Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

CONCOURS EXTERNE ET INTERNE DE TECHNICIEN DE CLASSE NORMALE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2020 -

Mardi 7 juillet 2020

Option « Solutions logicielles et systèmes d'information »

Traitement de questions et résolution de cas pratiques, à partir d'un dossier, portant sur l'une des deux options suivantes choisies par le candidat le jour de l'épreuve :

- infrastructures et réseaux,
- solutions logicielles et systèmes d'information.

Cette épreuve permet d'évaluer le niveau de connaissances du candidat, sa capacité à les ordonner pour proposer des solutions techniques pertinentes et à les argumenter.

Le dossier ne peut excéder 20 pages.

(Durée : 3 heures – Coefficient 2)

L'usage de la calculatrice est interdit

Le dossier documentaire comporte 17 pages (hors page d'énoncé du sujet).

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettrez en fin d'épreuve entraînera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A…,B…,Y…,Z…).

IMPORTANT

1. Les copies seront rendues en l'état au service organisateur. A l'issue de l'épreuve, celui-ci procédera à l'anonymisation de la copie.
2. Ne pas utiliser de correcteur d'orthographe sur les copies.
3. Ecrire en noir ou en bleu – Pas d'autre couleur.
4. Il est rappelé aux candidats qu'aucun signe distinctif ne doit apparaître sur la copie.

SUJET

QUESTIONS

Les réponses devront être rédigées sur la copie. L'ensemble des questions sera noté sur 10 points.

Question 1 :

Qu'est-ce qu'un WAF ?

Question 2 :

Qu'est-ce qu'un framework de développement ?

Question 3 :

Qu'est-ce qu'une API ?

Question 4 :

Sous Active Directory, que peut-on placer dans une unité d'organisation ?

Question 5 :

Qu'est-ce qu'un serveur RADIUS ?

Question 6 :

Qu'est ce que LemonLDAP : NG ?

Question 7 :

Comment utiliser le protocole TLS pour sécuriser une application ?

Question 8 :

Qu'est-ce qu'un hyperviseur de type 1 ? Citez le nom de 2 hyperviseurs de ce type.

Question 9 :

Le 25 mai 2018, le RGPD est entré en vigueur. De quoi s'agit-il ?

Question 10 :

Qu'est-ce qu'une vulnérabilité par injection SQL ?

CAS PRATIQUES

Le cas pratique se subdivise en deux parties distinctes. L'ensemble de ces parties sera noté sur 10 points. Lisez attentivement les documents du dossier avant de répondre aux questions.

Contexte :

En votre qualité de technicien(ne) SIC de classe normale, vous venez d'être affecté(e) au service interministériel départemental des systèmes d'information et de communication (SIDSIC), placé auprès du secrétaire général de la préfecture.
Le service interministériel a notamment en charge la conduite et l'intégration de projets applicatifs.
Le secrétaire général, après avoir pris connaissance de l'article « Un œil technique sur les sanctions de la CNIL » annexé au dossier, convoque le responsable SIDSIC et lui demande un rapport complet sur l'état de vulnérabilité des applications web développées en interne.

Étude de cas n° 1 (5 points) :

Vous êtes reçu(e) par le responsable du SIDSIC, qui vous expose la problématique soulevée par le secrétaire général.
Dans une application web, il existe des champs texte ou des formulaires HTML. Si vous tapez un nom d'utilisateur et un mot de passe, ils seront alors envoyés à la base de données pour pouvoir vous authentifier. Ces champs sont généralement la cible d'attaques.

Il vous demande de répondre aux questions suivantes :

1- Commentez et formalisez la requête SQL
SELECT * FROM laureats WHERE username='$username' AND password='$password'

2- Cette requête classique peut être contournée par le biais d'une injection SQL.
- 2.1- Proposez une injection sur la requête SQL précédente. Expliquez.
- 2.2- Est-il possible de sécuriser l'application directement dans le code ? Proposez une solution à votre choix précédent.

3- Proposez une méthode permettant de limiter les risques aux problèmes d'authentification, de contrôle d'accès et de protection des données.

Étude de cas n° 2 (5 points) :

Votre responsable SIDSIC souhaite poursuivre la sécurisation en profondeur de son système d'information. Depuis quelques mois, nous assistons à une augmentation impressionnante du nombre d'attaques visant les infrastructures Microsoft au centre desquelles nous trouvons l'annuaire Active Directory (AD).
Les cybercriminels, à l'origine de ces attaques, profitent de la masse de données accumulées pour gagner de l'argent en rançonnant les entreprises mais aussi les institutions publiques.

Il vous demande, sur la base de vos connaissances acquises et des documents joints au dossier, de répondre aux questions suivantes :

1- Quels sont les deux rôles principaux d'un contrôleur de domaine ?

2- Quelle est la différence entre une identification, une authentification et une autorisation ? Concernant les droits d'accès aux données stockées sur un serveur de fichiers, expliquez le rôle du contrôleur de domaine et celui du serveur de fichiers.

3- Les comptes à privilèges constituent un risque réel et majeur. Toute compromission d'un de ces comptes entraînerait une prise de contrôle instantanée et complète de tout le SI. Proposez une procédure de sauvegarde capable de faire face à ce scénario.

Dossier documentaire :

Document 1	Un œil technique sur les sanctions de la CNIL MISC n°108 mars 2020	Pages 4 à 7
Document 2	Top 10 OWASP https://www.owasp.org/	Pages 8 à 12
Document 3	Modèle Plan de sauvegarde	Page 13 à 15
Document 4	Memo_sauvegardes https://www.cybermalveillance.gouv.fr/	Page 16
Document 5	Extrait du guide Synology 3-2-1 https://download.synology.com/download/www-res/brochure/backup_solution_guide_fr-fr.pdf	Page 17 à 20

Document 1

Un œil technique sur les sanctions de la CNIL

Magazine MISC n°108 Mois de parution mars 2020

Près de trois quarts des sanctions prononcées par la Commission Nationale de l'Informatique et des Libertés (CNIL) ont parmi leurs causes des vulnérabilités techniques de sécurité. À partir de ce constat, et au prisme de notre expérience à la fois en cybersécurité technique et en protection des données à caractère personnel, nous avons analysé les sanctions de la CNIL publiées sur le site https://www.legifrance.gouv.fr/. Nous avons notamment établi une correspondance avec les catégories de vulnérabilités techniques identifiées dans la nomenclature du top 10 de l'OWASP 2017 (Open Web Application Security Project). Nous avons également étudié les fuites de données majeures survenues en Europe et dans le monde. Il en ressort que les vulnérabilités les plus communes sont liées à l'authentification, au contrôle d'accès et à la protection des données au repos et en transit.

Depuis l'entrée en application du Règlement Général sur la Protection des Données (RGPD) en mai 2018 jusqu'au moment de la rédaction de cet article (fin 2019), la CNIL a rendu publiques 4 sanctions. 3 d'entre elles concernent au moins un défaut de sécurité. Rapporté aux 99 articles qui composent le RGPD, force est de constater que seul l'un d'entre eux cristallise l'essentiel des sanctions, l'article 32 relatif à la sécurité. Ces sanctions illustrent en outre qu'il ne suffit pas de mettre en place une gouvernance et des procédures de sécurité pour être conforme au RGPD. Il s'agit aussi de « mettre les mains » dans les systèmes d'information pour mettre en place et contrôler les dispositifs techniques de sécurité, afin d'éviter les failles. En effet, la majorité des vulnérabilités ayant fait l'objet de sanctions auraient pu être détectées, au travers de tests d'intrusion par exemple, en amont des mises en production.

En matière de sécurité, le RGPD n'apporte pas de nouvelles exigences. La raison pour laquelle le sujet se retrouve sur le devant de la scène est l'explosion du plafond des sanctions imposables. Le règlement fixe deux plafonds : les violations et négligences les plus graves peuvent entraîner une amende de 4% du chiffre d'affaires annuel global ou 20 millions d'euros, les défauts de sécurité peuvent engendrer des amendes plafonnées à 2% du chiffre d'affaires annuel global ou 10 millions d'euros. Mais la récidive fait monter le plafond à 4% du chiffre d'affaires ou 20 millions d'euros.

Depuis 2016, la CNIL a prononcé 22 sanctions publiques dont l'une des causes était une vulnérabilité technique, sur un total de 32 sanctions publiées. Ces sanctions ont toutes ou presque débouché sur des amendes pécuniaires. Les montants des amendes dépendent des cas et de la taille de l'organisme contrôlé, et sont par conséquent fluctuants d'une sanction à l'autre, mais ils concernent au global une part croissante des chiffres d'affaires des entreprises. Notons également que tous les secteurs d'activité sont concernés.

Les vulnérabilités observées ont quant à elle quelque peu évolué. Là où en 2016, il s'agissait surtout d'exposition de données sensibles comme l'envoi de données en clair sur Internet, les vulnérabilités liées à l'authentification et au contrôle d'accès sont aujourd'hui prédominantes. Toutefois, l'un n'empêche pas l'autre. Certaines sanctions sont le résultat de plusieurs vulnérabilités simultanées. Dans la plupart des cas, l'infraction initiale qui mène à un contrôle - à distance ou sur place - de la CNIL conduit à l'identification de nouvelles vulnérabilités, qui viennent s'ajouter au socle de la sanction finale.

Les vulnérabilités mentionnées sont en phase avec les problèmes de sécurité les plus souvent constatés par la CNIL en 2018 **[1]**, à savoir des problèmes d'authentification (faiblesse ou absence totale), de contrôle d'accès (utilisation de paramètres incrémentaux dans les requêtes) et de protection des données en transit ou au repos. Cet article élargit le champ d'analyse en regroupant l'ensemble des sanctions et en les comparant au référentiel connu par tous les professionnels de la sécurité, à savoir l'OWASP.

1. Les sanctions de la CNIL à date

Les sanctions publiques de la CNIL prononcées entre 2016 et 2019, dont 70% présentant des vulnérabilités de sécurité, montrent un nombre assez réduit de typologies de vulnérabilités sanctionnées, comme illustré dans le tableau de la figure 1. Les vulnérabilités les plus observées sont les problèmes d'authentification, des faiblesses dans le contrôle d'accès, des erreurs de configuration et un manque de protection des données au repos et en transit. En effet, sur l'ensemble des 3 années cumulées, une vulnérabilité dans l'authentification a été identifiée pour 64% des sanctions, dans le contrôle d'accès pour 46% des sanctions, l'exposition de données sensibles pour 32% des cas et une mauvaise configuration de sécurité pour 14% des sanctions.

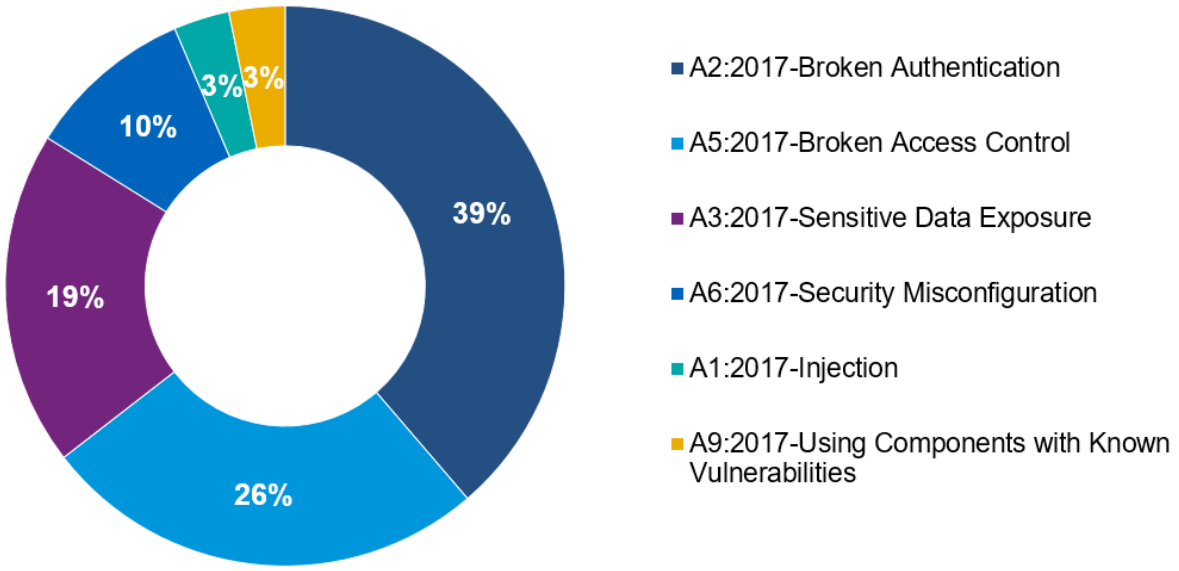
Sanctions publiques de la CNIL liées à la sécurité entre 2016 et 2019

Année	% de sanctions liée à la sécurité	Secteur d'activité	Sanction (en moyenne)*	% des sanctions ayant comme motif des vulnérabilités OWASP 2017*
2019	75%	Assureur Automobile Société de traduction Promoteur immobilier	3 amendes (~200 000 €) 1 injonction à la mise en conformité	100% Broken Authentication 33% Security Misconfiguration 33 % Broken access control
2018	77%	Télécommunication VTC Ingénierie informatique Association Multimédia Produits d'optique Assurance Produit d'électroménagers Télésurveillance	7 amendes (~940 000 €) 2 injonctions à la mise en conformité	66% Broken Authentication 66% Broken access control 22% Sensitive Data Exposure 11% Injection
2017	70%	Transports Jeux pour enfants Editeur de site web Entreprise de rénovation	4 amendes (~13 500 €) 1 avertissement 1 injonction à la mise en conformité	60% Broken Authentication 60% Broken access control 40% Security Misconfiguration 40% Sensitive Data Exposure
2016	50%	Parti politique Détaillant en ligne	2 avertissements 1 amende (~30 000 €)	100% Sensitive Data Exposure 33% Using Components with Known Vulnerabilities
de 2016 à 2019 (cumul)	70%	NA	68% d'amendes (~295 875 €) 18% d'injonctions à la mise en conformité 14% d'avertissement	64% Broken Authentication 46% Broken access control 32% Sensitive Data Exposure 14% Security Misconfiguration 5% Using Components with Known Vulnerabilities 5% Injection

(*) Une sanction peut être liée à plusieurs vulnérabilités techniques

Fig. 1 : Tableau récapitulatif des sanctions publiques de la CNIL liées à la sécurité par année, secteur d'activité, typologie de sanction et vulnérabilité OWASP.

Lorsque l'on recoupe l'ensemble des vulnérabilités avec le top 10 de l'OWASP (2017) sans distinction des sanctions, il ressort, comme illustré dans la figure 2, que les vulnérabilités de catégories « A2:2017-Broken Authentication », « A5:2017-Broken Access Control » et « A3:2017-Sensitive Data Exposure » dominent largement le paysage.



2. Analyse des sanctions liées à des défauts dans l'authentification

Dans 64% des sanctions liées à la sécurité, la CNIL a identifié des défauts d'authentification (A2:2017-Broken Authentication) comme l'absence d'une politique robuste de mots de passe, l'absence de mécanisme de protection contre les attaques par force brute ou l'absence totale d'authentification, causant l'accès à des données utilisateur par n'importe quel internaute.
Néanmoins, il ne suffit pas de prévoir des mesures d'authentification, encore faut-il sécuriser le stockage des informations de connexion.

3. Analyse des sanctions liées à des défauts dans le contrôle d'accès

Dans 46% des sanctions liées à la sécurité, la CNIL a identifié des vulnérabilités dans le contrôle d'accès (A5:2017-Broken Access Control) permettant par exemple, par la simple modification d'un paramètre de la requête envoyée au serveur, d'accéder aux données d'autres utilisateurs, en d'autres termes, un Direct Object Reference sur les données d'un utilisateur.

4. Analyse des sanctions liées à l'exposition de données sensibles

Dans 32% des sanctions liées à la sécurité, une vulnérabilité liée à la protection des données en transit et au repos (A3 : 2017 - comme Sensitive Data Exposure) a été identifiée. Les faits observés sont l'utilisation de protocoles vulnérables ou d'algorithmes cryptographiques faibles et l'absence totale de protocoles de sécurité comme l'utilisation de HTTP.

5. Analyse des sanctions liées à une mauvaise configuration de la sécurité

Dans 14% des sanctions liées à la sécurité, la CNIL relève un défaut dans la configuration de la sécurité (A6-2017-Security Misconfiguration). En 2017, une société de transports a ainsi été sanctionnée, entre autres, parce que l'API publiée par le site renvoyait des informations sur les utilisateurs qui étaient censées rester dans le backoffice. En effet, une requête comme https://www.example.com/api/car/search?dpt=75 retournait l'ensemble des voitures proposées dans le département donné en paramètre, ainsi que les données des propriétaires et des clients qui avaient loué ces voitures précédemment.

6. Analyse des sanctions liées à d'autres défauts de sécurité

Parmi les autres failles de sécurité recensées par l'OWASP, les injections et l'utilisation de composants présentant des vulnérabilités connues, sont présentes chacune dans 5% des sanctions de la CNIL liées à la sécurité.

En 2016, un parti politique français a écopé d'un avertissement pour avoir divulgué les noms de ses adhérents en raison de l'utilisation de la méthode GET qui envoie le secret d'authentification de l'utilisateur dans les paramètres de l'URL, sachant que le secret contenu au sein de l'URL était haché à l'aide de MD5 sans sel. En 2018, une société de multimédia a subi une attaque de type « injection SQL », qui a permis d'exécuter des requêtes SELECT sur les tables user et user_passwords de la base de données du site web. Le rapport de la CNIL fait état de la combinaison de six facteurs pour l'exploitation, à savoir « 1. un accès frauduleux au code source de la société (stocké sur GitHub), 2. l'identification d'un bug exploitable de manière malveillante au sein des centaines de milliers de lignes de code de la plateforme, 3. le développement d'une compréhension de l'architecture de la plateforme permettant d'identifier les conditions nécessaires et suffisantes à l'exploitation malveillante du bug, 4. le développement d'un code d'exploitation spécifique à même de déclencher et de tirer profit du bug, 5. la capacité de détourner un compte d'administration pour exploiter le bug identifié, 6. la propagation de l'intrusion depuis les serveurs web vers des données tout en masquant son identité réelle par un jeu de rebonds vers des serveurs loués spécifiquement à ces fins ».

Conclusion

Les sanctions de la CNIL à date révèlent que la sécurité technique reste un élément prépondérant de la question de la protection des données personnelles. L'article 32 représente 1% du RGPD, mais est invoqué dans près de trois quarts des sanctions de la CNIL. Les exemples mentionnés font état de vulnérabilités de sécurité plutôt bien connues par la communauté de la sécurité des SI, et maîtrisables quand on a pris le temps et les mesures pour les mettre sous contrôle en avance de phase.

La CNIL a profité de chaque sanction pour rappeler, dans ses délibérations, les règles de sécurité de base en la matière, à savoir la mise de place de mécanismes d'authentification, la mise en place de politique de mot de passe, le chiffrement des données au repos et en transit, la mise en place de contrôle d'accès et le fait de procéder à un protocole complet de test en amont de la mise en production d'un site Internet. Par ailleurs, la CNIL a publié sur son site web plusieurs guides portant sur la sécurité des données personnelles.

Enfin, notons que les sanctions publiques prononcées par la CNIL, entre 2016 et 2019, et liées à la sécurité l'ont été pour près de 3/4 d'entre elles suite à un signalement citoyen. Un peu comme si la CNIL avait son propre programme de bug bounty (citoyen) !

[1] https://www.cnil.fr/fr/securite-des-sites-web-les-5-problemes-les-plus-souvent-constates

Site officiel :https://www.owasp.org/

I Introduction

1- Les applications web sont partout

Aujourd'hui, les applications web sont partout. Elles sont utilisées quotidiennement dans nos activités personnelles ou professionnelles (réseaux sociaux, achats en lignes, démarches administratives…). Toute entreprise ou administration se doit d'avoir un site web. Ces applications facilitent les échanges et les transactions car elles sont accessibles de partout à l'aide d'un simple navigateur sur un smartphone ou un ordinateur de bureau.
Si au début des sites web, les aspects techniques et fonctionnels étaient suffisants, ce n'est plus du tout le cas aujourd'hui. L'actualité nous rappelle régulièrement que des entreprises voient leur site web attaqué. Les conséquences peuvent être lourdes (perte de données, baisse du chiffre d'affaire, effondrement de la réputation…). Avec comme enjeu, la survie de l'entreprise selon la gravité de l'attaque subie.
En outre, Le règlement règlement général sur la protection des données (RGPD), mis en place au sein de l'Union Européenne, oblige les entreprises à assurer la sécurité des données personnelles qu'elles collectent.

2- La sécurisation des applications web est indispensable

La sécurité des applications web est donc devenue un enjeu stratégique. Lors de son édition 2016, la société EY (http://www.ey.com/fr) a montré qu'une majorité des entreprises mondiales n'a pas de stratégie en matière de lutte contre les cybermenaces.
Au delà de l'aspect fonctionnel des outils de développement, il est indispensable pour tout développeur de savoir identifier les vulnérabilités potentielles et de prendre en compte les menaces en adaptant son développement à l'aide de bonnes pratiques. La phase de test ne doit pas se limiter au fonctionnement attendu du code mis en œuvre mais elle doit aussi anticiper les utilisations malveillantes comme les injections de code SQL dans les formulaires.
Afin de mettre en place une veille stratégique sur la sécurisation des applications web, le groupe OWASP a développé une base de données qui recense la liste des incidents de sécurité recensés sur les applications web. Cette base nommée WASC-WHID (Web application Security Consortium -Web Hacking Database Project) permet de disposer de statistiques sur les failles de sécurité relevées
sur les applications web. Les incidents sont déclarés et enregistrés afin d'alimenter une base de connaissance.

Le lien permettant d'accéder aux outils WHID est le suivant :
https://www.owasp.org/index.php/OWASP_WASC_Web_Hacking_Incidents_Database_Project

II Présentation d'OWASP

1- La communauté OWASP

OWASP (Open Web Application Security project) est une communauté travaillant sur la sécurité des applications web. Elle a pour but de publier des recommandations de sécurisation des sites web et propose des outils permettant de tester la sécurité des applications web.

2- Le top 10 d'OWASP

OWASP fournit une liste des risques de sécurité des applications web les plus courants. En 2017, OWASP a mis à jour son classement afin de sensibiliser les développeurs web aux risques encourus. Les 10 risques classés par ordre de dangerosité sont les suivants :

Top 10 OWASP - 2013	→	Top 10 OWASP - 2017
A1-Injection	→	A1:2017-Injection
A2-Violation de Gestion d'authentification et de Session	→	A2:2017-Violation de Gestion d'Authentification
A3-Cross-Site Scripting (XSS)	↓	A3:2017-Exposition de Données Sensibles
A4-Références Directes Non Sécurisées à un Objet [Fusionné avec A7 dans A5:2017]	F	A4:2017 Entités Externes XML (XXE) [Nouveau]
A5-Mauvaise Configuration Sécurité	↓	A5:2017-Violation du Contrôle d'Accès [Fusion des A4 et A7 de 2013]
A6-Exposition de Données Sensibles	↑	A6:2017-Mauvaise Configuration Sécurité
A7- Manque de Contrôle d'Accès au niveau Fonctionnel [Fusionné avec A7 dans A5:2017]	F	A7:2017-Cross-Site Scripting (XSS)
A8-Falsification de Requête Intersites (CSRF) [Supprimé]	S	A8:2017-Désérialisation Non Sécurisée [Nouveau, Communauté]
A9-Utilisation de Composants avec des Vulnérabilités Connues	→	A9:2017-Utilisation de Composants avec des Vulnérabilités Connues
A10-Redirection et Renvois Non Validés [Supprimé]	S	A10:2017-Supervision et Journalisation Insuffisantes [Nouveau, Communauté]

III Les risques du top 10 d'OWASP

1- Le risque A2 Violation de gestion d'authentification

Lors du développement d'une application, le codage des fonctions liées à l'authentification et à la gestion des sessions (cookie de session) peuvent être incorrectement implémentées, permettant ainsi à des attaquants de compromettre des mots de passe et des identifiants de session.

1.1- Conséquences

En cas de force brute sur des mots de passe ou de vol d'identifiant de session (session hijacking), une personne malveillante peut s'identifier avec le compte d'un autre utilisateur voire avec celui de l'administrateur. Les conséquences peuvent être particulièrement graves sur une application manipulant des données hautement confidentielles (applications médicales, bancaires…). Par ailleurs, le Règlement général sur la protection des données (RGPD) confère à la CNIL des missions supplémentaires et un pouvoir de contrôle et de sanction accru en matière de protection des données ce qui renforce l'obligation des entreprises d'assurer la sécurité des données manipulées.
Si le codage des fonctions liées à l'authentification et à la gestion des sessions est mal implémenté, l'application web risque d'offrir les vulnérabilités suivantes :

- Tests d'authentification possibles sur des listes de login et de mots de passe : énumération des logins valides puis force brute des mots de passe ;
- Identification à l'aide de mots de passe par défaut encore actifs lors de la phase de déploiement de l'application : certaines applications web comportent des comptes avec des mots de passe par défaut (glpi/glpi pour l'application GLPI ou nagios/nagiosadmin pour l'application nagios ou admin/cisco sur un routeur Cisco WRV215 , etc.) ;
- Création autorisée de comptes utilisateurs avec des mots de passe non sécurisés tels que admin ou password1 ;
- Codage non sécurisé des fonctionnalités permettant à un utilisateur de retrouver son mot de passe en cas d'oubli ;
- Mots de passe écrits en dur dans du code source, mots de passe non chiffrés ou faiblement hashés (absence de fonction de salage) ;
- Absence ou mauvais codage des fonctions gérant les authentifications multi-formes pour les applications très sensibles en terme de confidentialité des informations ;
- Mauvaise implémentation des cookies de session : cookie d'identifiant de session prévisible, exposition des sessions ID dans l'URL, absence de rotation des sessions ID après un succès d'authentification ou après une déconnexion, pas de timeout sur les sessions ID.

1.2- Bonnes pratiques

Les bonnes pratiques suivantes peuvent être mises en place en tant que limitations ou contre-mesures des vulnérabilités présentées en amont :

- Le développeur ne doit pas indiquer la raison d'un échec d'authentification : login incorrect ou mot de passe incorrect. Il faut simplement indiquer qu'il y a un échec d'authentification sans donner plus de détails par une phrase du type : échec d'authentification ;
- Il faut coder des fonctions qui imposent un changement de mot de passe lors de la première connexion et supprimer les comptes inutiles comportant des mots de passe par défaut lors du déploiement de l'application ;
- Il faut interdire les mots de passe non sécurisés (mots de passe du dictionnaire) en testant la solidité des mots de passe au moment de la création des comptes (codage qui impose une longueur minimale, la présence de caractères spéciaux…) ;
- Il faut s'assurer que les fonctions permettant de retrouver un mot de passe en cas d'oubli ne présentent pas un codage trop laxiste (demande d'une couleur préférée par exemple) ;
- Externaliser le stockage des mots de passe et les stocker sous forme chiffrée : ne pas stocker des mots de passe en clair dans du code source, utiliser des fonctions de salage lorsque les mots de passe sont hashés afin de prévenir les attaques du type table arc-en-ciel (rainbow table[1]) ;
- Les applications manipulant des informations hautement confidentielles doivent comporter des modules d'authentifications multi-formes en plus du traditionnel login/mot de passe : possession d'un objet pour déchiffrer un contenu, biométrie, géolocalisation… ;
- Générer des cookies d'identifiant de sessions non prévisibles, qui changent après un succès d'authentification, les désactiver après une déconnexion et programmer une durée de validité (timeout).

(1) Rainbow table : attaque permettant de cracker l'empreinte (hash) d'un mot de passe.

2- Le risque A3 Exposition de données sensibles

Au cours des dernières années, cela a été l'attaque impactante la plus courante. La principale erreur est de ne pas chiffrer les données sensibles. Les autres erreurs fréquentes sont : génération de clés faibles, choix et configuration incorrects des algorithmes et protection insuffisante des mots de passe. En ce qui concerne les données en transit, les faiblesses côté serveur sont pour la plupart faciles à détecter. C'est plus difficile pour les données déjà stockées.

2.1- Êtes-vous vulnérable ?

L’exploitation peut résulter en la compromission ou la perte de données personnelles, médicales, financières, d’éléments de cartes de crédit ou d’authentification. Ces données nécessitent souvent une protection telle que définie par le Règlement Général sur la Protection des Données ou les lois locales sur la vie privée.
Déterminer d’abord, quelles données doivent bénéficier d’une protection chiffrée (mots de passe, données patient, numéros de cartes, données personnelles, etc.), lors de leur transfert et/ou leur stockage.
Pour chacune de ces données :

- Les données circulent-elles en clair ? Ceci concerne les protocoles tels que HTTP, SMTP, et FTP. Le trafic externe sur inernet est particulièrement dangereux. Vérifiez tout le réseau interne, par exemple entre les équilibreurs de charge, les serveurs Web, ou les systèmes backend.
- Des algorithmes faibles ou désuets sont-ils utilisés, soit par défaut, soit dans le code source existant ?
- Est-ce que des clefs de chiffrement par défaut sont utilisées ? Des clefs faibles sont-elles générées ou réutilisées ? Leur gestion et rotation sont-elles prises en charge ?
- Les réponses transmises au navigateur incluent-elles les directives/en-têtes de sécurité adéquats ?
- Est-ce que l'agent utilisateur (l'application ou le client mail, par exemple) vérifie que le certificat envoyé par le serveur est valide ?

2.2- Bonnes pratiques

On veillera au minimum à suivre les recommandations suivantes, mais il reste nécessaire de consulter les références.

- Classifier les données traitées, stockées ou transmises par l'application. Identifier quelles données sont sensibles selon les lois concernant la protection de la vie privée, les exigences réglementaires, ou les besoins métier.
- Appliquer des contrôles selon la classification.
- Ne pas stocker de données sensibles sans que cela ne soit nécessaire. Les rejeter ou utiliser une tokenisation conforme à la norme de sécurité de l’industrie des cartes de paiement (PCI DSS) ou même une troncature. Les données que l’on ne possède pas ne peuvent être volées !
- S'assurer de chiffrer toutes les données sensibles au repos.
- Choisir des algorithmes éprouvés et générer des clés robustes. S'assurer qu'une gestion des clés est en place.
- Chiffrer toutes les données transmises avec des protocoles sécurisés tels que TLS avec des chiffres à confidentialité persistante (perfect forward secrecy - PFS). Chiffrer en priorité sur le serveur. Utiliser des paramètres sécurisés. Forcer le chiffrement en utilisant des directives comme HTTP Strict Transport Security (HSTS).
- Désactiver le cache pour les réponses contenant des données sensibles.
- Stocker les mots de passe au moyen de puissantes fonctions de hachage adaptatives, avec sel et facteur de travail (ou facteur de retard), comme Argon2, scrypt, bcrypt ou PBKDF2.
- Vérifier indépendamment l'efficacité de la configuration et des paramètres.

3- Le risque A5 Violation du contrôle d’accès

Les contrôles d'accès appliquent une politique assurant que les utilisateurs respectent leurs permissions. Les vulnérabilités de contrôles d'accès surviennent souvent par le manque de détection automatique, et le manque de tests fonctionnels effectifs par les développeurs d'applications.

3.1 Conséquences

Une faille entraînera généralement des fuites d'informations, des corruptions ou destructions de données, ou permettra des actions en dehors des autorisations de l'utilisateur.
Les vulnérabilités de contrôle d'accès consistent généralement :

- A contourner les contrôles d'accès en modifiant l'URL, l'état interne de l'application, ou la page HTML ; ou simplement en utilisant un outil dédié d'attaque d'API.
- A permettre la modification de la clef primaire pour pointer sur l'enregistrement d'un autre utilisateur, donnant ainsi la possibilité de voir ou modifier le compte de quelqu'un d'autre.
- A permettre une élévation de privilège, c'est à dire permettre d'agir comme un utilisateur connecté, ou comme administrateur alors que l'on est connecté comme utilisateur.
- A permettre les manipulations de meta-données, comme le rejeu ou la modification de JSON Web Token (JWT), de cookies ou de champs cachés, afin d'élever les privilèges, ou d'abuser les invalidations JWT.
- A permettre l'accès non-autorisé à des API, par mauvaise configuration CORS.
- A permettre la navigation forcée vers des pages soumises à authentification sans être authentifié, ou à des pages soumises à accès privilégié en étant connecté comme simple utilisateur. A permettre l'accès à des API sans contrôle pour POST, PUT et DELETE.

3.2- Bonnes pratiques

Les contrôles d'accès ne sont efficaces que s'ils sont appliqués dans du code de confiance côté serveur ou dans des API server-less, là ou un attaquant ne peut pas modifier les vérifications des contrôles ni les meta-données.

- A l'exception des ressources publiques, tout doit être bloqué par défaut.
- Centraliser l'implémentation des mécanismes de contrôle d'accès et les réutiliser dans l'ensemble de l'application. Cela comprend de minimiser l'utilisation de CORS.
- Le modèle de contrôle d'accès doit vérifier l'appartenance des enregistrements, plutôt que de permettre à l'utilisateur de créer, lire, modifier ou supprimer n'importe quel enregistrement.
- Les exigences spécifiques métier de l'application doivent être appliquées par domaines.
- Désactiver le listing de dossier sur le serveur web, et vérifier que les fichiers de meta-données (ex : .git) et de sauvegardes ne se trouvent pas dans l'arborescence web.
- Tracer les échecs de contrôles d'accès, les alertes administrateur quand c'est approprié (ex : échecs répétés).
- Limiter la fréquence d'accès aux API et aux contrôleurs d'accès, afin de minimiser les dégats que causeraient des outils d'attaques automatisés.
- Les jetons JWT doivent être invalidés côté serveur après une déconnexion.
- Les développeurs et les testeurs qualités doivent procéder à des tests unitaires et d'intégration sur les fonctionnalités de contrôle d'accès.

Plan de sauvegarde du système d'information

de [SERVICE]

Table des matières

Références :.....1
Glossaire :.....1
Historique des modifications.....1
Préambule :.....2
Instructions concernant la rédaction du document :.....2
Tableau de synthèse des sauvegardes.....3

Références :

- Note Préfecture n° 1 du 01/01/2010 Amélioration de la maîtrise des activités et des risques.
- Note Préfecture n° 1 du 01/01/2020 Rappel des mesures indispensables en matière SSI.

Glossaire :

- Sauvegarde complète : Sauvegarde permettant à elle seule de restaurer toutes les informations permettant la remise en service l'application (application + données).
- Sauvegarde non complètes : la remise en service de l'application nécessite en plus de cette sauvegarde, la restauration de sauvegardes précédentes, en fonction des cas :
  - Sauvegarde différentielle :Seules les données modifiées depuis la dernière sauvegarde complète sont sauvegardées : la remise en service nécessite donc la dernière sauvegarde complète et la dernière sauvegarde différentielle.
  - Sauvegarde incrémentale : Seules les données modifiées depuis la dernière sauvegarde (complète ou incrémentale) sont sauvegardées. : la remise en service nécessite donc la dernière sauvegarde complète et l'ensemble des sauvegardes incrémentales effectuées.

Historique des modifications

Version	Contenu	Date	Auteur
0.1	Création du modèle	01/01/10	
0.2	Mise à jour du modèle	01/01/11	

Préambule :

Dans ce document sont synthétisées les procédures de sauvegardes des données des systèmes d'information du service.

L'objectif de ce document est de permettre au lecteur (autorités hiérarchiques, auditeurs…), d'identifier les données présentes et utilisées sur le site du service et savoir où et comment elles sont sauvegardées.

Instructions concernant la rédaction du document :

Ce document doit être mis à jour régulièrement et au moins une fois par an.

Il doit mentionner toutes les données du service, même si elles ne font pas l'objet d'une sauvegarde pour l'instant.

Des informations complémentaires peuvent être ajoutées, telles que :

- La procédure détaillée de sauvegarde
- Les procédures de restauration
- Les temps de sauvegarde
- Occupation de la bande passante dans le cadre d'une sauvegarde sur site distant.
- La sensibilité des données
- Le Temps d'indisponibilité acceptable de la donnée
- Le Risque de perte de donnée

Tableau de synthèse des sauvegardes

- Où sont les données quand elles sont exploitées ? Nom du (ou des) serveur (s), nom de la salle
- Où et comment sont faites les sauvegardes ? (la description doit être exhaustive)
  - Préciser le type de fréquence (Quotidienne / hebdomadaire / mensuelle… Différentielle/incrémentielle/complète…), l'heure de lancement et la durée..
  - Les appareils de sauvegarde sont tous les appareils de stockage qui entrent dans la chaîne de sauvegarde (serveurs de sauvegarde, NAS, Disque dur Externe, Robot de sauvegarde…), ainsi que leur emplacement
  - Préciser si elles sont automatiques ou font l'objet d'une procédure manuelle et dans ce cas, par qui ?
  - Préciser la durée de rétention (durée jusqu'à laquelle il est possible de récupérer des données).

Données	Exploitation		Sauvegarde				Restauration
	Nom du serveur	Lieu d'exploitation	Appareil de sauvegarde	Lieu de sauvegarde	Description :	Durée de Rétention	Date du dernier test de restauration
					Type de sauvegarde Fréquence Temps Logiciel ...		Date Temps

Visa du responsable informatique.	Visa du RSSI	Visa du responsable du site

Document 4

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

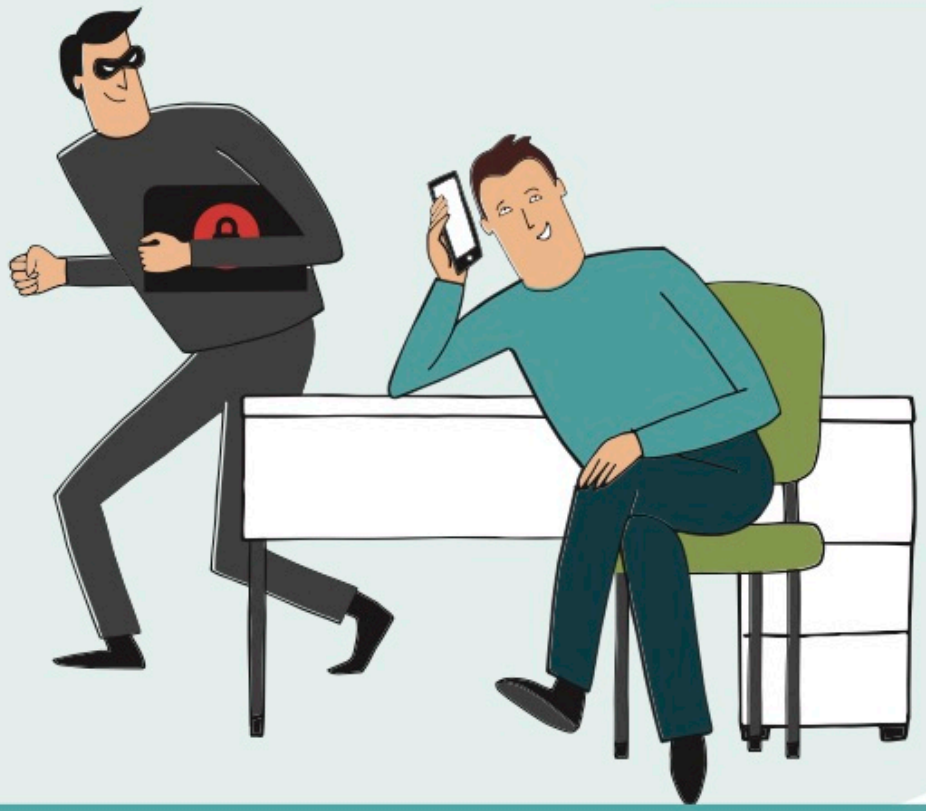
LES SAUVEGARDES

Mémo

ADOPTER LES BONNES PRATIQUES

10 CONSEILS POUR ÉVITER DE PERDRE VOS DONNÉES

1. Effectuez des sauvegardes régulières de vos données
2. Identifiez les appareils et supports qui contiennent des données
3. Déterminez quelles données doivent être sauvegardées
4. Choisissez une solution de sauvegarde adaptée à vos besoins
5. Planifiez vos sauvegardes
6. Déconnectez votre support de sauvegarde après utilisation
7. Protégez vos sauvegardes (perte, vol, casse...)
8. Testez vos sauvegardes
9. Vérifiez le support de sauvegarde
10 Pro. Sauvegardez les logiciels indispensables à l'exploitation de vos données



POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

Stratégie de protection des données : la règle de sauvegarde 3-2-1

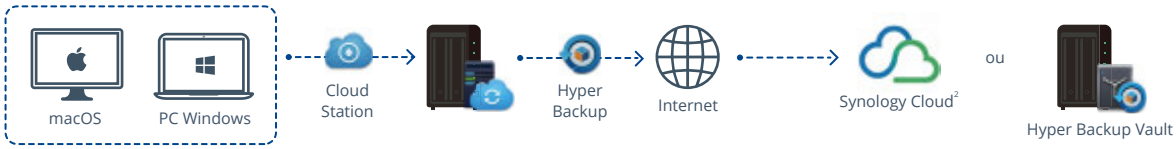
3 Créez au moins 3 copies de vos données.

2 Conservez ces copies sur 2 supports différents.

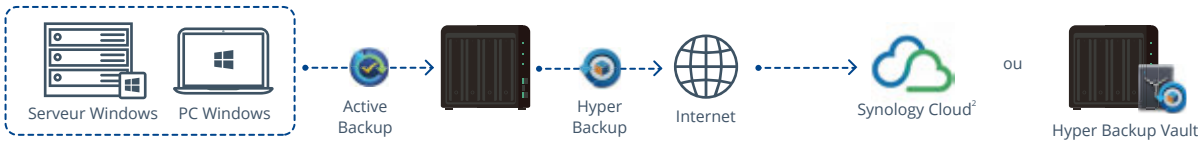
1 Stockez au moins 1 copie des données hors site.

Les pertes inattendues de données résultant de pannes de disque dur, de catastrophes naturelles et d'attaque par rançongiciels constituent de potentielles menaces pour vos données critiques. Utilisez la stratégie de sauvegarde 3-2-1 pour protéger vos photos de famille, vos vidéos et vos données d'entreprise, et pour réduire ainsi le risque de perte de données. Reportez-vous aux meilleures pratiques de sauvegarde répertoriées ci-dessous.

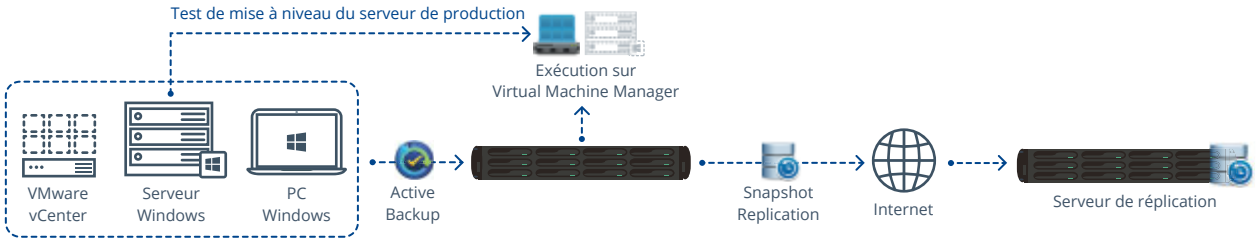
Utilisateurs particuliers à domicile (de 1 à 10 périphériques) : sauvegarde de fichiers uniquement



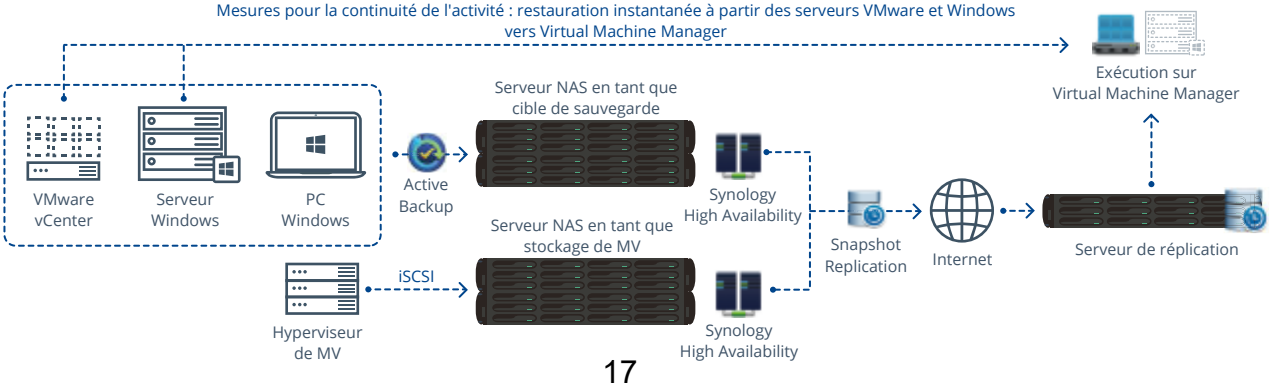
Petites entreprises et petits groupes de travail (de 11 à 50 périphériques) : sauvegarde de fichiers et sauvegarde complète



PME et réseaux de bureaux (de 51 à 200 périphériques) : sauvegarde de fichiers et sauvegarde complète



Entreprises (plus de 200 périphériques) : sauvegarde de fichiers, LUN et sauvegarde complète

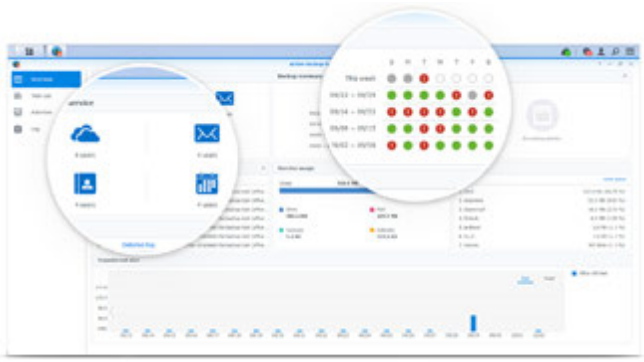


Active Backup for Business

Pour protéger les environnements informatiques d'entreprise complexes avec un coût total réduit

- Portail qui centralise et gère toutes les tâches de sauvegarde d'ordinateurs, de serveurs Windows et de machines virtuelles
- Sauvegarde de tous les périphériques avec un serveur NAS, sans aucune licence
- Exécution des images de MV directement sur Synology VMM, avec prise en charge de la vérification de sauvegarde, des tests de basculement, etc.

Tableau comparatif	Sans agent		Basé sur un agent	
	Serveur de fichiers	VMware		Serveur
Sauvegarde d'images	—	○	○	○
Restauration d'images	—	○	○	○
Restauration de fichiers/dossiers	○	○	○	○
Déduplication au niveau des blocs	Fichier	Entre les images	Entre les images	Entre les images

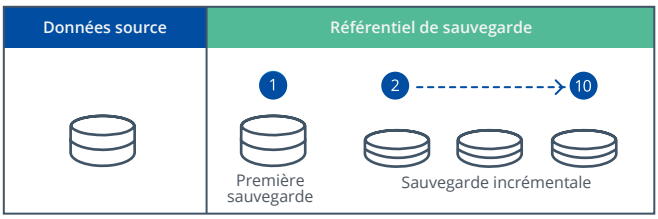


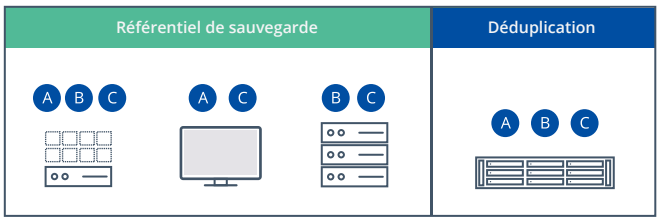
Gestion centralisée

Pour gérer plusieurs serveurs/clients avec un seul serveur NAS

Intégrez toutes les tâches de sauvegarde des ordinateurs, serveurs et machines virtuelles. Grâce à l'interface facile à utiliser, vous pouvez configurer et surveiller la sauvegarde de vos données en toute simplicité. D'autres fonctions sont également incluses, telles que les notifications et les rapports réguliers.

Optimisation de l'efficacité des sauvegardes





Pour déployer une technologie d'entreprise avec les fonctions payantes d'autres éditeurs de logiciels

La sauvegarde incrémentale au niveau des blocs et la déduplication globale réduisent considérablement la durée de la sauvegarde et la capacité de stockage requise. En outre, la technologie CBT (Changed Block Tracking) est prise en charge lors de la sauvegarde de serveurs Windows et VMware.

SCÉNARIO

C

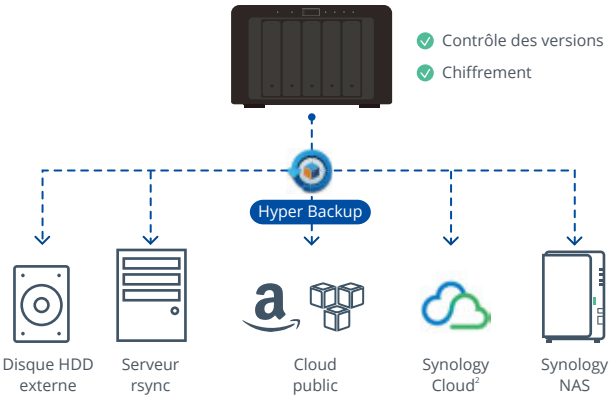
Sauvegarde d'un serveur NAS vers d'autres périphériques

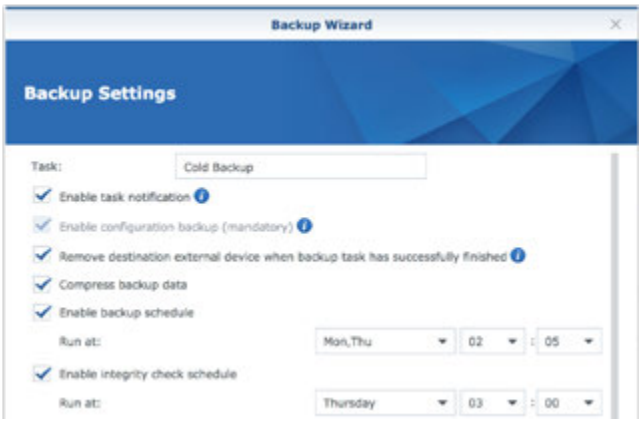
Sauvegardez les données stockées sur votre serveur Synology NAS sur un site distant ou sur un autre support pour pouvoir les récupérer efficacement après un sinistre ou une attaque par rançongiciel.

Hyper Backup

Pour sauvegarder des données et des configurations du serveur NAS vers un autre serveur/support

- Possibilité de définir un serveur Synology NAS ou un service de cloud public comme destination de sauvegarde
- Prise en charge de la sauvegarde des données pour les dossiers partagés et de la sauvegarde d'applications pour les paquets et les paramètres système
- Économie d'espace de stockage et de bande passante grâce à un taux élevée de compression des données
- Prise en charge du chiffrement des données et de la transmission
- Calcul du volume estimé de données, de l'espace requis et de la durée nécessaire avant l'exécution de tâches de sauvegarde





Configuration de planifications pour gérer efficacement la bande passante

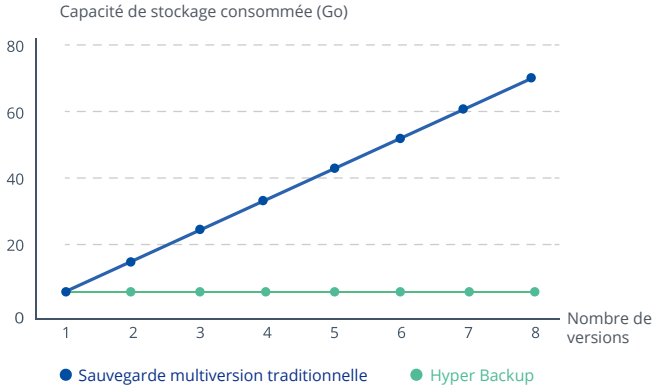
Pour effectuer des tâches de sauvegarde pendant les heures creuses

Planifiez les tâches de sauvegarde pendant les heures creuses du réseau, par exemple à minuit, afin de libérer la bande passante du réseau pendant la journée.

Sauvegarde multiversion

Pour exploiter la capacité de stockage pour plusieurs versions

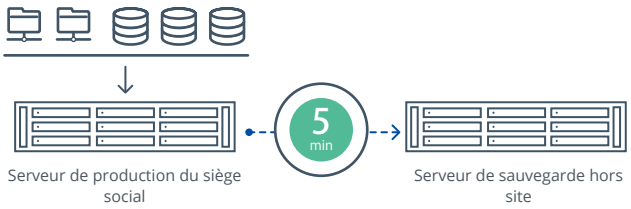
Vous pouvez conserver jusqu'à 65 535 versions, tandis que la sauvegarde incrémentale conserve l'espace de stockage nécessaire même si le nombre de versions augmente. Personnalisez votre propre stratégie de rotation des versions antérieures pour supprimer les sauvegardes inutiles.

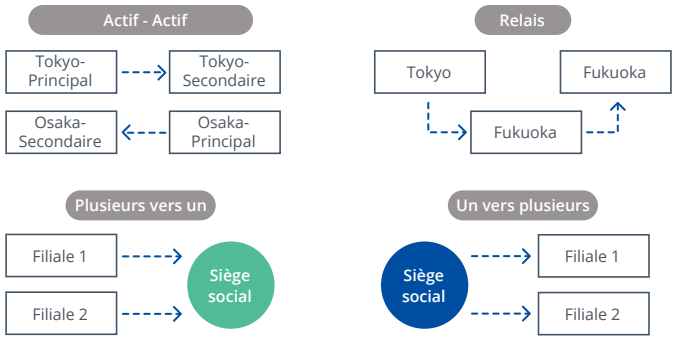


Snapshot Replication

Pour éviter les erreurs humaines grâce aux instantanés et utiliser la réplication comme solution de récupération après sinistre

- Prise d'instantanés toutes les 5 minutes pour les dossiers partagés et toutes les 15 minutes pour les iSCSI LUN, en un temps record
- Possibilité de réplication instantanée des instantanés de dossiers partagés et de LUN afin de limiter l'impact sur les performances globales du serveur NAS
- Basculement des services vers le serveur répliqué en cas de panne du serveur actif



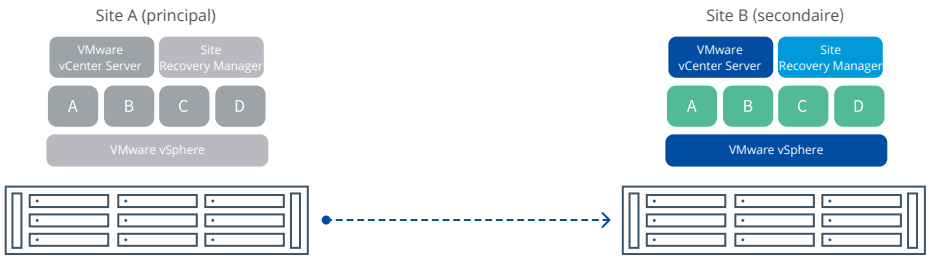


Diverses combinaisons de réplication

Pour personnaliser la réplication en fonction de la structure et des stratégies de l'entreprise

Configurez la réplication selon différentes combinaisons afin de l'adapter de manière flexible à chaque environnement professionnel après la prise d'instantanés.

Diminution de l'objectif de temps de récupération (RTO)



Compatibilité avec VMware Site Recovery Manager

En cas de panne du serveur actif, le système VMware Site Recovery Manager compatible effectue la restauration directement depuis vCenter, ce qui simplifie le processus de restauration.