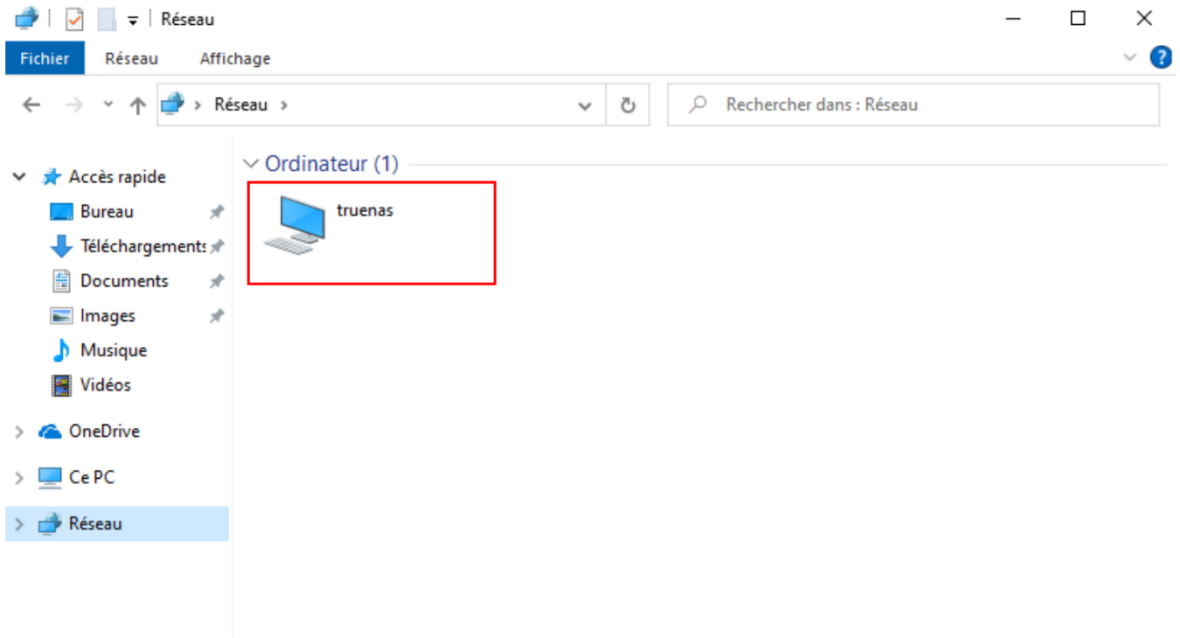
# Procédure utilisateurs :

Pour accéder au TrueNAS il faut se rendre sur l'explorateur de fichier dans « réseau » et rentrer l'adresse ip du serveur (172.16.0.15) dans la barre de recherche

L'ordinateur TrueNAS va apparaître.



# Politique de Sécurité pour TrueNAS

## 1. Objectifs de la Politique de Sécurité

La politique de sécurité a pour objectif principal de protéger les données stockées sur le serveur TrueNAS en assurant leur confidentialité, leur intégrité et leur disponibilité. Elle vise également à contrôler les accès aux données, à mettre en place des mécanismes de sauvegarde fiables, et à surveiller les vulnérabilités pour prévenir les attaques ou les pertes de données.

## 2. Gestion des Accès et Authentification

Pour garantir une sécurité optimale, il est essentiel de mettre en place une authentification forte pour tous les comptes administrateurs. Cela inclut l'utilisation de mots de passe complexes et l'activation de l'authentification à deux facteurs (2FA). Chaque utilisateur doit disposer d'un compte individuel avec des permissions adaptées à son rôle, comme l'accès en lecture seule ou en lecture-écriture. La gestion des permissions peut être simplifiée en utilisant des groupes de sécurité, par exemple un groupe pour les utilisateurs ayant besoin d'un accès en lecture seule et un autre pour ceux nécessitant un accès en lecture-écriture. Enfin, l'intégration de TrueNAS avec Active Directory (AD) permettra de centraliser la gestion des utilisateurs et des permissions.

## 3. Chiffrement des Données

Le chiffrement des données au repos est une mesure essentielle pour protéger les informations stockées sur le NAS en cas de vol ou de perte physique des disques. TrueNAS permet d'activer le chiffrement des volumes de stockage pour garantir que les données ne soient pas accessibles sans autorisation. De plus, les communications entre les clients et le NAS doivent être sécurisées en utilisant des protocoles tels que HTTPS, SFTP ou SMB3, qui chiffrent les données en transit.

## 4. Sauvegarde et Récupération

Un plan de sauvegarde régulier doit être mis en place pour protéger les données critiques. Les sauvegardes peuvent être effectuées quotidiennement ou hebdomadairement, selon les besoins de l'entreprise, et stockées sur un support externe ou un autre NAS. Il est important de conserver plusieurs versions des sauvegardes pour permettre une récupération en cas de corruption ou de suppression accidentelle des données. Enfin, des tests de restauration doivent être réalisés régulièrement pour s'assurer que les sauvegardes sont fonctionnelles et que les données peuvent être récupérées en cas de besoin.

## 5. Surveillance et Mise à Jour

La surveillance des logs système est cruciale pour détecter toute activité suspecte ou tentative d'accès non autorisé. Les logs doivent être activés et consultés régulièrement pour identifier rapidement les éventuelles menaces. Par ailleurs, il est essentiel d'appliquer les mises à jour de sécurité et les correctifs pour TrueNAS dès qu'ils sont disponibles. Cela permet de protéger le système contre les vulnérabilités connues. Une veille active sur les Common Vulnerabilities

and Exposures (CVE) liées à TrueNAS et aux logiciels associés doit également être mise en place pour anticiper les risques.

## 6. Politique de Sécurité Physique

Le NAS doit être installé dans un environnement sécurisé, comme une salle serveur verrouillée, avec un accès restreint au personnel autorisé. Cela permet de limiter les risques d'accès physique non autorisé. De plus, le NAS doit être protégé contre les sinistres tels que les incendies, les inondations ou les coupures de courant. L'utilisation d'onduleurs (UPS) est recommandée pour garantir la continuité de service en cas de panne électrique.

## 8. Gestion des Incidents

Un plan de réponse aux incidents doit être établi pour réagir rapidement en cas de violation de sécurité ou de perte de données. Ce plan doit inclure les étapes à suivre pour isoler le problème, analyser l'incident et restaurer les services. Un processus de notification doit également être mis en place pour informer les responsables en cas de détection d'une activité suspecte ou d'une faille de sécurité.

## 9. Audit et Conformité

Des audits de sécurité réguliers doivent être réalisés pour vérifier la conformité avec la politique de sécurité et identifier les éventuelles faiblesses. Ces audits permettent de s'assurer que les mesures de sécurité sont correctement appliquées et que le système est protégé contre les menaces actuelles. Enfin, il est important de s'assurer que la configuration du NAS respecte les réglementations en vigueur, comme le RGPD, en matière de protection des données.

## Conclusion

Cette politique de sécurité a pour but de protéger les données d'Assurmer en utilisant TrueNAS comme solution de stockage. Elle couvre les aspects techniques, organisationnels et humains de la sécurité, en mettant l'accent sur la prévention des risques, la gestion des accès, et la récupération en cas d'incident. Il est essentiel de revoir et mettre à jour cette politique régulièrement pour s'adapter aux nouvelles menaces et aux évolutions technologiques.