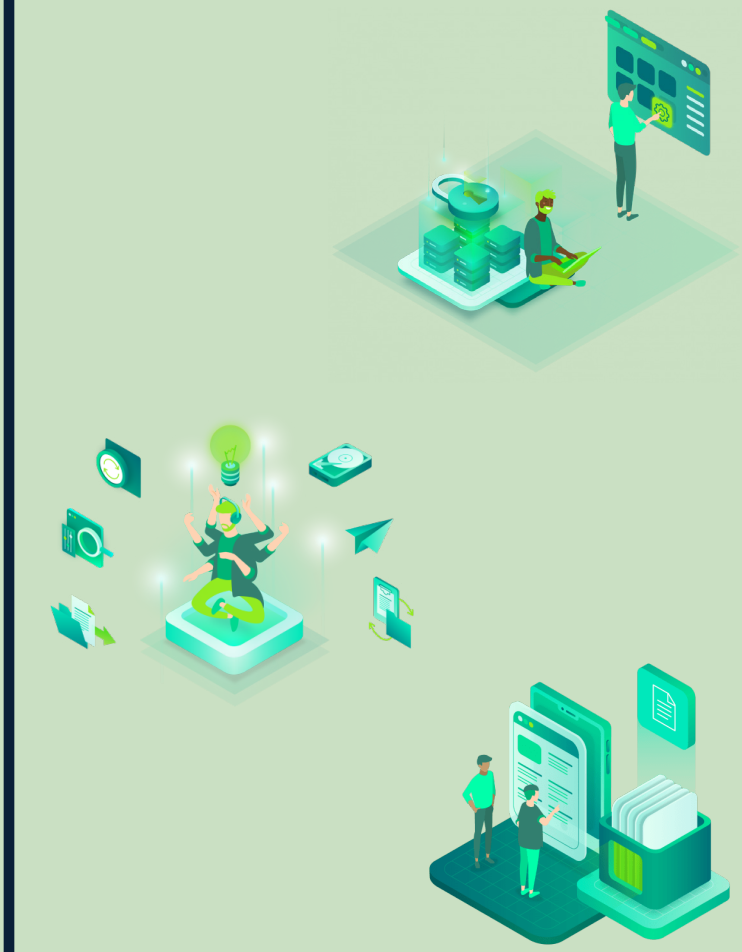
CCN-CERT

BP/34



Recommandations de sécurité sur Veeam Data Platform

RAPPORT DE BONNES PRATIQUES

AVRIL 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional

Éditeur :

Date d'émission : Mai 2024

LIMITATION DE LA RESPONSABILITÉ

Le présent document est fourni conformément aux termes qu'il contient, rejetant expressément tout type de garantie implicite qui puisse y être liée. Le Centre National de Cryptologie ne peut en aucun cas être tenu responsable des dommages ou préjudices directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et des logiciels mentionnés, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

La reproduction totale ou partielle de ce document par quelque moyen ou procédé que ce soit, y compris la reprographie et le traitement informatique, ainsi que la location ou le prêt public de copies, sont strictement interdites sans l'autorisation écrite du Centre National de Cryptologie, sous peine des sanctions prévues par la loi.

Indice

1. Introduction

Veeam fournit aux entreprises et aux organisations une plateforme unifiée pour la protection des environnements cloud, virtuels, physiques, SaaS et Kubernetes.

Il fournit une plateforme unifiée pour la protection de divers environnements, gérée de manière centralisée et adaptable à différentes architectures.

Les principaux composants de la solution sont les suivants :

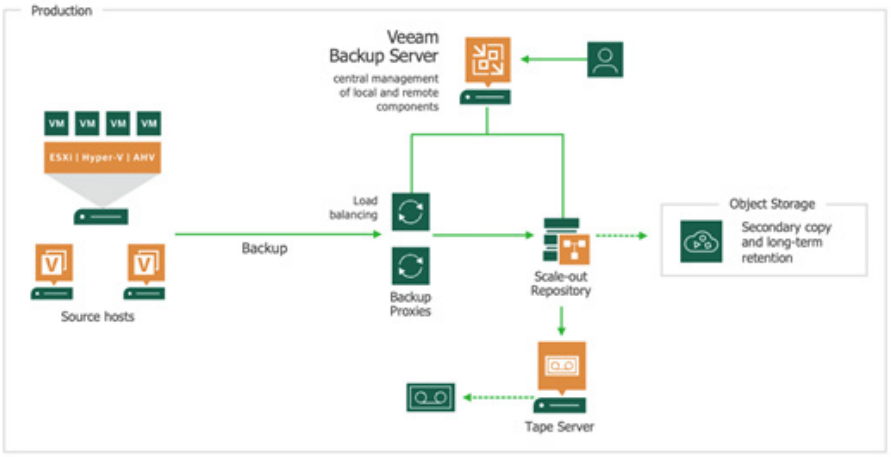
- **Veeam Backup Server :** Il s'agit du composant central, utilisé pour configurer et gérer les composants de la solution.
- **Veeam Backup Proxy :** Le rôle principal du serveur proxy est de lire les données de l'environnement de production et de les traiter afin de les transférer au référentiel de sauvegarde.
- **Veeam Repository Server :** Les référentiels sont responsables du stockage des images de sauvegarde et des métadonnées.

Toutes les informations relatives aux métadonnées sont contenues dans la sauvegarde elle-même (dans le référentiel local et dans la copie qui déborde sur le cloud), de sorte qu'aucune base de données d'index, de volume ou de déduplication stockée sur le serveur de sauvegarde n'est nécessaire. Cela présente des avantages en cas de reprise après un sinistre total ou partiel dans le centre de données local.

Il est important de mentionner que, selon les besoins ou la taille de l'infrastructure, ces composants peuvent être installés dans un seul appareil (installation tout-en-un) ou découplés dans différents appareils.

1. Introduction

Une architecture de haut niveau de la solution pourrait être la suivante :



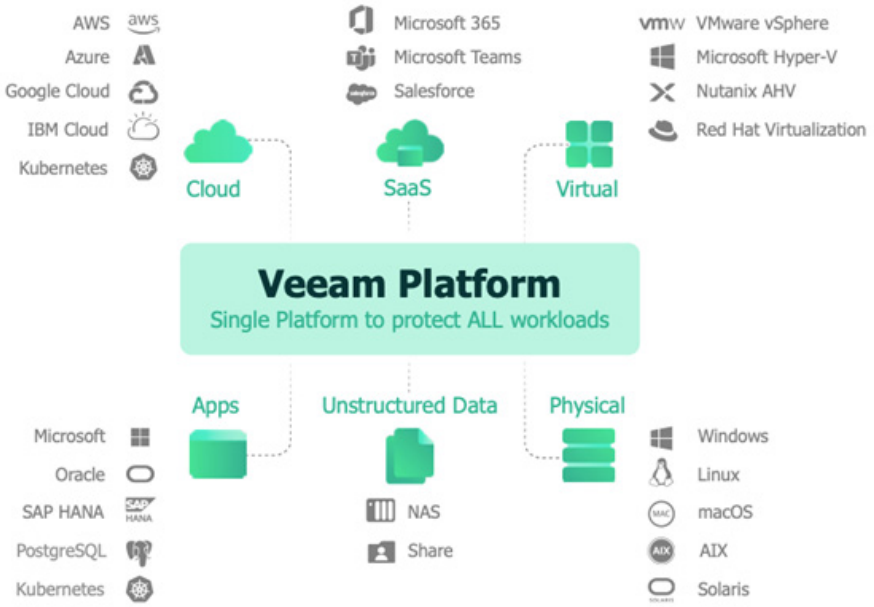
Le diagramme montre :

- Les multiples sources de données supportées par Veeam. Entre autres, les environnements virtualisés, les serveurs physiques, les environnements NAS ou les serveurs de fichiers.
- Au cœur du processus de copie se trouvent les proxys de sauvegarde ou “Backup proxies”, qui lisent et traitent les données sources et les envoient au référentiel de sauvegarde, compressées et dédupliquées.
- Sur le côté droit de l’image se trouve le référentiel de sauvegarde. Celui-ci sera généralement local afin de fournir à la solution des performances élevées dans les processus de génération et de restauration des sauvegardes. Il est possible de répliquer ou d’étendre le référentiel, localement ou dans le cloud, afin de suivre la règle 3-2-1 typique que toute solution de sauvegarde devrait appliquer.
- En option, il est possible d’externaliser les copies sur bande, ce qui garantit la disponibilité de ces copies hors ligne et même dans différentes installations.
- Le tout est géré de manière centralisée par le Veeam Server via une console protégée avec des mécanismes d’authentification multifactorielle pour aider à répondre aux exigences techniques et réglementaires.

2. Ransomware, résilience et sécurité

“Veeam Data Platform” est modulaire et extensible, ce qui signifie qu’elle peut offrir une protection virtuelle et physique dans les environnements locaux, une protection cloud-native dans les environnements AWS, Azure et Google Cloud, Kubernetes anywhere, ainsi qu’une protection SaaS dans les environnements Microsoft 365 et Salesforce.

Offre une protection complète pour les environnements virtuels, physiques, SaaS et Kubernetes, avec des options de sauvegarde sans agent et des mesures anti-ransomware avancées.



- **Charges de travail virtuelles.** Veeam permet d'effectuer une sauvegarde d'image, tant au niveau de la machine virtuelle que de l'application, sans l'installation d'aucun agent, ni pour la copie, ni pour la restauration.

  Dans le cas des bases de données (Microsoft SQL Server, PostgreSQL ou Oracle), Veeam permet également de protéger les journaux de transactions de manière régulière, sans installer d'agents.

- **Charges de travail physiques.** Veeam permet de protéger les machines physiques Windows, Linux, MAC, AIX et Solaris au moyen de "Veeam Agents". Pour ce faire, un seul agent doit être installé sur le système pour protéger le serveur dans son ensemble (le système d'exploitation, les dossiers et les applications).

  Les agents seront gérés de manière centralisée à partir du serveur Veeam et les données voyagent directement du serveur au référentiel de sauvegarde. Comme pour les charges de travail virtuelles, afin de protéger les données de l'organisation, l'ensemble du processus de sauvegarde est chiffré de bout en bout (source, réseau et destination).

- **Charges de travail NAS / Serveur de fichiers.** La fonctionnalité NAS Backup est utilisée pour la protection des environnements de fichiers (NAS ou File Servers Windows/Linux, physiques ou virtuels).

  La sauvegarde des périphériques NAS (SMB/CIFS et NFS) est effectuée via le réseau local et les données sont traitées par les "File Proxies" qui traitent les données et les envoient directement sur le disque.

- **Charges de travail de conteneur avec Kubernetes.** K10 de Veeam a été spécifiquement conçu pour Kubernetes et il offre aux équipes opérationnelles des entreprises un système simple à utiliser, évolutif et sécurisé pour la sauvegarde, la restauration, la DR et la mobilité des applications Kubernetes.

  Il est intégré en mode natif dans Kubernetes pour découvrir automatiquement tous les composants applicatifs qui s'exécutent sur le cluster et traitent l'application comme une unité. D'un autre côté, il prend en charge la gestion multi-tenant qui comporte une sécurité intégrée, la gestion multicluster et le stockage d'objets immuables pour assurer la protection anti-ransomware.

- **Charges de travail cloud natives.** Une autre approche possible consiste à effectuer une sauvegarde et une restauration modulaire cloud-native pour protéger les charges de travail spécifiques sur AWS, Azure ou Google Cloud.

2. Ransomware, résilience et sécurité

Aujourd'hui, les attaques par ransomware constituent l'une des menaces les plus graves et les plus fréquentes pour les organisations. Le meilleur moyen de se protéger contre ce type de menace est de disposer d'une défense solide, d'une stratégie de protection des données robuste et de plans de reprise d'activité agiles et éprouvés.

Les sauvegardes validées et vérifiées constituent la dernière ligne de défense contre les cyber-attaques et peuvent être le facteur décisif pour éviter des temps d'arrêt importants, des pertes de données et un impact négatif sur l'activité et la réputation des organisations.

Il est recommandé **de suivre la règle 3-2-1-1-0 lors de la planification des sauvegardes.** Il s'agit d'une amélioration apportée par Veeam à la fameuse règle 3-2-1.

Selon la **règle 3-2-1-1-0,** il est suggéré de conserver **(3) copies différentes** des données sur **(2) types de supports** différents, dont l'un **(1)** soit conservé dans un **emplacement hors site** et l'autre **(1)** soit conservé **hors ligne, isolé ou immuable,** et ne possède aucune **(0) erreur dans les copies de sauvegarde,** étant donné qu'elles ont été testées à l'avance et qu'il a été vérifié qu'elles sont récupérables.

Une **stratégie de cyberdéfense solide et complète** commence toujours par les sauvegardes, et celles-ci doivent être fiables, vérifiées et testées. En outre, **l'immuabilité est une étape clé** qui empêchera les cybercriminels d'accéder aux données de sauvegarde, de les chiffrer ou de les supprimer.

L'immuabilité offre la **protection d'un stockage hors ligne** de type WORM (Write Once, Read Many), rendant les données de sauvegarde impénétrables aux attaques. Diverses options d'immuabilité sont possibles dans le cloud public (AWS, Azure, Wasabi, etc.), ainsi que des référentiels S3 compatibles avec "Object lock" pour l'immuabilité dans l'environnement local, sans parler des options de sauvegarde sur bande.

3. Bonnes pratiques de sécurité sur Veeam

3.1 Protéger

3.1.1 Protéger les sauvegardes – La règle 3-2-1-1-0

Une infrastructure de sauvegarde correctement conçue doit **inclure un mécanisme de protection des données.** Cela peut être offert par des fonctionnalités telles que :

- "Appliances de déduplication" de stockage via un mécanisme propriétaire tel que l'immuabilité ou des instantanés protégés.
- Stockage d'objets grâce à l'immuabilité.
- Les dispositifs à bande, avec un "air gapping" physique.
- Les mécanismes WORM (Write Once, Read Many).

Idéalement, **toutes les rétentions doivent être protégées par un "air gap" ou une immuabilité.** Mais comme le temps d'intervention des attaquants est d'environ un mois en moyenne, il est fondamental de protéger au moins **quatre (4) semaines de points de restauration** pour atténuer l'attaque.

La règle 3-2-1 est très générale et fonctionne pour tous les types de données (particuliers et entreprises) et tous les types d'environnements (physiques et virtuels). Lors de la sauvegarde de vos environnements avec Veeam, cette règle devient la « règle de sauvegarde 3-2-1-1-0 » où 1 média est hors site et 1 média est isolé, immuable ou hors ligne. 0 signifie « 0 erreur » lors de l'application de la vérification automatique de la capacité de récupération de chaque sauvegarde avec SureBackup de Veeam.

En suivant la règle **3-2-1-1-0**, vous créez plusieurs couches de résilience et de sécurité. Les données et les charges de travail seront rendues immuables (protection contre la suppression et la modification),

stockées hors ligne (protégées contre les menaces internes), isolées (protégées contre les menaces internes et autres catastrophes liées à la continuité des activités, par exemple incendie, inondation, tremblement de terre, etc.).

De plus, ce que nous appelons un **"écart de protocole"** peut être ajouté afin de rendre plus difficile la destruction de vos données par les attaquants. L'idée est d'utiliser différents types de référentiels, qui s'appuient sur différentes technologies (bloc de disque, CIFS, NFS, S3, protocoles propriétaires d'appliances de déduplication, etc.), pour rendre plus difficile le ciblage de vos données par les outils d'attaque.

3.1.2 Protection de l'infrastructure de sauvegarde

Pour protéger efficacement votre infrastructure Veeam, il est recommandé de prendre des **contre-mesures telles que le durcissement** des composants. Vous devez au moins protéger les composants suivants :

- **Serveur de sauvegarde Veeam (Veeam Backup Server)**
- **Comptes utilisateur**
- **Référentiels de sauvegarde**
- **Flux de données de sauvegarde**

Considérez le "Veeam Backup" comme la **cible numéro un de votre infrastructure.** Son accès doit être très restreint et contrôlé à tout moment, tout comme son déploiement.

Les **proxys de sauvegarde** doivent être considérés comme des **cibles de compromission**. Lors de la sauvegarde, les proxys obtiennent du serveur de sauvegarde les informations d'identification requises pour accéder aux serveurs d'infrastructure virtuelle. Une personne disposant de privilèges d'administrateur sur un proxy de sauvegarde peut intercepter les informations d'identification et les utiliser pour accéder à l'infrastructure virtuelle.

3.1.3 Formation du personnel

En déployant une formation de sensibilisation des employés, vous vous assurez que vos employés sont capables de **repérer des comportements suspects** et qu'ils sont conscients de l'importance de leur rôle vis-à-vis de la protection des services et des données de l'organisation.

Cela ne concerne pas seulement le service informatique, mais aussi tous les membres de l'organisation, car ils peuvent tous être **témoins de comportements suspects, ou être la cible d'une attaque par ingénierie sociale, ce qui pourrait ouvrir une brèche de sécurité** s'ils n'ont pas reçu une formation et une sensibilisation adéquates en matière de sécurité.

3.2 Détection des menaces

3.2.1 Visibilité

Pour savoir quand vous êtes attaqué ou victime d'une violation de données, il est essentiel d'avoir une **visibilité sur l'ensemble du chemin du flux de données**. Vous devriez être capable de savoir ce qu'est un "comportement normal" et ce qui ne l'est pas. Surveillez vos comptes et votre infrastructure Veeam pour détecter toute activité suspecte.

Placez des **fils-pièges virtuels**, comme par exemple en créant un compte administrateur non utilisé auquel sont liées des alarmes (par exemple "Utilisateurs Honeypot"). Lorsqu'une activité sur ce compte est observée, une alerte rouge est instantanément déclenchée.

Il est important de recevoir des alertes le plus rapidement possible tout en vous défendant contre d'autres attaques telles que les virus, les logiciels malveillants et les ransomwares. La plus grande crainte de ces attaques est qu'elles puissent se propager rapidement à d'autres systèmes. **Avoir une visibilité sur, par exemple, l'activité potentielle des ransomwares s'avère fondamental.**

3.2.2 Serveurs Honeypot

Les serveurs Honeypot avec surveillance de l'authentification aideront à détecter les attaques ciblant votre infrastructure Veeam. Ces pots de miel doivent être visibles et leurs entrées DNS doivent être très compréhensibles, comme par exemple « vbrsrv01 » ou « vbrrepo », afin qu'ils soient des cibles faciles pour l'attaquant.

Un pot de miel approprié pourrait inclure un faux référentiel, sur lequel les modifications des fichiers de sauvegarde seront étroitement surveillées.

3.2.3 Utilisateurs Honeypot

Les utilisateurs Honeypot bénéficiant d'une surveillance de l'authentification aideront à détecter les attaques ciblant votre infrastructure Veeam. Comme dans le cas précédent, ces pots de miel doivent être visibles et leurs noms doivent être très compréhensibles, comme par exemple "VBRAdmin" ou "BackupAdmin" afin qu'ils soient des cibles faciles du point de vue de l'attaquant.

Bien entendu, **ces utilisateurs devront être configurés de manière à ce que leur exposition et leur éventuelle exploitation malveillante soient rendues inutiles,** de sorte que leur compromission n'aura donc aucun effet sur la sécurité de l'infrastructure.

3.2.4 Alarmes

"Veeam One" offre la possibilité de surveiller une éventuelle activité de ransomware via un ensemble **d'alarmes prédéfinies telles que "état d'immuabilité", "activité possible de ransomware" ou "suivi des modifications d'immuabilité".**

Ces alarmes doivent être activées à la fois sur le serveur de production et sur le pot de miel.

3.3 Stratégie de rétablissement

Ayez une stratégie de rétablissement en place et sachez quoi faire en cas de compromission pour minimiser l'impact et les pertes économiques associées à celle-ci. **Sauvegardez vos données et assurez-vous que les sauvegardes ne sont pas accessibles à un attaquant pour les effacer ou les modifier.**

Une copie hors site (air gap) ou en lecture seule sur n'importe quel support est fortement recommandée. De plus, vous devez être conscient qu'en cas de violation, il est très probable que vos actifs soient scellés par des entités gouvernementales à des fins d'analyse et de criminalistique et qu'ils ne soient pas disponibles pour la récupération. Vous devez **compter sur du matériel de récupération dédié en plus de conserver des copies hors site.**

Il est également très probable que votre **connexion Internet soit coupée pour chasser les intrus** et/ou empêcher les fuites de données. Par conséquent, vous aurez peut-être besoin d'un autre moyen pour accéder à vos sauvegardes hors site.

La préparation est la clé. Vous devez avoir testé la récupération en gardant à l'esprit que vous devrez redémarrer à partir de rien d'autre que des fichiers de sauvegarde et une infrastructure vierge.

D'autres recommandations à prendre en compte: **Préparez le groupe de travail (de réponse),** connaissez vos actifs pour **prioriser la récuperation,** et utilisez largement (et de manière adequate) les outils d'automatisation des tests, tels que "Veeam SureBackup" ou "Veeam Disaster Recovery Orchestrator".

3.4 Rôles et utilisateurs

Déployez une politique de contrôle d'accès, la gestion des accès aux composants de gestion est cruciale pour une bonne protection. **Utilisez le principe du moindre privilège.**

Un attaquant qui a obtenu un accès privilégié aux serveurs de l'infrastructure de sauvegarde peut obtenir les informations d'identification des comptes d'utilisateurs et **compromettre d'autres systèmes de votre environnement** ou exploiter les procédures de récupération.

Assurez-vous que **tous les comptes ont un rôle spécifique et qu'ils sont ajoutés à ce groupe spécifique.** Certaines mesures et politiques standard sont :

- N'utilisez pas de comptes d'utilisateurs pour l'accès administrateur.
- Donnez à chaque administrateur Veeam son propre compte administrateur pour une traçabilité et un ajout et une suppression faciles.
- Supprimer le rôle par défaut "Administrateur Veeam Backup" du groupe Administrateurs local.
- Ne donnez accès qu'à ce qui est nécessaire pour le travail, en limitant l'accès à une ressource spécifiée à une période spécifique (accès "juste à temps" ou JIT).
- Limiter strictement les utilisateurs pouvant se connecter à l'aide de "Veeam Console".
- Ajoutez une authentification à 2 facteurs aux actifs de grande valeur.
- Surveillez vos comptes pour détecter toute activité suspecte.

3.4.1 Anonymisation

De nombreuses entreprises suivent les meilleures pratiques et utilisent des comptes dédiés aux administrateurs pour exécuter des tâches privilégiées, en plus de leur compte utilisateur permettant les tâches bureautiques de base.

Ces comptes sont souvent précédés de "adm_", ce qui peut être pratique, mais aide les attaquants à identifier les comptes privilégiés. **Essayez d'utiliser les comptes "adm_" pour les utilisateurs Honeypot uniquement et choisissez une autre stratégie pour les vrais comptes d'administrateur.**

Les réseaux sociaux peuvent également aider à identifier un propriétaire potentiel de compte privilégié au sein d'une entreprise. Ainsi, l'utilisation de tout ce qui n'est pas le nom d'un utilisateur ajoutera de la complexité à l'identification des comptes privilégiés et ralentira les attaquants.

3.4.2 Politique de gestion des mots de pase

Utilisez une **politique de gestion des mots de passe intelligente, adaptée à votre organisation.** Imposer l'utilisation de mots de passe forts dans votre infrastructure constitue un contrôle précieux. Il est plus difficile pour les attaquants de deviner des mots de passe ou de déchiffrer des hachages pour obtenir un accès non autorisé aux systèmes critiques.

Assurez-vous que les comptes et mots de passe par défaut **ont été modifiés** sur tous vos actifs. Pour les comptes administrateur, **l'ajout d'une authentification à 2 facteurs (2FA)** est également indispensable pour sécuriser l'infrastructure.

Assurez-vous que l'outil de mot de passe et la base de données sont disponibles sur un **site de récupération** afin de les rendre disponibles en cas de sinistre. Gardez à l'esprit qu'une sauvegarde récente de votre outil de mot de passe et de votre base de données doit résider sur un support protégé "air gap", tel qu'un DVD, un CD-ROM ou une bande. Le plus crucial est le mot de passe du "Veeam Repository" qui permettra de restaurer à partir des fichiers de sauvegarde.

L'accès aux systèmes de production à partir de l'infrastructure de sauvegarde peut s'appuyer sur des **comptes de service gérés de groupe (gMSA ou "Group Managed Service Accounts")** pour faciliter l'obtention d'un bon niveau de sécurité, car **des mots de passe complexes sont définis et alternés automatiquement** dans ce cas. Les comptes de service gérés de groupe peuvent être utilisés avec "Veeam Backup and Replication" depuis la version 12.

3.4.3 Politique de verrouillage

Utilisez une politique de verrouillage qui complète une politique intelligente de gestion des mots de passe. Les comptes seront verrouillés après un petit nombre de tentatives incorrectes. Cela peut empêcher les attaques par pulvérisation de mot de passe.

Mais attention, cela peut également bloquer le système de sauvegarde et de réplication pendant un certain temps. Pour les comptes de service, il est parfois préférable de déclencher l'alarme rapidement au lieu de verrouiller les comptes. De cette façon, vous gagnez en visibilité sur les comportements suspects envers vos données ou votre infrastructure.

3.4.4 Autorisations requises

Comme indiqué ci-dessus, utilisez le **principe du moindre privilège;** c'est-à-dire, fournissez les autorisations minimales requises pour que les comptes d'utilisateurs ou de service s'exécutent.

3.5 Protocoles d'authentification

Choisissez des **algorithmes de chiffrement forts pour SSH.** Pour communiquer avec les serveurs Linux déployés dans le cadre de l'infrastructure de sauvegarde, "Veeam Backup & Replication" utilise SSH. Assurez-vous que pour le tunnel SSH, vous utilisez un **algorithme de chiffrement robuste et éprouvé,** avec une longueur de clé suffisante. Assurez-vous que les clés privées sont conservées dans un endroit hautement sécurisé et ne peuvent pas être découvertes par un tiers.

Depuis "Veeam Backup & Replication v12", seule une architecture Kerbero est possible, **désactivez donc l'authentification NTLM chaque fois que cela est possible.**

3.6 Chiffrement

3.6.1 Au repos

Utilisez le **chiffrement intégré de Veeam Backup & Replication** pour protéger les données lors des sauvegardes. Pour garantir la sécurité des données dans les sauvegardes, suivez les meilleures pratiques de chiffrement au repos :

- Utilisez des **mots de passe forts,** difficiles à déchiffrer ou à deviner.
- Conservez vos mots de passe dans un **endroit sûr.**
- **Changez** régulièrement **les mots de passe** des tâches chiffrées.

3.6.2 En transit

Les données de sauvegarde et répliquées peuvent être interceptées en transit, lorsqu'elles sont communiquées de la source à la destination via un réseau. Pour sécuriser le canal de communication pour le trafic de sauvegarde, tenez compte de ces directives :

- **Isolez le trafic de sauvegarde.** Utilisez un réseau isolé pour transporter les données entre les composants de l'infrastructure de sauvegarde : serveur de sauvegarde, proxys de sauvegarde, référentiels, etc.
- **Chiffrez le trafic réseau.** Par défaut, "Veeam Backup & Replication" chiffre le trafic réseau circulant entre les réseaux publics. Pour garantir une communication sécurisée des données sensibles dans les limites du même réseau, vous pouvez également chiffrer le trafic de sauvegarde dans les réseaux privés.

3.7 Durcissement

Le renforcement consiste à sécuriser l'infrastructure contre les attaques en réduisant la surface d'attaque et en éliminant ainsi autant de risques que possible.

L'une des principales mesures de renforcement consiste à **supprimer tous les programmes logiciels et utilitaires non essentiels** des composants Veeam déployés. Bien que ces composants puissent offrir des fonctionnalités utiles à l'administrateur, s'ils fournissent un accès supplémentaire au système, ils doivent être supprimés pendant le processus de renforcement.

De plus, **créer de la visibilité sur ce qui se passe dans l'infrastructure** fait partie du renforcement de votre infrastructure. Assurez-vous que vous remarquerez quand une attaque peut avoir lieu ou a déjà eu lieu, puis assurez-vous que les journaux et les traces sont enregistrés pour que les forces de l'ordre et les spécialistes de la sécurité puissent les utiliser en cas de besoin.

Rendre les choses plus compliquées pour les attaquants les ralentira, alors **nommez vos serveurs d'infrastructure de sauvegarde en utilisant des noms non liés à la sauvegarde.** Évitez les noms contenant des acronymes comme "bkp", "pxy", "repo", "vbr" ou tout autre nom qui pourrait faciliter la tâche d'un attaquant pour identifier les composants de l'infrastructure de sauvegarde.

3.7.1 Segmentation

Une bonne protection implique une stratégie de **défense en profondeur qui inclut toutes les couches.** Pour cela, vous devez identifier les données les plus précieuses et **construire des couches de défense** autour d'elles pour protéger leur disponibilité, leur intégrité et leur confidentialité.

Une zone est une zone ayant une caractéristique, une destination, un usage particulier et/ou soumise à des restrictions particulières. Au lieu de tout protéger avec le même niveau de protection, vous associez les systèmes et les informations à des zones spécifiques. Comme effet secondaire, les systèmes soumis à la conformité réglementaire peuvent être regroupés en sous-zones pour limiter la portée du contrôle de conformité et ainsi réduire les coûts et le temps nécessaires pour mener à bien des processus d'audit de longue haleine.

Pensez à l'importance des données et des systèmes dans cette zone particulière et à qui devrait y avoir accès. **La communication n'est autorisée qu'entre les systèmes situés dans des zones adjacentes.** Une classification courante des données pour une zone concerne les exigences de disponibilité partagée, de confidentialité, d'intégrité, de contrôle d'accès, d'audit, de journalisation et de surveillance.

Ces caractéristiques et exigences communes conduisent intrinsèquement à un certain niveau d'isolement, mais cet isolement ne se produit pas seulement entre les zones, mais également au sein de zones appelées sous-zones.

La surface d'attaque des données et des systèmes au sein d'une zone **peut être considérablement réduite en exposant un nombre limité de services** à travers le périmètre de la zone et en mettant en œuvre des **contrôles d'accès** stricts pour limiter l'accès à des groupes spécifiques d'utilisateurs. Un attaquant potentiel devrait accéder à toutes les zones extérieures avant d'accéder à la zone restreinte où les données critiques sont stockées, réduisant ainsi le risque de vol ou de mutilation de données. De plus, vous augmentez la disponibilité de ces systèmes critiques.

Vous pouvez utiliser un **modèle de zone comme modèle de défense stratégique** qui divise les différents composants Veeam en zones distinctes. Gardez les **règles suivantes** à l'esprit **lors de la conception :**

- **Sécurisé dès la conception**
- **Sachez ce qui est important pour le sécuriser et le classer**
- **Connaissez vos vecteurs d'attaque et les moyens possibles de les sécuriser**
- **Utiliser le principe du moindre privilège**
- **Avoir un aperçu des coûts et des avantages**

Sachez qu'il n'existe pas de solution miracle qui résoudra tous vos besoins en matière de sécurité à la fois. Il existe de nombreuses façons d'atteindre votre objectif. Si vous pensez être en sécurité, parce que vous avez suivi toutes les meilleures pratiques, vous obtenez un faux sentiment de protection.

Examinez les besoins de votre organisation, puis choisissez la meilleure méthode qui lui convient en tenant compte de l'argent (budget), des risques (vecteurs d'attaque) et des résultats possibles (comment cela s'intègre-t-il, quels seraient les dommages).

3.7.2 Couches entre zones

Chaque zone adjacente peut être considérée à travers les **sept (7) couches du modèle de cybersécurité :**

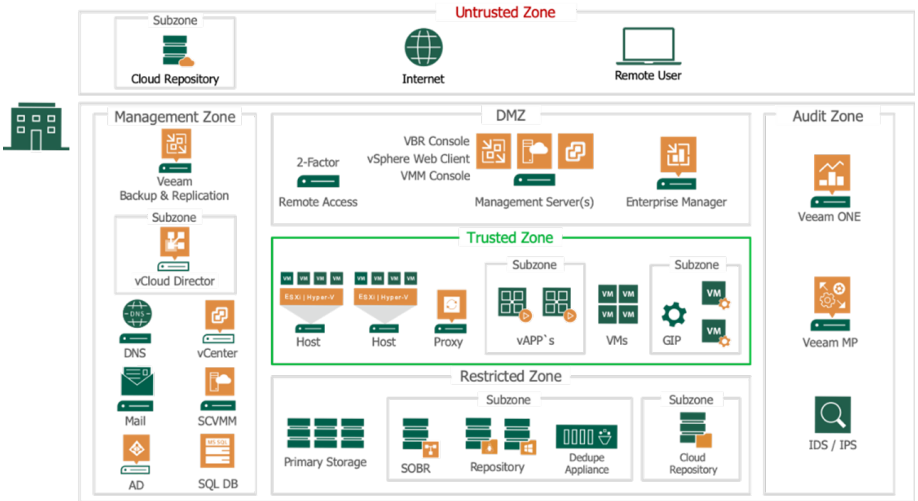
- **Couche Humaine :** Formation, accès physique…
- **Périmètre :** Pare-feu, Filtre anti-spam, Détection/Prévention des intrusions…
- **Réseau :** Conception et topologie sécurisées, VLAN, pare-feu/commutateurs multicouches…
- **Endpoint :** Antivirus, pare-feu logiciels, agents de détection de violations…
- **Application :** Patching (correctifs), mises à jour…
- **Données :** Chiffrement au repos et en transit…
- **Mission critique :** Sauvegardes, plan de réponse et de récupération…

3.7.3 Exemples d'utilisation de zones

La plupart des menaces viennent aujourd'hui de l'intérieur. Diviser votre infrastructure en zones est un excellent moyen d'offrir une meilleure visibilité sur les parties de plus grande importance. Pour renforcer les composants de l'infrastructure "Veeam Availability", nous les plaçons dans plusieurs zones logiques.

L'un des vecteurs d'attaque les plus recherchés sera **l'accès aux comptes et composants de gestion.** En survolant les principaux composants de "Veeam Backup & Replication", vous remarquerez que trois (3) composants de gestion sont disponibles.

- La console "Veeam Backup & Replication" également appelée "console"
- Le serveur "Veeam Backup & Replication", qui est le composant principal orchestrant toutes les différentes tâches et ordonnant le mouvement des données à travers l'infrastructure.
- Le "Veeam Backup Enterprise Manager" qui fédère plusieurs serveurs de sauvegarde dans une seule interface.



3.7.3.1 Zone non fiable

Pour maintenir un équilibre entre sécurité et efficacité opérationnelle, **vous ne souhaitez pas installer la console "Veeam Backup & Replication" sur un système extérieur à l'infrastructure** de votre organisation.

Déployez un pare-feu sur le périmètre entre la zone non fiable et la zone DMZ. Sur le pare-feu et/ou le serveur "RDS Gateway" dédié, ajoutez une **authentification à 2 facteurs** pour que les administrateurs distants puissent accéder à la passerelle RDS.

Refusez le mappage des lecteurs, imprimantes, presse-papiers, etc. sur la passerelle RDS pour sécuriser votre infrastructure contre la suppression de contenu ou de fichiers depuis n'importe quelle machine distante.

3.7.3.2 DMZ

La DMZ héberge des **systèmes qui nécessitent une exposition à la zone non fiable.** Cette zone assure l'accès entre les systèmes de la DMZ et de la zone de gestion.

La console "Veeam Backup & Replication" est un composant côté client qui permet d'accéder au serveur de sauvegarde. La console permet à plusieurs opérateurs de sauvegarde et administrateurs de se connecter simultanément à "Veeam Backup & Replication" et d'effectuer toutes sortes d'opérations de protection des données et de reprise après sinistre comme si vous travailliez sur le serveur de sauvegarde.

Installez la console "Veeam Backup & Replication" sur un **serveur de gestion central positionné dans la zone DMZ** et assurez-vous qu'elle est protégée par une **authentification à 2 facteurs (2FA).** Vous pouvez également installer d'autres outils d'infrastructure sur ce serveur de gestion comme par exemple la console Microsoft VMM et/ou VMware vSphere Client pour gérer le déploiement de votre hyperviseur.

"Veeam Enterprise Manager" se trouvera également dans la zone DMZ, car il sert de **portail libre-service pour des groupes d'utilisateurs spécifiques** de l'organisation.

3.7.3.3 Zone de gestion

Dans la zone de gestion, vous placez des **services d'infrastructure comme DNS, Active Directory et SMTP**. Mais aussi, le serveur VMware vCenter et/ou Microsoft System Center Virtual Machine Manager (SCVMM).

À partir des composants Veeam, le(s) serveur(s) "Veeam Backup & Replication" se trouveront dans cette zone de gestion. Le "Veeam Backup Server" orchestrera toutes les tâches et mettra à jour tous les composants Veeam dans les différentes zones à partir d'un emplacement central.

Le **serveur Microsoft SQL Database**, nécessaire pour héberger la base de données "Veeam Backup" et la base de données "Veeam Enterprise Backup", **doit être placé dans cette zone s'il est dédié uniquement à Veeam.** C'est une bonne pratique **d'utiliser un serveur SQL dédié** qui héberge les différentes instances SQL pour les composants d'infrastructure et **un serveur SQL différent pour les instances SQL pour les processus métier.**

Le serveur "Veeam Backup & Replication" est un grand utilisateur du serveur SQL, et placer le serveur de base de données SQL à proximité vous permet d'améliorer votre efficacité opérationnelle. VMware vCloud Director fait partie d'une sous-zone au sein de la zone de gestion et contrôle l'exécution des vAPP dans les sous-zones de la zone de confiance.

La zone de gestion **nécessite un accès sécurisé et contrôlé à Internet pour télécharger les licences et les mises à jour** des différents composants de l'infrastructure. Il est fortement recommandé d'utiliser **un proxy Internet ou un proxy inverse** situé dans la DMZ comme passerelle contrôlée vers Internet.

Tous les types de référentiels cloud doivent être placés dans des **sous-zones au sein de la zone non fiable**. Les données de l'organisation dépassent les limites de sécurité. **Assurez-vous donc que, par mesure de précaution supplémentaire, les données vers ces référentiels cloud sont chiffrées** pendant le transport et lorsqu'elles sont stockées dans le référentiel cloud.

Le serveur "Veeam Backup & Replication" communiquera avec le service Cloud Gateway pour le transport des données vers Cloud Provider, Azure Proxy ou AWS Deployment.

3.7.3.4 Zone de confiance

La zone de confiance sera remplie **d'hôtes hyperviseurs** tels que des hôtes VMware ESXi et/ou Microsoft Hyper-V. Tous les composants de la zone de confiance devront accéder à différents services de la zone de gestion. Les serveurs "Veeam Proxy", qui assurent le transfert des données, font partie de la zone de confiance.

Les proxys Veeam peuvent sauvegarder les machines virtuelles sans avoir accès aux systèmes d'exploitation invités eux-mêmes. Si vous sauvegardez ou répliquez des machines virtuelles en cours d'exécution, vous pouvez activer les options de traitement des invités.

Les options de traitement des invités sont des tâches avancées qui nécessitent que "Veeam Backup & Replication" communique avec le système d'exploitation invité de la VM. Lorsque les machines virtuelles sont séparées en sous-zones, vous pouvez déployer et exploiter le "Veeam Guest Interaction Proxy" (GIP) dans la sous-zone de confiance, qui disposera d'un accès sécurisé et déploiera le runtime nécessaire dans la VM pour les tâches de traitement des invités.

Dans le cas où différentes unités commerciales ou clients s'exécutent dans la zone de confiance, vous devez penser à les exécuter dans des sous-zones de la zone de confiance. Mais sachez que **des conceptions trop complexes peuvent être contre-productives** et donner un sentiment déplacé de sécurité.

Les vAPP VMware vCloud Director font également partie de la zone de confiance et sont normalement divisées en sous-zones par unité commerciale ou locataire. Veeam peut capturer des configurations entières de vApp et de vCloud Director dans les tâches de sauvegarde.

3.7.3.5 Zone restreinte

Le stockage principal, où résident les données de production et les VM, mais également les autres composants stockant des données doivent être placés dans cette zone restreinte.

Cette zone ne doit jamais être accessible directement par un utilisateur. Uniquement disponible pour les composants de l'infrastructure virtuelle, les serveurs d'applications et les administrateurs disposant de droits stricts.

De plus, le "Veeam Scale Out Backup Repository" (SOBR), le "Simple Repository", les appareils de déduplication ou le "Cloud Repository" lorsqu'ils sont utilisés en combinaison avec "Veeam Cloud Connect for Enterprise" (VCC-E) doivent faire partie de cette zone. Pour les organisations utilisant VCC-E, il est possible de définir des référentiels cloud en plus de leur SOBR ou en tant que référentiels cloud définis séparément dans une sous-zone de zone restreinte.

3.7.3.6 Zone de vérification

La visibilité est essentielle pour protéger, détecter et contenir les menaces le plus tôt possible. Dans cette zone, des solutions de surveillance telles que "Veeam ONE" et/ou "Veeam Management Pack" en combinaison avec Microsoft System Center sont placées. Les systèmes IDS et IPS doivent également être placés dans cette zone d'audit.

3.7.4 Réduction de la surface d'attaque

3.7.4.1 Accès aux consoles

La console "Veeam Backup & Replication" est un composant côté client qui permet d'accéder au serveur de sauvegarde. La console permet à plusieurs opérateurs de sauvegarde et administrateurs de se connecter simultanément à "Veeam Backup & Replication" et d'effectuer toutes sortes d'opérations de protection des données et de reprise après sinistre comme si vous travailliez sur le serveur de sauvegarde.

Il est préférable d'**installer la console "Veeam Backup & Replication" sur un serveur de gestion central positionné dans une zone réseau sécurisée et protégé par une authentification à 2 facteurs (2FA)** plutôt que d'installer la console sur les bureaux locaux des administrateurs de sauvegarde et de restauration. **Appliquez toujours l'authentification MFA** lors de l'authentification auprès de la console "VBCR" elle-même (prise en charge à partir de la version 12).

L'accès à "Veeam Backup & Replication Server" doit être limité à la "Veeam Backup & Replication Console". Désactivez l'accès au bureau à distance, tout protocole d'accès à distance doit être interdit.

3.7.4.2 Désinstallation de la console du serveur de sauvegarde

La console de sauvegarde et de réplication doit être supprimée du serveur Veeam Backup & Replication lorsque cela est posible. La console est installée localement sur le serveur de sauvegarde par défaut.

La console ne peut pas être supprimée via le programme d'installation ou en utilisant Ajouter/Supprimer sous Windows. Ouvrez une invite "cmd" avec un accès administratif. Sur l'invite de commande, tapez : *wmic product list brief > installed.txt*. Cela créera un document texte avec tous les produits installés et leurs codes de produit respectifs.

Pour désinstaller “Veeam Backup & Replication Console”, désinstallez d’abord tous les “Veeam Explorers” :

- **Explorateur Veeam pour Microsoft Exchange.**
- **Veeam Explorer pour Microsoft Sharepoint.**
- **Veeam Explorer pour Microsoft Active Directory.**
- **Veeam Explorer pour Microsoft SQL.**
- **Veeam Explorer pour Oracle.**

Vous pouvez désinstaller ces composants en utilisant : *msiexec /x {ProductCode}*

Exemple de désinstallation de la console Veeam Backup & Replication : msiexec /x {D0BCF408-A05D-45AA-A982-5ACC74ADFD8A}

REMARQUE : La désinstallation de la console “Veeam Backup and Replication” supprime le module PowerShell et rend impossible l’utilisation des applets de commande “Veeam Backup PowerShell” sur le serveur de sauvegarde. Cela peut affecter les scripts d’automatisation ou les produits qui s’appuient sur PowerShell pour interagir avec “Veeam Backup and Replication”, par exemple “Veeam Availability Orchestrator” (ancien “Veeam Disaster Recovery Orchestrator”).

3.7.4.3 Protection des bases de données de sauvegarde et de réplication Veeam

La base de données de configuration de sauvegarde et de réplication stocke les informations d’identification pour se connecter aux serveurs virtuels et à d’autres systèmes de l’infrastructure de sauvegarde et de réplication.

Tous les mots de passe stockés dans la base de données sont chiffrés. Cependant, un utilisateur disposant de privilèges d’administrateur sur le serveur de sauvegarde peut déchiffrer les mots de passe, ce qui présente une menace potentielle.

Pour sécuriser la base de données de configuration de sauvegarde et de réplication, suivez ces instructions :

- **Restreindre l'accès des utilisateurs à la base de données.** Vérifiez que seuls les utilisateurs autorisés peuvent accéder au serveur de sauvegarde et au serveur qui héberge la base de données de configuration "Veeam Backup & Replication" (si la base de données s'exécute sur un serveur distant).

- Il est recommandé de **chiffrer les données dans les sauvegardes de configuration.** Activez le chiffrement des données pour la sauvegarde de la configuration afin de sécuriser les données stockées dans la base de données de configuration. Veuillez noter que les comptes d'utilisateurs et les mots de passe ne sont pas stockés dans les sauvegardes de configuration lorsque le chiffrement n'est pas actif.

3.7.4.4 Suppression des composants inutilisés

Supprimez tous les programmes logiciels et applications non essentiels des composants Veeam déployés. Bien que ces programmes puissent offrir des fonctionnalités utiles à l'administrateur, s'ils **fournissent un accès supplémentaire** ("portes dérobées") au système, ils doivent être supprimés pendant le processus de renforcement.

Désinstallez les logiciels supplémentaires tels que les navigateurs Web, Java, Adobe Reader, etc. **Supprimez toutes les fonctionnalités qui n'appartiennent pas au système d'exploitation** ou aux composants actifs de Veeam. Cela facilitera grandement le maintien d'un niveau de correctif à jour.

3.7.4.5 Suppression des services inutilisés

Désactivez le service "Veeam vPower NFS" sur chaque composant pour lequel vous ne prévoyez pas d'utiliser les fonctionnalités Veeam suivantes : "SureBackup", "Instant Recovery" ou opérations FLR (File Level Recovery) sur un autre système d'exploitation.

Supprimez le rôle de proxy et de référentiel par défaut du serveur VBR si vous ne prévoyez pas de les utiliser. Lorsqu'Enterprise Manager n'est pas utilisé, désinstallez-le et supprimez-le de votre environnement.

3.7.4.6 Correctifs et mises à jour

Corrigez les systèmes d'exploitation, les logiciels et les micrologiciels sur les composants Veeam. La plupart des attaques réussissent parce qu'il existe déjà des logiciels vulnérables utilisés qui ne sont pas alignés sur les niveaux de correctifs actuels.

Assurez-vous donc que tous les logiciels et matériels sur lesquels les composants Veeam sont exécutés sont à jour. L'une des causes les plus probables d'un vol d'identifiants est l'absence de mises à jour du système d'exploitation invité et l'utilisation de protocoles d'authentification obsolètes.

Pour atténuer les risques, suivez ces directives :

- Suivez les vulnérabilités et expositions courantes (CVE) de vos systèmes.
- Assurez des mises à jour opportunes du système d'exploitation invité sur les serveurs d'infrastructure de sauvegarde.
- Installez les dernières mises à jour et correctifs sur les serveurs d'infrastructure de sauvegarde pour minimiser le risque d'exploitation des vulnérabilités du système d'exploitation par des attaquants.

Vous pouvez choisir d'isoler votre serveur "Veeam Backup and Replication" d'Internet, dans ce cas vous devrez procéder aux **mises à jour hors ligne** : télécharger les mises à jour depuis une autre machine, copier les binaires sur le serveur VBR et appliquer les mises à jour.

Si vous choisissez d'autoriser votre "Veeam Backup and Replication Server" à accéder à Internet, veillez à **restreindre strictement l'accès aux serveurs de mise à jour pour les applications et les systèmes d'exploitation.** Encore une fois, supprimez tout outil et navigateur pour empêcher l'installation/le téléchargement de morceaux de code potentiellement dangereux. Bien entendu, **n'exposez pas votre "Veeam Backup and Replication Server à Internet".**

3.7.4.7 Ports

Essayez de **ne pas utiliser de ports obscurs et d'autres astuces** pour tenter de masquer les ports et protocoles Veeam utilisés, même si cela peut sembler un bon choix. En pratique, cela rend souvent l'infrastructure plus difficile à gérer, ce qui ouvre d'autres possibilités aux attaquants. L'obscurité n'est pas toujours synonyme de sécurité.

Deux (2) outils ont été développés pour faciliter l'identification des ports entre les composants Veeam :

- **"Veeam Network Port Mapping Tool".**
- **"Ports List Finder".**

Appliquez des **règles de pare-feu appropriées** pour limiter les communications réseau aux besoins minimaux des applications.

3.7.5 Groupe de travail ou domaine

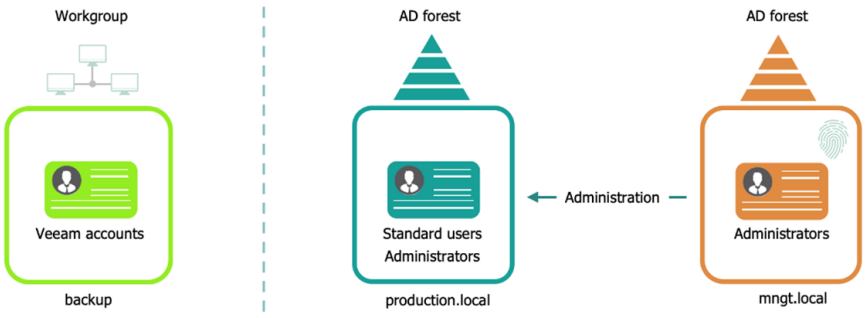
Microsoft Active Directory est au cœur de l'infrastructure informatique de presque toutes les organisations. Lors de la configuration de l'infrastructure "Veeam Availability", gardez à l'esprit le principe selon lequel **un système de protection des données ne doit en aucun cas dépendre de l'environnement qu'il est censé proteger.**

En effet, lorsque votre environnement de production tombe en panne avec ses contrôleurs de domaine, cela aura un impact sur votre capacité à effectuer des restaurations réelles en raison de la dépendance du serveur de sauvegarde à l'égard de ces contrôleurs de domaine pour l'authentification de la console de sauvegarde, du DNS pour la résolution de noms, etc.

Lors de la sécurisation des comptes administratifs et de l'installation de l'infrastructure Veeam, vous disposez **de quelques options, de la plus sécurisée à la moins sécurisée :**

- Ajoutez les composants Veeam à un domaine de gestion qui réside dans une forêt Active Directory distincte et protégez les comptes administratifs avec des mécanismes d'authentification à deux facteurs (2FA).
- Ajoutez les composants Veeam à un groupe de travail distinct et placez les composants sur un réseau distinct le cas échéant.

Ajoutez les composants Veeam au domaine de production mais assurez-vous que les comptes dotés de privilèges administratifs sont protégés par une authentification à deux facteurs (2FA).



3.7.5.1 Bonnes pratiques

Pour le déploiement le plus sécurisé, **ajoutez les composants Veeam à un domaine de gestion** qui réside dans une forêt Active Directory distincte et protégez les comptes administratifs avec des mécanismes d'authentification à deux facteurs (2FA).

De cette manière, la "Veeam Availability Infrastructure" ne dépend pas de l'environnement qu'elle est censée protéger.

3.7.5.2 Groupe de travail Windows

Lorsque vous utilisez un **groupe de travail, vous devrez tout documenter soigneusement pour des raisons de gestion et de conformité.** Chaque système doit être configuré indépendamment par système avec une politique de sécurité locale, ainsi que des utilisateurs, des autorisations, etc.

Si vous disposez de plusieurs serveurs et utilisateurs Veeam, cela peut devenir **extrêmement fastidieux dans des environnements plus vastes.** Oubliez également l'authentification Kerberos avec un serveur de groupe de travail, vous utiliserez plutôt **NLTM ce qui en soi peut constituer un risque supplémentaire.**

Sachez cependant qu'un groupe de travail est plus difficile à défendre contre les menaces de l'intérieur, comme un employé mécontent, car vous utiliserez des comptes locaux sur les serveurs du groupe de travail et vous ne pouvez pas simplement désactiver un seul compte AD, bloquant cet employé spécifique de l'infrastructure critique.

En outre, **il est plus difficile de prouver, pour des raisons de conformité, que les systèmes sont sûrs** et utilisés comme ils le devraient. Une configuration de groupe de travail est une bonne solution pour les petits environnements.

Avantages

- Rapide et facile à configurer.
- Sépare les comptes Veeam des comptes privilégiés de domaine (aide contre les keyloggers et la violation du domaine de production).
- Ne dépend pas de l'environnement qu'il est censé proteger.
- Aucun serveur d'infrastructure supplémentaire requis comme : contrôleurs de domaine, NTP et DNS.

Inconvénients

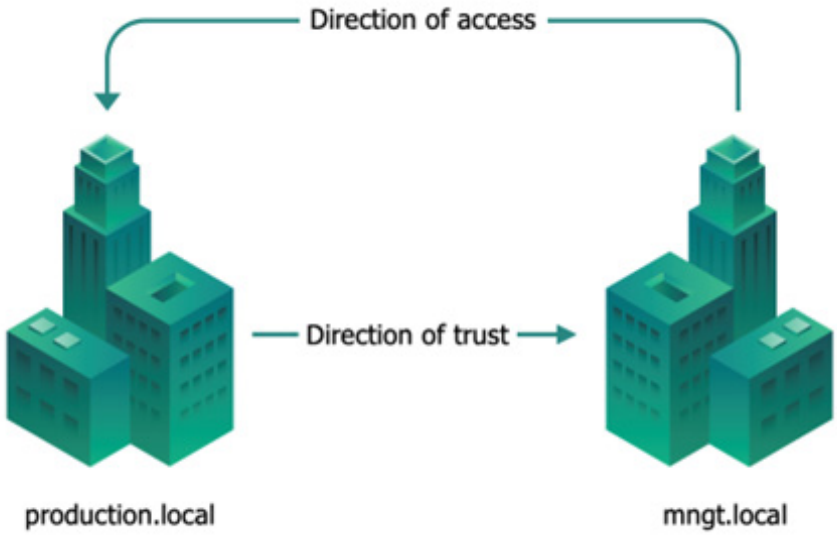
- Charge de gestion importante dans les grands environnements.
- Aucune communication Kerberos lors de la connexion à un serveur autonome (groupe de travail) uniquement NTLM.
- Il est plus difficile de se conformer à la réglementation, d'effectuer des contrôles de conformité et démontrer le respect des cadres de référence adoptés.
- Il est impossible d'utiliser le système d'authentification gMSA pour l'interaction des sauvegardes des systèmes d'exploitation invités.

3.7.5.3 Domaine de la gestion

Bien que cette approche ajoute une forêt à un environnement Active Directory, le coût et la complexité sont limités par la conception fixe, la faible empreinte matérielle/logicielle et le petit nombre d'utilisateurs. La gestion centralisée des politiques, des droits des utilisateurs et des autorisations facilite la gestion. Il permet également de désactiver en un clic un seul compte AD lorsque vous faites face à une menace interne.

La **configuration d'une forêt distincte avec un domaine de gestion est une excellente solution pour les grands environnements.** Vous pouvez également ajouter une **authentification multifacteur** sur le domaine pour protéger encore davantage les comptes administratifs, en bloquant les attaques "Man in the Middle" et les "keyloggers".

Les approbations entre forêts (Forest trusts) vous aident à gérer une infrastructure de services de domaine Active Directory (AD DS) segmentée et prennent en charge l'accès aux ressources et autres objets dans plusieurs forêts. Ces approbations sont également utiles pour les entreprises qui recherchent une solution d'autonomie administrative puisqu'elles permettent de lier deux (2) forêts différentes pour former une relation d'approbation transitive unidirectionnelle ou bidirectionnelle. Une approbation entre forêts permet aux administrateurs de connecter deux (2) forêts AD DS avec une relation d'approbation unique pour fournir une expérience d'authentification et d'autorisation transparente dans toutes les forêts.



Si une approbation de forêt unidirectionnelle est créée entre deux forêts, les membres de la forêt approuvée ("trusted forest") peuvent utiliser les ressources situées dans la forêt approuvante ("trusting forest"). Cependant, ce processus ne fonctionne que dans un seul sens.

3.7.6 Stockage WORM avec le référentiel renforcé Veeam

"Veeam Hardened Repository" est une solution de stockage WORM qui protège contre les modifications indésirables apportées aux fichiers de sauvegarde. Il est disponible depuis la version 11. "Veeam Hardened Repository" a passé un audit externe pour le stockage WORM et supporte les fonctionnalités suivantes :

- **Immuabilité :** lorsque vous ajoutez un référentiel renforcé, vous spécifiez la période pendant laquelle les fichiers de sauvegarde doivent être immuables. Pendant cette période, les fichiers de sauvegarde stockés dans ce référentiel ne peuvent pas être modifiés ou supprimés.

- **Identifiants à usage unique :** identifiants utilisés une seule fois pour déployer le Veeam Data Mover, ou service de transport, lors de l'ajout du serveur Linux à l'infrastructure de sauvegarde. Ces informations d'identification ne sont pas stockées dans l'infrastructure de sauvegarde. Même si le serveur Veeam Backup & Replication est compromis, l'attaquant ne peut pas obtenir les informations d'identification et se connecter au référentiel renforcé.

En rappel ou en complément du guide utilisateur, envisagez les actions suivantes pour créer un référentiel renforcé :

- **Déployer le référentiel Veeam à l'aide d'informations d'identification à usage unique :** Veeam ne stockera pas le compte racine du référentiel, gardant ainsi les fichiers de sauvegarde en sécurité si le serveur "Veeam Backup" est compromis. N'oubliez pas de supprimer l'utilisateur du groupe "sudoers" après l'installation.

- **Désactiver SSH après le déploiement :** La connexion SSH est nécessaire uniquement pour le déploiement ou la mise à niveau de "Veeam Data Mover". Une fois Veeam déployé, il est possible de désactiver SSH pour une meilleure sécurité. Si vous laissez SSH activé, alors MFA sur SSH sera pris en compte.

- **IPMI :** N'importe quel outil de gestion, tel que iLO ou DRAC, peut être utilisé pour accéder au référentiel et même pour effacer les disques durs. Il est fortement recommandé de débrancher ces outils du réseau lorsqu'ils ne sont pas utilisés.

- **NTP :** La gestion du temps est cruciale lorsqu'on parle d'immuabilité. Il n'est pas conseillé d'utiliser des serveurs NTP publics, car cela signifierait une exposition Internet du serveur de référentiel. Utiliser votre propre serveur NTP est une option, mais cela reste une faille de sécurité au cas où un attaquant en prendrait le contrôle.

L'utilisation de l'horloge CMOS est une option conseillée, mais la contrepartie consiste à vérifier régulièrement et à régler manuellement l'heure du système. En outre, un décalage horaire entre le référentiel et le serveur de sauvegarde rendrait l'analyse des journaux plus complexe par l'analyse forensique des journaux. Une deuxième option conseillée et intéressante consiste à utiliser un dongle DCF77 (ou équivalent localement) avec le package XNTP pour synchroniser le référentiel sur un signal à ondes longues.

3.7.7 Traitement des demandes

L'Application Aware Processing nécessite que l'infrastructure "Veeam Backup and Replication" se connecte aux serveurs de production pour interagir avec les systèmes d'exploitation et les applications.

Bien que cela permette aux applications et au système de fichiers d'être cohérents au moment de la sauvegarde, **cela peut être considéré comme un risque dans la mesure où toutes les informations d'identification fournies seront stockées dans la base de données de configuration** de "Veaam Backup and Replication".

Les solutions alternatives seraient :

- Sauvegarder les actifs sans "Application Processing", c'est-à-dire effectuer des sauvegardes cohérentes en cas de crash.
- Utilisez gMSA (Groupe Managed Service Accounts) si vous utilisez VBR v12 ou version ultérieure.
- Utilisez des agents pour sauvegarder vos actifs.

REMARQUE : Les éléments d'application granulaire peuvent toujours être restaurés à partir d'une sauvegarde non compatible avec les applications via les explorateurs. Pour cela, lancez une restauration "Guest file", et depuis l'explorateur forcez une "Applicartion Item restore".

3.7.7.1 gMSA

Même s'il n'est pas entièrement sécurisé , si vous ressentez le besoin de déléguer la gestion des mots de passe à Microsoft gMSA, vous devez penser que **le serveur VBR devra alors faire partie du domaine.**

3.7.7.2 Sauvegarde Active Directory

Une sauvegarde cohérente d'Active Directory nécessite des informations d'identification "Built-in Administrator" sur l'invité. Pour éviter de stocker ces informations d'identification dans la base de données Veeam, **il est recommandé de sauvegarder les serveurs Active Driectory à l'aide d'un agent non géré** sur un référentiel Veeam.

De cette façon, le compte administrateur restera protégé et la restauration des éléments Active Directory à l'aide de l'explorateur demandera une connexion appropriée au moment de la restauration.

3.7.7.3 Placement du proxy d'interaction avec les invités

Les "Guest interaction proxies" permettent d'interagir avec les machines virtuelles Microsoft Windows dans des zones moins sécurisées sans exposer le serveur de sauvegarde dans ces zones.

L'utilisation du "Guest interaction Proxy" avec les invités limitera considérablement l'exposition du serveur de sauvegarde et de réplication Veeam. Les ports nécessaires au traitement des interactions avec les invités sont disponibles dans le guide de l'utilisateur.

3.7.7.4 Placement de la console pour les explorateurs

Le déploiement de "Veeam Console" dans des zones isolées sera utile en matière de restauration des éléments invités, car il **permettra un fonctionnement sans avoir besoin d'ouvrir la plage de ports dynamiques Microsoft RPC** de la zone de gestion vers la zone isolée. La console peut être déployée sur le "Guest interaction Proxy" qui devrait déjà se trouver dans cette zone.

3.7.7.5 Restaurer les informations d'identification

Au moment de la restauration, lors de l'utilisation des "Veeam Explorers", l'authentification sur le serveur de destination est effectuée à l'aide des informations d'identification d'interaction invité configurées dans la tâche de sauvegarde. La modification des informations d'identification dans la configuration du travail modifiera le compte utilisé au moment de la restauration.

La suppression de la configuration de l'interaction invité entraînera la saisie interactive des informations d'identification au moment de la restauration.

4. Décalogue de recommandations

Voici dix recommandations de sécurité pour l'utilisation de Veeam Data Platform.

Dix recommandations pour Veeam Data Platform

1. Il est recommandé de mettre en œuvre la **sécurité dès le début de la conception** de l'environnement, de même qu'une infrastructure de sauvegarde correctement conçue.

2. Il est recommandé de **protéger les sauvegardes** et l'infrastructure et de former le personnel de l'organisation.

3. Il est recommandé d'élaborer une stratégie de **surveillance des alertes, des utilisateurs, des serveurs et d'autres éléments critiques** faisant partie du système.

4. Il est recommandé de mettre en place un **plan de reprise** et de former le personnel nécessaire à sa mise en œuvre, ce qui réduira le temps de réponse en cas d'incident.

5. Il est recommandé de déployer une **politique de contrôle d'accès** aux composants de gestion en appliquant le principe du moindre privilège. Appliquer l'isolement pour empêcher les attaquants de se déplacer trop facilement (changer les règles du jeu en notre faveur).

6. Il est recommandé de créer une **politique de mots de passe forts** et de mettre en œuvre une **politique de blocage/verrouillage** des tentatives de connexion infructueuses afin de prévenir les attaques par force brute.

7. Il est recommandé de choisir des **algorithmes de chiffrement puissants** pour l'accès à distance à l'infrastructure de sauvegarde.

8. Pour le chiffrement des données, il est recommandé d'**activer le chiffrement à la fois en transit et au repos** afin d'éviter les violations et les lectures indésirables.

9. Il est recommandé de **réduire la surface d'attaque** en supprimant tous les logiciels et utilitaires non essentiels des composants Veeam déployés.

10. Il est recommandé de **segmenter en différentes zones**, de réduire la surface d'exposition en supprimant les add-ons ou fonctionnalités inutiles, de disposer de sauvegardes immuables, ainsi que de gérer correctement les autres produits ou solutions utilisés en conjonction avec Veeam.

Centro Criptológico Nacional 20 ANIVERSARIO

CCN-CERT centro criptológico nacional

Annexe A. Mesures de sécurité de l'ENS et contrôles de sécurité

Le tableau ci-dessous met en relation les différentes mesures de sécurité fixées par le Décret Royal 311/2022, du 3 mai, qui réglemente le Cadre National de Sécurité espagnol (*Esquema Nacional de Seguridad*) et les solutions de Veeam Backup, en soulignant leur applicabilité, ainsi qu'une référence à la section correspondante de ce guide où cette applicabilité est justifiée :

Mesure ENS	Justification de l'applicabilité	Section de ce guide
Sauvegardes [mp.info.6]	L'objectif des solutions "Veeam Backup" est précisément de réaliser des sauvegardes qui permettent de récupérer des données perdues accidentellement ou intentionnellement **[mp.info.6.1]**. Elles permettent également de déterminer la fréquence des sauvegardes, de stocker les sauvegardes sur site et/ou hors site, et d'établir des contrôles pour limiter les accès autorisés aux sauvegardes **[mp.info.6.2]**. Ces solutions permettent également d'effectuer des tests de récupération **[mp.info.6.r1.1]** et de stocker l'une des copies séparément dans un endroit différent, de sorte qu'un incident potentiel ne puisse pas affecter simultanément l'information originale et la copie **[mp.info.6.r2].**	1. Introduction. 3.3 Stratégie de rétablissement.
Identification [op.acc.1] **Exigences d'accès [op.acc.2]**	La gestion des comptes sera supportée par la gestion des comptes du domaine où la solution de sauvegarde Veeam est déployée. Les informations d'identification à usage unique fournies par l'utilisateur sont utilisées de manière interactive au moment de l'installation initiale et lors de l'installation des mises à jour du produit. Elles ne sont jamais stockées dans la base de données de configuration.	3.4 Rôles et utilisateurs. 3.7.6 Stockage Worm avec Veeam Hardened Repository.

Mesure ENS	Justification de l'applicabilité	Section de ce guide
Mécanisme d'authentification [op.acc.5], [op.acc.6]	Toute utilisation du protocole SSH a été encapsulée dans un protocole de transport étendu. Par conséquent, la connectivité SSH n'est requise qu'au moment du déploiement initial et lors de l'installation des mises à jour du produit. Cela permet aux clients de protéger SSH avec une authentication multifactorielle interactive (MFA) ou même de désactiver entièrement le serveur SSH pour protéger leur référentiel, même pour faire face aux futures vulnérabilités de type "zero-day". Depuis "Veeam Backup & Replication v12", seule une architecture Kerberos est possible, et il est recommandé de désactiver l'authentification NTLM dans la mesure du possible.	3.5 Protocoles d'authentification.
Plan de continuité [op.cont.2]	Il est recommandé que les sauvegardes au niveau image soient immuables pendant la durée spécifiée dans la politique de conservation, soit au moins quatre (4) semaines, suivant un schéma GFS (Grand Father, Father, Son). Cette fonctionnalité utilise la fonction native d'immuabilité des fichiers Linux.	3.1.1 Protection des sauvegardes.
Cryptographie [mp.si.2]	Le chiffrement intégré "Veeam Backup & Replication" est disponible pour protéger les données au repos des sauvegardes **[mp.si.2.r2.1]**. Les modules de chiffrement sont basés sur la norme FIPS.	3.6.1 Chiffrement au repos.
Séparation des flux d'informations dans le réseau [mp.com.4]	Pour isoler le trafic de sauvegarde, il est recommandé d'utiliser un réseau segmenté entre les principaux composants de l'infrastructure de sauvegarde : serveur de sauvegarde, proxys de sauvegarde, référentiels de sauvegarde, etc. **[mp.com.4.1]** Par défaut, "Veeam Backup & Replication" chiffre le trafic réseau entre les réseaux publics, mais il est recommandé d'activer le chiffrement du trafic également sur les réseaux privés afin d'assurer une communication sécurisée dans le réseau interne. **[mp.com.2.r5.1]**	3.6.2 Chiffrement en transit.
Enregistrement de l'activité [op.exp.8]	Les solutions de sauvegarde Veeam peuvent ajouter des entrées dans le journal des événements du système afin de fournir une meilleure visibilité aux utilisateurs effectuant une surveillance basée sur les journaux **[op.ep.8.1].**	3.7 Durcissement. 3.7.1 Segmentation.
Dimensionnement / gestion des capacités [op.pl.4]	L'utilisation de référentiels de sauvegarde évolutifs à l'aide de Scale-Out Backup Repositories (SOBR) facilite la gestion de la capacité disponible pour les sauvegardes. **[op.pl.4.2], [op.pl.4.r1.2]**	

Annexe B. Liste de contrôle

Élément	Vérification	Résultat
RÈGLE 3-2-1-1-0		
3 copies	Existe-t-il 3 copies différentes des données ?	Oui/Non/Partiellement/ Incertain
2 médias	Les copies sont-elles hébergées sur deux supports différents ?	Oui/Non/Partiellement/ Incertain
1 hors site	Y a-t-il une copie hors site ?	Oui/Non/Partiellement/ Incertain
1 copie immuable/ séparée	Une copie est-elle immuable ou séparée ?	Oui/Non/Partiellement/ Incertain
0 erreur	Les sauvegardes sont-elles régulièrement testées pour garantir qu'elles peuvent être restaurées ?	Oui/Non/Partiellement/ Incertain
DÉTECTION DES MENACES		
EDR-XDR	Un EDR ou un XDR sont-ils déployés pour détecter les menaces ?	Oui/Non/Partiellement/ Incertain
Honeypots	Y a-t-il des honeypots déployés ?	Oui/Non/Partiellement/ Incertain
VeeamOne	Veeam One est-il déployé et surveille-t-il les menaces ?	Oui/Non/Partiellement/ Incertain
STRATÉGIE DE RÉTABLISSEMENT		
Existence d'une stratégie de rétablissement	Existe-t-il une stratégie de rétablissement en place ?	Oui/Non/Partiellement/ Incertain
Test de stratégie de rétablissement	La stratégie de rétablissement est-elle régulièrement testée ?	Oui/Non/Partiellement/ Incertain
Infrastructure de rétablissement dédiée	Existe-t-il une infrastructure de rétablissement dédiée ?	Oui/Non/Partiellement/ Incertain
RÔLES ET UTILISATEURS		
Comptes anonymes	Les noms de compte contiennent-ils une référence à leurs rôles ?	Oui/Non/Partiellement/ Incertain
Politique de changement de mot de passe	Les mots de passe sont-ils changés régulièrement ?	Oui/Non/Partiellement/ Incertain

Annexe B. Liste de contrôle

Élément	Vérification	Résultat
Politique de verrouillage	Les utilisateurs sont-ils déconnectés après une période d'inactivité donnée ?	Oui/Non/Partiellement/ Incertain
Contrôle d'accès basé sur les rôles	L'infrastructure de sauvegarde est-elle accessible uniquement aux comptes de sauvegarde ?	Oui/Non/Partiellement/ Incertain
Comptes Honeypot	Y a-t-il des comptes Honeypot visibles qui sont surveillés ?	Oui/Non/Partiellement/ Incertain
Authentification multifactorielle	La MFA est-elle utilisée pour se connecter à l'infrastructure de sauvegarde ?	Oui/Non/Partiellement/ Incertain
CHIFFREMENT		
Au repos	Les données sont-elles chiffrées sur les référentiels ?	Oui/Non/Partiellement/ Incertain
En transit	Les données sont-elles chiffrées lors du transit ?	Oui/Non/Partiellement/ Incertain
DURCISSEMENT		
Segmentation spécifique	L'infrastructure de sauvegarde est-elle sur des segments spécifiques ?	Oui/Non/Partiellement/ Incertain
MFA	L'authentification MFA est-elle activée sur le segment de l'infrastructure de sauvegarde ?	Oui/Non/Partiellement/ Incertain
Base de données Veeam	L'accès à la base de données Veeam est-il restreint ?	Oui/Non/Partiellement/ Incertain
Console	La console est-elle désinstallée du serveur VBR ?	Oui/Non/Partiellement/ Incertain
Nettoyage des serveurs d'infrastructure de sauvegarde	Les serveurs ont-ils été nettoyés de tous les rôles/ composants inutiles ?	Oui/Non/Partiellement/ Incertain
Correctifs et mises à jour	Les serveurs sont-ils régulièrement corrigés/mis à jour ?	Oui/Non/Partiellement/ Incertain
Gestion à distance	Les outils de gestion à distance sont-ils désactivés/ désinstallés ?	Oui/Non/Partiellement/ Incertain
Immuabilité	Le référentiel est-il immuable ?	Oui/Non/Partiellement/ Incertain
Durcissement	Le référentiel est-il renforcé ?	Oui/Non/Partiellement/ Incertain
TRAITEMENT DES DEMANDES		
Identifiants du contrôleur de domaine	Le compte d'administrateur de domaine est-il stocké dans Veeam ?	Oui/Non/Partiellement/ Incertain
gMSA	gMSA est-il utilisé pour l'interaction avec les invités ?	Oui/Non/Partiellement/ Incertain

Annexe C. Glossaire

Terme	Description
AES-256	Algorithme de chiffrement
Air gap	Mesure de sécurité pour isoler un objet du réseau
API	Interface de programmation d'applications
Appliance	Élément logiciel ou matériel conçu pour fournir une ressource informatique spécifique
Backup	Sauvegarde
Baremetal	Serveur physique dédié
CCTV	Télévision en circuit fermé
CIFS	Protocole de transfert de fichiers
Cloud	Ensemble de serveurs distants connectés à l'internet qui fournissent un service ou un objectif.
Cluster	Ensemble de nœuds dans une infrastructure Kubernetes.
CMOS	Complementary Metal Oxide Semiconductor, semi-conducteur à oxyde métallique complémentaire, également appelé batterie de type bouton. Sur la carte mère, il permet au BIOS ou à l'UEFI de stocker les paramètres de configuration du matériel.
Configmaps	Fichier de données clé-valeur
CPU (Central Processing Unit)	Unité centrale de traitement
Criptoprocesadores	Microprocesseur optimisé pour effectuer des opérations cryptographiques
Deduplicar	Processus informatisé de suppresion de données dupliquées
DMZ	La Zone Démilitarisée (DMZ) est une zone de l'infrastructure où les services sont exposés à des réseaux non sécurisés tels que l'internet.
DNS (Domain Name System)	Service qui traduit les noms de domaine en adresses IP ou vice versa.

Annexe C. Glossaire

Terme	Description
Dongle	Un adaptateur ou clé (dongle) est un petit appareil qui se connecte à un autre appareil pour fournir une fonction supplémentaire.
DR (Disaster Recovery)	Processus défini pour la récupération des données en cas de panne du système
Durcissement	Le renforcement ou “durcissement” consiste à protéger l’infrastructure contre les attaques en réduisant la surface d’attaque et en éliminant ainsi le plus grand nombre possible de risques.
Failback	Capacité de transfert de l’environnement réparé à l’environnement d’origine après la défaillance
Failover	Capacité d’un système à continuer à fonctionner en cas de défaillance
Forêt	Ensemble de domaines Microsoft Windows
GDPR (General Data Protection Regulation)	Règlement Général sur la Protection des Données
GPO (Group Policy Object)	Stratégie de groupe, objet de l’Active Directory qui attribue une stratégie ou une valeur de configuration
Honeypot	Pot de miel utilisé pour visualiser les attaques possibles
IDS	Système de détection d’intrusion
IPS	Système de prévention des intrusions
Kerberos	Protocole d’authentification
keyloggers	Logiciel malveillant qui enregistre ce qui est tapé sur le clavier
Kubernetes	Plateforme de conteneurs open source
LAN	Réseau local
Multi-Tenant	Architecture logicielle permettant à une instance unique de servir plusieurs clients
Namespace	Espace de travail / espace nominatif
NAS (Network Attached Storage)	Technologie de stockage en réseau
NDMP	Protocole de gestion des données du réseau
NFS	Protocole de système de fichiers en réseau

Annexe C. Glossaire

Terme	Description
NTLM	Ensemble de protocoles d'authentification Microsoft
NTP	Protocole de synchronisation d'horloge
Object Storage	Stockage basé sur des objets
OIDC	Protocole d'authentification
RBAC (Role-Based Access Control)	Contrôle d'accès basé sur les rôles
RPC	Programme d'appel de procédure à distance
RPO	Objectif de point de reprise
RTO	Objectif de délai de restauration
SaaS	Logiciel en tant que service (Software as a service)
Secret	Fichier de données confidentielles
SMB	Protocole de transfert de fichiers
SSH	Secure Shell est un protocole d'administration à distance
Token	Identificateur de validation
UPS	Alimentation sans interruption
WAN	Réseau étendu
Workgroup	Groupe de travail Microsoft Windows
WORM (Write Once, Read Many)	Méthode de sauvegarde (écriture unique, lecture multiple)

Centro Criptológico Nacional

20 ANIVERSARIO

CCN-CERT
centro criptológico nacional

VEEAM

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es