RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SAUVEGARDE DES SYSTÈMES D'INFORMATION

LES FONDAMENTAUX

ANSSI-BP-100
18/10/2023

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Sauvegarde des systèmes d'information »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	18/10/2023	Version initiale

Table des matières

1
Contexte

La menace liée aux rançongiciels est prégnante [1] à la date de publication de ce document. Toute entité peut subir une attaque opportuniste ou ciblée d'un groupe cybercriminel. La sauvegarde des systèmes d'information, initialement utile dans le cas d'incidents opérationnels (ex. : panne matérielle) est aujourd'hui indispensable pour répondre efficacement aux incidents de sécurité.

Il est fréquent qu'un attaquant tente de chiffrer, d'effacer ou de rendre indisponible l'infrastructure de sauvegarde, dans le but de ralentir la reconstruction du SI impacté et donc d'augmenter ses chances d'obtenir la rançon.

Les recommandations de ce document ont pour objet de sécuriser l'infrastructure de sauvegarde mise en place. Elles doivent être prises en compte au cas par cas en fonction du contexte, de la taille et de la criticité du SI que l'on souhaite protéger. Les recommandations en **gras** sont considérées comme les plus importantes et les plus prioritaires.

1. Panorama de la cybermenace 2022 consultable sur https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/.

2
Rappels

- Une stratégie de sauvegarde doit notamment tenir compte de la perte de données maximale admissible (PDMA [2]) et de la durée maximale d'interruption admissible (DMIA [3]) définies pour l'ensemble des valeurs métier du SI de l'entité (applications, données) [4].
- Certains cas d'usage ne sont pas couverts par la sauvegarde, par exemple :
  - le besoin d'une PDMA de moins de 24h ; dans ce cas, privilégier d'autres solutions telle que la réplication (synchrone ou asynchrone) ;
  - le besoin d'archivage légal, impliquant parfois un besoin d'authenticité des données (qui n'est pas forcément couvert par une solution de sauvegarde).
- Les composants essentiels d'une infrastructure de sauvegarde sont :
  - le catalogue/index qui permet de savoir ce qui est sauvegardé ;
  - l'agent logiciel de sauvegarde présent sur les serveurs sauvegardés ;
  - le serveur de sauvegarde qui traite le flux de sauvegarde avant envoi sur un support ;
  - le support de sauvegarde : disques, bandes magnétiques, disque externe USB, etc.
- La stratégie de sauvegarde doit notamment définir les durées de rétention des sauvegardes. Cette stratégie précise la répartition à long terme : 15 jours de sauvegardes journalières, 1 an de sauvegardes mensuelles, 5 ans de sauvegardes annuelles par exemple.
- Une sauvegarde dite hors ligne est une sauvegarde sur un support déconnecté de tout SI. La bande magnétique reste le moyen le plus efficace encore aujourd'hui pour cet usage.
- L'opérateur de sauvegarde doit être considéré comme un administrateur à hauts privilèges sur le SI. Il faut donc être vigilant sur le niveau de confiance accordé à ces opérateurs, et intégrer des clauses de sécurité spécifiques en cas de recours à de la sous-traitance.

2. PDMA : RPO (*recovery point objective*) en anglais.
3. DMIA : RTO (*recovery time objective*) en anglais.
4. Voir également le standard ISO/IEC 27031 :2011 : « Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité ».

3
Recommandations

3.1 Architecture

- **Les serveurs de sauvegarde doivent être cloisonnés et positionnés au sein du SI d'administration, ou au moins dans une zone réseau distincte de la zone de production hébergeant les serveurs sauvegardés.**
- **Les flux de sauvegarde doivent transiter au sein du réseau d'administration.**
- **Les flux de sauvegarde doivent transiter au sein d'un sous-réseau logique dédié (VLAN).**
- **Il est recommandé de dédier une instance de serveur de sauvegarde et un magasin de données par niveau de sensibilité des données et/ou applications.** Par exemple, les éléments suivants doivent disposer d'une instance de sauvegarde dédiée :
  - le SI d'administration ;
  - les systèmes stockant des secrets (ex. : annuaire, infrastructure de gestion de clés, coffre-fort) ;
  - les postes bureautiques, si ceux-ci doivent être sauvegardés.
- **Les serveurs hébergeant l'infrastructure de sauvegarde ne doivent pas faire partie d'un domaine Windows (Active Directory) de production. Ils doivent disposer d'un système d'authentification indépendant (comptes locaux, annuaire dédié à l'administration).**
- **Les flux de sauvegarde doivent être filtrés strictement au moyen d'un pare-feu interne.**
- En particulier, les magasins de données [5] ne doivent être accessibles que depuis les serveurs de sauvegarde.
- Les flux de sauvegarde doivent être à l'initiative du serveur vers les clients sauvegardés.
- Si une infrastructure de sauvegarde est obsolète mais doit néanmoins être conservée, elle doit être maintenue hors ligne en condition de sécurité. L'éventuelle reconnexion de celle-ci en cas de besoin doit se faire depuis un réseau déconnecté ou cloisonné logiquement du reste du SI.
- Les actions réalisées sur l'infrastructure de sauvegarde doivent être journalisées et centralisées sur un collecteur de journaux d'événements.

5. Un magasin de données (ou *datamart* en anglais) est un ensemble de données organisées et regroupées pour répondre à un besoin métier ; c'est un sous-ensemble d'un entrepôt de données (ou *datawarehouse* en anglais).

3.2 Opérations

- Il est recommandé d'appliquer la règle « 3 – 2 – 1 » : 3 copies distinctes des données, c'est-à-dire les données en production et 2 sauvegardes stockées sur des supports différents, dont 1 hors ligne.
- **Il est indispensable de mettre en place une sauvegarde hors ligne (ou au moins hors site en ligne sous certaines conditions) même si celle-ci est moins fréquente que les sauvegardes locales régulières en ligne (cf. tableau 2 en section 3.5).**
- Les opérations de sauvegarde sont des opérations d'administration, elles doivent donc respecter les bonnes pratiques du guide d'administration sécurisée de l'ANSSI.
- **Chaque instance de sauvegarde doit disposer de comptes d'administrateurs dédiés.**
- **Les comptes d'administrateurs pour la sauvegarde doivent être nominatifs et dédiés.**
- En fonction des capacités du logiciel, il est recommandé de segmenter les rôles des opérateurs de sauvegarde (RBAC [6]) en définissant au minimum un rôle d'exploitation (actions quotidiennes) et un rôle d'administration avancée (stratégie, configuration).
- Les comptes techniques de sauvegarde (qui exécutent les agents logiciels notamment) doivent faire l'objet d'une sécurisation : réduction des privilèges système au strict minimum, renouvellement des secrets régulier et si possible automatisé.
- Il n'est pas recommandé d'autoriser les utilisateurs à exécuter directement une action de sauvegarde ou de restauration sur le SI (fonction parfois proposée par certains éditeurs de logiciels). Cela fait encourir un risque d'accès illégitime à des données et un risque d'élévation de privilèges sur le SI [7]. Si ce besoin existe, il est recommandé de cadrer strictement cet emploi (limiter les utilisateurs autorisés) et de journaliser ces actions.
- Il est recommandé de s'assurer que la « restauration croisée » est désactivée [8] par défaut sur le logiciel de sauvegarde.
- **L'ensemble des composants de l'infrastructure de sauvegarde doit être mis à jour de manière proactive (logiciel de sauvegarde, micrologiciels, etc.). Il est recommandé de suivre les CVE et les bulletins d'alertes fournis par l'éditeur de la solution.**
- La sauvegarde doit systématiquement faire l'objet d'un contrôle par les opérateurs de sauvegarde. Ce contrôle doit inclure une liste de vérifications permettant de détecter un comportement inhabituel : volume de données ou de fichiers incohérent, lenteurs réseaux, modifications de la configuration des politiques de sauvegarde, etc.
- Les sauvegardes doivent être testées régulièrement. Une procédure de restauration du SI doit être rédigée et régulièrement mise en œuvre.
- Une stratégie et un ordre de restauration doivent être définis en tenant notamment compte des critères suivants : dépendance du SI vis-à-vis de services d'infrastructure (DNS, NTP, an-

6. *Role based access control*.
7. Par exemple, un utilisateur malveillant pourrait restaurer un fichier `/etc/shadow` connu de lui-même sur un serveur ciblé.
8. Une instance de serveur de sauvegarde ne doit pas pouvoir restaurer depuis un magasin de données ou un support référencé sur une autre instance.

nuaire, etc.), criticité des applications métier, durée de restauration et de resynchronisation des données, mode de restauration (machines virtuelles, BMR [9], etc.).

- **En cas d'incident de sécurité, la mesure prioritaire doit être d'isoler l'infrastructure de sauvegarde du reste du SI. Cela suppose de prévoir un mode « bouton rouge » d'urgence (ex. : script automatisé, déconnexion d'un commutateur).**
- **Il est important de sauvegarder les médias d'installation et les configurations des applications métier.**
- La sauvegarde de l'infrastructure de sauvegarde doit être prise en compte. Elle doit contenir au moins : les binaires pour installer une infrastructure minimaliste (systèmes d'exploitation, logiciels et leurs correctifs), les procédures d'import des sauvegardes, le catalogue de sauvegarde, la liste du matériel pour un déploiement sur un site de secours et, si les données sont chiffrées par le logiciel de sauvegarde, les procédures d'import des clés de chiffrement.
- En cas de restauration après un incident de sécurité, les sauvegardes peuvent contenir des implants de l'attaquant (ex. : code malveillant, porte dérobée). Il faut tenir compte de ce risque lors de la reconstruction du SI, et s'assurer de l'innocuité des éléments restaurés en opérant de manière granulaire dans la mesure du possible :
  - réinstaller les systèmes d'exploitation à partir d'images officielles de confiance ;
  - réinstaller les applications métier à partir de binaires signés par les éditeurs ;
  - réaliser un contrôle de conformité des configurations des applications avant leur redémarrage ;
  - réaliser un scan antivirus des données métier avant leur importation dans l'application ;
  - disposer d'un historique de sauvegardes cohérent par rapport aux valeurs métier.

3.3 Protection des données

- Les flux de sauvegarde doivent être protégés au moyen de chiffrement et d'authentification mutuelle entre client et serveur à l'état de l'art (avec TLS par exemple).
- **Le niveau de robustesse de la protection des sauvegardes (chiffrement, etc.) doit être aligné avec le niveau de protection de ces mêmes données dans le SI de production.**
- Si les sauvegardes sont chiffrées, la gestion des clés de chiffrement doit être étudiée : les opérateurs qui les détiennent, leur stockage (coffre-fort), leur sauvegarde (hors ligne).
- **Dans le cas où la sécurité physique d'un site de sauvegarde n'est pas jugée satisfaisante, il est important de chiffrer systématiquement les sauvegardes (disques, bandes magnétiques, etc.).**
- Lors de la mise au rebut des supports de sauvegarde, il est important de réaliser au préalable un effacement sécurisé (suppression des clés de chiffrement des sauvegardes, mise à zéro [10] ou *zeroisation* en anglais) ou de détruire physiquement les supports (déchiquetage ou incinération).

9. *Bare Metal Restore*, restauration complète d'un serveur physique.
10. Séquencement de plusieurs écritures de données aléatoires sur le support.

3.4 Virtualisation

Dans le cas de la virtualisation, il est recommandé d'étudier la pertinence de sauvegarder directement l'image disque d'une machine virtuelle ou d'installer l'agent de sauvegarde sur la machine virtuelle. Cette étude doit tenir compte des critères suivants :

- le volume de données modifiées sur la machine virtuelle à chaque sauvegarde ;
- les besoins en granularité dans le processus de restauration ;
- le chiffrement ou non de la machine virtuelle (selon les outils, cela peut nécessiter un déchiffrement et re-chiffrement, exposant ainsi des données en clair) ;
- la capacité à reconstruire la machine virtuelle à partir de zéro (automatisation).

Le tableau 1 liste les avantages et inconvénients de chaque solution. Il est possible d'opter pour une solution hybride : sauvegarder à la fois la machine virtuelle entièrement (fréquence faible) et les données au sein de la machine virtuelle (fréquence plus forte).

	Sauvegarde fichiers disque de la machine virtuelle	**Installation agent au sein de la machine virtuelle**
Avantages	■ L'opérateur de sauvegarde n'a pas accès au contenu de la machine virtuelle si celle-ci est chiffrée. ■ Possible optimisation du volume de sauvegarde si l'installation des machines virtuelles est automatisée avec distinction entre les disques « vivants » (données, journaux) et les disques « figés » (systèmes d'exploitation, applications).	■ Granularité possible pour la sauvegarde et restauration de fichiers. ■ Homogénéité de l'exploitation dans le cas où l'on sauvegarde également des serveurs physiques.
Inconvénients	■ La restauration peut poser problème pour le redémarrage de certaines applications (bases de données, Active Directory) ou être inadaptée pour certaines demandes de restauration (serveur de fichiers). ■ Problèmes de performances avec les sauvegardes en mode déduplication par blocs si la machine virtuelle est chiffrée.	■ Augmentation de la surface d'attaque sur les serveurs sauvegardés (agent local avec privilèges élevés). ■ L'opérateur de sauvegarde peut accéder aux données en clair des serveurs sauvegardés.

TABLE 1 – Avantages et inconvénients selon le mode de sauvegarde des machines virtuelles

Si les serveurs de sauvegarde sont virtualisés, ils doivent être mutualisés exclusivement avec des serveurs de même sensibilité que le SI d'administration.

3.5 Externalisation

Le tableau 2 résume les principaux risques et solutions possibles dans le cas de sauvegardes dans un environnement non maîtrisé par l'entité (ex. : hébergement *cloud* public, sous-traitance) :

	Hors site connecté (en ligne)	Hors site déconnecté (hors ligne)
Risques	Vigilance sur la sensibilité des données sauvegardées : ■ localisation des sauvegardes sur le territoire de l'Union européenne (attention à la réplication interne de l'hébergeur dans le cas « en ligne »); ■ chiffrement des sauvegardes par un moyen propre à l'entité avant envoi chez l'hébergeur ou le prestataire. Vigilance sur la durée de restauration compatible avec les besoins de DMIA : ■ délai de mise à disposition de la sauvegarde dans les deux cas : > priorité contractuelle dans le cas « en ligne » (ex. : AWS Glacier), > rapatriement des bandes dans le cas « hors ligne »; ■ débit et latence du lien Internet dans le cas « en ligne »	
Solutions	Une solution WORM [11] est envisageable, mais il est important d'étudier le mécanisme d'immuabilité [12] dont la robustesse varie en fonction des technologies utilisées : ■ protection logicielle (code applicatif) ou matérielle (verrou disque); ■ comptes techniques et droits RBAC distincts entre opérations d'écriture unique (sauvegarde) et opérations de lectures multiples (restauration).	Une solution de sauvegarde hors ligne reste considérée comme plus robuste qu'une solution WORM en ligne. Néanmoins, un compromis acceptable peut être d'effectuer des sauvegardes régulières avec une solution WORM et d'effectuer des sauvegardes hors ligne à une fréquence moindre.

TABLE 2 – Risques et solutions dans le cas de sauvegardes dans un environnement non maîtrisé

11. *Write once read many.*
12. Le concept d'immuabilité empêche toute modification de la donnée une fois celle- ci écrite sur le support et assure ensuite l'intégrité et la disponibilité de cette donnée lors des opérations de lecture.

Version 1.0 - 18/10/2023 - ANSSI-BP-100

ISBN : 978-2-11-167146-1 (numérique)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité