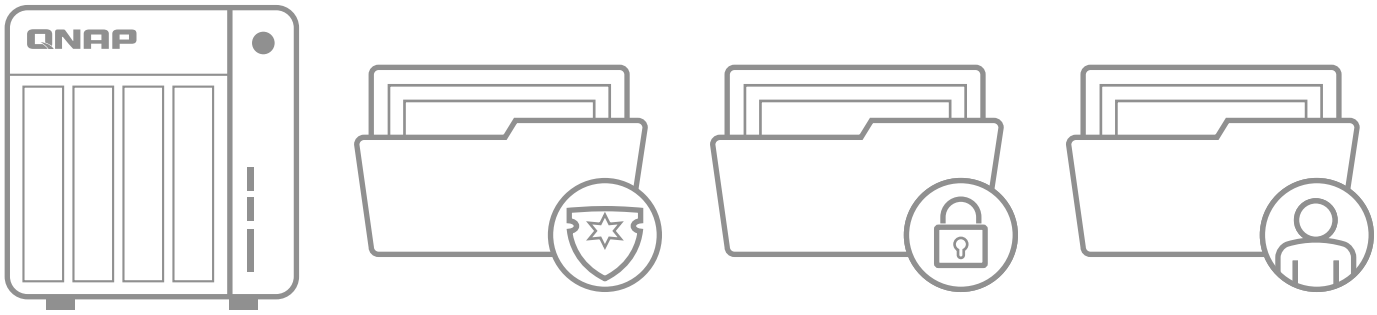
Protection dans les environnements mixtes



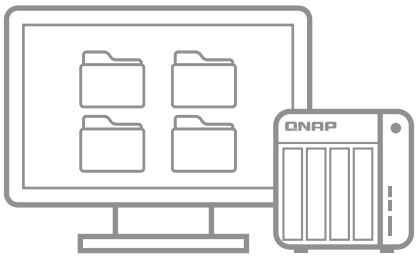
En général, tous les utilisateurs professionnels utilisent un anti-virus approprié. Cependant, il n'est pas possible de prévoir le développement des virus et il n'est pas possible d'arrêter les tentatives volontaires des utilisateurs de se connecter à des sites Web dangereux. Étant donné que les fichiers infectés dans un environnement mixte peuvent entraîner des dommages substantiels, il est important de disposer d'une solution anti-virus sur le NAS QNAP qui offre un partage de fichiers multiplateforme.
Détection intelligente : La solution anti-virus intégrée au NAS QNAP garantit un fonctionnement sans heurts des activités professionnelles via la détection des derniers virus, programmes malveillants, cheval de troie avec des mises à jour continues gratuites de la base de données des virus. Les analyses anti-virus peuvent être personnalisées et définies pour s'exécuter suivant une planification, avec des notifications par e-mail en cas de détection d'un virus.

Meilleure protection du système

En général, un NAS doté de plusieurs ports réseau permet à tous les services réseau activés d'accéder au contenu dans le serveur via chaque ports réseau. La protection des données est réduite. Dans les sociétés, seules des personnes habilitées doivent être en mesure d'accéder aux données importantes à l'aide d'un protocole réseau défini qui est une adresse IP interne. La concordance du service NAS QNAP offre aux administrateurs informatiques l'option d'autoriser ou de bloquer des services sélectionnés d'interfaces réseau définies afin de garantir la protection du système.



Paramètre d'autorisation de Windows ACL



Le NAS QNAP prend en charge Windows ACL, ce qui vous permet de mieux tirer profit des paramètres d'autorisation et des contrôles d'accès aux dossiers partagés du système Windows au NAS. Des autorisations de base et 13 niveaux d'autorisations avancées peuvent être définis sous Windows et synchronisés avec les paramètres d'autorisation des dossiers partagés du NAS. Les autorisations des sous-dossiers et les paramètres de privilèges au niveau fichier sont également pris en charge. Il est possible d'appliquer les mêmes autorisations à AFP, FTP, File Station et Samba si Autorisations de dossiers avancées est activée afin de garantir un contrôle d'accès strict pour une plus haute sécurité des données.

Windows Active Directory (AD)

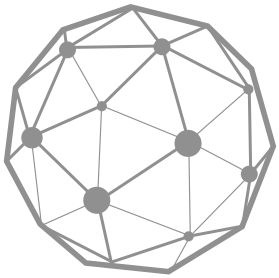
Le NAS QNAP peut facilement être joint au Windows AD pour une gestion efficace des comptes utilisateur. Les administrateurs informatiques peuvent bénéficier d'une vérification centralisée des droits d'accès afin de réduire les paramètres de privilèges complexes ; alors que les utilisateurs de domaines peuvent facilement utiliser le nom et le mot de passe de leur compte Windows AD afin de se connecter à différents NAS QNAP sur le réseau local. Le NAS QNAP prend en charge le déploiement AD à grande échelle de jusqu'à 200.000 utilisateurs et groupes AD.

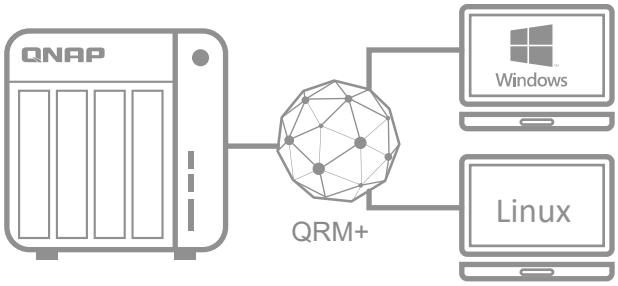
Service d'annuaire LDAP

La prise en charge du LDAP par QNAP permet d'ajouter le NAS aux services d'annuaire LDAP, tels que OpenLDAP. Ainsi, le serveur LDAP peut authentifier les utilisateurs de manière centralisée, et ces derniers peuvent utiliser le même nom et mot de passe de compte LDAP pour accéder à tout NAS QNAP ajouté sur le serveur LDAP. Grâce à un serveur LDAP intégré et simple d'utilisation, le NAS QNAP peut aussi être utilisé comme serveur LDAP pour authentifier de manière centralisée les utilisateurs et les groupes pour tous les autres appareils et applications avec le LDAP activé afin d'économiser l'effort de gestion tout en améliorant la sécurité des données.

Comment QNAP peut vous aider à gérer vos systèmes

QNAP QRM+ (QNAP Remote Manager Plus) et Q'center sont des solutions de gestion centralisée à interface unique pour permettre aux équipes informatiques de détecter, mapper, surveiller et de gérer de façon centralisée les appareils en réseau tels que les PC, les serveurs, les clients légers et les NAS QNAP. De plus, le NAS QNAP fournit des journaux d'affichage basés sur le Web pour un suivi efficace et qui peuvent être utilisés comme serveur Syslog pour stocker de manière centralisée les journaux système de tous les appareils en réseau.



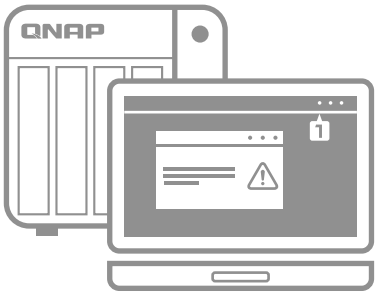


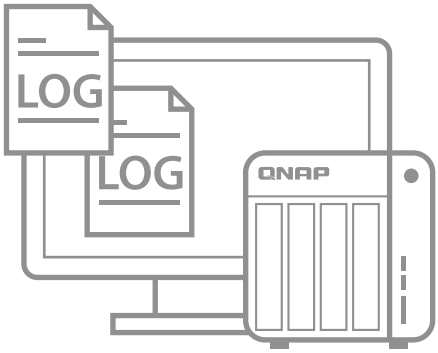
QRM+ : Surveillance et gestion centralisée des appareils en réseau

QRM+ peut créer une liste d'appareils connectés pour que les administrateurs puissent surveiller rapidement leur état - dont les appareils compatibles IPMI. Le cas échéant, QRM+ peut être utilisé comme surveillance en temps réel, afin d'évaluer l'état des appareils (dont la température, la vitesse du ventilateur, les capteurs, l'alimentation et les notification d'événements IPMI) de chaque point final. Avec QRM+, la gestion à distance des appareils informatiques est sécurisée, rapide et facile.

Alertes et notifications : Recevez des alertes avant qu'un désastre ne se produise

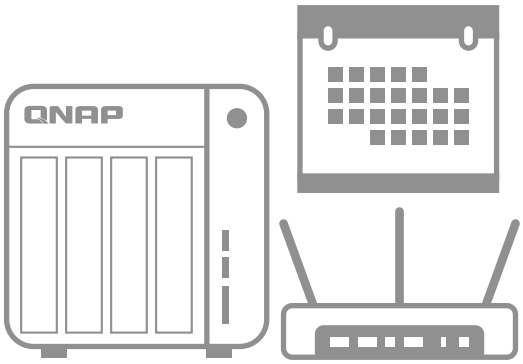
QRM+ possède des alertes pour aider le personnel informatique à corriger les problèmes de performance avant que les utilisateurs, les applications et la société ne soient touchés.





Système de journal complet

Le NAS QNAP aide les administrateurs informatiques à suivre efficacement les systèmes en fournissant des journaux affichés sur le Web : les journaux d'événement système tiennent les administrateurs informatiques au courant des événements d'informations, d'avertissement et d'erreurs du NAS QNAP ; les journaux de connexion système permettent aux administrateurs informatiques d'afficher l'historique d'accès de chaque fichier (qui, quand, et quelles actions ont été effectuées). De plus, une liste d'utilisateurs en ligne est à disposition pour surveiller l'accès des utilisateurs. En cas de détection d'une connexion suspecte, les administrateurs peuvent faire un clic droit sur l'utilisateur pour l'ajouter immédiatement à la liste de blocage ou à la liste de déconnexion.



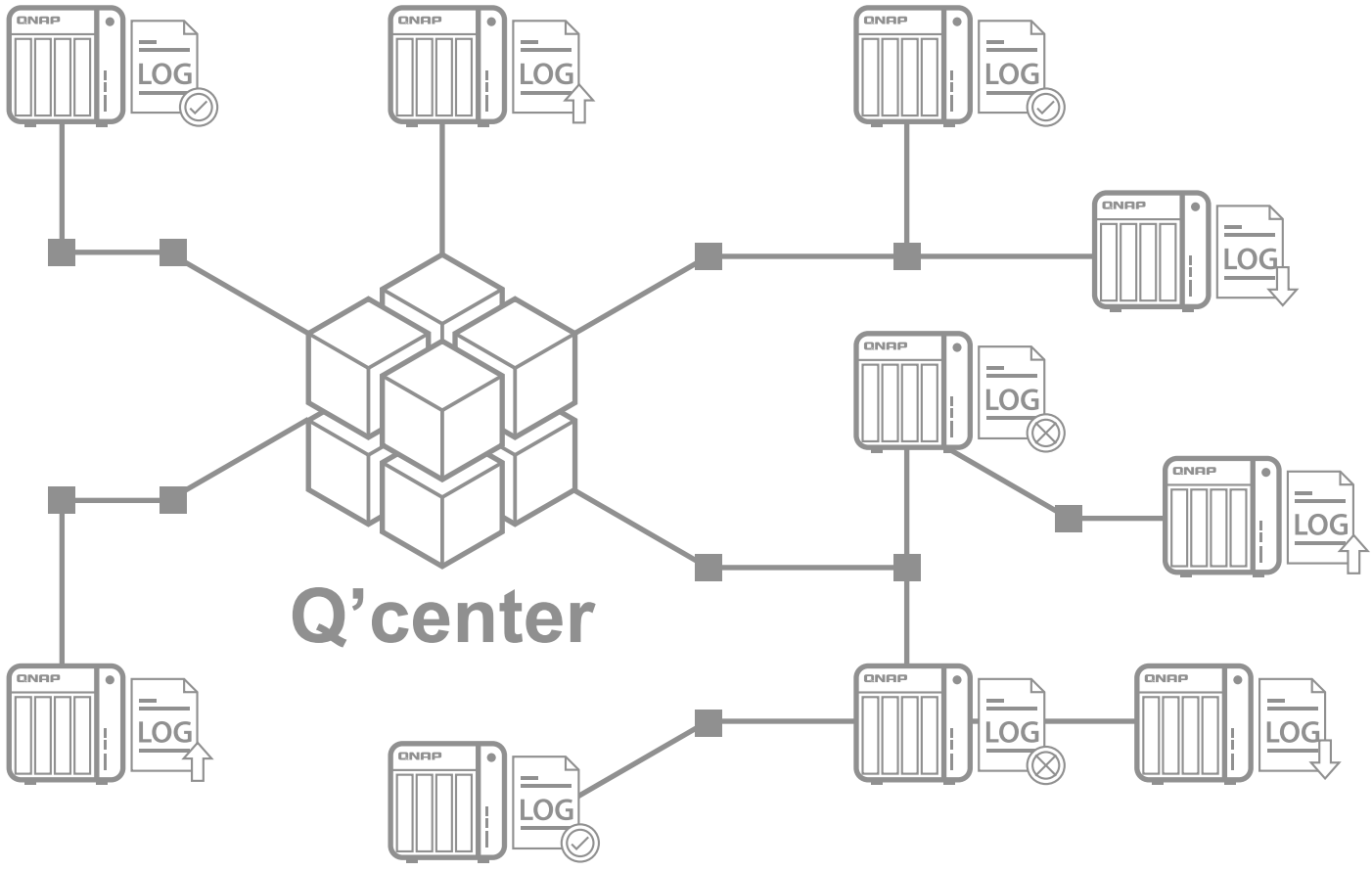
NAS QNAP comme serveur Syslog

Un référentiel central de données de journaux des différents appareils du réseau permet une gestion efficace et un audit de la sécurité dans les entreprises. En prenant en charge les protocoles UDP et TCP, le NAS QNAP peut servir de serveur Syslog, permettant aux administrateurs informatiques de recueillir et de stocker facilement les journaux d'autres appareils en réseau vers le NAS QNAP afin d'améliorer, le cas échéant, l'efficacité de la gestion et de la résolution des pannes. Des filtres avancés et des notifications par e-mails sont fournis pour faciliter l'identification rapide des pannes ou des menaces de sécurité.

En plus de jouer le rôle de serveur pour recueillir les journaux des autres appareils, le NAS QNAP peut aussi agir comme un client pour envoyer ses propres journaux vers le serveur Syslog.

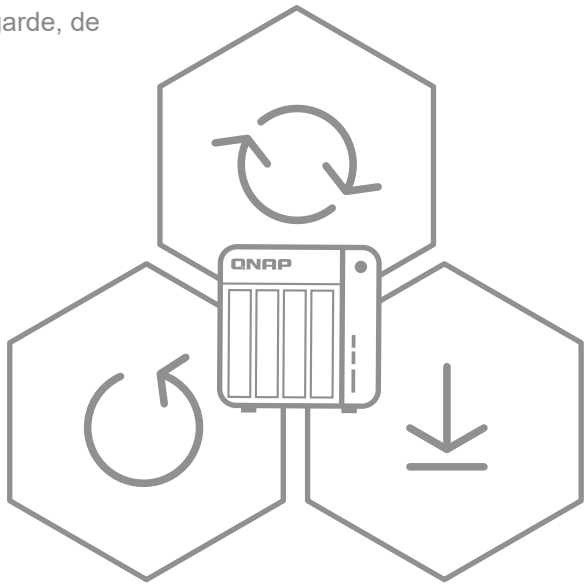
Q'center : Surveillez et gérez tous vos NAS de manière centralisée

Q'center peut gérer et surveiller mutuellement plusieurs NAS clients, remplissant en même temps les besoins de gestion centralisée et de segmentation des cibles de contrôle. Les informations comme les températures système et les vitesses de ventilateurs permettent de réduire les risques de défaillances système en contrôlant les conditions ambiantes. Vous pouvez aussi allumer/éteindre plusieurs NAS à la fois grâce aux options d'alimentation prédéfinies, et ainsi améliorer l'accessibilité et l'efficacité de votre NAS. Q'center permet également la surveillance centralisée des journaux système et peut gérer les mises à jour et la maintenance du firmware de tous les NAS QNAP en un minimum d'efforts.



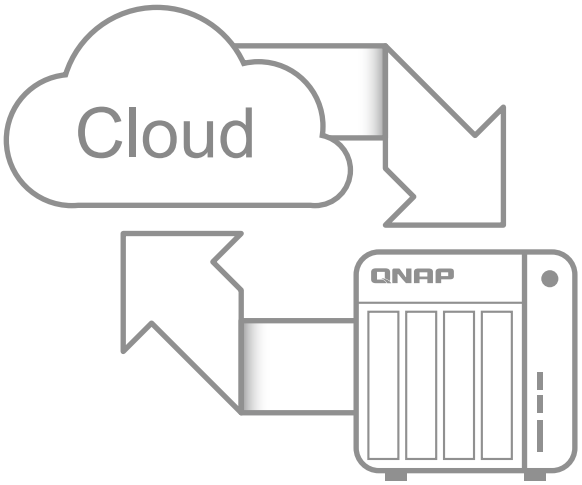
NAS QNAP : Une solution efficace de récupération après sinistre

Le NAS QNAP prend en charge plusieurs méthodes de sauvegarde, de synchronisation et de restauration des données.



Hybrid backup sync

QNAP Hybrid Backup Sync réunit des fonctions de sauvegarde, de restauration et de synchronisation dans une seule application. Ainsi, les utilisateurs peuvent facilement transférer des données vers des espaces de stockage locaux, distants et dans le cloud à l'aide du RTRR (Réplication à distance en temps réel), rsync, FTP et CIFS/SMB.



Sauvegarde dans le cloud :

Le NAS QNAP propose des solutions de sauvegarde sécurisées, simples d'utilisation et remplies de fonctionnalités pour sauvegarder les données sur les services de stockage disponibles à partir des cloud publics de classe entreprise tels que Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, Dropbox* et IBM SoftLayer. Même les solutions de stockage en cloud privé compatibles avec OpenStack Swift et WebDAV sont prises en charge.

Lors de la conception d'un Plan d'adaptation pour le GDPR, les sociétés peuvent choisir de se mettre en conformité uniquement avec les exigences du règlement actuel ou de saisir cette chance pour ajouter de la valeur à leur organisation. Ainsi, elles contribuent à étendre une nouvelle culture sur le traitement des données personnelles et créent une réelle transformation numérique dans la manière dont la société traite la gestion des données des clients et des salariés.

Les criminels informatiques sont en constante recherche de points faibles et développent toujours des attaques plus ciblées. Les solutions de sécurité durables doivent évoluer et s'adapter en suivant de fréquentes mises à jour et en utilisant des informations sur les menaces dès qu'elles sont disponibles. La sécurité n'est uniquement utile que si elle détecte les menaces, si elle déclenche une réaction et garantit une protection globale de toute la structure, des points de terminaison aux réseaux et au cloud hybride.