

Mise en place d'une solution de type NAS

Auteurs : COMBETTES Elise, Gana Stéphane

Validateurs : DEGEN Loïc, EDOUARD Claire



SOMMAIRE

Étude des fonctionnalités d'un serveur NAS	.4
Analyse des solutions de type RAID	5
Proposition de politique de sécurité pour l'intégrité et la sauvegarde des données	.6
Comparatif de deux solutions NAS	.7
Installation de la solution choisie	.8
Phase de testing	16
Note aux utilisateurs1	17
Mise en place d'une veille informationnelle TRUENAS1	18
Planning1	19

Étude des fonctionnalités d'un serveur NAS

Dans le cadre de la création du serveur pour Assurmer, il est important de permettre aux utilisateurs d'accéder facilement et de manière sécurisée à des données stockées, un serveur NAS est un choix plus que judicieux.

Un serveur NAS (Network Attached Storage) est une solution de stockage réseau permettant de centraliser, partager et sécuriser des données. Il facilite l'accès aux fichiers pour plusieurs utilisateurs tout en assurant une gestion collaborative et sécurisée.

Les NAS utilisent des protocoles comme SMB, NFS ou FTP, compatibles avec différents systèmes d'exploitation et couramment adoptés pour leur fiabilité et la gestion des droits d'accès. La sécurité est renforcée par le chiffrement des données, qui les rend inaccessibles sans clé, même en cas de vol des disques.

Les snapshots permettent de conserver des copies instantanées des fichiers à différents moments. Contrairement aux sauvegardes traditionnelles, ils enregistrent uniquement les modifications, offrant une récupération rapide tout en consommant moins d'espace.

Les NAS prennent en charge des configurations RAID, assurant la tolérance aux pannes en répartissant les données sur plusieurs disques. Certains modèles proposent aussi la réplication entre serveurs pour une redondance géographique.

L'intégration avec Active Directory simplifie la gestion des utilisateurs. Par exemple, un NAS peut attribuer automatiquement des droits d'accès en fonction des groupes définis dans l'annuaire. La synchronisation avec des services cloud permet de combiner stockage local et sauvegarde distante.

En résumé, le NAS constitue une solution fiable et évolutive pour centraliser, sécuriser et partager des données dans un cadre professionnel.

Analyse des solutions de type RAID

Les solutions RAID (Redundant Array of Independent Disks) permettent d'assurer la sécurité des données et d'améliorer les performances des systèmes de stockage. Voici une comparaison des principales configurations RAID adaptées aux NAS :

- RAID 0 (Striping) : Répartit les données sur plusieurs disques pour améliorer les performances. Il n'offre aucune tolérance aux pannes : la perte d'un disque entraîne la perte totale des données.
- RAID 1 (Mirroring) : Duplique les données sur deux disques. Il garantit la sécurité en cas de panne d'un disque, mais réduit la capacité de stockage disponible de moitié.
- RAID 5 : Nécessite au moins trois disques. Il répartit les données et les informations de parité, offrant tolérance aux pannes avec une capacité utile égale au nombre de disques moins un. Cependant, les performances peuvent être réduites lors de la reconstruction après une panne.
- RAID 6 : Similaire au RAID 5 mais avec deux blocs de parité, il supporte la panne de deux disques simultanément. Il offre une meilleure sécurité mais nécessite au moins quatre disques et consomme plus d'espace.
- RAID 10 (1+0) : Combine RAID 1 et RAID 0. Il offre à la fois des performances élevées et une bonne tolérance aux pannes, mais utilise seulement 50 % de la capacité totale pour le stockage.

Le choix d'une configuration RAID dépend des besoins spécifiques en matière de sécurité, de performances et de capacité. Pour une entreprise comme Assurmer, qui nécessite une sécurité accrue, le RAID 1 ou le RAID 5 est souvent recommandé, car ils offrent un bon équilibre entre protection des données et utilisation de l'espace de stockage.

Proposition de politique de sécurité pour l'intégrité et la sauvegarde des données d'Assurmer

La sécurité des données est essentielle pour assurer la continuité des activités d'Assurmer. Voici les principes fondamentaux d'une politique de sécurité visant à garantir l'intégrité et la sauvegarde des données professionnelles.

- <u>Sécurisation des accès</u> : L'accès aux données doit être limité aux utilisateurs autorisés uniquement. L'utilisation de mots de passe complexes, combinée à une authentification à deux facteurs, est obligatoire. Un contrôle d'accès basé sur les rôles (RBAC) permettra de restreindre l'accès en fonction des responsabilités de chaque utilisateur.
- <u>Sauvegarde des données</u> : Il est impératif d'effectuer des sauvegardes régulières des données critiques. La solution NAS, configurée avec un système RAID, offrira une redondance pour assurer une disponibilité constante des données. Les sauvegardes doivent être automatiques et incrémentielles, avec une révision périodique de la politique de sauvegarde.
- <u>Cryptage des données</u> : Pour protéger les données sensibles, un cryptage des fichiers doit être activé, tant pour les données stockées que pour les transferts. Cela garantit que même en cas de vol physique des supports de stockage, les données restent inaccessibles sans la clé de décryptage.
- <u>Surveillance et journalisation</u> : La surveillance continue des accès et des opérations sur les données est essentielle. Les logs d'accès seront enregistrés et analysés pour détecter toute activité suspecte. En cas d'anomalie, des alertes en temps réel permettront de réagir rapidement.
- <u>Gestion des vulnérabilités</u> : Le NAS et les systèmes associés doivent être maintenus à jour pour se prémunir contre les failles de sécurité. Un processus de veille technologique sera mis en place pour suivre l'apparition de nouvelles vulnérabilités et assurer une gestion proactive des risques.
- <u>Plan de reprise d'activité (PRA)</u> : En cas de panne ou d'incident majeur, un plan de reprise d'activité permettra de restaurer rapidement les données et les services. Des tests réguliers garantiront l'efficacité de ce plan pour limiter les impacts sur l'activité.

Cette politique vise à garantir la confidentialité, l'intégrité et la disponibilité des données d'Assurmer, tout en mettant en place des processus de protection et de récupération adaptés aux risques identifiés.

Comparatif de deux solutions NAS

Puisque les solutions NAS logicielles jouent un rôle clé dans la gestion des données des entreprises, le choix de la solution logicielle est crucial.

Parmi les solutions les plus populaires, TrueNAS et OpenMediaVault se démarquent par leurs fonctionnalités et leur fiabilité.

TrueNAS, développé par iXsystems, est une solution open source basée sur FreeBSD, connue pour sa robustesse, sa sécurité avancée et son système de fichiers ZFS. Il est souvent privilégié dans les environnements professionnels pour sa capacité à assurer l'intégrité des données et sa compatibilité avec les environnements Active Directory.

OpenMediaVault, quant à lui, repose sur Debian Linux. Il est apprécié pour sa simplicité d'installation et d'utilisation, ce qui en fait une solution intéressante pour les petites entreprises ou les particuliers. OpenMediaVault propose une interface web conviviale et une large gamme de plugins permettant d'ajouter des fonctionnalités supplémentaires.

Voici un tableau comparatif des deux solutions :

Critères	TrueNAS	OpenMediaVault
Système d'exploitation	FreeBSD	Debian
Système de fichiers	ZFS	EXT4, XFS, Btrfs
Sécurité	Chiffrement natif, snapshots	Chiffrement via plugins
Gestion AD	Intégration native	Via plugins
Interface	Interface web avancée	Interface web simple
Performances	Optimisé pour les environnements professionnels	Adapté pour les petites infrastructures
Support de la communauté	Large communauté professionnelle	Communauté orientée particuliers

>Le choix de TrueNAS s'impose pour Assurmer en raison de sa stabilité, de son intégration native avec Active Directory et de la sécurité qu'offre ZFS.

De plus, sa capacité à gérer des snapshots et des sauvegardes automatiques permet d'assurer l'intégrité des données, un enjeu majeur pour une entreprise. Bien que plus complexe à prendre en main, TrueNAS représente une solution pérenne pour une infrastructure professionnelle.

Installation de la solution choisie

Tout d'abord, téléchargez et installez sur une machine virtuelle la dernière solution de TrueNAS-Core disponible via ce <u>lien</u> :

https://download-core.sys.truenas.net/13.0/STABLE/U6.7/x64/TrueNAS-13.0-U6.7.iso

Une fois installé, au redémarrage, vous aurez une adresse IP renseignée par défaut, tenant compte de votre réseau.

Dans notre cas, nous avons eu l'adresse 172.16.0.22.

Starting nginx. Starting collectd_daemon. daemon: process already running, pid: 0 Configuring vt: blanktime. net.inet.carp.allow: 0 -> 1
Wed Feb 19 09:24:58 PST 2025
Console setup
 Configure Network Interfaces Configure Link Aggregation Configure VLAN Interface Configure Static Routes Configure DNS Reset Root Password Reset Configuration to Defaults Shell Shut Down
The web user interface is at: http://172.16.0.22

En la tapant dans la barre d'adresse de votre navigateur internet, vous tomberez alors sur la page de connexion de votre interface TrueNAS.

L'identifiant par défaut est « root » et le mot de passe est celui qui vous a été demandé lors de l'installation.



Vous voici alors sur la page d'accueil de TrueNAS.



La prochaine étape sera, tout d'abord de créer un utilisateur dans notre Active Directory. Rendez-vous dans votre AD et créez un utilisateur.

Cliquez droit dans une zone vide de votre fenêtre d'AD, puis « Nouveau » / « Utilisateur ».

🔶 🙋 🛅 📋 📷 🖄	🛛 📰 😤 📚	ii 🍸 🗾 🔽				
Utilisateurs et ordinateurs Active	Nom		Type	~	Description	/
Requêtes enregistrées	Administrateurs D	HCP	Groupe de sécu	urité - Domaine local	Les membres qui ont un	
ASSURMER.local	A DasAdmins		Groupe de sécu	urité - Domaine local	Groupe des administrate	
> 🖹 Accounts	Editeurs de certifie	cats	Groupe de sécu	urité - Domaine local	Les membres de ce grou	
Builtin	Groupe de réplica	tion dont le mot	Groupe de sécu	urité - Domaine local	les mots de passe des	
Computers	Roupe de réplica	tion dont le mot	Groupe de sécu	urité - Domaine local	Les mots de passe des	
Domain Controllers	Serveurs RAS et IA	s	Groupe de sécu	urité - Domaine local	Les serveurs de ce group	
ForeignsecuntyPrincipals	Utilisateurs DHCP		Groupe de sécu	urité - Domaine local	Les membres qui ont un	
NINERA	Administrateurs c	lés	Groupe de sécu	urité - Global	Les membres de ce grou	
> LostAndFound	Admins du doma	ine	Groupe de sécu	urité - Global	Administrateurs désigné	
> Managed Service Accourt	Contrôleurs de do	omaine	Groupe de sécu	urité - Global	Tous les contrôleurs de	
> 🧮 Program Data	Contrôleurs de do	omaine clonables	Groupe de sécu	urité - Global	Les membres de ce grou	
> 🧾 System	😤 Contrôleurs de do	omaine en lecture	Groupe de sécu	urité - Global	Les membres de ce grou	
🔛 Users	A DnsUpdateProxy		Groupe de sécu	urité - Global	Les clients DNS qui sont	
> 📋 NTDS Quotas	🙉 Invités du domain	ie	Groupe de sécu	urité - Global	Tous les invités du doma	
> 🔛 TPM Devices	😤 Ordinateurs du do	omaine	Groupe de sécu	urité - Global	Toutes les stations de tra	
	Ropriétaires créat	teure de la stratégi	Groune de céci	ité - Global	Les membres de ce grou	
	Reprotected Use	Délégation de cont	trôle	ité - Global	Les membres de ce grou	
	📇 Utilisateurs du	Rechercher	×	ité - Global	Tous les utilisateurs du d	
	Administrateu	Nouveau	>	Ordinateur	ce grou	/
	Administrater	Toutes les tâches	>	Contact	désigné	
	Contrôleurs d	A		Groupe	ce grou	
		Actualiser		InetOrgPerson	teur d'au	
	B DHCP	Exporter la liste		mcDS-KeyCradential		
	GLPI	Affichage	>	msDS-ResourcePropertyl	list	
	🛃 Invité	Réorganiser les icô	ner)	mcDS_ShadowBringinalC	teur inv	
	🛃 krbtgt	Allow los los	1125	insb3-ShadowPhilepare	e du c	
	SRV-AD	Aligner les icones		msImaging-PSPs		
		Propriétés		Alias de file d'attente MS	MQ	
		Aide		Imprimante		
				Utilisateur		
				Dossier partagé		

Ensuite, nous allons nommer notre nouvel utilisateur pour Truenas avec son propre nom d'utilisateur ainsi que son mot de passe.

	Créer dans : ASSURMER.local/Users	
	Mot de passe : Confirmer le mot de passe :	
	L'utilisateur doit changer le mot de passe à la procha	sine ouverture de session
~	Le mot de passe n'expire jamais	
Annuler	< Précédent	Suivant > Annuler
	Annuler	Mot de passe : Confirmer le mot de passe : L'utilisateur doit changer le mot de passe à la procha L'utilisateur ne peut pas changer de mot de passe Le mot de passe n'expire jamais Le compte est désactivé Annuler

Ensuite, nous allons ajouter notre utilisateur dans les groupes qui nous intéressent.

Ouvrez les propriétés de votre utilisateur.

Dans l'onglet « <u>Membre de</u> », ajoutez l'utilisateur dans les groupes nécessaires. Dans notre cas, nous choisirons surtout « <u>Admins du domaine »</u>. Puis <u>validez</u>.

	Environnement		Session	9		Contrôl	e à dis	tance	
	Profil des services Bureau	à listance	00001011	COM		Êd	liteur d	l'attrouts	
	Général Adresse Compt	e Profil	Té	éphones	Organis	sation	Cert	ificats pu	ublié
	Membre de Réplication	de mot de r	asse	Appel	entrant	Ob	iet	Sécu	urité
a 🗕									
1	Membre de :								
e	Nom		Doss	er Service	s de doma	aine Act	tive Di	rectory	
	Admins du domaine		ASSI	IRMER loc	al/Users				
2	GRP NAS		ASSI	IRMER loc	al/Group	A0			
	1 Milesterne de demoires		ACCI	IDMED I	-1/11				
s u u			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	JAMEN JOC	507 00010				
s a r r			,	STALL SOC					
	< 2								>
	< 2 Ajouter Supprime	r							>
	< 2 Ajouter Supprime	r							>
	< 2 Ajouter Supprime Groupe principal : Utilisateu	r urs du domai	ine			_			>
* aurrre (r	< 2 Ajouter Supprime Groupe principal : Utilisateu	r urs du domai lin 'est p	ne	e de modifie	er le group	be princ	ipsl, so	auf si voi	>
3 2 1 1 1 1 1 1 5	< 2 Ajouter Supprime Groupe principal : Utilisateu Définir le groupe principal	r urs du domai li n'est j dispose	ine pas utile z de clie	e de modifie	er le group tosh ou d	pe princ	ipal, sa tions (auf si voi compatib	> us bles
3 a u m m m e « m m u 3 a	< 2 Ajouter Supprime Groupe principal : Utilisateu Définir le groupe principal	r II n 'est dispose POSIX.	ne pas utile z de clie	e de modifie	er le group tosh ou d	oe princ	ipal, sa itions (auf si voi compatib	> us bles
's a u n n n e « n n l 's a	< 2	r II n'est j dispose POSIX.	ne pas utile z de clie	e de modifie	er le group tosh ou d	be princ applica	ipal, sa stions (auf si voi compatib	> us bles

Nous avons besoin d'avoir un utilisateur Admin afin que TrueNAS puisse accéder à notre AD afin de mieux gérer les groupes et utilisateur pour les partages.

Retournez sur votre interface TrueNAS.

Modifiez l'adresse IPV4 afin d'attribuer une IP fixe à notre serveur NAS

Vous pouvez également en profiter pour modifier la langue, l'interface, l'heure de votre NAS.

_	/			_	
	🛠 TrueNAS		🗱 systems 🛛 🕸	ê (
55	Dashboard	System / General	TrueNAS C	ORE® © 2	2025 - iX
*	Accounts 👻	GIL			
	System 🔺	601 50. Centeurs * freenas_default	* (?)		
	General	Web Interface IP-4 Address * 172.16.0.15	* (?)		
	NTP Servers	Visib Insertace IPVA Address *	• (?)		
	Boot	Web Interface HTTP Purt BD	0		
	Advanced	Web Interface HTTPS Port	0		
	Email	HTTPS Pestoola TLSV1.2, TLSV1.3	* (?)		
	System Dataset	Web Interface HTTP-> HTTPS Redirect 🕜	0		
	Reporting				
	Alert Services	Localization Language			
	Alert Settings	French (2) Console Kayboard Map	* (?)		
	Cloud Credentials	Sort languages by: Name Language code Europe/Paris Das Format	0		
	SSH Connections	2025-03-01 • ⑦ 15:26:48 (24 Hours)	* (?)		

Ensuite, rendez-vous dans <u>Réseau/Configuration globale</u>. Rentrez-y le nom de votre serveur TrueNAS, le nom de votre domaine ainsi que le serveur DNS associé.

Ensuite, validez en cliquant sur « Enregistrer ».

	🛠 TrueNAS	.≡ <					≬≫ systems [.]	٢	Ê	
	root truenas.assurmer.local	Réselu / Configurat	ion globale				Т	rueNAS	CORE®	
	Tableau de bord		Nom de Domaine e	Domaine		Annonce de service				
h	Comptes 👻		truenas		(MetBIOS-NS (2)				
	Système 👻		assurmer.local		0	WS-Discovery 🕥				
•	Tâches 👻		Domaines supplémentair	ires	(D				
¢.	Réseau 🔺]	Serveur de noms 1 (DNS) 172 16 0 1		(Passerelle par défaut		(2)	
	Résumé réseau		Serveur de noms 2 (DNS) 9.9.9.9		(Passerelle IPv6 par défaut 			อ	
	Configuration globale		Serveur de noms 3 (DNS)	5)		2				
	Interfaces		Autres Paramè res		```````````````````````````````````````	2				
	Routes statiques		Proxy HTTP					0	0	
	Stockage 👻		Activer la fonction N	Netwait ⊘						
9	Services d'annuaire 👻		Base de données des nor	oms d'hôtes				(D	
3	Partages -									
÷	Services		ENREGISTRER							

Allez dans Système / Général :

Désormais, nous allons joindre le serveur au domaine.

Dans la rubrique <u>Service d'annuaire / Active Directory</u>, rentrez le nom de domaine, le nom d'utilisateur créé pour l'occasion dans l'AD et son mot de passe. Cliquez sur «<u>Activer »</u> Puis « Enregistrer ».

ru					3
	Strue NAS				🐠 systems 💿 🖻 🌲
	Stockage 👻	Services d'annuaire /	Active Directory		TrueNAS CORE® © 2025
•	Services d'annuaire		Identifiants du Domaine		
	Active Directory		assurmer.local		0
	LDAP		TRUENAS		0
	NIS		NOU DE passe du compre de domaine		2 0
	Realms Kerberos		Activer (requiert le mot de passe ou le principal Activer (requiert le mot de passe ou le principal	Kerberos) 🕜	
	Kerberos Keytabs	4	ENREGISTRER OPTIONS AVANCÉES	RECONSTRUCTION DU CACHE DU SERVICE D'ANNUAIRE	
	Paramètres Kerberos				-

Vous aurez, en haut à droite de votre interface, une fenêtre qui vous permettra de voir l'état de la connexion à votre AD.



Désormais notre NAS est bien relié à notre Active Directory.

Désormais nous allons créer un Volume de donnée, ou « Pool » Allez dans <u>Stockage/Volumes</u> et cliquez sur <u>« Ajouter »</u>

			()∕∕systems	۲	0	Ê	4	۰	
		Stockage Volumes		Tru	eNAS C	ORE®	0 2025	iXsyste	ms, Inc.
	truenas.assurmer.local				-				
5	Tableau de bord	Volumes			2		٨J	OUTER	
	Comptes -								
	Système 👻	Aucun volume							
	Tâches 🗸								
*	Réseau 👻								
	Stockage								
	Volumes								
	Instantanéa								

Pour le bien de la démonstration, nous avons un disque virtuel de 5Go.

Tout d'abord, nommez-le (par ex : DataPool). Déplacez-le sur la droite grâce aux flèches.

Dans notre cas, nous avons à <u>forcer</u> » la création et confirmer que nous prenons en compte le fait que tout sera supprime sur notre stockage. Cliquez sur « Créer un volume ».



Attention		
Le contenu de to	us les disques a	joutés sera effacé.
Confirmer	ANNULER	CRÉER UN VOLUME

Ensuite, nous allons ajouter un « dataset », soit l'équivalent d'un dossier, que nous pourrons partager, ou non. Cliquez sur les <u>3 points</u> à droite puis <u>« Ajouter un dataset ».</u>

		5	≡ <			1				₫ ∕∕s	ystems ⁻	ê 🖻	۵	\$ ()
	A rest		Stockage / Volu	imes							Π	ueNAS CORE	® © 2025	- iXsystems, Inc.
	truenas.assurmer.local													
5	Tableau de bord		Volumes							\checkmark			Α.	JOUTER
*	Comptes	•	DataPool			ON	ILINE 🥑 372 Kie	8 (0%) Utilisé 2.62 GiB Lib	re					\$ ^
	Système	•	Nom ¢	Type 🗢	Utilisé 🗢	Available 🗢	Compression 🗢	Compression Ratio 🗢	Readonly 🗢	Dedup 🗢	Commenta	ires 🗢		<u> </u>
Ē	Tâches	•	DataPool	FILESYSTEM	372 KiB	2.62 GIB	lz4	1.00	false	OFF	$\mathbf{\lambda}$			
*	Réseau	•										Actions data	set	
	Stockage										L	Ajouter un da	ataset	_
	Volumes											Modifier les	options	
	Instantanés											Modifier les		ons
												Quatas utilia	atour	

Nous allons nommer notre Dataset (par ex : share), vous pouvez ajouter un commentaire pour décrire brièvement son utilité. Ensuite, pour le type de partage, nous voulons du <u>SMB</u>. Enfin, sélectionnez « <u>Envoyer »</u>.



Une fois de retour dans notre page de volumes, nous avons bien notre <u>« share »</u> et allons désormais <u>« Modifier les autorisations »</u>.

DataPool			ONLI	INE 🥑 588 KiB (0%) Utilisé 2.62 GiB Libr	e			\$
Nom 🗢	Туре 🗢	Utilisé 🗢	Available 🗢	Compression 🗢	Compression Ratio 🗢	Readonly 🗢	Dedup 🗢	Commentaires 🗢	
✓ DataPool	FILESYSTEM	588 KiB	2.62 GiB	Iz4	1.00	false	OFF		
share	FILESYSTEM	96 KiB	2.62 GIB	Hérite (lz4)	1.00	false	OFF	Partage local	
						$\overline{}$		Actions dataset	
								Ajouter un datase	t
								Ajouter un zvol	
								Modifier les optio	ns
								Modifier les autor	isations
									_

Cette étape est très importante, nous allons déterminer les autorisations, via les ACL.

L'utilisateur est celui (utilisateur ou groupe) considéré comme propriétaire du dossier. Groupe, est le groupe de sécurité autorisé à accéder/interagir avec le dossier.

Chemin /mmt/DataPool/share Villiastar SSURREStart Groupe ASSURREStutilisateu ✓ Appliquer Groupe SELECT AN ACL	s du domaine 🔹 🕜	Qui * Utilisateur ASSURNER(\srv-ad Type dACL * Autoriser Type d'autorisations * Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	• ⑦ ⑦ • ⑦ • ⑦ • ⑦ • ⑦
/mrt/DataPool/share Wilsenur ASSURMER(srv-ad	s du domaine	Utilisateur Utilisateur ASSURMER\srv-ad Type d'ACL* Autoriser Type d'autorisations * Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	• ⑦ ⑦ • ⑦ • ⑦ • ⑦ • ⑦ • ⑦
Williamer ASSURMER(\srv-ad @rwge ASSURMER(utilisateu	s du domaine	Utilisateur * ASSURMER\srv-ad Type d'ACL * Autoriser Type d'autorisations * Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	⑦ - ⑦ - ⑦ - ⑦ - ⑦ - ⑦
ASSUMMERIsm-ad	s du domaine [®] ⑦ ⑦ ⑦ PRESET	ASSURMER\srv-ad	2 • (2) • (2) • (2) • (2) • (2)
Appliquer Utilisat Groupe ASSUMAER/utilisateu	rs du domaine 🔹 🕈 🕜	Type dACL * Autoriser Type d'autorisations * Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	• ⑦ • ⑦ • ⑦ • ⑦
Groupe ASSURMER\utilisateu ☑ Appliquer Groupe SELECT AN ACL	rs du domaine 🔹	Autoriser Type d'autorisations * Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	- 0 - 0 - 0 - 0
ASSURMER/utilisateu	rs du domaine 🔹 🕜	Type d'autorisations * Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	• 0 • 0 • 0
SELECT AN ACL	PRESET	Basique Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	- 0 - 0 - 0
SELECT AN ACL	PRESET	Autorisations * Full Control Type de drapeaux * Basique Flags * Hériter	• (?)
SELECT AN ACL	PRESET	Full Control Type de drapeaux * Basique Flags * Hériter	• 0
SELECT AN ACL	PRESET	Type de drapeaux * Basique 	• (?)
SELECT AN ACL	PRESET	Basique Flags* Hériter	* ?
		Flags * Hériter	
		Hériter	
			• 🔅
			SUPPRIMER
		Qui *	
		group@	• ?
		Type d'ACL *	
		Autoriser	• (?)
		Type d'autorisations *	
		Basique	• ⑦
		Autorizations *	
		Lire	• ⑦
		Turne dia diagramma di	
		Basique	* @
		First A	0

Ensuite, pour nos tests, sur la partie gauche, comme à droite, nous avons deux éléments d'ACL, d'abord, l'utilisateur, que nous avons désigné comme étant propriétaire du dossier avec comme autorisation « Full Control ».

Pour le groupe, nous avons choisi « Utilisateurs du domaine » avec les mêmes réglages (à gauche) mais seulement la capacité de « lire ».

Une fois validé, vous aurez donc un partage disponible sur l'adresse suivante, en SMB soit *ip_du_nas*\share.

Phase de testing

Maintenant que tout est en place, nous pouvons tester le bon fonctionnement de la restriction. Grâce au compte Admin « SRV-AD » nous avons pu ajouter un fichier de texte « Test.txt » dans ce dossier partagé.

Ensuite, dans une machine de test virtualisée, nous avons connectés une machine au domaine et connecté un utilisateur du domaine.

Ensuite nous allons sur notre partage, comme présenté ci-dessous :



Puisque nous sommes authentifiés avec un utilisateur du domaine, le dossier apparait sans avoir à retaper d'identifiants.

Désormais, le texte peut s'ouvrir, mais si nous essayons de le supprimer, soit, modifier l'intégrité et la disponibilité du fichier, nous serons alors dans l'impossibilité de supprimer le fichier.

👻 🛧 🚽 > Rése	au > 172.16.0.15 > share	ٽ ~	Rechercher dans	: share	P
-314-	Nom	Modifié le	Туре	Taille	
ies rapide	Test	02/03/2025 14:11	Document texte		1 Ko
léchargements 🖈					
ocuments 🖈					
iages 🖈		Accès au fichier refusé		-	E
ages 🖈 usique		Accès au fichier refusé Vous devez disposer d'une a	autorisation pour eff		E ction.
nages 📌 usique déos		Accès au fichier refusé Vous devez disposer d'une a Vous devez disposer d'une a	autorisation pour eff		ction.
nages 🖈 Iusique déos eDrive		Accès au fichier refusé Vous devez disposer d'une a Vous avez besoin d'une aut modifier ce fichier.	autorisation pour eff orisation de la part d	 fectuer cette ac de ASSURMER\s	Ction. srv-ac
nages 🖈 Iusique idéos eDrive PC		Vous devez disposer d'une au Vous avez besoin d'une aut modifier ce fichier. Test Type : Docume	autorisation pour eff orisation de la part d ent texte		C ction. .srv-ac
mages 🖈 Musique idéos reDrive PC reau		 Accès au fichier refusé Vous devez disposer d'une aut vous avez besoin d'une aut modifier ce fichier. Test Type : Docum Taille : 7 octett Modifié le : 02 	autorisation pour eff orisation de la part d ent texte 5) /03/2025 14:11	— fectuer cette ac de ASSURMER\s	ction. srv-ac

Cela prouve que nous n'avons que le droit de lecture mais pas de modification.

Note aux utilisateurs

Chers utilisateurs,

Dans le cadre de notre engagement à vous offrir un environnement de travail toujours plus sécurisé et fiable, nous mettons en place une solution de stockage de données sur un serveur NAS (Network Attached Storage). Cette démarche a pour objectif de garantir la sécurité et la disponibilité de vos données professionnelles, tout en répondant aux normes les plus strictes en matière de protection des informations.

Pourquoi cette solution ?

Les données que vous manipulez chaque jour sont cruciales pour le bon fonctionnement de l'entreprise. Qu'il s'agisse de documents, de rapports ou de tout autre fichier professionnel, leur intégrité doit être préservée. En cas de panne de système, de perte accidentelle ou de cyberattaque, il est vital de pouvoir récupérer rapidement vos fichiers sans compromettre la sécurité.

C'est pourquoi nous avons décidé de mettre en place un NAS qui centralisera toutes les données sur un support sécurisé et de mettre en œuvre plusieurs niveaux de protection :

- Sauvegardes régulières pour éviter toute perte de données.
- Cryptage des informations sensibles pour garantir leur confidentialité.
- **Contrôle d'accès rigoureux** pour s'assurer que seules les personnes autorisées peuvent accéder à certaines informations.

Comment cela fonctionne-t-il ?

À partir du moment où vous stockez vos fichiers sur le NAS, plusieurs mécanismes de sécurité se déclenchent automatiquement :

- Accès restreint : Vous n'aurez accès qu'aux données dont vous avez besoin pour votre travail. L'accès à des informations sensibles sera limité à certains utilisateurs en fonction de leur rôle.
- **Sauvegardes automatiques** : Tous les fichiers seront régulièrement sauvegardés. En cas de problème, nous pourrons restaurer vos données rapidement et facilement.
- **Cryptage des données** : Pour protéger vos fichiers, ceux-ci seront cryptés. Cela signifie qu'en cas de vol ou de perte du support, les données ne seront pas accessibles sans la clé de décryptage.

Votre collaboration et votre vigilance sont essentielles pour garantir le succès de cette nouvelle solution. Nous vous encourageons à respecter les règles d'accès et de stockage des données et à signaler toute anomalie dès que vous en avez connaissance.

Nous vous remercions pour votre compréhension et votre coopération.

Bien cordialement, L'équipe IT d'Assurmer

Mise en place d'une veille informationnelle sur TrueNAS

Mise en place d'une veille informationnelle automatisée sur TrueNAS

Afin de garantir la sécurité continue de notre serveur NAS TrueNAS, nous mettons en place une veille informationnelle automatisée. Cette solution nous permettra de suivre de manière proactive les mises à jour, les failles de sécurité (CVE) et les alertes importantes, sans nécessiter de surveillance manuelle constante.

Objectif de la veille automatisée

L'objectif principal est de :

- Suivre automatiquement les vulnérabilités et mises à jour de sécurité pour TrueNAS.
- Assurer une gestion rapide des risques sans intervention manuelle.
- Garantir une réactivité instantanée en cas de menace ou de mise à jour critique.

Outils utilisés pour la veille automatisée

Pour rendre cette veille entièrement automatisée, nous utiliserons plusieurs outils :

- Flux RSS : TrueNAS propose des flux RSS qui nous informeront directement des nouvelles mises à jour et alertes de sécurité. Ces informations seront envoyées automatiquement à notre système de gestion des alertes.
- Suivi des CVE : Grâce à des outils comme CVE Search, nous suivrons automatiquement les vulnérabilités affectant TrueNAS. Ces informations seront intégrées dans un tableau de bord qui nous alertera dès qu'une vulnérabilité critique est détectée.
- **Mises à jour automatiques** : Nous configurerons des mises à jour automatiques pour appliquer rapidement les patchs de sécurité dès leur disponibilité.
- Alertes par e-mail : Dès qu'une vulnérabilité ou mise à jour importante est identifiée, nous recevrons une alerte par e-mail, nous permettant d'agir immédiatement.

Actions après réception des alertes

Lorsque nous recevons une alerte :

- 1. **Évaluation automatique** : L'outil analysera la gravité de la vulnérabilité et priorisera les actions à entreprendre.
- 2. **Mise à jour** : Si nécessaire, une mise à jour de sécurité sera automatiquement appliquée.
- 3. **Vérification** : Des tests automatisés seront effectués pour s'assurer que le système est toujours fonctionnel après la mise à jour.

Cette veille automatisée nous permettra de garantir la sécurité de notre serveur NAS en toute simplicité. Grâce à ces outils, nous serons en mesure de répondre rapidement aux nouvelles vulnérabilités, tout en minimisant les interventions manuelles. Cela assurera la protection continue de nos données de manière efficace.

Planning

STATUT	NOM DE LA TÂCHE	Début de la tâche	FAIT PAR
Terminée	Planning de travail et des tâches	9 février 2025	Elise
Terminée	Fonctionnalités principales d'un NAS dont chiffrage et sécurité des données	11 février 2025	Elise
Terminée	Comparaison des différentes solutions RAID et présentation de votre solution retenue	12 février 2025	Elise / Stéphane
Terminée	Procédure d'installation et de configuration de la solution NAS choisie	19 février 2025	Stéphane
Terminée	Testing de la solution	25 février 2025	Stéphane
Terminée	Document d'accompagnement utilisateur	29 février 2024	Stéphane / Elise
Terminée	Veille (outils et résultats) concernant la solution retenue	01 mars 2025	Stéphane / Elise